

ROBERT M. CLARK

Seventh Edition

INTELLIGENCE ANALYSIS

A Target-Centric Approach



Intelligence Analysis

Seventh Edition

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

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

Intelligence Analysis

A Target-Centric Approach

Seventh Edition

Robert M. Clark



FOR INFORMATION:

CQ Press

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

SAGE Publications Ltd.

1 Oliver's Yard
55 City Road
London, EC1Y 1SP
United Kingdom

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

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

Acquisitions Editor: Christy Sadler

Editorial Assistant: Avren Keating

Production Editor: Astha Jaiswal

Copy Editor: Amy Marks

Typesetter: diacriTech

Indexer: Integra

Cover Designer: Scott Van Atta

Marketing Manager: Jennifer Haldeman

Copyright © 2023 by CQ Press, an Imprint of SAGE Publications, Inc. CQ Press is a registered trademark of Congressional Quarterly Inc.

All rights reserved. Except as permitted by U.S. copyright law, no part of this work may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without permission in writing from the publisher.

All third party trademarks referenced or depicted herein are included solely for the purpose of illustration and are the property of their respective owners. Reference to these trademarks in no way indicates any relationship with, or endorsement by, the trademark owner.

Printed in the United States of America

ISBN 9781071895283

Library of Congress Control Number: 2022911456

This book is printed on acid-free paper.

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

BRIEF CONTENTS

Tables, Figures, and Boxes	xix
Preface	xxv
Acknowledgments	xxix
PART I THE PROCESS, THE PARTICIPANTS, AND THE PRODUCT	1
Chapter 1 Introduction	3
Chapter 2 Intelligence in the Age of Contested Norms and Persistent Disorder	13
Chapter 3 The Intelligence Process	35
Chapter 4 The Customer	57
Chapter 5 The Analyst	73
Chapter 6 The Analytic Network	89
Chapter 7 The Intelligence Product	101
PART II THE ANALYSIS PROCESS	119
Chapter 8 The Intelligence Issue	121
Chapter 9 Target Models	143
Chapter 10 The Target Framework	161
Chapter 11 Analyzing Existing Intelligence	183
Chapter 12 The Information Sources	215
Chapter 13 Denial, Deception, and Signaling	237
Chapter 14 Gaining Customer Acceptance	259

PART III	ANTICIPATORY INTELLIGENCE	277
Chapter 15	Anticipatory Analysis: Forces	281
Chapter 16	Anticipatory Analysis: Methodology	297
Chapter 17	Scenarios	327
Chapter 18	Systems Modeling and Analysis	343
Chapter 19	Relationship Modeling and Analysis	363
Chapter 20	Geospatial Modeling and Analysis	387
Chapter 21	Simulation Modeling	407
Chapter 22	Prescriptive Intelligence	429
Chapter 23	Case Study	441
List of Commonly Used Acronyms		457
Index		461
About the Author		477

CONTENTS

Tables, Figures, and Boxes	xix
Preface	xxv
Acknowledgments	xxix
PART I THE PROCESS, THE PARTICIPANTS, AND THE PRODUCT	1
Chapter 1 Introduction	3
Why Intelligence Fails	3
Failure to Share Information	5
Failure to Analyze Collected Material Objectively	6
Failure of the Customer to Act on Intelligence	7
What the Book Is About	8
Summary	10
Notes	10
Chapter 2 Intelligence in the Age of Contested Norms and Persistent Disorder	13
Nature of Twenty-First-Century Conflict	15
Networks	15
Nonstate Actors	16
Tools of Conflict	19
Diplomatic	19
Information	19
Military	20
Economic	21
Synergy of the Tools	22
The Function of Intelligence	23
The Nature of Intelligence	24
Strategic Intelligence	25

Operational Intelligence	26
Tactical Intelligence	29
Summary	31
Critical Thinking Questions	32
Notes	32
Chapter 3 The Intelligence Process	35
The Traditional Intelligence Cycle	36
Intelligence as a Target-Centric Process	40
The Target	46
The Target as a Complex System	47
The Target as a Network	48
Spatial and Temporal Attributes of the Target	51
Summary	52
Critical Thinking Questions	53
Notes	53
Chapter 4 The Customer	57
Overview of Customers	57
Understanding the Customer	59
Policymakers	59
<i>How Policymakers Differ</i>	60
<i>The Policymaker's Environment</i>	60
<i>The Policymaker's Mindset</i>	61
<i>Policymaker Priorities</i>	62
<i>Effective Analyst Interaction with Policymakers</i>	62
Congress	63
Military Leadership	64
Military Operations	65
Homeland Security	65
Law Enforcement	66
Business Leaders	67
What All Customers Want	68
Summary	69
Critical Thinking Questions	70
Notes	70
Chapter 5 The Analyst	73
Critical and Logical Thinking	73
Objectivity	75
Broad Perspective	76

Good Instincts	77
The Analyst's Role	78
Analytic Teams	79
Organizing the Analysis Team	79
<i>Customers</i>	80
<i>Collectors</i>	81
<i>External Sources</i>	81
Managing the Analysis Process	81
Summary	84
Critical Thinking Questions	85
Notes	87
Chapter 6 The Analytic Network	89
The US National Intelligence Network	89
Homeland Security and Law Enforcement	92
Military	94
Nongovernmental Entities	94
Network Collaboration and Sharing	95
Summary	98
Critical Thinking Questions	98
Notes	99
Chapter 7 The Intelligence Product	101
Intelligence Research	102
Current Intelligence	102
Indications and Warning	103
What Should an Intelligence Unit Produce?	106
Constraints on the Intelligence Product	107
Limits	108
Boundaries	109
<i>The Policy Divide</i>	109
<i>All-Source versus Single-Source Intelligence</i>	110
<i>Domestic versus Foreign Intelligence</i>	111
<i>Operational Information versus Intelligence</i>	111
Constraining Pressures	112
<i>Internal</i>	112
<i>External</i>	113
<i>The Defense Analysis Challenge</i>	114
<i>Temporal Pressures</i>	115

x	Intelligence Analysis	
Summary	116	
Critical Thinking Questions	117	
Notes	117	
PART II THE ANALYSIS PROCESS	119	
Chapter 8 The Intelligence Issue	121	
Preliminary Questions	122	
Issue Definition	124	
Clarify the Question	124	
<i>Issue Categories</i>	125	
<i>The PMESII Perspective</i>	125	
<i>A Check on Question Clarification</i>	129	
Identify Assumptions	129	
Focus the Question	131	
Issue Decomposition	133	
Complex Issue Decomposition	136	
Structured Analytic Techniques for Issue Decomposition	138	
Summary	139	
Critical Thinking Questions	140	
Notes	141	
Chapter 9 Target Models	143	
Modeling the Intelligence Target	143	
General Target Models	147	
Comparative Models	148	
<i>A Pitfall of Comparative Modeling</i>	150	
Profile Models	150	
Mathematical Models	152	
Pattern Models	155	
<i>Timelines</i>	156	
<i>Histograms</i>	157	
Summary	157	
Critical Thinking Questions	158	
Notes	159	
Chapter 10 The Target Framework	161	
Creating a Target Framework	161	
Issue 1: Al-Shabaab Ideology	163	
Issue 2: Influencing Azerbaijan Political Model	165	
	166	

Military Model	167
Economic Model	168
Social Model	168
Infrastructure Model	170
Information Model	172
Issue 3: The Monopolitania Biological Warfare Threat	173
Submodels	173
Collateral Models	174
Alternative and Competitive Target Frameworks	176
Alternative Frameworks	176
Competitive Frameworks	178
The Dynamic Framework	179
Summary	179
Critical Thinking Questions	180
Notes	181
Chapter 11 Analyzing Existing Intelligence	183
Reviewing Existing Finished Intelligence	183
Acquiring Raw Intelligence	184
Evaluating Evidence	187
Evaluating the Source	188
<i>Competence</i>	188
<i>Access</i>	189
<i>Vested Interest or Bias</i>	189
Evaluating the Communications Channel	191
Evaluating the Credentials of Evidence	193
<i>Is It True?</i>	194
<i>Is It the Whole Truth?</i>	195
<i>Is It Nothing but the Truth?</i>	196
Pitfalls in Evaluating Evidence	196
<i>Vividness Weighting</i>	196
<i>Weighing Based on the Source</i>	197
<i>Favoring the Most Recent Evidence</i>	198
<i>Favoring or Disfavoring the Unknown</i>	198
<i>Trusting Hearsay</i>	198
<i>Reliance on Expert Opinions</i>	199
<i>Premature Closure and Philosophical Predisposition</i>	201
Combining the Evidence	203
Divergent Evidence	203
Convergent Evidence	204
<i>Corroborative Redundancy</i>	204
<i>Cumulative Redundancy</i>	204
Formal Methods for Evaluating and Combining Evidence	205

Structured Argumentation	205
Analysis of Competing Hypotheses	205
Bayesian Techniques for Combining Evidence	207
A Note about the Role of Information Technology	208
Summary	209
Critical Thinking Questions	210
Notes	211
Chapter 12 The Information Sources	215
Filling Gaps	215
Using the Issue Decomposition and Target Framework	216
Identifying Gaps	220
Developing the Collection Strategy	222
Using Existing Collection Assets	222
Basic Collection Strategy Development	223
Advanced Collection Strategy Development: Cost-Benefit Analysis	225
Executing Collection Strategies	226
Analyst-Collector Interaction	227
Evaluating Collection	229
Collection Requirements	230
Summary	232
Critical Thinking Questions	233
Notes	234
Chapter 13 Denial, Deception, and Signaling	237
Denial	239
Deception	239
Defense against Denial and Deception: Protecting Intelligence Sources and Methods	242
Countering Denial and Deception	247
The Analyst	248
Collectors	249
The Customer	250
Signaling	252
Summary	254
Critical Thinking Questions	255
Notes	256

Chapter 14 Gaining Customer Acceptance	259
Structuring the Message	259
Write for the Customer	260
Support Every Analytic Conclusion	261
Separate Facts from Analysis	261
Presenting the Message	262
Get to the Point	263
Write or Brief to Inform, Not to Impress	263
Make It Easy and Enjoyable to Read or Listen to	263
Write as You Would Talk	264
Avoid Acronyms	264
Present the Message Visually	265
Reviewing the Analytic Product	265
Peer Review	265
Management Review	266
Red Teams	266
Devil's Advocate	267
Customer Interaction	267
Analyst as Advocate: Getting Buy-In	268
Aftermath: Dealing with Unexpected Outcomes	270
Summary	272
Critical Thinking Questions	273
Notes	274
PART III ANTICIPATORY INTELLIGENCE	277
Chapter 15 Anticipatory Analysis: Forces	281
Background Forces	283
Inertia	283
Opposition	285
Contamination	286
Feedback	288
Synergy	290
Causal Models	291
Summary	294
Critical Thinking Questions	295
Notes	295

Chapter 16 Anticipatory Analysis: Methodology	297
Convergent and Divergent Phenomena	298
The Estimative Approach	301
High-Impact/Low-Probability Analysis	304
Extrapolation	305
Projection	308
<i>Generating Alternatives</i>	308
<i>Influence Trees or Diagrams</i>	309
<i>Influence Nets</i>	313
<i>Methods for Probabilistic Projection</i>	315
<i>Sensitivity Analysis</i>	315
Forecasting	316
<i>The Nonlinear Approach to Forecasting</i>	318
<i>Techniques and Analytic Tools of Forecasting</i>	319
<i>Evaluating Forecasts</i>	320
Unintended Consequences	321
Summary	322
Critical Thinking Questions	323
Notes	324
Chapter 17 Scenarios	327
Why Use Scenarios?	328
Types of Scenarios	330
Driving-Force Scenario	330
System-Change Scenario	331
Scenario Perspectives	332
How to Construct Scenarios	332
Shell Energy Scenario	333
1. Define the Issue and the Target Framework	335
2. Identify and Rank the Driving Forces or Factors	335
3. Select the Scenario Logics	336
4. Flesh Out the Scenarios	336
<i>Case-Based Models</i>	336
<i>Cross-Impact Analysis</i>	337
5. Draw Out the Implications	337
6. Identify and Monitor Indicators	338
Summary	338
Critical Thinking Questions	339
Notes	340

Chapter 18 Systems Modeling and Analysis	343
Systems Analysis Methodology	345
Performance	346
Comparative Modeling	347
The Mirror-Imaging Challenge	350
Process	351
Program Cycle Model	354
Program Staffing Model	356
The Technology Factor	357
Risk	358
Cost	359
Summary	360
Critical Thinking Questions	361
Notes	361
Chapter 19 Relationship Modeling and Analysis	363
Link Models	364
Network Models	366
Network Model Types	367
Manual Modeling	368
Computer-Assisted and Automated Modeling	369
Network Analysis	370
Nodal Analysis	370
Social Network Analysis	371
<i>Centrality</i>	372
<i>Equivalence</i>	374
Organizational Network Analysis	374
<i>Commercial Networks</i>	375
<i>Financial Networks</i>	378
Target Network Analysis	379
<i>Threat Network Analysis</i>	380
<i>Automating Network Analysis</i>	381
Summary	382
Critical Thinking Questions	383
Notes	384
Chapter 20 Geospatial Modeling and Analysis	387
Static Geospatial Models	389
Human Terrain Modeling	392
The Tools of Human Terrain Modeling	394

Dynamic Geospatial Models	395
Movement Intelligence	395
Activity-Based Intelligence	397
Geographic Profiling	399
Intelligence Enigmas	400
Summary	402
Critical Thinking Questions	403
Notes	404
Chapter 21 Simulation Modeling	407
Types of Simulations	407
Economic Simulations	408
Military Simulations	409
<i>Weapons Systems</i>	409
<i>Wargaming Simulations</i>	410
Social Simulations	412
<i>Social Networks</i>	412
<i>Geospatial</i>	413
Political Simulations	414
<i>Rational Models</i>	415
<i>Administrative Models</i>	416
<i>Cultural Models</i>	417
<i>Emotional Models</i>	418
<i>The Operational Code Model</i>	419
<i>Group Decision-Making Models</i>	419
<i>Game Theory</i>	420
Using Simulations	422
Creating a Simulation	422
Running a Simulation	423
Summary	423
Critical Thinking Questions	424
Notes	425
Chapter 22 Prescriptive Intelligence	429
The Process	431
Scenarios	431
Normative Scenarios	431
Demonstration Scenarios	432
Operations Research	433
Defining the Problem	433
Allocating Resources	433
Targeting a Physical Network	434

Simulations	435
Economic Simulations	435
Military Simulations	435
Geospatial Simulations	436
Political and Social Simulations	436
Prescriptive Analytics	436
Summary	438
Critical Thinking Questions	439
Notes	439
Chapter 23 Case Study	441
A Tale of Two NIEs	441
The Yugoslavia NIE	442
The Setting	442
First Draft (the “Muddle-Through” NIE)	443
Second Draft (Alternative Projection)	444
The Customer View	445
The Iraqi Weapons of Mass Destruction NIE	446
The Setting	446
The NIE	448
<i>Poor Issue Definition</i>	448
<i>Poor Evaluation of Sources and Evidence</i>	449
<i>Failure to Consider Alternative Target Models</i>	450
<i>Poor Analytic Methodology</i>	451
<i>Poor Interaction with Collectors and Customers</i>	452
The Customer View	452
Capstone Critical Thinking Questions	453
Notes	455
List of Commonly Used Acronyms	457
Index	460
About the Author	477

TABLES, FIGURES, AND BOXES

PART I	THE PROCESS, THE PARTICIPANTS, AND THE PRODUCT	1
Chapter 2	Intelligence in the Age of Contested Norms and Persistent Disorder	13
BOX 2.1	Netwar I: Erdoan versus Glen	18
BOX 2.2	Silk Road	22
BOX 2.3	Netwar II: Erdoan versus Glen	23
BOX 2.4	Operation Desert Shield/Desert Storm	27
BOX 2.5	Lebanon War, 2006	28
BOX 2.6	Symantec’s Tactical Intelligence	30
Chapter 3	The Intelligence Process	35
Figure 3.1	The Traditional Intelligence Cycle	36
BOX 3.1	The Automobile Production Cycle	39
Figure 3.2	DoD View of the Intelligence Process	39
Figure 3.3	A Target-Centered View of the Process	41
BOX 3.2	Dodging Missiles at Al Asad	43
Figure 3.4	Example Target: Cocaine Network	48
Figure 3.5	Netwar Competition: Network versus Network	50
Figure 3.6	Netwar Example against a Cocaine Network	50
Chapter 6	The Analytic Network	89
BOX 6.1	The Team A/Team B National Intelligence Estimate	91
PART II	THE ANALYSIS PROCESS	119
Chapter 8	The Intelligence Issue	121
Figure 8.1	The PMESII View	127
BOX 8.1	The Lebanon Debacle	129
Figure 8.2	Political Situation Issue Decomposition for Azerbaijan	134
Figure 8.3	Azerbaijan Economic Issue Decomposition	136
Figure 8.4	Economic Sanctions Issue Decomposition	136

Chapter 9 Target Models	143
Figure 9.1 The Model Hierarchy	145
Table 9.1 Target Matrix—Gas Pipeline Proposals	149
Table 9.2 Matrix for Merger and Acquisition Analysis	149
Figure 9.2 The Exponential (or Disaster) Curve	154
Figure 9.3 The S Curve	154
Figure 9.4 The Normal Curve	154
Figure 9.5 Chronological Model of Indian BMD Development	156
Figure 9.6 Opium Production in Afghanistan, 1994–2017	157
Chapter 10 The Target Framework	161
Figure 10.1 Clandestine Network Target Framework—Top Level	164
Figure 10.2 Clandestine Network Target Framework Deconstruction I	164
Figure 10.3 Clandestine Network Target Framework Deconstruction II	165
Figure 10.4 Countries Having Diplomatic Relations with Azerbaijan	166
Figure 10.5 Cooperative Relationships of the Azeri Armed Forces	167
Figure 10.6 Petroleum Production and Consumption in Azerbaijan, 2003–2015	168
BOX 10.1 The Taliban Take Back Afghanistan	169
Figure 10.7 Ethnic Model of Azerbaijan	171
Figure 10.8 Oil and Natural Gas Structure in Azerbaijan	172
Figure 10.9 Percentage of Internet Users in Azerbaijan by Year	173
Figure 10.10 Generic Biological Weapons System Process Model	174
Figure 10.11 Biological Weapons System Test Process Submodel	174
Figure 10.12 Monopolitarian Biological Weapons Development Organizational Model	175
Figure 10.13 A Collateral Model of Monopolitarian Biological Weapons Facilities	175
Figure 10.14 Chronological Model of Monopolitarian Biological Weapons Development	176
Table 10.1 Competitive Target Frameworks of the Lebanon Situation in 1982	179
Chapter 11 Analyzing Existing Intelligence	183
Figure 11.1 The US Collection Taxonomy	185
Figure 11.2 An Analyst's View of the Collection Taxonomy	186
BOX 11.1 The Almanac Trial	189

Figure 11.3	The Effect of Entropy on the Communications Channel	192
BOX 11.2	The Flawed Channel	193
BOX 11.3	The V-2 Rocket	200
BOX 11.4	The Cuban Missile Crisis I	202
Chapter 12 The Information Sources		215
Figure 12.1	Generic Target Framework for Money Laundering	217
Figure 12.2	Customers' Issue Connections to the Generic Target Framework	218
BOX 12.1	The Khanani Network	218
Figure 12.3	The Altaf Khanani Network	219
Table 12.1	Khanani Money Laundering Organization Associations	220
Figure 12.4	Khanani MLO Network	222
Chapter 13 Denial, Deception, and Signaling		237
BOX 13.1	The Man Who Never Was	240
BOX 13.2	The 1998 Indian Nuclear Test	244
BOX 13.3	The Cuban Missile Crisis II	246
BOX 13.4	The Farewell Dossier	250
Figure 13.1	Cultural Differences in Signaling	253
PART III ANTICIPATORY INTELLIGENCE		277
Chapter 15 Anticipatory Analysis: Forces		281
BOX 15.1	Changing the Bessemer Process	284
BOX 15.2	Improving Naval Gunnery	285
Figure 15.1	Views of Iraqi Situation Dependencies	293
Chapter 16 Anticipatory Analysis: Methodology		297
Figure 16.1	The Estimative Methodology	298
BOX 16.1	The Operating System That Might Have Been	300
Figure 16.2	Applying an Iterative Approach to the Methodology	303
Figure 16.3	Kurzweil's Extrapolation of Moore's Law	306
Figure 16.4	Correlation of Perceived Corruption with Ease of Doing Business	307
Figure 16.5	An Influence Tree for the al-Shabaab Insurgency	310
Figure 16.6	Influence Tree for the al-Shabaab Insurgency with Probabilities	312

Figure 16.7 An Example Influence Net Model	314
Figure 16.8 Sensitivity Analysis for al-Shabaab Smuggling through Kenya	317
Chapter 17 Scenarios	327
Figure 17.1 Four Global Energy Scenario Logics	334
Chapter 18 Systems Modeling and Analysis	343
BOX 18.1 The Mujahedeen Insurgency	344
BOX 18.2 The Würzburg Radar	347
BOX 18.3 Knickebein	348
BOX 18.4 The Caspian Sea Monster	349
BOX 18.5 The German Engine Killer	350
BOX 18.6 The P5+1 Negotiations	352
Figure 18.1 Process Model for an Iranian Nuclear Warhead	354
Figure 18.2 Analysis of a Revised Process Model	354
Figure 18.3 The Generic Program Cycle	355
Figure 18.4 The Brooks Curves for Projects	356
Chapter 19 Relationship Modeling and Analysis	363
Figure 19.1 Khanani MLO Link Model	365
Figure 19.2 Khanani MLO Network Model	367
Figure 19.3 Network Diagram Features Used in Law Enforcement Intelligence	367
Figure 19.4 Social Network Analysis Diagram	371
BOX 19.1 The Abu Sayyaf Raid	372
Figure 19.5 Social Network Analysis: A Star Network	373
BOX 19.2 The Enron Network	375
Figure 19.6 Partial Social Network of Enron Corporation	377
Chapter 20 Geospatial Modeling and Analysis	387
BOX 20.1 Identifying the Rabta Plant	387
BOX 20.2 The Inchon Landing	389
BOX 20.3 The Natural Gas Pipeline	390
Figure 20.1 Trans-Afghanistan Natural Gas Pipeline	391
BOX 20.4 The 1919 Paris Peace Conference	393
Figure 20.2 The “Human Terrain” of Europe, 1914	394
BOX 20.5 The Dayton Peace Accords	394

Figure 20.3	The 1991 “Human Terrain” of Former Yugoslavia	395
BOX 20.6	Malaysia Airlines Flight MH17	396
Figure 20.4	Flight Profile of Malaysia Airlines Flight MH17	397
Figure 20.5	Population Flees Ramadi, 2015	399
BOX 20.7	The Leeds Rapist	400
BOX 20.8	URDF-3	401
BOX 20.9	Yamantau Mountain	401
Chapter 21 Simulation Modeling		407
Figure 21.1	Expected Growth in GDP for Some Major World Economies	408
BOX 21.1	The Backfire Bomber Simulations	409
Figure 21.2	Geospatial Network Simulation of Syrian Refugee Movement within Turkey	413
Figure 21.3	Estimate of Syrian Refugee Movement over a 12- to 24-Month Period	414
BOX 21.2	Cultural Mirror Imaging: Pearl Harbor	417
Chapter 22 Prescriptive Intelligence		429
Figure 22.1	Customer Questions in Anticipatory and Prescriptive Intelligence	431

PREFACE

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

This approach accomplishes three basic tasks. First, it makes it easy for customers to ask questions and for analysts to clarify them. Second, it uses the existing base of intelligence information to provide immediate responses to the customer. Third, it manages the expeditious creation of new information to answer remaining questions. The community must provide what is called “actionable intelligence”—that which is relevant to customer needs, is accepted, and is used in forming policy and in conducting operations. And above all, intelligence customers want anticipatory¹ intelligence, or answers about what will happen next. Collaboration enables such an outcome; and as this seventh edition goes to press, the US intelligence community has just produced a sterling illustration.

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

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

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

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

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

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

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

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

What's New?

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

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

² CIA, “Handbook of Problem-Solving Techniques for Intelligence Analysts,” January 3, 1985.

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

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

ACKNOWLEDGMENTS

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

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

Robert M. Clark

Wilmington, North Carolina

THE PROCESS, THE PARTICIPANTS, AND THE PRODUCT

Chapter 1	Introduction	3
Chapter 2	Intelligence in the Age of Contested Norms and Persistent Disorder	13
Chapter 3	The Intelligence Process	35
Chapter 4	The Customer	57
Chapter 5	The Analyst	73
Chapter 6	The Analytic Network	89
Chapter 7	The Intelligence Product	101

Part I describes what intelligence is all about: the setting in which intelligence is created, how it is conducted and how it should be conducted, the people who develop and use it, and the distinct types of intelligence. Chapters 1 and 2 establish the setting. Chapter 3 introduces two views of the process: one based on the traditional intelligence cycle, and a more current view, the target-centric approach. After this overview, the remainder of part I discusses the participants in the process, beginning with the most important one in chapter 4: the customer. Chapter 5 considers the qualities and roles of the intelligence analyst, and chapter 6 details the analytic environment, with emphasis on the team that supports the creation of quality intelligence for the customer. Part I concludes with chapter 7, a discussion of intelligence products and cautions to consider.

1

INTRODUCTION

Intelligence analysis long existed in the shadows. When it appeared in early films and novels, the focus was on covert action rather than clandestine collection. The plotlines rarely focused on analysis—a boring subject, from the viewpoint of the storyteller. Even the nongovernment version, competitive intelligence¹ analysis, remained a subject to be avoided. Companies simply didn’t talk about their intelligence efforts and the topic certainly didn’t appear in popular media.

In the past two decades, that has changed. The discipline has emerged from the shadows, in part as the result of two trends. First has been the *commercialization of intelligence*. Much raw intelligence is now available from companies that provide imagery and signals intelligence from satellites and drones. Second, and a consequence of the first, is often described as the *globalization of intelligence*; intelligence analysis now has reached beyond its national level and military origins, and is practiced in homeland security, law enforcement, and commercial organizations around the globe. Intelligence has become known as more than spying and covert actions. And in the process, many participants have discovered that intelligence analysis is anything but boring. In fact, its practice often most closely resembles a Sherlock Holmes adventure.

But where Sherlock Holmes inevitably came up with the right answer, intelligence analysis sometimes misses the mark. And, as noted in the preface, we tend to learn more from our failures than from our successes. There is much to be learned from what have been called the two major US intelligence failures of this century—the September 11, 2001, attack on US soil and the subsequent miscall on Iraqi weapons of mass destruction. We’ll cover both events later on; but let’s begin with an overview of why we sometimes miss the mark.

WHY INTELLIGENCE FAILS

As a reminder that intelligence failures are not uniquely a US problem, it is worth recalling notable setbacks encountered by other countries in the past century:

- *Operation Barbarossa, 1941.* Josef Stalin acted as his own intelligence analyst, and he proved to be a very poor one. Russia was unprepared for a war with Nazi Germany, so Stalin ignored the mounting body of incoming intelligence indicating that the Germans were preparing a surprise attack. German

deserters who told the Russians about the impending attack were considered provocateurs and shot on Stalin's orders. When the attack, named Operation Barbarossa, came on June 22, 1941, Stalin's generals were surprised, their forward divisions trapped and destroyed.²

- *Singapore, 1942.* In one of the greatest military defeats that Britain ever suffered, 130,000 well-equipped British, Australian, and Indian troops surrendered to 35,000 weary and ill-equipped Japanese soldiers. On the way to the debacle, British intelligence failed in a series of poor analyses of their Japanese opponent, such as underestimating the capabilities of the Japanese Zero fighter aircraft and concluding that the Japanese would not use tanks in the jungle. The Japanese tanks proved highly effective in driving the British out of Malaya and back to Singapore.³
- *Yom Kippur, 1973.* Israel is regarded as having one of the world's best intelligence services. But in 1973, its leadership was closely tied to the Israeli cabinet and often served as both policy advocate and information assessor. Furthermore, Israel's past military successes had led to a degree of hubris and belief in inherent Israeli superiority. Israel's leaders considered their overwhelming military advantage a deterrent to their opponents. They also assumed that Egypt needed to rebuild its air force and forge an alliance with Syria before striking. In this atmosphere, Israeli intelligence was vulnerable to what became a successful Egyptian deception operation. Relying on these assumptions, Israel's chief of military intelligence dismissed reporting that correctly predicted the impending attack. The Israeli Defense Forces were caught by surprise when, without a rebuilt air force and having kept their agreement with Syria secret, the Egyptians launched an assault during Yom Kippur, the most important of the Jewish holidays, on October 6, 1973. The attack was ultimately repulsed, but only at a high cost in Israeli casualties.⁴
- *Falkland Islands, 1982.* Argentina wanted Great Britain to relinquish the Falkland Islands, which Britain had occupied and colonized in 1837. Britain's tactic was to conduct prolonged diplomatic negotiations without giving up the islands. There was abundant evidence of Argentine intent to invade, including a report of an Argentine naval task force headed for the Falklands with a marine amphibious force. But the British Foreign and Commonwealth Office did not want to face the possibility of an attack because it would be costly to deter or repulse. Britain's Latin America Current Intelligence Group (dominated at the time by the Foreign and Commonwealth Office) concluded accordingly, on March 30, 1982, that an invasion was not imminent. Three days later, Argentine marines landed and occupied the Falklands, provoking the British to assemble a naval task force and retake the islands.⁵

- *Afghanistan, 1979–1989.* The Soviet Union invaded Afghanistan in 1979 to support the existing Afghan government, which was dealing with an open rebellion. The Soviet decision to intervene was based largely on flawed intelligence provided by KGB chairman Yuri Andropov. Andropov controlled the flow of information to the general secretary of the Communist Party, Leonid Brezhnev, who was partially incapacitated and ill for most of 1979. KGB reports from Afghanistan created a picture of urgency and strongly emphasized the possibility that Afghan prime minister Hafizullah Amin had links to the CIA and US subversive activities in the region.⁶ The conflict developed into a pattern in which the Soviets occupied the cities while the opposing forces, the mujahedeen, conducted a guerrilla war and controlled about 80 percent of the country. The mujahedeen were assisted by the United States, Pakistan, Saudi Arabia, the United Kingdom, Egypt, and the People's Republic of China. As the war dragged on, it saw an influx of foreign fighters from Arab countries, eager to wage jihad against the Soviet infidels. Among these fighters was a young Saudi named Osama bin Laden, who later would gain notoriety in another conflict. Faced with increasing casualties and costs of the war, the Soviets began withdrawing in 1987 and were completely out of the country by 1989, in what has been called the "Soviet Union's Vietnam War."

The common theme of these cases and others like them discussed in this book is *not* the inability to collect intelligence. In each of these cases, it had been collected. Three themes are common in all of them: failure to share information, failure to analyze collected material objectively, and failure of the customer to act on intelligence.

Failure to Share Information

From Pearl Harbor to 9/11 to the erroneous intelligence estimate on Iraq's possession of weapons of mass destruction (WMD), the inability or unwillingness of collectors and analysts to share intelligence was emblematic.

The Iraqi WMD Commission (the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, which issued its formal report to President George W. Bush in March 2005) found that collectors and analysts failed to work as a team.⁷ They did not share information effectively. Progress has been made since then; however, the root causes for the failure to share remain in almost all intelligence services worldwide:

- Sharing requires openness. But any organization that requires secrecy to perform its duties will struggle with and often reject openness.⁸ Most governmental intelligence organizations, including the US intelligence community, place more emphasis on secrecy than on effectiveness.⁹ The penalty

for producing poor intelligence usually is modest. The penalty for improperly handling classified information can be career-ending.¹⁰ There are legitimate reasons not to share; the US intelligence community has lost many collection assets because details about them were shared too widely. A balancing act is required between protecting assets and acting effectively in the world.

- Experts on any subject have an information advantage, and they tend to use that advantage to serve their own agendas.¹¹ Collectors and analysts are no different. At lower levels in the organization, hoarding information may confer job security benefits. At senior levels, unique knowledge may help protect the organizational budget. The natural tendency is to share the minimum necessary to avoid criticism and still protect the most valuable material. Any bureaucracy has a wealth of tools for hoarding information, and this book discusses the most common of them.
- Finally, both collectors and analysts find it easy to be insular. They are disinclined to draw on resources outside their own organizations.¹² Communication across organizations has long-term payoffs in access to intelligence from other sources, but in the short term, it requires more time and effort.

Although collectors, analysts, and intelligence organizations have a number of incentives to conceal information, leaders since 9/11 have acknowledged that intelligence must be a team sport. But effective teams require cohesion, formal and informal communication, cooperation, shared mental models, and similar knowledge structures—all of which contribute to sharing of information. Without such a common process, any team—especially the interdisciplinary teams that are necessary to deal with today’s complex problems—will fall apart quickly.¹³ Today’s intelligence analysts, acting as project managers, are on the forefront in managing the required components and processes for sharing, a topic discussed in chapter 5.

Failure to Analyze Collected Material Objectively

In each of the cases of failure cited earlier, intelligence analysts or national leaders were locked into a *mindset*—a consistent thread in analytic failures. Louis Pasteur warned about that trap in his profession when he observed that “the greatest derangement of the mind is to believe in something because one wishes it to be so.”

Mindset can manifest itself in the form of many biases and preconceptions, a short list of which would include the following:

- *Ethnocentric bias* involves projecting one’s own cultural beliefs and expectations onto others. It leads to the creation of a “mirror-image” model, which looks at others as one looks at oneself, and to the assumption that others will act “rationally” as rationality is defined in one’s own

culture. The Yom Kippur attack was not predicted because, from Israel's point of view, it was irrational for Egypt to attack without extensive preparation. Similarly, Soviet analysis of social processes in Afghanistan was done through the bias of Marxist-Leninist doctrine, which blinded the leadership to the realities of traditional tribal society and Islamic culture.¹⁴ Put simply, Afghanistan did not fit into the ideological constructs of the Soviet leadership.¹⁵

- *Wishful thinking* involves excessive optimism or the avoidance of unpleasant choices. The British Foreign Office did not predict an Argentine invasion of the Falklands because, despite intelligence evidence that an invasion was imminent, they did not want to deal with it. Stalin made an identical mistake for the same reason prior to Operation Barbarossa. In Afghanistan, Soviet political and military leaders expected to be perceived as a progressive anti-imperialist force and were surprised to discover that the Afghans regarded the Soviets as foreign invaders and infidels.¹⁶
- *Parochial interests* cause organizational loyalties or personal agendas to affect the analysis process. That mindset was apparent in Andropov's shaping of the reporting that Brezhnev received about Afghanistan: Andropov wanted to see the USSR intervene there.
- *Status quo biases* cause analysts to assume that events will proceed along a straight line. The safest weather prediction, after all, is that tomorrow's weather will be like today's. An extreme case is the story of the British intelligence officer who, on retiring in 1950 after forty-seven years' service, reminisced: "Year after year the worriers and fretters would come to me with awful predictions of the outbreak of war. I denied it each time. I was only wrong twice."¹⁷ The status quo bias causes analysts to fail to catch a change in the pattern.
- *Premature closure* results when analysts make early judgments about the answer to a question and then, often because of ego, defend the initial judgments tenaciously. This can lead the analyst to select (usually without conscious awareness) subsequent evidence that supports the favored answer and to reject (or dismiss as unimportant) evidence that conflicts with it. Israel's chief intelligence officer did exactly that in 1973.

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

Failure of the Customer to Act on Intelligence

In some cases, as in Operation Barbarossa and the Falkland Islands incursion, the customer failed to understand or make use of the available intelligence.

A senior State Department official once remarked, half in jest, “There are no policy failures; there are only policy successes and intelligence failures.”¹⁸ The remark rankles intelligence officers, but it should be read as a call to action. Intelligence analysts shoulder partial responsibility when their customers fail to make use of the information provided. Analysts must meet the challenge of engaging the customer during the analysis process and help ensure that the resulting intelligence is accepted and considered when the customer must act.

In this book, considerable discussion is devoted to the vital importance of analysts being able to assess and understand their customers and their business or field. The collaborative, *target-centric approach* to intelligence analysis demands a close working relationship among all stakeholders, including the customer, as the means to gain the clearest conception of needs and the most effective results or products. Some chapters also illuminate ways to ensure that the customer considers the best available intelligence when making decisions.

Intelligence analysts have often been reluctant to closely engage one class of customer—the policymakers. In its early years, the CIA attempted to remain aloof from its policy customers to avoid losing objectivity in the national intelligence estimates process.¹⁹ The disadvantages of that separation became apparent, as analysis was not addressing the customers’ current interests and, therefore, was becoming less useful to policymaking. During the 1970s, CIA senior analysts began to expand contacts with policymakers. As both the Falklands and Yom Kippur examples illustrate, such closeness has its risks. In recent years, however, research has shown that analysts are able to work closely with policymakers and to make intelligence analyses relevant without losing objectivity.

WHAT THE BOOK IS ABOUT

This book describes a process for successful intelligence analysis that avoids the three themes of failure just outlined. All intelligence analysis depends on following a process that is based on a *conceptual framework* for crafting the analytic product.²⁰ In fact, all problem solving depends on starting from a conceptual framework,²¹ and intelligence is about problem solving.

In addition to being an organizing construct, conceptual frameworks sensitize analysts to the underlying assumptions in their analysis and enable them to better think through complex problems.²² Conceptual frameworks also are essential in identifying the target—which intelligence may be better equipped (or willing) to do than customers.

This book is about that process and conceptual framework. It develops the ideas of defining the intelligence issue, creating a model of the intelligence target, and extracting useful information from that model. All analysts naturally do this. The key to making it work is to *share* the model with collectors of information and customers of intelligence.

While all analysis follows that basic process, within that process and framework many tools have been developed to deal with specific disciplines and issues. These generally are referred to as *analytic methodologies* or *techniques*.

First, in contrast to the conceptual framework, no standard analytic methodology exists in the US intelligence community. Any large intelligence community is made up of a variety of disciplines, each with its own analytic methodology.²³ Furthermore, intelligence analysts routinely generate ad hoc methods to solve specific problems. This individualistic approach to analysis has resulted in a wide variety of analytic methods, more than 160 of which were identified in 2005 as available to US intelligence analysts.²⁴

There are understandable reasons for the proliferation of methods. Methodologies are developed to handle very specific problems, and they are often unique to a discipline, such as economic or scientific and technical (S&T) analysis (which probably has the largest collection of problem-solving methodologies). As an example of how methodologies proliferate, after the Soviet Union collapsed, economists who had spent their entire professional lives analyzing a command economy were suddenly confronted with free market prices and privatization. No model existed anywhere for such an economic transition, and analysts had to devise from scratch methods to, for example, gauge the size of Russia's private sector.²⁵

Second, an analyst's toolset also includes standard, widely used analytic techniques. An effective analyst must have a repertoire of them to apply in solving complex problems. They might include pattern analysis, trend identification, literature assessment, and statistical analysis. A number of these are presented throughout the book.

A few techniques, though, are used across all the analytic subdisciplines. They are called *structured analytic techniques*, or SATs. SATs are taught in most courses on intelligence analysis. Their use, however, has resulted in some criticism. For instance, as one author notes,

The problem is that many SATs stunt broad thinking and the kind of analysis that busy policymakers want. At the same time, single-minded attention to technique runs the risk of reducing analyses to mechanical processes that require only crunching of the "right" data to address policymaker needs.²⁶

Furthermore, as one senior intelligence officer has observed, “a reliance on structured analytic techniques does not necessarily produce better results” and that “blind faith in SATs is no more redemptive than any other blind faith.”²⁷ Consequently, research indicates that SATs are seldom used in at least some parts of the US intelligence community.²⁸

Despite the criticisms, SATs can have value in analysis if used at the right point in the process. The challenge is that novices can become overwhelmed by the number of SATs, and uncertain where to apply them in the process. And many are not commonly used by intelligence analysts, in part because they're cumbersome and time consuming

to apply. In this book, the focus is on the most useful SATs, and they are introduced at the point where they should be applied. SATs are not discussed in detail herein, as they are well covered in other texts.²⁹

Sherman Kent, who is generally regarded as the father of US intelligence analysis, noted that an analyst has three wishes: “To know everything. To be believed. And to exercise a positive influence on policy.”³⁰ This book will not enable an analyst to know everything; that is why we will continue to need estimates. But it should help analysts to learn or refine their tradecraft of analysis, and it is intended to help them toward the second and third wishes as well.

SUMMARY

Intelligence failures have three common themes that have a long history:

- Failure of collectors and analysts to share information. Good intelligence requires teamwork and sharing.
- Failure of analysts to objectively assess the material collected. The consistent thread in these failures is a mindset, primarily biases and preconceptions that hamper objectivity.
- Failure of customers to accept or act on intelligence. This lack of response is not solely the customer’s fault. Analysts have an obligation to ensure that customers not only receive the intelligence but also fully understand it.

This book is about an intelligence process that can reduce such failures. The process begins with establishing a conceptual framework for analyzing any intelligence issue, followed by the application of analytic tools to deal with the issue.

A large intelligence community develops many such tools, comprising analytic methodologies and techniques, to deal with the variety of issues that it confronts. Structured analytic techniques may be the most valuable when properly applied. But the tools all work within a fundamental process: defining the intelligence issue, creating a model of the intelligence target, and extracting useful information from that model. Success comes from sharing the target model with all stakeholders.

NOTES

1. Large corporations typically have a staff that provides management with intelligence about competitors’ plans, technologies, and products—called, not surprisingly, *competitive intelligence*.
2. John Hughes-Wilson, *Military Intelligence Blunders* (New York, NY: Carroll and Graf, 1999), 38.

3. Ibid., 102.
4. Ibid., 218.
5. Ibid., 260.
6. Svetlana Savranskaya, ed., "The Soviet Experience in Afghanistan: Russian Documents and Memoirs," National Security Archive, October 9, 2001, <https://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB57/soviet.html>.
7. Overview, *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, https://fas.org/irp/offdocs/wmd_report.pdf.
8. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, CIA, 2005), xvi.
9. Ibid., 11.
10. There exists some justification for the harsh penalty placed on improper use of classified information; it can compromise and end a billion-dollar collection program or cut short the life of a dedicated and valued agent.
11. Steven D. Levitt and Stephen J. Dubner, *Freakonomics* (New York, NY: HarperCollins, 2005), 13.
12. Johnson, *Analytic Culture*, 29.
13. Ibid., 70.
14. Savranskaya, "The Soviet Experience in Afghanistan."
15. Ibid.
16. Ibid.
17. Amory Lovins and L. Hunter Lovins, "The Fragility of Domestic Energy," *Atlantic Monthly*, November 1983, 118.
18. William Prillaman and Michael Dempsey, "Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A.," *Intelligence and National Security* 19, no. 1 (March 2004): 1–28.
19. Harold P. Ford, *Estimative Intelligence* (Lanham, MD: University Press of America, 1993), 107.
20. Itai Shapira, "Strategic Intelligence as an Art and a Science: Creating and Using Conceptual Frameworks," *Intelligence and National Security* 35 [no. 2]: 283–99.
21. Shapira, "Strategic Intelligence as an Art and a Science."
22. Jason U. Manosevitz, "Needed: More Thinking about Conceptual Frameworks for Analysis—The Case of Influence," *Studies in Intelligence* 57, no. 4 (December 2013): 22, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-57-no-4/pdfs/Manosevitz-FocusingConceptual%20Frameworks-Dec2013.pdf>.
23. Johnson, *Analytic Culture*, xvii.
24. Manosevitz, "Needed: More Thinking about Conceptual Frameworks for Analysis – The Case of Influence."

12 Part I • The Process, the Participants, and the Product

25. Gerald K. Haines and Robert E. Leggett, eds., "Watching the Bear: Essays on CIA's Analysis of the Soviet Union," CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, 8, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/>.
26. Ibid.
27. Joseph W. Gartin, "The Future of Analysis," *Studies in Intelligence*, vol 63, no. 2 (2019).
28. Michael Landon-Murray. "Putting a Little More "Time" into Strategic Intelligence Analysis," *International Journal of Intelligence and CounterIntelligence*, 30:4, 785–809 (2017).
29. For two very good examples, see CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009), and Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2011).
30. George J. Tenet, "Dedication of the Sherman Kent School." *CIA News & Information*, May 4, 2000, https://www.cia.gov/news-information/speeches-testimony/2000/dci_speech_05052000.html.

2

INTELLIGENCE IN THE AGE OF CONTESTED NORMS AND PERSISTENT DISORDER

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

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

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

If in the days to come mankind has no choice but to engage in war, it can no longer be carried out in the ways with which we are familiar.

... The degree of destruction is by no means second to that of a war, representing(s) semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare.

War which has undergone the changes of modern technology, globalization, and the market system will be launched even more in atypical forms. In other words, while we are seeing a relative reduction in military violence, at the same time we are seeing a defined increase in political, economic, and technological³ violence.

The new principles of war are no longer exclusively "using armed force to compel the enemy to submit to one's will," but rather are "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."⁴

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

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

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

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

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

NATURE OF TWENTY-FIRST-CENTURY CONFLICT

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

Networks

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

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

- Iran was providing financial and military support to Hezbollah in Lebanon, to President Bashar Al-Assad’s regime in Syria, to the Zaydi Houthis in Yemen, and to Shiite militias in Iraq. Under the banner of Shiite solidarity, Iran also provided nonmilitary aid for industrial projects, madrasas, mosques, and hospitals in Shiite regions.⁹
- Saudi Arabia, for its part, provided weaponry and funding to Sunni combatants in Syria, Iraq, and Yemen. Riyadh also deployed its military forces to support the Sunni cause in some cases. In 2011, it sent armored units into Bahrain to quell the pro-democracy rallies of the country’s Shiite majority. Beginning in 2015, it intervened in Yemen to support opponents of the Zaydi Houthis in what has become a proxy war with Iran.¹⁰

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

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

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

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

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

Nonstate Actors

Participants in twenty-first-century conflicts are not all governments. Many networks, as the preceding section indicates, are composed of criminal groups, commercial enterprises, and many other types of nonstate actors. The Zapatista netwar described earlier displayed the effectiveness of such actors. Some commercial enterprises, for example, engage in illicit arms traffic, support the narcotics trade, and facilitate money laundering. While states continue to be the principal brokers of power, increasingly there exists

a profusion of nonstate centers of power that include unconventional and transnational organizations. These groups operate with their own rules and norms that differ markedly from the traditional rules observed by governments.¹³ Intelligence is most concerned with the following major nonstate actors:

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

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

BOX 2.1 NETWAR I: ERDOĞAN VERSUS GÜLEN

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

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

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

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

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

TOOLS OF CONFLICT

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

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

Diplomatic

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

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

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

Information

The information instrument has always had power to shape events. Propaganda has been used in conflicts for centuries. But the vehicles for delivering information have steadily expanded its reach and effectiveness. Its current form, information technology,

has been a game changer in the twenty-first century, enabling more effective use of the other tools as well as being a method for mobilizing supporters, recruiting fighters, and obtaining funding.

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

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

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

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

Military

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

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

The other class involves indiscriminate weapons, often used as instruments of terror or in a form of asymmetric warfare used against advanced military powers or hostile populations. This class includes IEDs and vehicle-borne IEDs (VBIEDs); suicide

bombers; rockets launched into urban areas; and chemical, biological, nuclear, and radiation weapons.

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

Economic

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

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

- The hawala informal system for transferring money long has existed in the Middle East, North Africa, and India. It comprises a large network of funds brokers that functions on mutual trust. Hawala operates in parallel to but separate from international banking and financial channels. It now relies heavily on the internet for communicating the details of funds transfers.
- Since its invention in 2008, Bitcoin has become an important online payment mechanism. This virtual currency relies on peer-to-peer transactions. Although it is widely used in legitimate financial transactions, Bitcoin (along with a variety of other major cryptocurrencies such as Ethereum and Cardano) also serves those who want to avoid having their transactions tracked.
- The dark web—the clandestine side of the deep web—is a primary vehicle for online payments of all types that participants wish to conceal. Darknet markets sell drugs, software exploits, and assassination and fraud services, among others. The Silk Road case, described below, illustrates how the practice works.

BOX 2.2 SILK ROAD

Between 2011 and 2013, Ross Ulbricht led a team that created and managed the world's largest online black market for illegal drugs. Named "Silk Road" for the ancient trade route between China and Europe, the website operated as a dark-net, concealing itself and its users by relying on the Tor browser. (Tor protects the identity, location, and transactions of users by bouncing communications through a distributed network of relays run by volunteers around the world.) Silk Road handled illegal goods, mostly drugs such as heroin, methamphetamine, MDMA, and LSD, using only Bitcoin for transactions. During its nearly three years in operation, the Silk Road team collected 614,305 Bitcoin in commissions—worth approximately \$80 million at the time of Ulbricht's arrest in October 2013.¹⁹ In May 2015, Ulbricht was sentenced to a double life sentence plus forty years in prison without the possibility of parole. His appeal to the US Supreme Court unsuccessful, he turned to the information instrument, employing both traditional and social media attention. A clemency petition has obtained 500,000 signatures; however, at the close of 2021, he remained in prison.

SYNERGY OF THE TOOLS

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

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

BOX 2.3 NETWAR II: ERDOĞAN VERSUS GÜLEN

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

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

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

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

THE FUNCTION OF INTELLIGENCE

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

The Nature of Intelligence

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

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

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

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

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

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

Strategic Intelligence

Strategic intelligence deals with long-range issues. For the military customer, it is produced for senior leadership. It is used to prepare contingency plans, determine what weapons systems to build, and define force structures.²⁵ For national customers generally, strategic intelligence is used to create national policy, monitor the international situation, and support such diverse actions as trade or national industrial policymaking. For law enforcement, it might concern reducing the incentives to gang formation and operation or suppressing the narcotics trade. For corporations, it typically supports strategic planning, market development plans, and investment guidance.

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

Strategic intelligence is tougher to produce than tactical intelligence, which we'll discuss later. The analyst must command more sophisticated analytic techniques. The process resembles that used for tactical intelligence but is more complex because of the longer predictive time frame. The analyst must spend more time because there are lots of options. One has to consider many possible scenarios, and the situation can evolve in different ways.

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

Strengths

Weaknesses

Opportunities

Threats

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

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

Operational Intelligence

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

At the national level, once policy has been established, the intelligence customers have to develop operational plans to execute the policy or to carry out the strategic plan. Consider the following operational planning scenarios and how intelligence could inform them:

- Planning for diplomatic negotiations—Intelligence must determine what the opposing negotiators want and what they will agree to.
- Planning for a trade embargo—Intelligence must determine what sanctions are likely to be effective and what the target country might do to defeat sanctions.
- Support to research and development (R&D) that will result in new weapons systems—R&D intelligence must determine how effective the system will be in a future environment, because development can take years.

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

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

The US military has coined specific names for operational intelligence. The Army and Air Force call it *intelligence preparation of the battlefield*. The Navy likes to use the term *intelligence preparation of the battlespace*. Whatever the name, the process involves the detailed analysis of the surface conditions (terrain or sea) and weather within a specific geographic area. That—along with an understanding of the adversary's forces, doctrine, and tactics—leads to identifying their probable courses of action.

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

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

BOX 2.4 OPERATION DESERT SHIELD/DESERT STORM

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

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

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

BOX 2.5 LEBANON WAR, 2006

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

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

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

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

Operational intelligence to support intelligence-led policing can take several forms. Analysts can anticipate crime trends so that law enforcement can take preventive measures to intervene or mitigate the impact of those crimes. Intelligence that supports, for example, planning to shut down a gang operation or a narcotics ring would be operational. As another example, to help fight terrorism and domestic extremism,

the California Department of Justice examines criminal group characteristics and intervention consequences to determine which groups pose the greatest threat to the citizenry and how best to deal with them.

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

Tactical Intelligence

The military uses the term *tactical intelligence* to refer to quick-reaction intelligence that supports ongoing operations by identifying immediate opportunities and threats (SWOT, again). As was true at both the strategic and operational levels, intelligence has a well-established role at tactical levels in military doctrine. This form of intelligence is associated with a concept that the US military calls *battlespace awareness*. It is used at the front line of any conflict by field commanders for planning and conducting battles and engagements. It locates and identifies the opponent's forces and weaponry, giving a tactical commander the ability to gain a combat advantage.³¹

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

The result, as one author notes, is that

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

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

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

Much of law enforcement intelligence also tends to be tactical in orientation. Tactical intelligence is defined here as that which contributes to the success of specific investigations.³⁴ It is driven by the need for fast response much like in the military arena. For the national customers, it's more like a classified form of the news and is called current intelligence. And tactical intelligence is used every day in the commercial world, as the following example illustrates.

BOX 2.6 SYMANTEC'S TACTICAL INTELLIGENCE

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

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

Symantec maintains this control center to defend banks, Fortune 500 firms, and millions of its software users against cyber threats. It was the front line of the battle against SQL Slammer as it surged through the internet, knocking out police and fire dispatch centers and halting freight trains; against MSBlaster, as it clogged corporate networks and forced websites offline; and in 2017 against a new wave of ransomware such as Petya and WannaCrypt0r.

The analysts in Symantec's war room succeed in their tactical combat because they are expert at employing the intelligence methodology discussed in chapter 3. They have *shared models* of viruses, worms, and Trojans instantly available. They model the operational patterns of North Korean groups that use ransomware such as WannaCry to track a user's keystrokes and to lift passwords and credit card numbers. They have models of the computers that are used to spread viruses. The great plasma screen itself displays a massive model of the internet battlefield, where the beginning of new threats can be seen. Using these models and creating new ones on the fly, these tactical intelligence analysts can analyze and defeat a new virus in minutes.

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

There is a caveat. Dealing with immediate issues can easily consume all available resources. Short-term tactical support will always seem the most critical. An intelligence analyst is seldom able to put aside those assignments in order to develop a clientele having the long-term view.³⁵ But, strategic intelligence is the key to reducing that load over time. Therefore, analysts need a champion in the customer suite to support them in the production of strategic intelligence.

SUMMARY

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

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

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

- Analysis to support strategic intelligence tends to be in-depth research focused on capabilities and plans and to consider many possible scenarios. Its time reference is long term.
- Operational intelligence is more mid- to near term, involving support to planning for specific operations. The military specifies it as *intelligence preparation of the battlefield* (or *battlespace*). It also supports planning for economic and political activities such as trade embargoes and treaty negotiations. In law enforcement, it supports intelligence-led policing to identify or anticipate crime trends.

- Tactical intelligence support tends to be rapid response, or current intelligence, to support plan execution or crisis management. It is focused on the immediate situation. Again, the military gives it a specific name: *battlespace awareness*. Battle damage assessment is one phase of battlespace awareness. Much of the intelligence support to law enforcement, to business, and to countering cyber threats is tactical in nature.

CRITICAL THINKING QUESTIONS

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

NOTES

1. Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute, December 2007, http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
2. Alan Dupont, "Transformation or Stagnation? Rethinking Australia's Defence," *Australian Journal of International Affairs* 57, no. 1 (2003): 55–76.
3. In this context, *technological* refers to the use of information technology.

4. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, 1999), 5.
5. US Joint Chiefs of Staff, *The Joint Force in a Contested and Disordered World*, July 14, 2016, <https://fas.org/man/eprint/joe2035.pdf>.
6. Ibid., iii.
7. John Arquilla and David Ronfeldt, "Cyberwar Is Coming," in *Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Washington, DC: RAND Corporation, 1997), https://www.rand.org/pubs/monograph_reports/MR880.html.
8. David Ronfeldt and Armando Martinez, "A Comment on the Zapatista 'Netwar,'" in *Athena's Camp*, 369.
9. Ben Hubbard, "Iran Out to Remake Mideast with Arab Enforcer: Hezbollah," *New York Times*, August 27, 2017, <https://www.nytimes.com/2017/08/27/world/middleeast/hezbollah-iran-syria-israel-lebanon.html>.
10. Mohamad Bazzi, "No End in Sight for Saudi-Iran Proxy War," *The Straits Times*, November 16, 2017, <http://www.straitstimes.com/opinion/no-end-in-sight-for-saudi-iran-proxy-war>.
11. Anthony Blair, "Enemy Hacked," *The Sun*, April 4, 2022, <https://www.thesun.co.uk/news/18160552/anonymous-russia-leak-soldiers-putin-ukraine-war/>.
12. Jonathan Zittrain, "'Netwar': The Unwelcome Militarization of the Internet Has Arrived," *Bulletin of the Atomic Scientists* 73, no. 5 (2017): 300–4, <https://doi.org/10.1080/00963402.2017.1362907>.
13. U.S. Joint Forces Command, *Commander's Handbook for Attack the Network* (Suffolk, VA: Joint Warfighting Center, 2011), http://www.dtic.mil/doctrine/doctrine/jwfc/atn_hbk.pdf.
14. David Jablonsky, "National Power," *Parameters* (Spring 1997): 34–54.
15. A darknet is a private network overlaid on the web that relies on connections between trusted peers.
16. "US Security Chief Warns of 'New Phase' in Terror Threat," *MSN News*, May 10, 2015, <http://www.msn.com/en-us/news/us/us-security-chief-warns-of-new-phase-in-terror-threat/ar-BBjy1fG>.
17. Robert K. Ackerman, "Unmanned Systems the New Weapon for Terrorists," *Signal*, July 1, 2017, <https://www.afcea.org/content/Article-unmanned-systems-new-weapon-terrorists>.
18. Stephen Shankland, "Ukraine, Fighting Russia With Drones, Is Rewriting the Rules of War," *CNET*, April 11, 2022, <https://www.cnet.com/news/ukraine-is-fighting-russia-with-drones-and-rewriting-the-rules-of-war/>.
19. Patrick Howell O'Neill, "Silk Road Founder Ross Ulbricht Sentenced to Life in Prison," *The Daily Dot*, May 29, 2015, <http://www.dailydot.com/crime/ross-ulbricht-sentencing-silk-road/>.
20. Nate Schenkkan, "The Remarkable Scale of Turkey's 'Global Purge,'" *Foreign Affairs*, January 29, 2018, <https://www.foreignaffairs.com/articles/turkey/2018-01-29/remarkable-scale-turkeys-global-purge>.

21. James V. Grimaldi, Shane Harris, and Aruna Viswanatha, "Mueller Probes Flynn's Role in Alleged Plan to Deliver Cleric to Turkey," *Wall Street Journal*, November 10, 2017, <https://www.wsj.com/articles/mueller-probes-flynns-role-in-alleged-plan-to-deliver-cleric-to-turkey-1510309982>.
22. Christina Maza, "Donald Trump's Fight with Turkey's Erdoğan, Explained," *Newsweek*, August 18, 2018, <https://www.newsweek.com/donald-trumps-fight-turkeys-erdogan-explained-1070848>.
23. Margaret Brennan and Jennifer Janisch, "Are Some U.S. Charter Schools Helping Fund Controversial Turkish Cleric's Movement?" CBS News, March 29, 2017, <https://www.cbsnews.com/news/is-turkish-religious-scholar-fethullah-gulen-funding-movement-abroad-through-us-charter-schools/>.
24. Walter D. Barndt Jr., *User-Directed Competitive Intelligence* (Westport, CT: Quorum Books, 1994), 21–22.
25. Ibid.
26. Joint Chiefs of Staff, "Intelligence Operations," chapter III in *Joint and National Support to Military Operations*, DoD Joint Publication 2-01 (Washington, DC: U.S. Department of Defense, July 5, 2017).
27. Marilyn Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," U.S. Department of Justice Publication No. NCJ 210681 (September 2005), 3.
28. US Navy, *Naval Doctrine Publication 2: Naval Intelligence*, http://www.dtic.mil/doctrine/jel/service_pubs/ndp2.pdf.
29. LTCOL Scott C. Farquhar, "Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD," May 2009, <http://usacac.army.mil/cac2/cgsc/CARL/download/csipubs/farquhar.pdf>.
30. Peterson, "Intelligence-Led Policing," 8.
31. Ibid.
32. Geodesy is concerned with the size, shape, and gravitational field of the Earth, its coordinate systems, and reference frames.
33. Jeffrey R. Cooper, *Curing Analytic Pathologies* [monograph]. Center for the Study of Intelligence (December 2005), 32.
34. Peterson, "Intelligence-Led Policing," 3.
35. Bill Fiora, "Moving from Tactical to Strategic Intelligence," *Competitive Intelligence Magazine*, 4 (November–December 2001): 44.

3

THE INTELLIGENCE PROCESS

George Lucas's original *Star Wars* movie describes the final stages of a human intelligence (HUMINT) operation. The hero, Princess Leia, places the plans for the evil Galactic Empire's ultimate battle machine, the Death Star, into the robot R2-D2, which is functioning as a mobile dead drop.¹ R2-D2 gets the plans to the rebel forces, whose scientific intelligence analyst briefs the rebel command on the plans, pinpoints the weak spot on the Death Star, and presents a brilliant analysis of the enemy defenses. Rebel fighter jockeys deliver proton torpedoes to the weak spot and destroy the Death Star. End of movie.

This *Star Wars* vignette accurately summarizes the intelligence process as it is popularly viewed. The people who collect information and execute the operations get the glory, the press, and the money. The intelligence analyst, working behind the scenes, gets the interesting problems to solve to make it all work.

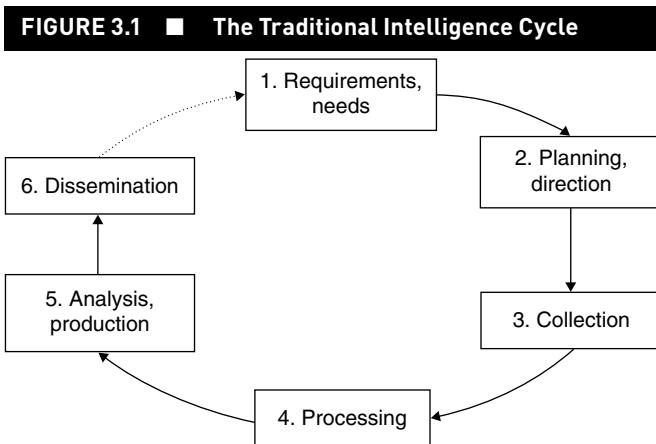
Although the popular focus is on collection and operations, many major failures are due to nonexistent or inadequate analysis, and most of the rest are due to failure to act on the analysis, as noted in chapter 1. The information is usually there, at least in hindsight. So, unfortunately, is a large volume of misleading or irrelevant material that must be examined and discarded. All intelligence organizations today are saturated with incoming information. Furthermore, critical information may not be shared effectively if the intelligence activity is still being organized around the flawed concept of the outdated “traditional intelligence cycle.”

Intelligence is always concerned with a *target*—the focus of the problem about which a customer wants answers. The analyst’s primary job is to develop a level of *understanding* of the target and communicate that knowledge to the customer. In the *Star Wars* example, the target was the Death Star. The rebel intelligence effort supported operations by identifying its weak point and communicating that level of understanding to the customer.

Logic dictates that the process should revolve around how best to approach the target. That is exactly what the remainder of this book is concerned with: the steps to solving a problem, using a target-centric approach, and communicating *understanding* to the customer so that the customer can act based on that. This is the direction that intelligence has taken in practice, and a brief review of the traditional intelligence cycle will illustrate why.

THE TRADITIONAL INTELLIGENCE CYCLE

Historically, intelligence has been described as following a series of steps called the intelligence cycle. It is depicted in elementary form in figure 3.1.



The cycle typically begins with a *requirements* or *needs* step, which amounts to a definition of the intelligence problem. It usually takes the form of a rather general question from a customer, such as, “How stable is the government of Ethiopia?”

Then comes *planning*, or *direction*—determining how the other components of the cycle will address the problem. Collectors must be tasked to gather missing pieces of information. Analysts must be assigned to do research and produce a report on Ethiopian government stability.

The cycle then proceeds to *collection*, or gathering information. Openly available Ethiopian material such as printed newspapers and electronic media must be accessed. Communications intelligence (COMINT) must be focused on Ethiopian government communications. HUMINT operatives must ask questions of sources with knowledge of Ethiopian internal affairs.

From there, the information has to be *processed*. Foreign language material must be translated. Encrypted signals must be decrypted. Digital signals must be translated into visible imagery. Responses from HUMINT sources must be validated and organized into a report format.

Next, the newly collected and processed material is brought together with relevant historical material to create intelligence in the *analysis* phase. An analyst must generate profiles of Ethiopian leaders and assess their likely responses to possible events. The analyst will create models based on the current Ethiopian situation and produce outcome scenarios. This phase also typically includes a peer and supervisory review of the finished product, except in fast-moving, combat intelligence situations, in which simple fusion (discussed in chapter 6) is done.

The finished intelligence must be *disseminated* to the customer in a written report (sent electronically) or a briefing. Then comes a transition to new requirements or needs, and the cycle begins anew.

Over the years, the intelligence cycle became almost a theological concept: No one questioned its validity. Yet when pressed, most intelligence officers admitted that the process “really doesn’t work like that.” Here are some reasons why.

The cycle defines an *antisocial* series of steps. It separates collectors from processors from analysts and too often results in “throwing information over the wall” to become the next person’s task. Everyone neatly avoids responsibility for the quality of the final product. Because such a compartmentalized process results in formalized and relatively inflexible requirements at each stage, it is more predictable and therefore more vulnerable to an opponent’s countermeasures. In intelligence, as in most forms of conflict, if you can predict what your opponents will do, you can defeat them.

The cycle-defined view, when it considers the customer at all, tends to treat the customer in the abstract as a monolithic entity. The closure inherent in a true cycle is absent; in practice, a gap exists between dissemination and needs. Customers, being outside the loop, cannot make their changing needs known. Why does this gap exist?

In government, intelligence officers and policymakers historically had a poor understanding of each other’s business.² That has changed substantially in recent decades as intelligence organizations provided rotational assignments to policy positions for their analysts. In the military the gap has never been wide—the importance of intelligence has been ingrained in military culture over a long time. But as in the civilian side of government, an organizational demarcation usually exists. Most commanders and their staffs have not had intelligence assignments, and intelligence officers typically have not had operations assignments. They tend to speak different jargons, and their definitions of what is important in an operation differ. Military intelligence officers often know more about an opponent’s capability than they do about their own unit’s capability, and the commander often has the inverse problem.

In large intelligence organizations, such as those of the US government, the collection element (see figure 3.1) typically is well organized, well funded, and automated to handle high volumes of traffic. In contrast, the step wherein one moves from disseminated intelligence to new requirements is mostly unfunded and requires extensive feedback from intelligence customers. The system depends on the customers voicing their needs. Military organizations have a formal structure for that to occur; policymakers, with one important exception that is discussed in chapter 4, less so. The policymaker’s input is largely informal, dependent on feedback to the analyst, and may pass through several intermediaries. And for the newest class of customers of US intelligence—law enforcement—the feedback is rudimentary. No entity has the clear responsibility to close the loop. Analysts and their managers, who typically have the closest ties to intelligence customers, usually determine customer needs. But it is too often a hit-or-miss

proposition because it depends on the inclination of analysts who are dealing with other pressing problems.

The traditional conception of the intelligence cycle persisted because it fit a conventional paradigm for problem solving. It flows logically from the precept that the best way to work on any problem is to follow a sequential, orderly, and linear process, working from the question (the problem) to the answer (the solution). One begins by understanding the question; the next step is to gather and analyze data. Finally, apply analysis techniques to answer the question. This pattern of thinking is taught in the simplest problem-solving texts. In fact, conventional wisdom says that the more complex the problem, the more important it is to follow this orderly flow. The flaw of this linear problem-solving approach is that it obscures the real, underlying cognitive processes: The mind does not work linearly; it jumps around to different parts of the problem in the process of reaching a solution. In practice, intelligence officers might jump from analysis back to collection, then to requirements, to collection again, then back to analysis, in what seems a very untidy process, and which in no way resembles a cycle.

Some of the foremost experts in US and British intelligence, such as former director of national intelligence Mike McConnell and noted British author Michael Herman, questioned the traditional cycle's relevance. Both McConnell³ and Herman⁴ observed that the so-called cycle is actually a collection of feedback loops.

US intelligence analysis guru Sherman Kent noted that the problems with the intelligence cycle—the compartmentation of participants, the gap between dissemination and needs, and the attempt to make linear a nonlinear process—are worse in large organizations and in situations far removed from the heat of conflict.⁵ As Keith Hall, former director of the National Reconnaissance Office (NRO), observed, “During crisis the seams go away and all the various players pull together to create end-to-end solutions . . . but we don’t do that well in a noncrisis situation.”⁶

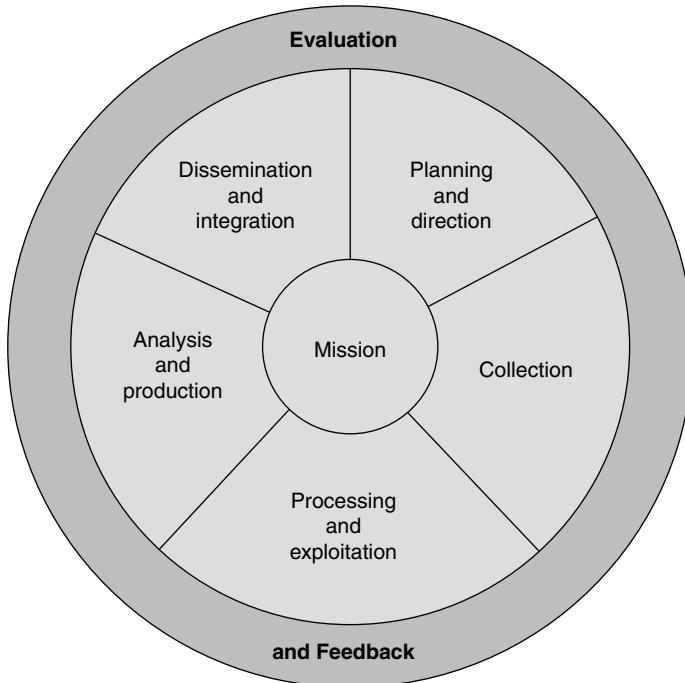
In summary, the traditional cycle may help to explain the structure and function of an intelligence community, but it does not describe the intelligence process. In the constantly evolving world of information technology, the traditional cycle is even less relevant. Informal networks increasingly are forming to address the problems that Kent identified and to enable a nonlinear intelligence process using secure web technology.

The US Department of Defense (DoD) has moved away from the concept of an intelligence cycle, instead describing it as an “intelligence process.” The DoD’s most recent publication on the subject presents the process as shown in figure 3.2.⁷ The figure lists the same steps as in figure 3.1 but removes the idea of a cycle, and instead emphasizes the centrality of the mission (basically, the target) and the importance of evaluation and feedback.

Though nascent, the cycle still appears in some texts, because it embodies a convenient way to convey the organization of large intelligence communities. And it is in some respects a defensive measure; the cycle makes it difficult to pinpoint responsibility

for intelligence failures. Where did this type of cycle come from? It has a long lineage, tracing back to an automaker named Henry Ford.

FIGURE 3.2 ■ DoD View of the Intelligence Process



Source: DoD Joint Publication 2-01.

BOX 3.1 THE AUTOMOBILE PRODUCTION CYCLE

Over a century ago, Henry Ford divided the labor involved in assembling his Model T into eighty-four distinct steps. Each worker was trained to do just one of these steps. So, Ford had interchangeable parts, division of labor, and a continuous flow of a standard product.

And it worked. The Model T had a remarkable run; first produced in 1908, it kept the same design until the last one, number 15,000,000, rolled off the line in 1927—something that hasn't happened since. Industry adopted the assembly line concept. Many governments did also. The Soviets built their entire economic system (for industrial and consumer goods) on the Ford model. If you're producing one thing and demand is stable, it's efficient and easy to manage.

Fifty years ago, the automobile production "cycle" looked a lot like the traditional intelligence cycle. Marketing staff would come up with requirements for new cars. Designers would create a design and feed it to production. Production

would retool the factory and produce the cars in a long assembly line. The cars came out at the end and went to a sales force that sold the cars to customers. And then marketing started on a new requirements set, beginning the cycle anew. If the customer was unhappy with the product, finger pointing could go in all directions.

Today, automobile production is a team effort—with marketing, design, production, and sales staff sitting in the same room with consumer representatives, working together on a common target: the new automobile. This complex, interactive, collaborative, and social process results in the faster production of higher-quality, more market-oriented products.

Just as the original Ford production cycle was developed to deal with the movement of hardware on an assembly line, the intelligence cycle was designed to deal with the movement of reporting in cable or paper form. It provided an orderly, one-way flow. We set up intelligence organizations based entirely on slow movement of intelligence around the cycle. We kept that system even when, first, secure telephones and, then, secure computer communications made it possible to speed things along. We even kept the name “production” as though we were building automobiles.

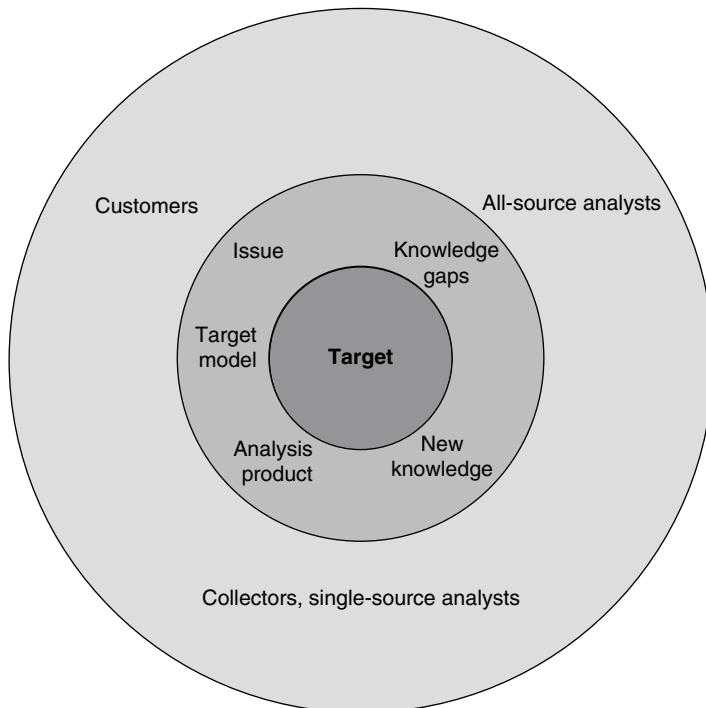
This book defines an alternative, interactive, team approach that describes how intelligence communities actually work today, for a world in which intelligence problems will always be increasingly complex.

INTELLIGENCE AS A TARGET-CENTRIC PROCESS

An alternative to the traditional cycle is to make all stakeholders, *including customers*, part of the intelligence process. Stakeholders within the intelligence community include collectors, processors, analysts, and the people who plan for and build systems to support them. US customers on a given issue could include, for example, the president, the National Security Council (NSC) staff, military command headquarters, diplomats, the Department of Homeland Security (DHS), state or local law enforcement, and the commanders of US naval and Coast Guard vessels.

Figure 3.3 defines this *target-centric* view of the intelligence process. Here the goal is to construct a shared picture of the target, to which all participants can contribute from their resources or knowledge, and from which all can extract the elements they need to do their jobs. It is not a linear sequence, nor is it a cycle (though it contains many feedback loops, or cycles); it is a *network process*, a social process, with all participants focused on the objective. It has been accurately described within the US intelligence community as a “network-centric collaboration process.”⁸

It is especially important to have intelligence collectors and processors be part of the process. In the past, they were seldom consulted by analysts. But as veterans of the traditional process have observed,

FIGURE 3.3 ■ A Target-Centered View of the Process

Both [collectors and processors] write and distribute intelligence information—pieces of the puzzle—but neither shares everything in their minds at any given time: what they are thinking and why. Lots of valuable information lies beyond these officers' formal reports.⁹

That thinking and reasoning needs to be captured.

As director of the National Geospatial-Intelligence Agency (NGA), Letitia Long endorsed the idea of a fresh approach. She termed it “sequence neutrality,” observing that

it turns the traditional TCPED (tasking, collection, processing, exploitation, and dissemination) process focused on a suite of fixed targets inside out. It allows the analyst to form a hypothesis first and then search the data and even drive new collection to test the hypothesis. It also allows the analyst to integrate data before exploitation to focus an analyst's investigation on anomalies in the data that have been correlated. Our ability to know the unknown depends on this new approach to collecting and processing data.¹⁰

Subsequently, the US intelligence community has endorsed the basics of the target-centric approach. Called *object-based production*, or OBP, it involves organizing intelligence efforts around “objects” (targets) of intelligence interest.¹¹ Or as Director of National Intelligence (DNI) James Clapper described it in 2016, “organizing intelligence around what we’re studying: a person, place, or thing.”¹² It features cloud-based sharing of the state of knowledge of the intelligence target. Defense intelligence writers have described it this way:

*Object-based production is a concept being implemented as a whole-of-community initiative that fundamentally changes the way the IC organizes information and intelligence. Reduced to its simplest terms, OBP creates a conceptual “object” for people, places, and things and then uses that object as a “bucket” to store all information and intelligence produced about those people, places, and things. The object becomes the single point of convergence for all information and intelligence produced about a topic of interest to intelligence professionals. By extension, the objects also become the launching point to discover information and intelligence. Hence, OBP is not a tool or a technology, but a deliberate way of doing business.*¹³

The OBP concept is a step in the target-centric direction, though there are two significant differences between the two. First, OBP concerns sharing information about objects, or entities. But the target-centric approach recognizes that a target of intelligence interest is typically an interrelated set of such objects (people, places, and things). OBP needs to capture the interrelationships, and it’s not clear how it would do that. Second, OBP implies sharing knowledge among intelligence community components. But, as the preceding quote indicates, OBP doesn’t include sharing with customers—policymakers, warfighters, and foreign partners—except through the traditional finished intelligence production. The target-centric approach views the customer as a vital team member.

In figure 3.3, the all-source analyst normally is the “manager” of this process, with the task of engaging both customers and collectors (including the single-source analysts in collection agencies). In some cases, the single-source analyst will be the manager. The analyst’s job is to take inputs from disparate sources and provide support to many customers who have different timeline requirements and need different levels of analysis about the same target. The major characteristics of intelligence in such an environment are as follows:

- Analysis can take many forms and draw on many sources. It’s common to make use of several types of sources to get a more complete picture. In addition to traditional intelligence collection, extrinsic sources include expertise from academia, social media, or industry.

- Analysis on any subject is a continuous process. Customers require intelligence support every day, some on shared issues, some on issues unique to them. Consequently, the functions in the process (collection, processing, exploitation, analysis, and dissemination) are happening all the time on any given subject.

The traditional cycle wasn't designed to handle that environment. The target-centric approach is.

This question arises occasionally: How do you implement it? The answer is that *it already has been implemented repeatedly in the online world*. To name three well-known examples: Wikipedia maintains a textual model on almost any target of interest. Wikimedia contains a set of visual models on a wide range of targets. And Google Earth provides detailed interactive geospatial models that anyone can contribute to, in the form of hand-held photography.

The good news is that the target-centric approach is now being put into action in the US and allied intelligence communities. It faces some hurdles that still must be dealt with, especially in the security and information validation areas. In a perfect implementation, any customer with appropriate security clearances would be able to see not only the target model but also the original source information (raw intelligence) used to create it. However, source information sometimes is inaccurate, misleading, or the opposite of the truth, so it requires validation far beyond, for example, a Wikipedia post.

In the process depicted in figure 3.3, customers who have operational problems can view the current state of knowledge about the target (the current target picture) and identify the information they need. Intelligence analysts, working with collectors who share the same target model, translate the needs into "knowledge gaps" or "information requirements" for the collectors to address. As collectors obtain the needed information, it is incorporated into the shared target model. From this picture, analysts and collectors extract actionable intelligence, which they provide to the customers, who may in turn add their own insights. That is, the customers of intelligence can also be information sources. Customers may also add new information needs. Let's bring some meaning to the process shown in figure 3.3 with an example.

BOX 3.2 DODGING MISSILES AT AL ASAD

On January 3, 2020, Iranian Major General Qasem Soleimani arrived at Baghdad International Airport on a flight from Damascus, Syria. As he left the airport fifteen minutes later, a US MQ-9 Reaper strike drone launched three Hellfire missiles at the two vehicles in his convoy, killing the occupants. The strike was ordered after US officials determined that Soleimani was in Iraq to complete plans for an attack on US forces there.

Soleimani had been the commander of Iran's Quds Force, considered to be the second most powerful person in Iran—so the United States expected some kind of response. Five days later it got one. If not for the teamwork of US intelligence and the military operations people at Al Asad Airbase in Iraq, it could have been a major disaster. Possibly the start of another war in the region.

Within days after the strike, US intelligence identified the movement of Iranian ballistic missiles into launch positions. Then on January 7 the intelligence officer at Al Asad gave an ominous report to his commander: "We have information that Iran is fueling 27 medium-range ballistic missiles and their intention is to level this base and we may not survive."

Al Asad had no antimissile defense. The only option for reducing casualties was to evacuate more than 50 aircraft and more than 1,000 troops. But when? Iranian intelligence was known to be monitoring the base using imagery purchased from commercial satellite companies. Evacuate too soon, and the Iranians would undoubtedly spot it and reschedule the attack.¹⁴

General Frank McKenzie, commanding US forces in the Middle East, gave the order: Evacuate after Iran downloads its last commercial satellite picture of the day. According to him, in that last picture, "They would have seen airplanes on the ground and people working."¹⁵ After the order was transmitted, about half the troops quickly moved out into the surrounding desert, leaving a base protection force behind.

On January 8 at approximately 1:20 a.m., the Iranians fired a total of sixteen missiles at Al Asad each carrying 1,000 pounds of high explosives. Eleven of the missiles hit the base; five missed.

For the troops remaining on base, it was a matter of take cover and hope—in bunkers not capable of withstanding a direct hit. Loudspeakers blared out the warning: "Incoming! Incoming! Incoming!" The sound of the incoming warheads was like "a freight train going by you." That was followed by the explosions and massive blast waves. The blast concussions caused more than a hundred cases of traumatic brain injury; but miraculously, no one who stayed behind was killed.¹⁶

This remarkable outcome was the result of an intense cooperative effort between operations and intelligence. Of course, the US military already has a close relationship between the two, developed over many decades. But many organizations had to contribute knowledge to avert a deadly surprise at Al Asad. Certainly imagery, but likely SIGINT and HUMINT, contributed. Knowing when missiles were fueled, and how long after fueling it would take for a launch; when Iranian intelligence would get the last satellite imagery of Al Asad: All of those details required exquisite knowledge and timing.

Contrast the smoothly functioning US response to the impending attack with that of Iranian intelligence and operations afterward. The Iranian air defense system was on alert for a possible counterstrike. A few hours after the attack on Al Asad, one unit mistook a Ukrainian airliner departing from Tehran's international airport for an American bomber. The unit fired three missiles, bringing down the airliner and killing all 176 passengers aboard.

In the Al Asad case, as in other, less time-critical operations, analysis is implicit and pervasive. But the intelligence is not all done by analysts. The customers and the providers of information also participate and will do so whether the analyst welcomes it or not. Both customers and collectors possess valuable insights about the target, and both want their insights included in the analytic product. However, someone must manage the process for it to work. The analyst is best positioned to create and maintain the model of the target, elicit customer needs and change them into requirements for new information, incorporate new information into the target model, and then extract actionable intelligence and ensure that it gets to the customer. These are functions that analysts have always performed. In the target-centric process, they still do them, but collectors and customers can see into the process and have more opportunity to contribute to it.

Because the target-centric approach is more interactive, or social, than the intelligence cycle view, it is a better way to handle complex problems. Because all participants share knowledge of the target, they are better able to identify gaps in knowledge and understand the important issues surrounding it. The team-generated view brings the full resources of the team to bear on the target even when the collectors, analysts, and customers may be geographically remote from one another, via an electronic web. During US operations in Afghanistan in 2002, intelligence officers used screens that resembled internet chat rooms to share data in an interactive process that in no way resembled the traditional intelligence cycle,¹⁷ and they continued that successful pattern during subsequent operations such as Operation Iraqi Freedom and the conflict with Daesh in Syria and Iraq. It now is an established method of producing tactical intelligence likely to be used in all future US and coalition operations.¹⁸

The target-centric approach is resilient. Because the participants collaborate, there is no single point of failure; another member of the network could step in to act as facilitator, and the whole team shares responsibility for the product.

This process is also able to satisfy a wide range of customers from a single knowledge base. There are usually many customers for intelligence about a given problem, and each customer has unique needs. For example, military, foreign relations, financial, and foreign trade organizations all may need information about a specific country. Because there is a common target, their needs will overlap, but each organization also will have its own special needs.

Involving customers increases the likelihood that the resulting intelligence will be used. It also reminds customers of (or introduces them to) the value of an analytic approach to complex problems. It has been asserted that in the United States, government has detached itself from the analytic process and relied too much on the intelligence community to do its analytic thinking.¹⁹ Increasing policymakers' exposure to the analytic process could help reverse that trend.

The collaborative team concept also has the potential to address two important pressures that intelligence analysts continue to face:

- *The information glut.* Analysts are overloaded with incoming material. The target-centric approach expands the team of analysts to include knowledgeable people from the collector, processor, and customer groups, each of whom can take a chunk of the information glut and filter out the irrelevant material. Business organizations have been doing this for years, and they now rely heavily on web-based private networks.
- *The customer demand for more detail.* All intelligence customers are requesting increasingly greater detail about targets. This should not be surprising given that targets are more networked and the range of the customer's options to apply the DIME instruments against opponents has become richer. If the operations target is a building (such as an embassy or a command-and-control center), for example, intelligence may need to include the floor plan; the number of levels; whether it has a basement; the type of construction; roof characteristics; what type of heating, ventilation, and air conditioning it uses; when the building is empty; and so forth. Such details become critical when the objective is to place a smart bomb on the building or to take out the building's electric power.

For collaboration to work—for the extended team to share the data overload and provide the needed target detail—intelligence organizations must provide incentives to share that outweigh the disincentives discussed in chapter 1. Team members must have a wealth of mutual trust and understanding; both of those require team building and extended social interaction.

It is important to note also what the collaborative process is not. As preeminent author and former assistant director of central intelligence Mark Lowenthal has stated, it is not a substitute for competitive analysis—the process by which different analysts present alternative views of the target.²⁰ Collaboration, properly handled, is intended to augment competitive analysis by ensuring that competing views share as much information about the target as possible.

THE TARGET

In Norfolk, Virginia, a young intelligence officer controls a Predator unmanned aerial vehicle on patrol over Afghanistan. The Predator's video display shows a vehicle racing along a mountain road. Moving the Predator closer for a better view, the officer identifies the vehicle as a BMP, a type of armored personnel carrier. He calls in an AC-130 Spectre gunship on patrol nearby. As the AC-130 appears on the scene, the BMP lurches to a stop. The rear doors open, and the BMP disgorges Taliban soldiers running for cover. The Spectre's guns open up. In the Predator's video feed, the soldiers crumple one by one as the stream of gunship fire finds them.

The intelligence officer was able to order the attack by the AC-130 Spectre gunship because he had a mental image of potential Taliban targets, and the BMP fit the picture in its location and characteristics. The BMP in Afghanistan was a specific operations target, but the intelligence view of the target was much larger. It included, for example, details of the road network in Afghanistan that could support the BMP and maps delineating areas of Taliban control. A comprehensive mental model is essential when intelligence provides such close support to operations. The intelligence officer is under intense pressure to distinguish quickly between a troop carrier and a bus full of villagers, and the consequences of an error are severe.

The Target as a Complex System

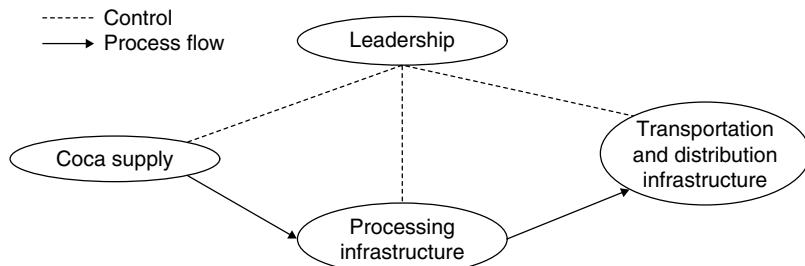
As the BMP example suggests, the typical intelligence target is a *system*, not a single vehicle or building. Intelligence analysis therefore begins by thinking about the target in that fashion. A system comprises structure, function, and process, and the analyst must deal with each of the three in systems thinking.²¹ The *structure* is defined by a system's components and the relationships among them. *Function* involves the effects or results produced, that is, the outputs. *Process* refers to the sequence of events or activities that produce results.

A drug cartel is an example of a system. Figure 3.4 is a macro-level model of a cocaine cartel's structure, showing its major components and the relationships among them. Each of the components has a structure of its own, comprising subcomponents and their relationships. The coca supply, for example, has subcomponents such as farmers, land, seed, and farm equipment. A cocaine cartel also has several major functions, such as surviving in the face of state opposition, making a profit, and providing the illegal drug to its customers. Each component also performs additional functions. The transportation and distribution infrastructure has the functions of getting cocaine from the processor to the customer, selling the drugs, and obtaining payment for them. Most intelligence targets are systems that have subordinate systems, also called *subsystems*. The cartel leadership comprises a subsystem whose structure includes components such as security and finance; it has a function (managing the drug network) and a process for carrying it out.

As a counterpoint, a geographic entity is not a system. A country, for example, is much too abstract a concept to be treated as a system. It does not have structure, function, or process, though it contains within it many systems that have all three. Consequently, a geographic entity alone could not be considered an intelligence target. The government of a region *is* a system—it has structure, function, and process.

Most intelligence targets also are *complex systems* because

- They are dynamic and evolving.
- They are nonlinear, in that they are not described adequately by a simple structure such as a tree diagram or the linear structure depicted in figure 3.1 to illustrate the traditional intelligence cycle.

FIGURE 3.4 ■ Example Target: Cocaine Network

A cocaine supply network is a complex system. It is constantly evolving, and its intricate web of relationships does not yield easily to a hierarchical breakout. It can also be described as a network. Most complex systems of intelligence interest are, in fact, networks—introduced in the next section.

The Target as a Network

Though intelligence has always targeted opposing systems, it has often tended to see them as individual, rather than connected, entities. Such a narrow view downplays the connections among organizations and individuals—and those can be the real strength or weakness of an opposing system taken as a whole. That is why we focus on networks (treated in detail in chapter 19).

Networks, by definition, comprise *nodes* with *links* between them. Several types have been defined, and they vary in the nature of their nodes and links. In communications networks, the nodes are points, usually geographically separated, between which the communications are transmitted. A communications satellite and its ground terminals are communications nodes. The links are the communications means—for example, fiber optics, satellite communications, and wireless (cellular) telephones. In social networks, the nodes are people. The links show the relationships between people and usually the nature of those relationships. A social network exists, for example, at a neighborhood party, an investment club, or, of course, on web applications.

In this book, unless otherwise specified, *network* means a *target network* in which the nodes can be almost any kind of entity—people, places, things, or concepts. A cocaine supply system is obviously a target network. The links define relationships among the nodes. Sometimes the links quantify the relationship. Whereas communications networks and social networks are useful concepts in intelligence, the more powerful target network is a better concept for intelligence analysis and is widely used.

The opposing target network typically is some combination of governments; non-state actors such as environmental, human rights, religious, and extremist groups; individuals; commercial firms; or illicit organizations—along with the resources available to them—all interrelated because they have a shared purpose or in some way support each other, as suggested in figure 3.5. In conflicts, the goals of intelligence are to

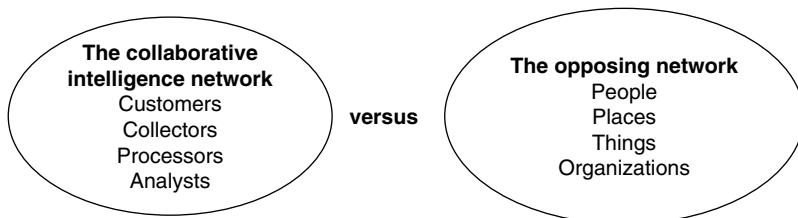
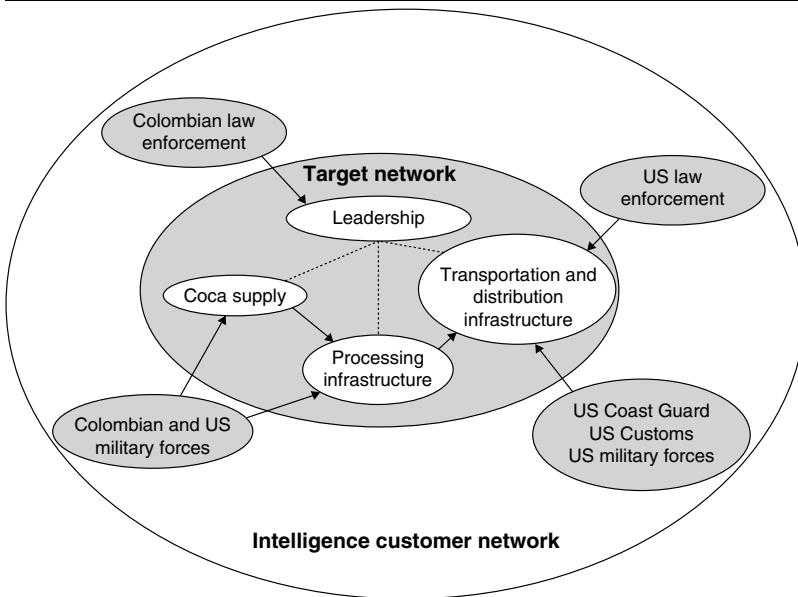
develop an understanding of the opposing network, make the analyst's own network as effective as possible, and render the opponent's network ineffective.

Analysts responsible for assessing the capabilities of an air defense network, a narcotics production and distribution network, or a competing commercial firm or alliance must take a network view. As an example, an analyst concerned with the balance of power in the Middle East might be tempted to look at Syria, Saudi Arabia, Iran, and Iraq separately. Yet no assessment of the future of the Middle East should ignore the continuing tensions among them—the constraining effects of past hostilities on any country's likely future actions and the opportunities that they provide for opponents. These individual countries are part of a larger target network that includes state and nonstate actors from outside the region, all bound by ties of mutual mistrust and suspicion.

It may be easier, especially in a bureaucracy, to see the opponent's side as a network than to see that one's own intelligence and operational assets form a network and to fully exploit its strengths. General Stanley McChrystal, reflecting on his experiences in trying to make networks function effectively in Afghanistan, writes,

It takes a network to defeat a network. But fashioning ourselves to counter our enemy's network was easier said than done, especially because it took time to learn what, exactly, made a network different. As we studied, experimented, and adjusted, it became apparent that an effective network involves much more than relaying data. A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to see, decide, and effectively act. But transforming a traditional military structure into a truly flexible, empowered network is a difficult process.²²

The collaborative, collector-analyst-customer, target-centric approach creates an effective network to deal with an opposing network. Figure 3.6 shows the example of a hypothetical cocaine supply target network located in Colombia and some components of the opposing (that is, US and Colombian) intelligence customer network. As the figure indicates, US law enforcement would target the transportation and distribution infrastructure, because much of that infrastructure is located within US borders or in areas outside Colombia. (US law enforcement would not normally be able to target the cartel leadership in Colombia.) Colombian law enforcement, by contrast, could target both the cartel leadership and its processing infrastructure, though it would probably find the leadership a more profitable target. The customer network shown in the figure is far from complete, of course; it might include political leadership in the United States and Colombia, for example, or regional and European government entities concerned about the cocaine trade.

FIGURE 3.5 ■ Netwar Competition: Network versus Network**FIGURE 3.6 ■ Netwar Example against a Cocaine Network**

Chapter 2 introduced the concept of netwar and the network target. Within the US Department of Defense, netwar has been referred to as *network-centric warfare*.²³ Defense planners have identified three themes:

- A shift in perspective from the single-node target to the network target
- A shift from viewing actors as independent to viewing them as part of a continuously adapting system
- A focus on making strategic choices to adapt—or merely to survive—in the changing system

Network-centric conflict is not a new concept in the business world.²⁴ Companies such as Royal Dutch Shell were creating networks of this kind, including allied outsiders, more than three decades ago. Participants in that network found it a powerful

mechanism for bringing a wide range of expertise to bear on problems.²⁵ The internet has speeded the formation of such networks, and the network-centric approach has been adopted widely in the commercial world. Companies such as Cisco Systems and Walmart have made the collaborative network a key part of their business strategies. In Walmart's retailing approach, the company shares sales information with suppliers in near real time so that they can better control production and distribution, as well as manage their own supply chains for Walmart products.²⁶ Another example is Deutsche Bank's network-centric securities trading system, Autobahn.²⁷ Autobahn replaces the traditional, trader-centered (hierarchical) system of securities trading with a network system in which participants have equal access to securities pricing information. The advantage that the network-centric approach gives companies such as Walmart and Deutsche Bank forces their competitors to adopt similar approaches or lose out in competition. And Amazon, now the world's largest online retailer, with its global network of suppliers and third-party sellers, has demonstrated a new level of network-centric competition. The major difference today in network-centric business competition is temporal; the Walmart and Deutsche Bank networks took years to put into place. Business networks now can be created and changed quickly to meet market conditions, even internationally.

While competitive intelligence appears to be ahead of government intelligence in applying the netwar strategy, government intelligence may be catching up. Even military organizations, with their traditions of hierarchical structure, are adopting the advantages of the network structure, as the earlier General McChrystal quote illustrates. In cases when national intelligence efforts must deal with commercial entities, as they do in economic matters, weapons proliferation, and money laundering cases, intelligence analysts increasingly address network-centric conflict. Furthermore, NGOs are becoming more involved in military, economic, political, and social issues worldwide, and NGO involvement usually makes any conflict network centric, as it did with the Zapatistas in Mexico, described in chapter 2.

Any discussion of the network target should touch on the national intelligence target for a period spanning nearly a decade: Osama bin Laden. In person, he was a hard target to miss, being 6 feet, 5 inches tall and possessing a physical description that was well known throughout the world. But from 2001 to 2011, bin Laden proved to be an elusive target, almost impossible to find if considered alone. However, he had to run a large network and, of course, have some form of communication with it. Despite bin Laden's excellent security system, intelligence analysts and collectors focused on the network as a target and were able to pinpoint his location in Abbottabad, Pakistan, in 2010–2011. The result was the SEAL Team 6 raid on May 2, 2011, that resulted in bin Laden's death. It was a telling example of netwar in action.

Spatial and Temporal Attributes of the Target

Targets of intelligence interest typically have spatial and temporal attributes, and analysis must take these into account. Chapter 20 goes into detail on analyzing these attributes, but a basic description should be included here.

Many targets are fixed geographically. These are mostly elements of a region's infrastructure. Cities and towns, lines of communication (roadways, waterways, and railways), and most structures have fixed locations. The intelligence interest is typically in determining their location (usually in coordinates for smaller targets) or their position on a map if they are lines of communication, and their function.

Many targets of interest, though, are mobile. People, ships, vehicles in general, and satellites all move in space. They may be stationary for a while, but they generally must be characterized in both space and time.

And even fixed targets such as factories have events occurring around them or change physically over time in some way. A missile silo or an airfield, for example, is fixed. But patterns of activity around the silo or airfield may indicate that something of intelligence interest is occurring. We have to analyze even the fixed targets spatially and temporally.

Cyberspace presents a completely different locational challenge. Several techniques are available to locate and track internet users, including geolocating the IP address (if it isn't spoofed) or exploiting vulnerabilities of a smartphone or computer.

SUMMARY

Intelligence, when supporting policy or operations, is always concerned with a target, most often a complex target network. Traditionally, intelligence has been described as a linear cycle: a process starting from requirements, to planning or direction, collection, processing, analysis and production, dissemination, and then back to requirements. That view has several shortcomings. It separates the customer from the process and intelligence professionals from one another. A gap exists in practice between dissemination and requirements. The traditional cycle was once useful for describing structure and function and may serve as a convenient framework for organizing and managing a large intelligence community. But it has never and does not now describe how the actual intelligence process works or should work.

Intelligence is in practice a nonlinear, interactive, and target-centric process, practiced by a collaborative team of analysts, collectors, and customers collectively focused on the intelligence target for a specific purpose. The rapid advances in information technology have enabled this transition.

All significant intelligence targets are complex systems in that they are nonlinear, dynamic, and evolving. As such, they can almost always be represented structurally as dynamic networks—opposing networks that constantly change with time. In dealing with opposing networks, the intelligence network not only must be highly collaborative but also must see itself as a network. Historically, however, large intelligence organizations have provided disincentives to collaboration. To the extent that those disincentives are removed or tempered, US intelligence increasingly resembles the most advanced competitive intelligence organizations in being target network centric.

Targets of intelligence interest have spatial and temporal attributes: They exist somewhere in space at a given instant. They move around or change as time passes. Identifying the target's location and monitoring its movements or other changes are essential elements of the target-centric approach to intelligence.

CRITICAL THINKING QUESTIONS

1. The traditional intelligence cycle has a management structure; it has groups assigned to handle collection, processing, and analysis for all targets, with subunits responsible for specific targets (e.g., priority countries, terrorism, military support). Discuss ways in which the management structure could differ, and how it could be made most successful, in an intelligence community built on a target-centric approach.
2. Could the existing US intelligence community structure be kept yet somehow be made target centric? What physical (primarily information technology) features would be needed in such a system? What nonphysical features (consider incentives, rewards, and “rules of the game,” for example) would be needed?
3. In the existing US intelligence community structure, each agency has a defined product (raw intelligence reporting or an analytic product) that helps justify that agency’s budget and provides recognition for collectors and analysts. What are the implications for the existing system as it moves further in the direction of a target-centric approach? What changes could be made to encourage collaboration?
4. Select a target organization (that is not a drug cartel) about which extensive information is openly available. The organization does not have to be engaged in illicit or hostile activity; a multinational corporation, for example, would be a natural target in competitive intelligence. Create a diagram showing the organizations that are associated with the target, for example, as suppliers or allies. The diagram should include the links between the organizations.

NOTES

1. A *dead drop* is a temporary concealment place for material that is in transit between two clandestine intelligence operatives who cannot risk a face-to-face meeting. A tin can next to a park bench or the interior of a personable robot are classic examples of dead drops.
2. David Kennedy and Leslie Brunetta, “Lebanon and the Intelligence Community,” Case Study C15-88-859.0 (Cambridge, MA: Kennedy School of Government, Harvard University, 1988).

3. Quoted in William J. Lahneman, *The Future of Intelligence Analysis*, Center for International and Security Studies at Maryland, Final Report, vol. I (March 10, 2006), E-8.
4. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 100.
5. Sherman Kent, "Producers and Consumers of Intelligence," in *Strategic Intelligence: Theory and Application*, 2nd ed., ed. Douglas H. Dearth and R. Thomas Goodden (Washington, DC: US Army War College and Defense Intelligence Agency, 1995), 129.
6. Quoted in Stew Magnuson, "Satellite Data Distribution Lagged, Improved in Afghanistan," *Space News*, September 2, 2002.
7. Joint Chiefs of Staff, "Intelligence Operations," chapter III in *Joint and National Support to Military Operations*, DoD Joint Publication 2-01 (Washington, DC: US Department of Defense, July 5, 2017).
8. V. Joseph Broadwater, "I Would Make the T-PED Pain Go Away," memorandum for the record (US National Reconnaissance Office, Washington, DC, August 3, 2000, photocopy).
9. Frank Strickland and Chris Whitlock, "Understanding and Creating Colocated, Cross-Functional Teams, *Studies in Intelligence* 60, no. 1 (2016).
10. Letitia A. Long, "Activity-Based Intelligence: Understanding the Unknown," *Intelligencer: Journal of U.S. Intelligence Studies* (Fall/Winter 2013): 9.
11. Defense Intelligence Agency, "Modernizing Defense Intelligence: Object Based Production and Activity Based Intelligence," June 27, 2013, <http://www.slideshare.net/RDSWEB/dia-activity-basedintelligence>.
12. Remarks by the Honorable James R. Clapper, Director of National Intelligence at the GEOINT Symposium, May 17, 2016, <https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2016/item/1594-dni-clapper-s-as-delivered-remarks-at-the-2016-geoint-symposium>.
13. Catherine Johnston, Elmo C. Wright, Jr., Jessica Bice, Jennifer Almendares, and Linwood Creekmore, "Transforming Defense Analysis," *Joint Force Quarterly*, 4th Quarter 2015, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_12-18_Johnston-et-al.pdf.
14. CBS News, "Inside the Attack That Almost Sent the U.S. to War with Iran," February 28, 2021, <https://www.cbsnews.com/news/iran-missile-strike-al-asad-airbase-60-minutes-2021-02-28/>.
15. Ibid.
16. Ibid.
17. Magnuson, "Satellite Data Distribution."
18. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 14, https://fas.org/irp/offdocs/wmd_report.pdf.
19. Robert D. Steele, "The New Craft of Intelligence," February 1, 2002, <http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=217>.

20. Mark M. Lowenthal, "Intelligence Analysis," address to the Intelligence Community Officers' Course at CIA University, July 19, 2002.
21. Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity* (Boston, MA: Butterworth-Heinemann, 1999), 110.
22. General (Retired) Stanley McChrystal, "It Takes a Network," *Foreign Policy*, February 21, 2011.
23. Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124, no. 1 (1998): 28–35.
24. Liam Fahey, *Competitors* (New York, NY: Wiley, 1999), 206.
25. Peter Schwartz, *The Art of the Long View* (New York, NY: Doubleday, 1991), 90.
26. James F. Moore, *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems* (New York, NY: HarperBusiness, 1996).
27. Deutsche Bank, "Autobahn," March 5, 2017, <https://autobahn.db.com/microSite/htm/l/about.html>.

4

THE CUSTOMER

Intelligence is not about writing an item in hopes that someone will read it. An analyst always has a customer, perhaps many customers. But if you want your results to be used, you must understand the customer's perspective. The premier customer of intelligence, the policymaker, may be the most difficult to comprehend.

Some years ago, in a vignette that has been repeated many times, an elderly woman had invested most of her savings in a Ponzi scheme—and, of course, lost it all. When told of the loss, the woman's investment advisor asked, "Why didn't you talk to me first?" The woman's response: "Because I was afraid you'd try to talk me out of it!"

Policymakers are sometimes like that. If they're contemplating a risky policy with no good choices, the last thing they need on the record is an intelligence analyst's conclusion that their choice is likely to fail. That typically makes them the most difficult customers to serve. Still, policymakers respect and tend to listen to analysts who have spent the time needed to address their policy concerns and who have a demonstrated history of providing solid analytic products.

Along with policymakers, there are many other customers of intelligence analysis. Analysts should understand how the diverse customer types operate and learn their perspectives on intelligence—the subject of this chapter.

OVERVIEW OF CUSTOMERS

This chapter focuses on the customers and purposes of analysis. It describes the requirements of various clients in national government, law enforcement, and the private sector, and the purposes and objectives that intelligence has in serving those clients.

The proper term, incidentally, is *customers* (or clients)—not consumers. Many people "consume" the intelligence that analysts produce. Only a few qualify as customers or clients, that is, those persons who will use it in decision making.

Analysis is an addictive profession, in part because it poses frequent challenges and rewards. But it also can be frustrating, especially when after much hard work you have the answer to the intelligence problem and your customer chooses not to listen. Recall Sherman Kent's observation from chapter 1 that analysts have three wishes: "To know everything. To be believed. And to exercise a positive influence on policy." Let's look at each of these wishes in turn.

- The overall purpose of intelligence, as noted in chapter 2, is to reduce uncertainty in conflict. The key point is that analysis doesn't deal with certainty. Both new analysts and customers find that at least disconcerting, even uncomfortable. Analysis reduces but does not eliminate uncertainty, and a key role of analysts is to help the customers grasp that. Analysts may wish to know everything, but they are unlikely ever to reach that fortunate state. We just try to get as close as possible.
- Being believed depends on an analyst's credibility. The fulfillment of this wish can depend on the analyst's reputation, the persuasiveness of the arguments in support of the analyst's conclusions, and the evidence that the conclusions are based on. The target-centric approach is designed to strengthen the analyst's credibility, because the customer is part of the team and has been involved all along. That's much different from simply being presented with a set of conclusions.
- Having an influence on policy (or, more broadly, on ensuing events) depends on the importance of the analyst's findings. As Michael Herman put it, "Authority with governments is greatest where there is some connection with national security, and a need to cope with organized foreign concealment or deception."¹ Similarly, in a law enforcement or business context, the authority of the intelligence analyst is greatest when there is either some connection with the organization's priorities or a need to cope with an opposing (criminal or commercial) entity's concealment or deception. Stated another way: Just how much does the customer *perceive* the need for your intelligence?

The numbers of intelligence customers have expanded steadily over the past century from the traditional two groups—national and military leadership—to include a diverse set. In the United States, since 9/11, law enforcement and emergency response teams, for example, have become regular customers of intelligence. In many countries, such as China and France, commercial firms are major customers of government-provided intelligence because of the competitive advantage that it gives them internationally.

Consider the SWOT methodology, introduced in chapter 2. Identifying opportunities and threats is the job of intelligence. Most customers have some idea of their side's internal strengths and weaknesses, albeit often a distorted idea. Their uncertainty usually concerns the opportunities they have and the threats they face. National-level customers, law enforcement, and business leaders all tend to focus on the threats in looking at intelligence, because of their pervasive fear of surprise. But intelligence serves best when it can provide notice of the opportunities. From nonintelligence sources, customers often have some information on opportunities and threats. State Department policymakers and businesspeople often acquire good information on both from contacts made in the normal course of their jobs, for example. Intelligence analysis must provide something more to merit attention.

UNDERSTANDING THE CUSTOMER

The intelligence customer may be defined by your position. If you're in the US military services, it could be the secretary of defense, the chairman of the Joint Chiefs of Staff, a division commander, the division operations staff for intelligence to support strategic and operational planning, or an F-35 pilot or SEAL team leader about to embark on a mission.

In national, law enforcement, and competitive intelligence, the customer may not be defined so clearly. The US Department of Homeland Security has a diverse set of missions and an even more diverse set of customers both within and outside DHS. National and local law enforcement leaders also have a wide range of interests. All of these have dramatically different needs and want to receive intelligence tailored to their specific concerns.

Once you have identified your customers, you next must find out their needs. But customers often don't know what intelligence analysis can do for them. For example, a competitive intelligence unit may be told to focus on competitors' new products, when their customers really should be worrying about competitors' strategies for taking away market share. You must reach out to the customers, understand their current and long-term interests, and then prove that you can answer the questions they pose. You then should be in a position where the customers seek you out, instead of the other way around.

Single-source analysts have special challenges because of the diverse nature of their customer set. They produce intelligence that goes to all-source analysts, but it often goes to the end user as well. They also may find that other collection disciplines need their product. COMINT analysts, for example, make extensive use of the geospatial intelligence (GEOINT) product, and vice versa.

Policymakers

The elite customers of national intelligence are generally referred to as policymakers. In the United States, this group is topped by the president. High on the list are the members and staff of the National Security Council, which includes secretaries of the major cabinet departments. The premier current intelligence product for these customers is the President's Daily Brief. The national intelligence estimate (NIE) is their primary strategic intelligence product. But the NIE has been criticized over the years. According to an evaluation by Dick Kerr, a former deputy director of central intelligence (DCI),

The fundamental question is whether national intelligence estimates add value to the existing body of analytic work. Historically, with few exceptions, NIEs have not carried great weight in policy deliberations, although customers have often used them to promote their own agendas. The time may have come to reassess the value of NIEs and the process used to produce them.²

Despite the criticisms, NIEs continue to be produced, read by policy customers, and criticized by those who dislike their conclusions. Several factors shape the way that policymakers view finished intelligence reports such as NIEs. Let's look at a few of them.

How Policymakers Differ

The policy culture is quite dissimilar from the intelligence culture, and many of the issues that arise stem from the difficulty of the two cultures in understanding each other. Policymakers, though, are a diverse group; and those in the political, military, economic, and scientific and technical arenas contrast in how they interact with analysts. The differences derive from the complexity of problems policymakers must deal with. Nevertheless, they tend to fall into these broad categories:

- Policymakers in the political arena are traditionally the most difficult customers. They often understand politics better than the analysts do; most of them got where they are because of their political acumen. They generally possess good interpersonal skills; they believe that they read people well, regardless of cultural background. They have their own sources of information, independent of the intelligence community, which they often believe are better ones. And they feel that their experience gives them a better sense of how others make decisions.³
- Unlike in the political realm, policy-level customers of scientific, technical, and weapons intelligence are likely not to be able to match the technical competence of the analyst in the analyst's special field. They usually need help in understanding the implications of intelligence and, accordingly, will give the analyst's opinions a substantial amount of respect.
- Policy customers of military and economic intelligence tend to fall in between these extremes. They have a good understanding of the subject matter but are more receptive to the intelligence analyst's assessments than policy customers in the political arena.

The Policymaker's Environment

All policymakers work under severe time pressures in a disruptive environment. This work setting drives their preference for succinct messages. They need quality analytic insights to help them deal with complex problems, often in a brief time frame. It is difficult to provide the sort of in-depth study that characterizes strategic intelligence.

Former secretary of defense Robert McNamara well described the policymaker's (and executive's) environment. Looking back at his Vietnam mistakes, he observed, "One reason [we] failed to take an orderly, rational approach . . . was the staggering variety and complexity of the other issues we faced. Simply put, we faced a blizzard

of problems, there were only 24 hours in a day, and we often did not have time to think straight. This predicament is not unique to the administration in which I served or to the United States. It has existed at all times and in most countries.²⁴ As a result,

- Policymakers have little time to make their needs known or to dialogue with the analyst.
- The intelligence message must be clear, unequivocal, and usually brief—on one page or, better yet, in the title of the article.
- Policymakers have short memories. They need to be reminded of past material—past knowledge cannot be assumed. They typically don't retain copies of prior intelligence.
- Policymakers have a “today's news” orientation. They tend to prefer current intelligence; in-depth analysis often is less valued. Long-term research must provide an answer to a question that the policymaker is struggling with or identify a likely development that commands attention.

The Policymaker's Mindset

A policymaker's job is, obviously, to make policy. Many come to their work with a preconceived idea of what the policy should be. If not, they frequently adopt a mindset, and after having done so, the evidence must be overwhelming to change it. Receptivity to intelligence typically changes over time. At the start of a new administration, intelligence analysts have their greatest impact. As policy views begin to harden, it takes more and more evidence to change anyone's mind.⁵ Policymakers will demand more proof if the intelligence negatively affects their agenda and accept a much lower standard of proof when it complements their agenda.

Policymakers are apt to sift through available intelligence, selecting those items that support their mindsets. This executive habit has existed since there have been leaders. In the sixteenth century, Philip II ruled the Spanish empire as the ultimate “hands-on” executive, typical of leaders before and since. He chose to accept incoming information from his far-flung intelligence network that supported his preconceived ideas and to avoid or ignore anything that contradicted them.⁶ Like many executives since, Philip II was prone to wishful thinking, and one consequence was his decision to dispatch the Spanish Armada in an ill-fated attempt to invade England. There are many more recent examples:

- A CIA analyst in 1951 was studying the movements of the Chinese and reached the conclusion that they had surreptitiously introduced their forces into North Korea. He briefed the assistant secretary of state for Far Eastern affairs, Dean Rusk, who later became secretary of state under Presidents John

Kennedy and Lyndon Johnson. Rusk listened politely to the briefing, and at the end of it he said, “Young man, they wouldn’t dare.”⁷ Weeks later, the Chinese attacked UN forces in Korea.

- Even CIA directors have been trapped in mindsets on occasion. Former DCI Stansfield Turner believed that Ayatollah Khomeini was just another Iranian politician. Despite the arguments of his analysts, Turner briefed the NSC that after the overthrow of the shah of Iran, things would go on pretty much as they had before.⁸ Quite the opposite happened, and the disruptive effects of the Iranian revolution continue today.

An insidious problem with customer mindset is that subordinates (including both analysts and intermediaries) may be tempted to pander to it. It has been noted that Soviet intelligence—both the KGB and GRU—consistently told Soviet leaders only what they wanted to hear.⁹ During the Vietnam War, US defense leadership often did the same. Secretary of Defense Robert McNamara and the Joint Chiefs of Staff tightly controlled the flow of information to the president and maintained the ability to ensure that only favorable intelligence was shown to him. According to one briefer, President Johnson “got very depressed and hard to handle when shown bad news.”¹⁰

Policymaker Priorities

National customers have an insatiable appetite for intelligence (though, as noted earlier, not necessarily for *strategic* intelligence). The US intelligence community does not have the resources to satisfy all the demands of all its policy customers. Some sort of prioritization framework has to be established.

The United States does have a national-level prioritization scheme; in fact, it has had many of them. Several attempts have been made to formalize intelligence priorities since the National Security Act of 1947. The National Intelligence Priorities Framework (NIPF) is the current guidance from the director of national intelligence to the intelligence community on priorities. It is reviewed by the NSC, approved by the president, and updated semiannually. The NIPF guides prioritization for the operation, planning, and programming of US intelligence analysis and collection. It takes the form of a matrix of countries and nonstate actors of intelligence interest versus a set of intelligence topics.

Effective Analyst Interaction with Policymakers

In spite of policymaker mindsets, their uniquely charged environment, and their focus on current rather than strategic intelligence, analysts have a fighting chance to make a difference with this customer set.

James Madison University professor Stephen Marrin developed a set of recommendations to make the analyst-policymaker relationship work more effectively. His suggestions are as follows:

- Ensure that the intelligence analyst provides knowledge and expertise which the policymaker might have difficulty acquiring on his or her own.
- [Be] as transparent as possible in terms of the reliability of its sources, progression of its logic and argumentation, reflection of the analysts' confidence in its conclusions, and incorporating structured analytic techniques as a framework for providing decisionmakers with an understanding of the social scientific underpinnings of the process.
- Institutionalize mechanisms for the integration of both intelligence and policy perspectives in mutual assessments.
- Improve the quality and rigor of policymaker assessments.¹¹

The target-centric approach facilitates these ideas. Even the fourth recommendation—which would seem to be solely within the province of the policymaker—is more likely to happen when the policymaker has intimate contact with the analytic methodologies used by analysts. Marrin notes that the intelligence-policy divide is caused largely by the “duplication of function at different levels of responsibility within the overall decision-making process.”¹² A close, interactive relationship, as described throughout this book and captured in figure 3.3, results in a sharing of the function rather than a duplication.

Congress

Congress has become a major intelligence customer—primarily, but not exclusively, of the CIA. This role derives from Congress's responsibility to provide oversight of intelligence. Much focus of that oversight has been on collection and covert action, but analysis gets some attention.

From the very beginning, the CIA regarded Congress as an appropriate customer for its substantive analysis. Nevertheless, until the mid-1970s, Congress was not routinely given analytic products. Committees with a need to see such analysis might be permitted to read it, but for the most part, it was briefed to them by the DCI or other senior CIA officials. With the establishment of the Senate Select Committee on Intelligence in 1976 and the House Permanent Select Committee on Intelligence the following year, each with approved facilities for the storage of classified information, the main practical obstacle to sharing finished intelligence with Congress was removed.

Congress today has become an active consumer, and often critic, of intelligence. More often, what provokes challenges and criticism is not what is briefed or delivered on Capitol Hill. It is what members of Congress see or hear in the news media indicating an apparent failure to predict an event important to US interests. Earlier in this chapter, we noted the importance of not surprising the customer; that is true as well for Congress. Congress can handle almost anything but surprise. A study of Congress as a customer concluded, “Above all, the Agency [CIA] knew the chairmen of its subcommittees did not want to be surprised.”¹³

A difficulty in having Congress as a customer stems primarily from the tendency of individual senators and representatives to leak intelligence, using it as a weapon to affect policy they don’t like. To be fair, Congress isn’t the only source of such leaks in the government. They also tend to come from administration officials who are trying to undermine policies with which they disagree. Congress can exercise its influence on policy via its budget authority.

When Congress asks a question, the intelligence community must respond and must do so on the congressional schedule. But an unreasonable time frame is a factor that can contribute to an intelligence disaster. For instance, authors have emphasized that the October 2002 national intelligence estimate on Iraqi weapons of mass destruction

*was done under an unusually tight time constraint—three weeks—to meet a deadline for congressional debate. And it was the product of three separate drafters, each responsible for independent sections, drawing from a mixed bag of analytic product. Consistent application of analytic or evidentiary standards became next to impossible.*¹⁴

Another issue with congressional customers is that they often ask loaded questions intended to get answers that match their mindset—the “Have you stopped cheating on exams?” type of question. This sort of question or, more generally, poorly defined issue is an example of what is known as the *framing effect*, a topic we’ll revisit in chapter 8. Most members of Congress (policymakers, too) are quite competent at applying the framing effect when posing questions, to get the answer they want. Lawyers are experts at it. And a mantra throughout this book is that if the question is poorly defined up front, the best subsequent analysis won’t help. Even if the customer does not deliberately frame the question, inexperienced analysts can potentially frame it due to poor communication. A formal issue definition process (discussed in chapter 8) avoids that trap.

Military Leadership

The US military establishment, in contrast to policymakers and Congress, has high regard for strategic intelligence, because many organizations within the Department of Defense, the Joint Chiefs of Staff, and the services conduct strategic planning. The secretary of defense is the top defense customer, and in this century, the Department

of Defense has twice been headed by professionals who understood intelligence well: Robert Gates, a former DCI, and Leon Panetta, a former director of the CIA.

Military customers are usually clear about what they want from intelligence. It is an integral part of their world; they are accustomed to seeing it and understand its value. Still, military leaders, like policymakers, vary greatly in articulating needs. All of them, to some degree, want to act as their own analysts.

As noted earlier, leaders generally, but especially national-level military leaders, tend to focus on threats (as opposed to opportunities). Their questions to intelligence analysts tend to be threat oriented. And that emphasis is much like a framing effect as it naturally leads to the threat being overstated. (Factors that drive intelligence reporting in this direction are explained in chapter 7.) Perhaps the earliest example recorded is from Biblical times, when the Israelites were spying out the land of Canaan. Their leader's objective (and mindset) was to conquer Canaan. His spies brought back unwelcome news, reporting, "They are stronger than we . . . there we saw the giants."¹⁵ The Israelites wound up spending forty more years in the wilderness. There is no indication of what happened to the spies, though, not surprisingly, there were no giants in the reports from the next set of spies, forty years later.

The resulting pressure on defense intelligence analysts to provide threat information, and the consequent risk of overestimation, is well documented, and policymakers compensate for it—which leads to the desensitization issue (discussed in chapter 7).¹⁶ The result, unfortunately, is that the defense analyst's credibility often suffers.

Military Operations

At the military operational and tactical levels, intelligence has a well-established role spelled out in doctrine. Unit commanders are familiar with what it can and cannot do. The relationship between intelligence and operations has a long tradition, and analysis has become even more valuable to warfighters as it has become more sophisticated. As noted in chapter 2, precision strikes require precise knowledge of the target. The role of intelligence in warfighting has expanded steadily, to become a critical part of what is called a "revolution in military affairs."¹⁷

Homeland Security

The US Department of Homeland Security has broad responsibility for assessing both risks and threats to the homeland. In terms of the SWOT model, DHS therefore must assess weaknesses (risks) and threats. The major threats are as follows:

- Domestic extremists
- International terrorists operating in the homeland or directing attacks against it
- Systemic threats such as pandemics and transnational criminal organizations

In fulfilling this role, DHS is a customer for national intelligence organizations. But it also draws knowledge from state, local, and tribal officials and from the private sector. So it works with a wide range of sources.

DHS also has a large set of customers for both tactical and strategic intelligence. Many of the original efforts were focused on the immediate threats to the homeland and responding to incidents.¹⁸ In recent years, DHS has moved its focus to strategic threats such as cybersecurity.¹⁹

Homeland security intelligence at the tactical level includes providing information from overhead collection assets and airborne platforms to first responders after disasters, and to maritime and border security units. As an example, in the aftermath of Hurricane Katrina in 2005, Air Force U-2s and Air National Guard RC-26 aircraft flew photographic reconnaissance missions to support disaster relief. Since then, national-level assets have provided imagery and supporting analysis about oil spills (the 2010 Deepwater Horizon oil spill in the Gulf of Mexico)²⁰ and wildfires (California, 2007 and 2017).²¹ Worldwide, under an international agreement called the “International Charter ‘Space and Major Disasters,’” there now exists a unified system for delivering space-based imagery to those affected by natural or man-made disasters. The charter provides for the rapid tasking of member countries’ imagery satellites for response to such disasters.

Law Enforcement

Law enforcement officials fall somewhere between policymakers and military operations customers in their use of intelligence. Some, such as counternarcotics teams, have experience in dealing with intelligence. Local police traditionally have had limited experience with it as it is done at the national level. Increasingly, however, law enforcement groups rely on crime fusion centers (covered in chapter 6) to provide tactical intelligence, and acceptance of the value of intelligence analysis is increasing. Fusion centers are similar in operation to the watch centers that intelligence agencies rely on. And cybercrime centers have been created in many states to bring together intelligence from national and local sources.

There is a cultural challenge that shapes the nature of intelligence support across the strategic, operational, and tactical arenas in law enforcement. Tactical intelligence especially is intended to aid specific investigations. It is tied to action, usually in the form of making an arrest. The challenge has been stated as follows:

Pure law enforcement focuses on building a legal case related to a crime that already has been committed—an historical perspective with a forensic cast. A case is carefully constructed based on admissible evidence. The evidence is handled in a prescribed manner. The rules associated with chain-of-custody are designed to protect the integrity of information and reduce the pollution of evidence as much as possible. A set of

*procedures is followed precisely to ensure the case will be successfully prosecuted. In comparison, intelligence agencies often collect information in a way that is not admissible in a U.S. Court. Law enforcement agencies are traditionally reluctant to use such information because of the potential of it being challenged and thereby jeopardizing a case.*²²

Some law enforcement organizations are moving from this investigative focus to a strategic view. The emphasis on intelligence-led policing (discussed in chapter 2) has encouraged the trend. Much of the strategic intelligence deals with countering organized crime, specifically drug and human trafficking, and gangs. The strategy focuses on prevention as opposed to exclusively making arrests.

The security classification of intelligence creates difficulties for law enforcement. Raw reporting from HUMINT, imagery intelligence (IMINT), or COMINT sources is typically classified at the “Secret” level or higher, and local law enforcement officials usually have no security clearance. Conventionally this problem is handled by sharing information without source details—“I can’t tell you why, but . . .” Law enforcement officers are comfortable with that; they are used to taking unverified tips. Intelligence officers also occasionally use fictional sources, often creating elaborate reports to conceal the true source and get the material released at a lower classification. But this is a balancing act; you can’t protect sources and in doing so mislead analysts (who will evaluate a report depending on its source). Ideally, you use a fictional source that has the same general level of credibility as the real source.

Business Leaders

Business customers of intelligence resemble political policymakers, for many of the same reasons. Executives in business like to feel that they are in control and that they understand the competitive environment better than anyone else, including their intelligence staff. They have mindsets. They face constant time pressures and are action oriented. But because business leaders pay directly for their intelligence, they are more inclined to give specific guidance and pay attention to the analytic product. They are also more apt to take the analyst to task for poor outcomes.

Customers of competitive intelligence are highly varied in their interests and what they want from their intelligence units. In general, support to corporate strategy concerns issues such as acquisitions, identification of new markets or trends in existing markets, product development, and assessment of threats from competitors and criminal elements. Propensity to use intelligence varies by industry. The pharmaceutical industry, for example, has a tradition of relying on competitive intelligence.

As with national intelligence customers, business organizations must prioritize their needs. A commonly used approach is one that was developed by the US intelligence community during the early 1970s and subsequently abandoned. Competitive

intelligence units, though, picked it up and adopted it. The technique is called *key intelligence topics* (KITs), which define intelligence priorities. From these are derived *key intelligence questions* (KIQs), which provide the questions that need to be answered to address the KITs.²³ The use of KITs and KIQs has thrived in the competitive intelligence world because it provides a structured approach to defining priorities and applying intelligence assets to them.

What All Customers Want

We have pointed out repeatedly that the purpose of intelligence is to reduce uncertainty in conflict. Why is that so important? Because the effect of uncertainty on leaders is profound across the entire spectrum of conflict. Uncertainty can result in the wrong decision, but its *effect* can be even worse than that. The problem starts with a natural tendency of executives to fear loss (or poor outcomes) as a consequence of their decisions.

Most decision makers, including policymakers, military leaders, law enforcement commanders, and business executives, are guided by a principle known as *prospect theory*. It indicates that people will pay a higher price, or risk more, to prevent losses than they will to seek gains. This attitude is manifest in customers' emphasis on threat-related intelligence, discussed previously. Executives, especially in large bureaucracies, tend to be conservative and cautious. So they tend to believe intelligence that warns of losses, and to pay less attention to information that suggests opportunities for gain. This fear of loss, combined with uncertainty, can cause paralysis.

A 2006 study by economists Uri Gneezy, John List, and George Wu demonstrated a phenomenon that they called “the uncertainty effect.” The basic idea is this: Expected utility theory says that people make risky decisions by balancing the value of all possible outcomes. Suppose that you’re betting on the flip of a coin. If it’s heads, you win \$1.10. However, if it comes up tails, you lose \$1. Overall, the expected utility of this gamble comes out in your favor—the potential payout is ten cents more than the potential loss, so you should accept the bet. But studies show most people won’t accept this gamble. The possibility of a loss (and the associated uncertainty) outweighs the temptation of the extra dime. The Gneezy study cites specific examples of how the uncertainty effect leads people to make foolish decisions.²⁴

Fear of loss (or, for the decision maker, of a bad outcome), combined with the uncertainty effect, makes a deadly combination. We in the analysis business can’t cure the fear, but we can reduce uncertainty and thereby help our customers to make better decisions.

One opportunity for gain that will always catch the policymaker’s or military leader’s attention (or even a business leader’s attention) is the chance to deliver an asymmetric response. Although the phrase “asymmetric response” currently has cachet, it is an old technique in conflict, both historical and allegorical. John Milton’s epic poem, *Paradise Lost*, is premised on Satan’s asymmetric response after he is banished to hell.

Instead of conducting another futile assault on heaven, Satan contaminates God's creation on Earth. Around 1600, the Dutch conducted asymmetric warfare against the militarily superior Spanish in the Netherlands; they could move through waterways more quickly than the Spaniards could, in some cases reaching in two days places the Spaniards could reach only in fifteen.²⁵ The Dutch built their successful conflict strategy around this advantage. A superbly crafted asymmetric response to Soviet intelligence, known as the Farewell operation, is discussed in chapter 13. The intelligence officers supporting it received commendations, a rarity in the business. Intelligence that identifies opportunities for asymmetric response will always be welcome, so it is important to highlight opponents' weaknesses and identify their vulnerabilities.

SUMMARY

At the beginning, an analyst must identify the customers of an intelligence product. The customers may be defined by organizational structure—as is typical in military units and in businesses. In national and law enforcement intelligence, the primary customer may be trickier to identify, but proper identification is critical to getting an analysis product read or heard.

Intelligence customers vary greatly in their willingness and ability to express their needs and to make use of intelligence. Policymakers are probably the most difficult customers, because of their pressure-cooker work environment and their tendency to adopt a mindset. Customers of political intelligence are the least receptive of the group; weapons systems and scientific and technical intelligence customers are the most receptive. Military, economic, and business customers typically fall somewhere in between.

In the United States, Congress has become a major intelligence customer. But Congress does not have executive powers, so it cannot use intelligence to make policy or operational decisions. In practice, its role has been more to use intelligence to oppose such decisions and actions.

Military leaders and military operations customers understand and value intelligence. Intelligence has a well-established role, and it has become progressively more important especially at the tactical unit level. Law enforcement officials also increasingly understand the value of intelligence and how to use it; their problem is that they don't usually have the clearances needed to deal with classified material. Business leaders vary in their use of intelligence, depending on the industry and their own background. Because they pay for the intelligence, however, they are generally inclined to make use of it.

All customers rely on intelligence to reduce uncertainty. When the level of uncertainty is high enough, they will avoid making any decisions or make poor ones. As

explained by prospect theory, executives tend to be more willing to accept intelligence about risks of loss or poor outcomes and less willing to make use of intelligence about opportunities for gain.

CRITICAL THINKING QUESTIONS

1. Identify customer(s) in the following scenarios. You may want to research the HIDTA mission before responding.
 - a. You are an intelligence analyst working in the Washington/Baltimore High Intensity Drug Trafficking Area (HIDTA), a program run by the US Office of National Drug Control Policy. Your assignment is to prepare an estimate of the trends in gang violence in the Baltimore area.
 - b. You have the same role as above, but your assignment is to prepare an estimate of narcotics traffic in Northern Virginia (the Washington suburbs).
2. You have been assigned to brief the assistant secretary of state for Western Hemisphere affairs on a likely coup in Guatemala. Her previous job was as ambassador to that country. She has a reputation for being skeptical about intelligence reporting and reportedly once told a CIA briefer that he had no clue what was going on—before throwing him out of her office.
 - a. Describe in detail the research you would do before the briefing. Areas might include the raw intelligence supporting the conclusion, the background of previous briefers, and the backgrounds of others she might respect.
 - b. At the conclusion of your briefing, she tells you that she personally knows the leaders who you say are behind the coup attempt, and that they would do no such thing. How would you respond? Considering her assertion, is there other research that you wish you had performed in part a but didn't think to do?
3. This chapter discusses customers' general preference for intelligence about threats instead of opportunities, and the consequent skewing of intelligence reporting that overstates the threat. How would you compensate for this pressure in dealing with customers? In dealing with collectors?

NOTES

1. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 380.
2. Richard Kerr, Thomas Wolfe, Rebecca Donegan, and Aris Pappas, "Collection and Analysis on Iraq," *Studies in Intelligence*, 49, no. 3 (2007), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49n03/html_files/Collection_Analysis_Iraq_5.htm.

3. Stephen Benedict Dyson and Charles A. Duelfer, "Assessing How the U.S. Intelligence Community Analyzes Foreign Leaders," *International Journal of Intelligence and CounterIntelligence*, 33:4 [2020]: 768–96.
4. R. McNamara, with B. VanDeMark, *In Retrospect: The Tragedy and Lessons of Vietnam* (New York, NY: Vintage, 1966), xxi.
5. Gerald K. Haines and Robert E. Leggett, eds., "Watching the Bear: Essays on CIA's Analysis of the Soviet Union," CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, 18, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/>.
6. Geoffrey Parker, *The Grand Strategy of Philip II* (New Haven, CT: Yale University Press, 1998], 74.
7. Haines and Leggett, "Watching the Bear," 14.
8. Ibid., 18.
9. Dino Brugioni, *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis* (New York, NY: Random House, 1990), 147.
10. Ibid., 573.
11. Stephen Marrin, "Why Strategic Intelligence Analysis Has Limited Influence on American Foreign Policy," *Intelligence and National Security* 32, no. 6 (2017): 725–42.
12. Ibid., 738.
13. Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004* (Washington, DC: CIA Center for the Study of Intelligence, 2008), 10.
14. Kerr, Wolfe, Donegan, and Pappas, "Collection and Analysis on Iraq."
15. Bible, Numbers 13: 31–33.
16. Roger Z. George and James B. Bruce, *Analyzing Intelligence* (Washington, DC: Georgetown University Press, 2008), 80, 113.
17. Anthony D. McIvor, ed., *Rethinking the Principles of War* (Annapolis, MD: Naval Institute Press, 2005), part 5.
18. Mark A. Randolph, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress* (Washington, DC: Congressional Research Service, March 19, 2010).
19. Department of Homeland Security, "Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts," May 15, 2018, <https://www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts>.
20. Maj. Mirielle M. Petitjean, "Intelligence Support to Disaster Relief and Humanitarian Assistance," *The Intelligencer*, AFIO (Winter/Spring 2013), http://www.afio.com/publications/Petitjean_ISR_Spt_to_HA_DR_WinterSpring2013_AFIOIntelligencer.pdf.
21. Airman 1st Class Tristan D. Viglianco, "ANG Provides Aerial Imagery Support for Southern California Fires," *U.S. Air Force*, December 2014, <http://www.af.mil/News/Article-Display/Article/1397232/ang-provides-aerial-imagery-support-for-southern-california-fires/>.

22. AFCEA Intelligence Committee, *The Need to Share: The U.S. Intelligence Community and Law Enforcement* (Fairfax, VA: Author, April 2007), 5.
23. Jan P. Herring, "KITs Revisited: Their Use and Problems," *scip.insight* 5, no. 7 (July 2013), [http://www.growthconsulting.frost.com/web/images.nsf/0/CA6928E7B5561B6086257BB000452B41/\\$File/SCIP13V5I7_BFTP.htm](http://www.growthconsulting.frost.com/web/images.nsf/0/CA6928E7B5561B6086257BB000452B41/$File/SCIP13V5I7_BFTP.htm).
24. Jonah Lehrer, "The Uncertainty Effect," *Wired*, December 6, 2010, <http://www.wired.com/wiredscience/2010/12/the-uncertainty-effect/>.
25. Parker, *The Grand Strategy of Philip II*, 284.

5

THE ANALYST

Intelligence analysis is challenging, often frustrating—and just possibly the best job that you can have. Doing it well requires you to develop a mix of the skills, techniques, and methodologies discussed throughout the remaining chapters in this book. But if you wish to make a career of intelligence analysis, you *must* have these four salient qualities:

- The ability to think critically and logically
- A fierce commitment to objectivity
- A broad perspective on the world and an appreciation of history
- Good instincts

These qualities are described in the sections that follow.

CRITICAL AND LOGICAL THINKING

Critical thinking can be summarized as “thinking about thinking.” We all have made poor judgments at some time in our professional and personal lives. Often it is in hindsight that we apply the critical thinking methodology that could have aided us in identifying where we were about to go wrong.

Detailed, disciplined analysis offers a way to understand complex issues. Given the ramifications of a poorly made national public policy decision, critical thinking is the most essential skill that an analyst needs as a foundation in analysis, and it’s closely linked to the other three qualities we’ll cover. But it’s not something you learn simply by taking courses. It requires practice. It means carefully listening to arguments and reading through the publications of think tanks, nonprofit institutes, and academia for background and a thorough understanding of issues. It requires considering the priorities and biases of the person or organization presenting an argument and investing the time and effort to scrutinize their reports.

Though critical thinking is developed through practice, there are basic principles that apply. Robert Ennis devoted his academic career to, and authored several books on, the subject. He defined critical thinking as “reasonable, reflective thinking focused on deciding what to believe or do.” Ennis distilled critical thinking theory into ten

concrete actions anyone must take.¹ More recently, University of Hong Kong professor J. Y. F. Lau developed a list of the ten abilities of a critical thinker.² Here is a brief composite of the twenty items on the two lists, framed around the process of creating the intelligence product, and expressed in terms appropriate for intelligence analysis:

- *Approaching a problem or issue.* Be open minded and work to be well informed. Examine your own beliefs and values. Avoid looking at the problem, the issue, or the evidence from the viewpoint of *your* beliefs and values.
- *Defining the problem or issue.* Analyze the elements systematically. Define terms in a way appropriate for the context. Develop a model of the problem.
- *Generating hypotheses.* Formulate ideas succinctly and precisely. Rank the relevance and importance of ideas. Understand the logical connections between ideas.
- *Testing hypotheses.* Evaluate the evidence for and against each hypothesis. Judge the credibility of sources. Ask clarifying questions. Determine the quality of an argument, including the acceptability of its reasons, assumptions, and evidence. Identify inconsistencies and mistakes in reasoning.
- *Developing and defending your conclusions.* Draw conclusions when warranted, but with caution. Identify and support your conclusions and assumptions.

We'll delve more deeply into these guidelines in part II and discuss their application to anticipatory intelligence in part III. For now, let's turn to the simplest way of approaching an intelligence issue: by applying logical thinking.

Deductive and inductive reasoning are both based on paradigms drawn from the writings of ancient philosophers:

- The deductive approach is to pose a hypothesis, and search the existing or incoming information for evidence to confirm or reject it. Another way to describe this approach, which we'll return to, is this: We start from a generic model and fill in the elements of it from the evidence.
- The opposite, an inductive or synthesis approach, is to begin by looking at the evidence and to draw conclusions from it.³ We don't start with a model; we build the model from the evidence.

Deduction here can be described as starting from a hypothesis and using evidence to test it. Induction is described as evidence-based reasoning to develop a conclusion.⁴ Evidence-based reasoning is applied in several professions. In medicine, it is known as evidence-based practice—applying a combination of empirical evidence and a theory to make medical diagnoses and decisions.

Each approach has advantages and drawbacks; nevertheless, both are useful in intelligence analysis. The critical thinking guidelines described earlier follow a deductive approach and most analysis efforts proceed, at least initially, by deduction. In some cases that we'll touch on in later chapters, the analysis process starts without a hypothesis. Then we have to begin with induction and look at the evidence. In *all* cases, though, analysts must develop hypotheses—either when defining an issue or in evaluating evidence.

OBJECTIVITY

The CBS television show *60 Minutes* debuted in 1968 and still enjoys an enthusiastic following for its combination of news, investigative reporting, and interviews. In order to entertain, producers highlight dramatic dimensions of current news items and make use of visual images that carry a great deal of persuasive power. It formed a model for TV news and commentary that has been copied many times over. But in dealing with the tension between presenting an interesting story and maintaining objectivity, such programs opt for drama—highlighting interviews to support their point of view and ignoring or downplaying evidence that would undercut it.

Analysts do not have that luxury. It may seem obvious that to remain objective is the first commandment of analysts who desire credibility. Analysts know that a search for evidence to support preconceived notions has no place in intelligence. They know that observations cannot be discarded because they are contrary to expectations. In fact, they understand that their goal is to function like physical scientists. In the physical sciences, astronomers are not emotionally affected when they find that stars follow a certain development pattern. They do not think that this is good or bad; it simply is.

Typically, however, intelligence analysts are put into a position more like that of social scientists. Their thinking may be complicated by difficulty in isolating their emotional reactions from the problem being studied. Put simply, they can *care* about the outcome. But if you wish to assess foreign events, for example, you must put aside personal opinions about war, poverty, racism, police brutality, and government corruption, to name a few tough ones. For instance, “political corruption” is a normal way of life in many areas of the world. It is neither good nor bad in an absolute sense; it is merely the accepted standard of conduct for leaders who want to stay in office. Analysts who are given the task of assessing the international narcotics trade cannot begin with the view that the traffickers are opportunistic scum. Instead, they must practice empathy, or the concept of putting themselves in the shoes of their target. Empathy can be used as a tool of objectivity; it allows analysts to check their biases. You must try to see things from the traffickers’ perspective—they are a group of small businesspeople working to uphold the free enterprise system in the face of excessive government regulation. A well-rounded analyst who has read Machiavelli might find it helpful to reread him, this time from an analyst’s vantage point. One of Machiavelli’s major strengths

was his ability to assess conduct without being hindered by value judgments. Or better still, take time to read a more recent tome on the subject: *The Dictator's Handbook* by Bruce Bueno de Mesquita and Alastair Smith.⁵ It provides excellent insights into how leaders function in most of the world, a perspective quite different from what is typically taught in academic classes on leadership.

In business and industry, the challenge for analysts to keep an objective attitude reaches new heights. Competitive intelligence analysts often must make recommendations without specifically telling decision makers what to do.⁶ Intelligence professionals in government and in the military service long have avoided even making recommendations: They would never offer advice such as, “General, you should deploy your units to the positions I have indicated,” or “Madam Secretary, it would be prudent if your ambassador in Botswana initiated a dialogue with the rebel alliance.” And for good reason. Government intelligence officers typically have neither the operations nor the policymaking experience—nor the current understanding of the issues their customers are dealing with—needed to give such advice. But in many companies, competitive intelligence analysts have both the operations expertise and the credibility to make recommendations.

Government intelligence officers may never become like competitive intelligence analysts—qualified to make judgments on policy or operational issues. But in the give and take of a collaborative environment that includes customers, such judgments are more likely to emerge. Those judgments typically take the form of *prescriptive intelligence*, the topic of chapter 22.

BROAD PERSPECTIVE

Successful intelligence analysts have an inherent inquisitiveness and lifelong interest in learning about subjects and ideas that may seem to have little to no relevance to their current subject area. Wide-ranging reading about other cultures, economies, military traditions, religious and political doctrines, philosophies, and the like gives analysts a breadth of substantive competence that will serve them well throughout their careers.

A long-term perspective is essential in making assessments of a culture, a government, an industry, a system, or a technology. Each of these concerns, even technology, has a long history. With few exceptions, the policymakers or executives who control government organizations, military forces, and industries today earned their credentials fifteen to thirty years previously. Their organizations therefore are shaped by the worldview of key controlling individuals who likely have held on to biases based on the lessons learned through earlier experiences. Analysts cannot properly comprehend the present shape of an organization—public or private—or estimate its likely evolution and organizational behavior without an understanding of what has happened during its history. You cannot understand the 1989 crackdown by the People’s Republic

of China on student demonstrators in Tiananmen Square without understanding the Cultural Revolution from 1966 to 1976 and its impact on the Chinese people.⁷ And it is important for analysts to learn a nation's history as its people teach the subject—which may be quite different from what the analysts were taught in their studies.⁸

A historical perspective requires more knowledge than that of the past few decades. The study of organizations, management, and decision making has gone on for over a century, and some of the most pertinent observations on these subjects trace back to the thinking of Machiavelli, Sun Tzu, and Plato.

GOOD INSTINCTS

Analysts with the right instincts are very special people. Walter Laqueur describes them in his book:

Some people seem to possess an insight that cuts through the maze of history-making facts and factors to bare those that exert an overwhelming force. They select valid assumptions that lead to valid conclusions.⁹

Good instincts are not something we are born with, nor are they usually developed through formal education. They typically are honed through experience with different situations, and the reasoning process based on them has a name. Some writers in the intelligence field argue that intelligence employs a third method of reasoning called *abduction*, which seeks to develop the best hypothesis or inference from a given body of evidence. Abduction is much like induction, in that it begins from a body of evidence to develop a hypothesis; but its stress is on integrating the analyst's thoughts and intuitions into the reasoning process. And like induction, abduction has the difficulty that different analysts can come to different conclusions using the same set of facts. So, both induction and abduction are inherently probabilistic.¹⁰

Abduction has been described as “an instinct for guessing right.”¹¹ In fact, Gordon Negus, an electrical engineer and former executive director of the Defense Intelligence Agency, describes intelligence analysis as “the art of guessing right.”¹² That term doesn’t appeal to some; it’s a reminder that intelligence analysis is both art and science. But the term has a basis in experience. Many discoveries, many advances in science and engineering, came because a gifted and experienced scientist or engineer had a flash of insight. It is not truly a guess nor is it as sudden as it may appear; often the insight is simply the culmination of long-standing focus on the problem, allowing the subconscious to bring forth the idea.¹³ Albert Einstein summarized why this happens in two quotes: “It’s not that I’m so smart, it’s just that I stay with problems longer” and “I have no special talents. I am only passionately curious.”¹⁴ Both comments represent excellent advice for analysts.

THE ANALYST'S ROLE

The analyst's primary role, as described in chapter 3, is to be the facilitator of the target-centric process. Analysts traditionally have been tasked with thinking critically about the issue, the customer, and the target, and with crafting a response to the issue, in the form of a target assessment, that meets the customer's needs. The WMD Commission provided a detailed explanation of this role in its 2005 report:

Analysts are the link between customers and the Intelligence Community. They provide a conduit for providing intelligence to customers and for conveying the needs and interests of customers to collectors. This role requires analysts to perform a number of functions. Analysts must assess the available information and place it in context. They must clearly and concisely communicate the information they have, the information they need, the conclusions they draw from the data, and their doubts about the credibility of the information or the validity of their conclusions. They must understand the questions policymakers ask, those they are likely to ask, and those they should ask; the information needed to answer those questions; and the best mechanisms for finding that information. And as analysts are gaining unprecedented and critically important access to operations traffic, they must also become security gatekeepers, revealing enough about the sources for policymakers to evaluate their reporting and conclusions, but not enough to disclose tightly-held, source-identifying details.¹⁵

This job, as the commission describes it, is a tough one to do well. It can be thought of as having several phases: defining the issue, modeling the target, analyzing existing information about the target, filling gaps in knowledge, developing an answer to the issue, and gaining customer acceptance of the answer. Exceptional analysts need to call on different personal qualities to shepherd along each phase. And, as we have said, they also need a good understanding of the characteristics of their intelligence customers and how to best present intelligence results to win acceptance from those customers.

The role described above is one that analysts have long understood. But now an analyst must do more. In the target-centric intelligence process, the analyst no longer is simply a link between collectors and customers. Instead of having exclusive access to information, the analyst is just one of many people—including customers and collectors—having access. And customers and collectors contribute information as well. With many sources of incoming information that all participants can access, *someone* must be responsible for validating the material. That is the essential new role for the analyst. Analysts now take responsibility for being *curators* of information that goes into the target model; their job is to, as one observer describes it, “endow data with trust.”¹⁶

All of which means that the analyst must understand how to manage a team of people having differing interests, information, and insights—the subject of the next section.

ANALYTIC TEAMS

All analysis projects are, or should be, team efforts. It is the premise of this book that collaboration is the only practical approach for a relevant and successful intelligence community. The analyst functions as the project manager for the team—which may include several analysts from different organizations and expertise. Analysis team efforts have many benefits: You learn from each other and take advantage of a wider range of expertise. In dealing with complex problems, the inputs from a diverse group often are essential. And team efforts promote better information sharing and coordination of the final product. Of course, this is not unique to intelligence. Studies have shown that scientific advances and major engineering projects are increasingly the result of team efforts; the days of lone researchers and inventors such as Einstein and Edison have passed.¹⁷ (“Lone researcher” doesn’t even apply to those famous names. Einstein’s first wife, Mileva Marić, was his partner in developing his theory of relativity. Thomas Edison had a team of engineers to help, one of whom was essential in inventing the incandescent lightbulb.)

There are good reasons why team efforts are the norm: The problems we must solve in all fields have become far more complex, researchers have had to become more specialized to deal with the details, and the most important problems lie at the intersections between multiple disciplines. Collaboration has become the norm in most fields, but especially so in intelligence.

Team efforts also have their costs: They typically take longer to finish a project. Managing across organizational lines is always a challenge, even more so when the participants bring any organizational biases along with them. When analysts, collectors, and customers collaborate, their different writing styles and use of different nomenclatures must be reconciled for the final product. But the payoff in quality is worth the extra time and effort.

Finally, when one moves from descriptive to anticipatory intelligence—the subject of part III—analytic teams comprising several analysts are essential. The uncertainty involved in assessing likely futures requires different fields of expertise and different perspectives. And varying viewpoints help to avoid the cognitive traps that a single analyst might fall into.

Organizing the Analysis Team

An analysis team begins with a dedicated analyst who has the responsibility, authority, and substantive expertise to manage the analysis effort as the leader. Those characteristics are necessary, but not sufficient. The lead analyst also must understand and be committed to the *inclusive* nature of complex problem solving. That implies, for example, that the team leader possesses the qualities described in the next section, “Managing the Analysis Process.”

The target-centric approach helps facilitate such teamwork by emphasizing the benefit of sharing information and expertise among stakeholders, with the *expectation* that there should and will be multiple perspectives and points of view. In this way, the approach breaks down the long-held compartmental barriers that collectors, analysts, and customers have traditionally experienced. Instead, all stakeholders contribute to a target model to address the intelligence problem. The model remains accessible to all participants and available for their input as it evolves. Involvement begets better responsiveness from collectors and better acceptance of the final product by customers.

Customers

Stakeholders in an analysis effort clearly include the customers of intelligence. The team leader must be capable of fostering active participation by the customer community.

A recurring theme in intelligence analysis literature is the nature of the relationship between analysts and customers. How close should the two be? It's been a topic of debate for decades. One side of the argument is that intelligence should be organizationally close to where decisions are made. Those who argue against that arrangement worry that close proximity might affect analyst objectivity. Jack Davis, a forty-year intelligence veteran and author, disputes that premise: "Close professional ties between analysts and policymakers usually promote frankness, mutual respect, and eventually, mutual dependence. In my experience, these in turn promote analysis to help understand and deal with tough problems, not analysis to please."¹⁸ Davis also cites a policymaker's reflection on his profession's commitment to the need for objective analysis: "Policymakers are like surgeons. They don't last long if they ignore what they see when they cut an issue open."¹⁹

On balance, it's better for the two to be close, but that requires a lot of analyst "face time" with the customer. Senior policymakers and military leaders may share their thinking with senior intelligence community managers, but they are less likely to share that thinking with analysts unless there exists a long-standing bond of trust between them. Directors of central intelligence have in the past acted as the top analyst in their dealings with presidents. Sometimes they have been right. DCI John McCone got it right in his assessment that the Soviet Union was deploying ballistic missiles in Cuba, though his analysts disagreed. Sometimes they have been wrong:

- McCone subsequently blew the call when he concluded in 1962 that the real source of the threat in Vietnam was China. He overruled his leading analyst and head of the Board of National Estimates, Sherman Kent. Kent believed that the real threat was in the villages of Vietnam and Laos, and that a military victory was not possible.
- As noted in chapter 4, DCI Stansfield Turner concluded that Ayatollah Khomeini was "just another Iranian politician" and that business as usual would occur after the Iranian revolution. His analysts, who had a quite different view, got it right.²⁰

The lesson is this: Analysts usually are closer to the raw material and spend more time than the manager does in thinking about the problem.

Customers, though part of the team, may or may not be physically present in the deliberations. US and British intelligence services have two distinctly different approaches to the structure for producing their top-level estimates. In Britain, the process follows much like this: Estimates are prepared by a group that comprises both intelligence officers and policymakers.²¹ In the United States, NIEs are prepared in meetings composed exclusively of intelligence officers. Still, though the policymakers themselves are absent, their preferences are usually known and presented. Jack Davis refers to this phenomenon as the “elephant in the room.”²² The drawback to the US approach is that, unlike the British model, the policymaker-analyst dialogue does not take place directly. To continue the analogy, analysts and customers become like the blind men of Hindustan, each perceiving the “elephant” differently.

Therefore, analyst team leaders should expect and even insist that customers be a part of the team. Customer participation may increase the risk of politicization, but their absence from the process increases the risk that the product will not be useful and loses the unique insights that customers can provide. Active participation by the customer community improves not only the quality of the analysis but also support for the final product. When customers are integrated into the study process, their assistance can be invaluable and their resulting confidence in the product makes it more likely to be used.²³

Collectors

The collectors of intelligence—in particular the single-source analysts—also are an important part of the team. Being closely involved means that they can better understand the overall picture and help to fill future intelligence gaps. They also have a stake in how you use the product of their efforts and can provide valuable perspectives on the quality of specific reports. SIGINT representatives have long been participants in the NIE process because of the unique insights they provide on their reporting. HUMINT officers now participate as members of the NIE team, in part because of the erroneous evaluation of reporting by a human source nicknamed Curveball, discussed in chapter 23.

External Sources

Experts from academia and industry are often drawn into analytic teams where their unique knowledge can add value. Governments often tap contractors for expertise as well. Independent think tanks are a common source of contractor expertise, preparing reports by using government-supplied raw intelligence. It’s also common for contractor analysts to sit in intelligence centers alongside government analysts.

Managing the Analysis Process

In the ideal, analytic teams are staffed with experienced intelligence officers. The lead analyst’s job then is to provide the needed resources and encouragement, and to get out of the way and let the team members do their jobs.

That ideal seldom occurs. In most cases, managing a team requires somewhat more of a “hands-on” effort. Managing the process usually is a matter of helping team members to do the following:

- Promote good relationships within the network and understand the needs of all participants
- Implement a rigorous project-planning stage, especially the issue definition part
- Use sound tradecraft
- Coordinate their efforts with peers, working in a team environment

Complex issues involve many stakeholders. Customers, for example, are involved in defining the intelligence issue, while others, such as other analysts, may add constraints to the solution. Teams working on related projects have a particularly large stake, because one team’s answer affects that of the other team. An economic analyst’s assessment that the economy of Italy is headed for serious trouble would be a critical input for another analytic team assessing the political future of Italy. The great benefit of having a team is that individual team members—collectors, analysts, customers, independent experts—are no longer confined to using their expertise in just one area or at just one time during the process. Instead, synergistic discoveries and opportunities occur as pooled experience and talents are brought to bear on one relevant focus: the target model. As such, the process of getting to the answer on complex intelligence problems is fundamentally a *social* one.

As a result, interpersonal skills (including the ability to express and present ideas clearly) cannot be overemphasized. Admittedly, analysts who live by logic and the scientific method are not often described as “naturals” when it comes to soft skills. But practicing empathy, conflict resolution techniques, facilitation skills, and the art of knowing when and how to advocate versus when to sit tight and reflect are crucial to analysis and the resulting product. These project management skills, along with some mastery over one’s ego, can be learned (albeit sometimes through painful trial and error). Even the most logical and objective creature in popular culture history, *Star Trek*’s Mr. Spock, was a consummate listener, dialoguer, and when appropriate, advocate.

Experience has shown that five steps will produce a successful intelligence analytic team effort:

Even current intelligence items—such as intelligence reports that must be produced in the time frame of a day or less—have some form of project plan. It may not be stated formally, but any competent analyst has mentally worked through the needed steps.

1. *Define the issue.* The importance of issue definition is the subject of chapter 8. It is the critical first step in every analytic effort, an admonition that will be repeated throughout this book. Just as faithfully practicing an incorrect golf swing gives no hope of improving your stroke, the best analysis cannot save a team that is working from a flawed issue definition. Also up front, the team leader must manage the scope of the problem—choosing which constraints to be ruled by, which to bend, and which to ignore. In this way, the analyst can make conscious and responsible choices in addressing the scope of the issue.
2. *Settle on an analytic approach.* Take the time in the beginning to decide on the best methodology. Changing the analytic method or process in midstream can confuse the participants and potentially demoralize the team.
3. *Standardize terms.* When everyone is eager to get started, this seems like a trivial step in the process. But misunderstandings can develop after an analysis effort is finished because the meanings of terms were not agreed upon at the beginning. Estimates have been disregarded because an expression meant one thing to the analyst and something quite different to the customer. Standardizing terms ensures that the product flows smoothly from beginning to end. For this reason, an NIE uses the following nomenclature for precision in describing the likelihood that an event will occur:
 - Terms such as *probably*, *likely*, *very likely*, or *almost certainly* indicate a greater than even chance.
 - The terms *unlikely* and *remote* indicate a less than even chance that an event will occur; they do not imply that an event will not occur.
 - Terms such as *we cannot dismiss*, *we cannot rule out*, or *we cannot discount* reflect an unlikely, improbable, or remote event whose consequences are such that it warrants mentioning.²⁴

In addition, it is necessary for estimates to indicate the degree to which information sources are believed to be free from mistakes and errors. So NIEs use the following terms to indicate the accuracy of judgments:

- *High confidence* generally indicates that the judgments are based on high-quality information, or that the nature of the issue makes it possible to render a solid judgment. A high-confidence judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.
- *Moderate confidence* generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- *Low confidence* generally means that the information's credibility or plausibility is questionable, that the information is too fragmented or

poorly corroborated to make solid analytic inferences, or that there are significant concerns or problems with the sources.²⁵

4. *Develop a project definition or research plan.* All major intelligence analysis efforts (expected to last at least a few weeks and result in a finished product, such as a written report or a briefing) start with some sort of project definition or research plan. It has many different names in the US intelligence community, and many different formats. It is required for the following reasons:
 - The simple act of writing out a plan helps to organize thinking and planning. You can make connections and check for flaws in your logic. It is a first check on the quality of tradecraft that will go into the product.
 - The plan can be circulated among fellow analysts to get feedback. They can provide valuable insights or information (for example, by identifying sources of information that you may have overlooked).
 - The target-centric approach calls for the plan to be shared with partner organizations (such as intelligence collectors, other analysis agencies, and customers), so that they can understand what you intend to do and provide guidance and assistance.
 - When asking for assistance or information held by outside organizations, having a solid and defensible plan that you can discuss in detail can significantly improve your chance of getting cooperation.
1. *Conduct regular project review conferences.* Maintain an action item list and review it at these times. The conferences and action item lists are primarily for encouraging people to stick to the schedule and secondarily for coordination. Review conferences are not the setting to get into substantive details, which could be handled offline between two or three team members. The skillful team leader drives for making decisions quickly, even before the team is ready, knowing that decisions and partial solutions will flush out new contributions. This is equivalent to the concept of rapid prototyping in software development.

A final word about team leadership: There are likely thousands of books dedicated to the art and science of it. But if there is one key to successful team outcomes, it would be mutual trust—something that is difficult to build and easy to destroy in a large intelligence organization. The analyst as team leader must bear this in mind throughout each step and every interaction with all stakeholders.

SUMMARY

Analysis requires both critical and logical thinking.

Critical thinking involves approaching a problem with the proper investigative attitude. That is, analysts must be prepared to take an objective approach, relying on the scientific method. They should not have a value judgment about an intelligence problem when they begin an analytic effort. They should be prepared to observe and investigate the anomaly, the unexpected, or the things that simply don't fit into the existing target model. Whatever organizational structure they operate in, analysts must deal with the tradeoff of being close to the customer while maintaining objectivity.

Logical thinking about a problem may rely on a deductive, an inductive, or, on occasion, an abductive approach. The deductive approach starts with a hypothesis and then searches for evidence to support or reject the hypothesis. The inductive approach draws conclusions based on the evidence. The abductive approach starts from the inductive approach and incorporates the analyst's critical thinking and intuition based on experience with the issue. In practice, analysts make use of all three approaches, depending on the issue and the available intelligence.

A few attributes are essential in top-rated analysts. In addition to having the objective attitude required for critical and logical thinking, analysts should bring to the process a broad perspective, an appreciation for historical context, and an inquiring mind. Good instincts, usually acquired with long experience on the issue, are invaluable.

In the target-centric paradigm, analysts no longer are simply a conduit between collectors and customers. The analyst is responsible for validating the target model.

Because analysis is a collaborative process, analysts should be adept at teamwork. They should be familiar with the culture, processes, and problems of their team partners. Specifically, analysts should understand collectors and work closely with them to obtain intelligence and evaluate the collection process. They should maintain a network of fellow analysts within and outside the agency where a commonality of interests exists.

Major analysis projects start with some sort of project plan. Plans may go by many different names and appear in different formats, but they should include, at a minimum, an issue definition and a research plan. The project plan brings organization and discipline to the analysis effort, and it can be shared with peers, customers, and partner organizations that can contribute to the analysis process.

CRITICAL THINKING QUESTIONS

1. In October 2021, the director of national intelligence released a declassified National Intelligence Council assessment of the origins of COVID-19. The document is accessible at <https://www.dni.gov/files/ODNI/documents/assessments/Declassified-Assessment-on-COVID-19-Origins.pdf>. It contains two alternative hypotheses about the origins.

- a. Which alternative do you find more plausible? Why?
 - b. Did your alternative fit with your beliefs prior to reading it?
 - c. What argument would you make for the other hypothesis?
2. Choose a mainstream media item that takes a position with which you agree (your instructor may ask you to choose from a set of such articles or video presentations). Research the opposite position and present arguments to support that point of view, citing your sources. In your presentation, identify areas where the author of the article or video may have lacked objectivity. Additionally, indicate whether your original views may have pivoted as a result of completing the assignment.
3. On December 30, 2016, US Embassy staff members in Havana began hearing strange sounds in their homes. The sounds continued through August 2017. Many staff members subsequently became ill, reporting symptoms such as sharp ear pain, hearing loss, nausea, vertigo, and difficulty focusing. Similar problems were reported by Canadian government embassy staff in Havana. Some US officials accused the Cuban government of conducting sonic attacks on embassy personnel, and the United States reduced its diplomatic presence in Havana, in the process expelling some Cuban diplomats from Washington. The Cuban government, for its part, denied the allegations and Cuban researchers have presented other explanations for the illnesses. Two of many articles on the subject are “The Case of the Sick Americans in Cuba Gets Stranger” in *The Atlantic* (<https://www.theatlantic.com/technology/archive/2018/02/what-happened-to-american-diplomats-in-cuba-nobody-knows/553343/>) and “Sonic Weapons Attacks on U.S. Embassy Don’t Add Up—For Anyone” in *Scientific American* (<https://www.scientificamerican.com/article/ldquo-sonic-weapon-attacks-rdqo-on-u-s-embassy-don-rsquo-t-add-up-mdash-for-anyone/>).

Subsequently, in 2017–2018, a similar rash of illnesses developed among US diplomats and their families working in the consulate in Guangzhou, China. See “Mystery Illness Striking Diplomats in China Afflicts More Victims” in the *Washington Post* (https://www.washingtonpost.com/world/national-security/more-victims-of-mystery-illness-striking-diplomats-in-china/2018/06/06/b0bc7540-69d9-11e8-bf8c-f9ed2e672adf_story.html) for details.

- a. Using the composite list of critical thinking actions presented in this chapter, generate and test at least two hypotheses to explain the incidents. Then develop and explain your conclusions about the probable cause. Depending on instructor preference, you may be directed to confine or not to confine your research to the sources listed here.
- b. Be honest: Did you begin your investigation with a specific view of the likely answer? Were you able to set that viewpoint aside in the process of researching the conflicting claims about the cause? If yes, how did you do that? If no (or not completely), cite a few reasons for the difficulty.

NOTES

1. Robert H. Ennis, "Critical Thinking Assessment," *Theory into Practice* 32, no. 3 (Summer 1993).
2. J. Y. F. Lau, *An Introduction to Critical Thinking and Creativity: Think More, Think Better* (New York, NY: Wiley, 2011).
3. Roger Z. George and James B. Bruce, *Analyzing Intelligence* (Washington, DC: Georgetown University Press, 2008), 175–76.
4. Jeffrey R. Cooper, "Curing Analytical Pathologies," Center for the Study of Intelligence, December 2005, <http://www.fas.org/irp/cia/product/curing.pdf>.
5. Bruce Bueno de Mesquita and Alastair Smith, *The Dictator's Handbook* (New York, NY: Public Affairs, 2011).
6. John H. Hovis, "CI at Avnet: A Bottom-Line Impact," *Competitive Intelligence Review* (third quarter 2000): 11.
7. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005), 76–79.
8. Martin Petersen, "The Challenge for the Political Analyst," *Studies in Intelligence* 47, no. 1 (2003), <http://www.csi.cia/studies/vol47no1/article05/html>.
9. Walter Laqueur, *The Uses and Limits of Intelligence* (Piscataway, NJ: Transaction, 1993), 53.
10. George and Bruce, *Analyzing Intelligence*, 175–76.
11. Stéphane J. Lefebvre, "A Look at Intelligence Analysis," Poster Presentation TC99, International Studies Association Conference, Portland, OR, February 27, 2003, 25.
12. Gordon Negus, unpublished papers, 2007.
13. Hans Christian von Baeyer, *The Fermi Solution* (Portland, OR: Random House, 1993), 128.
14. Alice Calaprice, ed., *The Ultimate Quotable Einstein* (Princeton, NJ: Princeton University Press, 2011).
15. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 416, https://fas.org/irp/offdocs/wmd_report.pdf.
16. Chris Holmes, Christopher Tucker, and Ben Tuttle, "GEOINT at Platform Scale," *2018 State and Future of GEOINT Report*, 2018, http://usgif.org/system/uploads/5489/original/2018_SaFoG_PDF_Final.pdf.
17. Jonah Lehrer, "Groupthink," *The New Yorker*, January 30, 2012, 23.
18. Jack Davis, *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence* (Washington, DC: CIA, 1995), 4.
19. Ibid., 5.

20. Gerald K. Haines and Robert E. Leggett, eds., "Watching the Bear: Essays on CIA's Analysis of the Soviet Union," CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, 18, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/>.
21. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 275.
22. Quoted in George and Bruce, *Analyzing Intelligence*, 167.
23. Johnson, *Analytic Culture in the U.S. Intelligence Community*, xiv–xv.
24. See an example in the National Intelligence Estimate, "Iran: Nuclear Intentions and Capabilities," November 2007, www.dni.gov/press_releases/20071203_release.pdf.
25. Ibid.

6

THE ANALYTIC NETWORK

Chapter 5 focused on the qualities of a successful intelligence analyst and on managing analytic teams. Almost all analytic projects are team efforts; that is, they depend on the existence of a network across agencies. And those networks function within a larger intelligence community. Recall General McChrystal's words (from chapter 3): "It takes a network to defeat a network." The intelligence community itself—how it is organized and operated, and its relationship to its customers—determines how effective an analyst's network can be.

All national intelligence organizations must create a mechanism for getting information from sources to all those who need it—a requirement that is endemic in the business. The process involves moving information from a source (which is collection driven) to a specific topic (which is customer driven). The transition can be problematic. Former British intelligence officer R. V. Jones wrote, "Whereas information enters the intelligence machine by source, it has to leave it by subject; it is this changeover inside the machine that causes all the difficulty."¹

This is really a process challenge, but intelligence communities repeatedly try to deal with it structurally. The structure largely determines how information flows within the system, from source to customer. The most essential element of any of the different structures is the intelligence analyst, the subject of chapter 5. This chapter describes some of the top-level structures that have been used in the US intelligence community. It then addresses the vision, often articulated by senior leaders, of realizing the benefits from collaboration in the community network.

THE US NATIONAL INTELLIGENCE NETWORK

An up-front structural question is this: Should an analytic unit be organized along topical (functional) or regional (geographic) lines? A topical structure would have separate units responsible for political issues, economic issues, military issues, weapons intelligence, counternarcotics, counterterrorism, and so on. A regional structure would have units bundle all these topics into specific regions such as Europe, East Asia, and Africa, with subordinate units responsible for countries such as France, China, and Zimbabwe. Each structure has advantages, and each leaves gaps, includes overlaps, or both. The top managers of all-source analysis groups such as the CIA's Directorate of Analysis or the State Department's Bureau of Intelligence and Research have tried

different versions of these two structures over the years, frequently settling for a hybrid approach. An office having responsibility for East Asia, for example, might have divisions responsible for political and economic analysis for the region but choose to have a separate division focused only on China because of its importance in the region.

Even a small intelligence organization will struggle with structural issues. A law enforcement intelligence unit might, for example, have its analysts specialize in narcotics, gangs, human trafficking, white-collar crime, or money laundering (functional issues). But a single organized criminal group is sometimes involved in all five of these activities. Should a separate intelligence analyst be assigned responsibility for that criminal group? How would the analyst integrate with the other five units? No matter how the intelligence unit is organized, analysts will have to share information. Furthermore, it often is most efficient in regional law enforcement intelligence units, for example, to have a specific analyst responsible for acquiring raw intelligence from a source (for example, interviewing a local police chief) to serve all needs of the entire unit. This avoids inundating the local police chief with questions from many analysts. But this approach works only if the interviewer shares the results with *all* analysts who need the information. Returning to the earlier Jones quote, analytic responsibility for the product is divided by subject, and a single source will undoubtedly provide information that covers several subjects.

At the very top level of US intelligence, the structural issue was addressed following the 2005 publication of the WMD Commission report. It recommended that the intelligence community organize around *mission managers* who would be responsible for developing strategies against specific targets. The targets could be topical (for example, counterterrorism or counterproliferation) or regional (China, Iran).² They now are called *national intelligence managers*, or NIMs. NIMs serve as the focal point for all aspects of intelligence on their issue or region—developing collection and analysis strategies to address current and expected future needs. In setting up his NIMs during 2011, Director of National Intelligence James Clapper opted for a regional set that included Africa, East Asia, Eurasia, Europe, Iran, the Near East, South Asia, and the Western Hemisphere. Alongside those were functional managers of counterterrorism, counterproliferation, counterintelligence, cyber, economics, military issues, science and technology, and threat finance.³

Still, there appears to be no way to avoid an overlap of responsibilities. Even a casual glance at the lists of possible intelligence units makes apparent the potential for overlap and turf battles in this division of responsibilities. The counterterrorism NIM and the Iran NIM, for example, have common targets and interests and must cooperate to minimize the risk of duplication.

The result is that intelligence units, in the United States and elsewhere, often work within a management structure that is familiar in the business world—a *matrix*, where analysts have two reporting lines—one functional and one geographic. The matrix structure can also take the form of an *ad hoc team* when needed.

Ad hoc teams are pulled together for a limited time, to address specific high-priority or difficult problems. For example, in 2018, ad hoc teams were likely created in several NATO intelligence organizations to target the ongoing conflicts in Yemen and Ukraine as well as North Korea's nuclear ballistic missile threat. A similar team would have been created to deal with the 2022 Russian invasion of Ukraine.

Ad hoc teams may be organized formally, as are most NIE teams in the United States. Chapter 23 contains two examples of those. However, ad hoc teams are common. A well-known example of two ad hoc teams is both historical and controversial, known as the Team A/Team B National Intelligence Estimate.

BOX 6.1 THE TEAM A/TEAM B NATIONAL INTELLIGENCE ESTIMATE

In 1976, the President's Foreign Intelligence Advisory Board and the director of central intelligence, George H. W. Bush, responded to critics who argued that past NIEs had underestimated Soviet military power and misinterpreted Soviet strategic intentions. For the upcoming NIE on Soviet Strategic Capability and Objectives, the board created a second analysis team, known as Team B, to provide an alternative NIE.⁴ This effort was unusual in that the B team comprised sixteen experts from *outside* the intelligence community—virtually all of whom had expressed concerns that US intelligence had underestimated the Soviet strategic threat in previous NIEs.

What became known as the Team A/Team B exercise also is one of the best-known examples of both alternative and competitive analysis (discussed in chapter 10), though probably not a model of how to conduct such analysis. Some Team B members accused Team A of “mirror imaging” US strategic thinking onto the Soviets. Team B produced an alarming picture of Soviet capabilities and intentions, the main points of which were as follows:

- Soviet strategy was offensive, not defensive, intended to fight and win a nuclear war.
- The Soviets were pursuing several weapons programs—ballistic missiles; the Backfire bomber; and antisubmarine, antisatellite, and antimissile weaponry—that would erase the edge possessed by the NATO allies in a conflict.

The effort engendered considerable resentment among the intelligence community analysts who had prepared the Team A estimate, especially after the Team B conclusions were leaked to the press. Most observers subsequently concluded that the Team B conclusions were neither objectively arrived at nor accurate.⁵

Other analysis efforts besides NIEs require an ad hoc analysis team. Analysts and their managers in national, law enforcement, and competitive intelligence often must manage teams drawn from different organizations.

Most ad hoc teams today are *virtual*, pulled together online for a brief time and focused on a current issue. Virtual teams are commonly used by fusion centers (discussed next) to draw in outside expertise and in the military by joint intelligence centers, discussed later.

HOMELAND SECURITY AND LAW ENFORCEMENT

The US Department of Homeland Security is a national intelligence organization, but the network it operates within is somewhat different, as discussed in chapter 4. DHS works closely with law enforcement partners at the federal, state, local, tribal, and territorial levels, as well as with the rest of the national intelligence community. The department has a diverse set of responsibilities that include disaster response, border security, terrorism, economic crime, transportation security, and cybersecurity. As a result, its customers form an even more diverse set.

The DHS intelligence product often is perishable: It needs to get to the customers immediately. Disaster response and terrorist or cyber threats all require immediate action. A special category of current intelligence, “fast synthesis,” supports ongoing tactical operations and quick reaction for additional collection. Often called *fusion*—fast synthesis of data differs from typical analysis only in the emphasis: Time is of the essence. Fusion is aimed at using all available data sources to develop a more complete picture of a complex event. A target model already exists, and the analyst’s job is to fit in new data. Analysts work only with the incoming data plus anything they have in an immediately accessible database or in their memory, or by tapping into a virtual team.

The need for this type of information domestically has led to the creation of *fusion centers* to support US homeland security and law enforcement. They are a continuing collaborative effort by two or more organizations to share information that is of common interest, including intelligence and operational information. These centers accept incoming streams of information from the private sector and from federal, state, local, and tribal governments.⁶ They also access a range of public and private databases. They gather, correlate, and analyze intelligence and then provide information to patrol officers, detectives, managers, and other participating personnel and agencies on specific criminals, crime groups, and criminal activities. They also generate their own intelligence products, providing overviews of terrorist or other crime groups, analysis of trends, and other items of information for dissemination to participating agencies.⁷

One of the oldest fusion centers has operated in the United States for over two decades in the form of the High Intensity Drug Trafficking Area (HIDTA) Investigative Support Center (ISC). Since 1990, twenty-eight centers have been designated as such across the country. A HIDTA is a formal network that is structured to coordinate law enforcement, counterdrug, and countergang efforts across all levels of government within a given geographic area. In this respect, it functions within its area of responsibility much like the CIA’s Crime and Narcotics Center does internationally.

HIDTA ISCs deal with information from many sources, not simply intelligence sources. Most of these centers have statewide jurisdiction and are operated by law enforcement groups, typically state police or state bureaus of investigation. They focus on disruption and dismantlement of drug trafficking and money laundering.⁸

During the twenty-first century, fusion centers have proliferated in the United States to support law enforcement. Known as state and major urban area fusion centers, operated by state and local authorities, these were created after the 9/11 attacks. All are part of the National Network of Fusion Centers and facilitate the two-way intelligence and information sharing between the federal government and the center's state, local, tribal, and territorial and private-sector partners.⁹

The idea of intelligence-led policing had developed traction during the 1990s, and these fusion centers were a natural outcome of the idea. The original objective of the centers was to assess the risks to people, economic infrastructure, and communities from both natural disasters and terrorist attacks and to enable actions by first responders. Over time, the focus of many centers evolved to support state and local law enforcement by providing criminal intelligence and even to address all types of hazards. Consequently, other fusion centers with both intelligence and operational functions exist within the United States and internationally:

- The FBI has *field intelligence groups* comprising intelligence analysts, physical surveillance specialists, and language analysts, working with special agents to “function as the primary mechanism through which FBI field offices develop human intelligence; identify, evaluate, and prioritize threats and emerging trends within their areas of responsibility; and support the FBI’s investigative efforts.”¹⁰
- *Regional information sharing system (RISS) centers*, under the US Department of Justice, are focused on organized crime, gang activity, human trafficking, and identity theft.¹¹ The system comprises six regional centers, and its customers include law enforcement organizations in the United States, Canada, the United Kingdom, and New Zealand.¹²

There is no one model for how a fusion center should be constructed. Ideally, it might function like the Symantec war room described in chapter 2 (see box 2.6). In contrast to the Symantec model, though, most fusion centers must deal with more diverse sources and types of data and a wider breadth of threats.

Consequently, fusion centers continue to proliferate and take different forms. And not just in the United States. The United Kingdom, for example, created the Joint Terrorism Analysis Centre in 2003, with the role of providing threat warnings and in-depth reports on terrorism trends, networks, and capabilities.

At the local level, law enforcement organizations—at least those having an intelligence function—take a variety of approaches to structuring and operating their

units. Local law enforcement intelligence organizations typically are small and operate within a close network of police officers and citizens who interact frequently. They may have ties to national-level homeland security organizations, but their focus is more on networking with the population in their communities.

Very large law enforcement units may function more like a national-level organization. The New York Police Department (NYPD) has perhaps the largest one, the NYPD Intelligence Bureau. It has the mission of detecting and disrupting criminal and terrorist activity, following the intelligence-led policing approach. In combination with traditional policing methods, uniformed officers and civilian analysts in the Intelligence Bureau collect and analyze information from a variety of sources to advance criminal and terrorist investigations. The bureau makes use of field intelligence officers, serving in NYPD precincts, to collect intelligence in support of criminal investigations—especially on narcotics and firearms.¹³

The NYPD Intelligence Bureau also runs the controversial International Liaison Program, under which some officers are posted in law enforcement agencies in thirteen major cities around the world for liaison about transnational criminal activity and counterterrorism. Because the program overlaps with the FBI's overseas liaison responsibilities, it has received considerable criticism from US government officials.¹⁴

MILITARY

Military services rely on standard operating procedures and on formal structures for collecting, analyzing, and disseminating intelligence. But informal networks and personal relationships still are important. And, as with homeland security, fusion centers are needed in military intelligence when time is the critical element—such as in support of ongoing military operations and crisis management.

To meet this need, military commanders maintain fusion centers in their theaters of operation, though these centers usually don't use the term *fusion*, instead having names such as watch centers or joint intelligence centers. Such centers have a long history: A Joint Intelligence Center Pacific Ocean Area was established in 1943 to support US military operations against Japan. Today the centers often are set up to support multinational operations. In the fight against Daesh in Iraq, the Baghdad Combined Joint Operations Center provided intelligence support to both US and Iraqi forces.¹⁵

NONGOVERNMENTAL ENTITIES

Nongovernmental organizations and commercial companies have access to data that governments lack. They also have specialized analytic expertise that government intelligence organizations seldom can match. On topics such as international trade, manufacturing, disease incidence, and local attitudes and customs, to name a few, intelligence services often must turn to NGOs for help. China is especially adept at

using commercial entities to gather intelligence, but most advanced intelligence services have relied on commercial entities at one time or another.

Such cooperation is especially important in the case of disease outbreaks. It is well known that many countries suppress outbreak reporting, in part because of diagnostic uncertainty but also because of socioeconomic disruption, or for political reasons. The most dramatic example in recent years has been China's intransigence concerning the COVID-19 outbreak. Chinese authorities refused to provide the World Health Organization with data that could help it determine how and when the coronavirus first began to spread within China, and they continue to hinder any attempt at investigation of the disease's origin.¹⁶

In contrast, one of the first warnings of the COVID-19 outbreak came in late 2019 from two NGOs. One was the Program for Monitoring Emerging Diseases (ProMED). ProMED is a volunteer network, primarily of health professionals worldwide, who collect information from open sources (social media, health department announcements, and local media outlets). Their part-time staff analyzes the data to provide early warning of outbreaks. Prior to their COVID-19 alert, ProMED had warned of the SARS, MERS, Ebola, and Zika outbreaks. A second NGO, HealthMap, spotted the outbreak at the same time. HealthMap, comprising a team of researchers, epidemiologists, and software developers at Boston Children's Hospital, had previously identified H1N1 influenza, MERS, and Ebola prior to government sources.¹⁷

Even in the military intelligence field, commercial companies play a role. They are often used as intermediaries to buy military equipment for intelligence exploitation. And in assessing foreign advanced military technology, it is customary to turn to your own country's experts in that technology.

NGOs can be a valuable source of information, but collaborating with them can be difficult. Many international NGOs, such as Doctors Without Borders, prohibit their members from dealing with intelligence organizations. And for the intelligence services, the inability to share classified intelligence limits the extent to which NGOs can be part of the analytic network.

NETWORK COLLABORATION AND SHARING

In a 2007 DNI inventory of intelligence community assets, Tom Fingar, chairman of the National Intelligence Council (NIC), found that

the IC had more expertise than suggested by staffing patterns if it could find a way to tap what people already knew, even if that knowledge was from previous assignments, and if the IC found a way to enable analysts to collaborate at a distance. The goal was to facilitate voluntary formation of "virtual" teams with the advantages of proximity to key customers and synergistic benefits from collaboration. Realizing the potential benefits inherent in this vision requires overcoming many technical, policy, and cultural obstacles.¹⁸

In the years since that inventory was taken, new tools and new processes have developed in the intelligence community to make collaboration much easier than even a decade ago. Fingar's report notes the success of the DNI's efforts to integrate the intelligence community and to create a self-aware community of analysts. Intelligence for the president, for the National Security Council, and for interdepartmental meetings is now a product of interagency collaboration. The importance of these products, Fingar observes, drives analysts to commit the substantial amounts of time that they believe is necessary to "get it right." Much of this time, he says, is spent in "informal collaboration with colleagues within and beyond an analyst's parent agency."¹⁹

As chapter 5 indicates, an analyst's job is to initiate and manage the collaboration process. In this role, you should encourage every possible form of communication—welcoming disagreement as a sign that stakeholders are putting their cards on the table and using conferences as occasions for learning and building shared mental models. Dissent is inevitable in collaborative efforts. In fact, if all participants agree on something, it's a good idea to look closely at that issue; complete agreement can signal the possibility of groupthink. It is your responsibility as the analyst team leader to carefully manage dissent, being particularly cognizant of two potentially poor outcomes. First, avoid suppressing it. More than once in NIEs, the dissenter has turned out to be right. Second, do not allow dissent to devolve into compromise for the sake of harmony. Too often in NIEs and peer reviews, compromises have weakened overall conclusions. Remember that you are managing an *opportunity-driven* process and look for opportunities for breakthroughs, synergies, connections, and allies. One way of handling this is to make use of technologies that support communication among the stakeholders and promote the value of capturing and sharing soft information, such as ideas, questions, objections, opinions, assumptions, and constraints.

Analysts in the United States have available a number of collaborative networking tools. Intellipedia (the intelligence community's classified version of Wikipedia) allows for creation and wide sharing of target models, effectively implementing the concept of the target-centric approach.²⁰ Other informal means, mostly relying on the intelligence community's classified internet (called Intelink), allow analyst-initiated collaboration that bypasses the constraining influence of the community's hierarchical structure.

These tools and methods of collaboration are finding wide use, although some writers note time pressure as an issue. Fingar observes that some analysts and managers complain that "analysts 'must' spend too much time collaborating with colleagues or using new analytic tools"²¹—the implication being that the time spent in such activities could be better used. The availability of the tools has also caused increased focus on a long-standing conflict between sharing and protection of sources and methods, discussed next.

Sharing and collaboration are two different things, though collaboration relies on some form of sharing. Stung by criticism of their failure to share intelligence prior to

the 9/11 attack, the top leaders of the US intelligence community committed to better sharing and in many areas have made progress. But, in addition to some good reasons not to share, as mentioned in chapter 1, countervailing forces exist that make it difficult, even risky for national security. They mostly derive from the mantra of all intelligence collectors: *protect sources and methods*. Sharing, as noted in chapter 1, requires openness. And openness can result in the loss of sources and methods. In 2010, the United States had to deal with a WikiLeaks breach, when thousands of classified and sensitive government documents were posted on the internet. The incident resulted in extensive damage to US interests worldwide. Many of the leaked documents were US diplomatic cables that made politically embarrassing comments about foreign government leaders. But an even more damaging compromise occurred in 2013: A National Security Agency (NSA) contractor, Edward Snowden, began releasing to news media classified material that he had downloaded from NSA's classified network. The resulting casualties caused the pendulum to swing back in some cases, toward protection at the expense of sharing.

There also exist less noble reasons to avoid sharing. David Cohen, formerly CIA's deputy director for operations, once observed: "There's no such thing as information sharing; there's only information trading."²² Analysis managers know they must find a way to work with collection and other analysis units that hoard their most valuable information. The more important the information becomes, the more value it has for the unit that produces it. As a result, organizations tend to emphasize protecting the valuable information—perhaps even more so than protecting sources and methods.

Let's illustrate this point with an admittedly extreme example. Suppose the United States had a HUMINT source in an African country—a low-level mail clerk in the country's economic ministry. The source's material would primarily become economic intelligence, and the source's reporting would likely be classified no higher than Secret.

Now suppose one of the many letters coming into the ministry, and copied by the mail clerk as part of his espionage job, concerns a plot to assassinate the president of the United States. The letter from the plot leader is a request for a ministry employee to help provide cover for the plotters' travel arrangements. It is unlikely that the US intelligence community would release this information at the Secret level; it would probably be highly classified and receive extremely limited distribution. Yet the sources and methods remain unchanged; only the substance is different. The increased classification level has nothing to do with protecting the source. Does that seem like a far-fetched example? Overclassification in fact is not uncommon.

Information sharing is a workable concept in a small integrated intelligence organization where a high level of mutual trust exists. The large intelligence organizations common in major countries have found sharing more difficult to implement. Recent events, though, indicate that NATO countries have made substantial progress in this area.

SUMMARY

Intelligence analysts depend on both formal and informal networks in their work. Formal networks are shaped by the intelligence unit's structure and its relationship to both collectors and customers. The most common structures are by topic (for example, political, economic, counterterrorism), by region (a geographic division), or by some combination. Each arrangement has advantages, and each has the potential for gaps and overlapping responsibilities. The result often is a hybrid, or matrix, approach.

Informal analytic networks can take many forms. All analysis projects are team efforts, though not necessarily the product of formal teams. Ad hoc teams organized to deal with a specific issue probably are the most common. Teams are also created with an enduring mission and exist to support a specific set of customers. Fusion centers are used in the United States to support homeland security, law enforcement, and counternarcotics issues. The military services rely on joint intelligence centers to support deployed forces overseas.

Most intelligence issues require expertise from many sources, and the network provides that benefit. Team efforts also result in better information sharing, smoother coordination of the final product, and more buy-in from the customer. Analysts, collectors, customers, and external experts (academic and industrial) all can provide inputs to the target model and analysis process.

Sharing and collaboration are related in that collaboration relies on some form of sharing. Information sharing is most easily achievable in a small integrated intelligence organization where a high level of mutual trust exists. It is considerably more challenging to implement in a large intelligence organization. But information technology has provided a rich set of collaborative tools to aid in the process. In the United States, most of these rely on a classified version of the internet for sharing intelligence and ideas, and for creating and sharing target models.

CRITICAL THINKING QUESTIONS

1. The text mentions the dispute between the FBI and the NYPD over the NYPD's International Liaison Program. What arguments can you make that the program is a bad idea? From the NYPD perspective, what are the advantages to the program?
2. Choose a state or local fusion center to research (a number of them are described online) and examine the center's components and the external sources that it is associated with (analytic units, customers, and information sources). Develop at least three suggestions to help the fusion center function more effectively as a network; for example, improvements to sharing and collaboration, partnering

with other agencies or networks not currently cited as sources, or any other out-of-the-box suggestions.

3. Fusion centers and regional information sharing centers have been controversial in the United States. The justification for the centers is explained on DHS and Department of Justice websites. But the American Civil Liberties Union (“More about Fusion Centers,” at <https://www.aclu.org/other/more-about-fusion-centers>) and the Brookings Institution (“Fusion Centers: What’s Working and What Isn’t,” at <https://www.brookings.edu/blog/fixgov/2015/03/17/fusion-center-s-whats-working-and-what-isnt/>) criticize some of the practices. What sort of fixes (if any) to the center operations would you make in response to the criticisms?
4. Matrix structures and ad hoc teams are designed to deal with intelligence issues that cross organizational lines. But matrix configurations and ad hoc teams come with their own sets of problems. From independent research, identify and discuss three or more of those problems. How might they be mitigated?

NOTES

1. R. V. Jones, “Scientific Intelligence,” lecture to the Royal United Services Institution on February 19, 1947, *Journal of the Royal United Services Institute* 92 (1947): 357.
2. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 19, 24, https://fas.org/irp/offdocs/wmd_report.pdf.
3. Office of the Director of National Intelligence, “ODNI Mission and Vision,” *ODNI’s Weekly Intercept*, May 25, 2011.
4. Douglas H. Dearth and R. Thomas Goodden, eds., *Strategic Intelligence: Theory and Application*, 2nd ed. (Carlisle, PA: US Army War College and Defense Intelligence Agency, 1995), 305.
5. Douglas Gartoff, “Estimating Soviet Military Intentions and Capabilities,” in *Watching the Bear: Essays on CIA’s Analysis of the Soviet Union*, ed. Gerald K. Haines and Robert E. Leggett, CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, chapter V, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article05.html>.
6. John Rollins, *Fusion Centers: Issues and Options for Congress*, CRS Report RL34070, January 18, 2008, 18–19, <http://www.fas.org/sgp/crs/intel/RL34070.pdf>.
7. US Department of Justice, “Intelligence-Led Policing: The New Intelligence Architecture,” NCJ 210681 (September 2005), 9.
8. US Department of Homeland Security, “Fusion Centers and HIDTA Investigative Support Centers,” November 11, 2021, <https://www.dhs.gov/fusion-centers-and-hidta-investigative-support-centers>

9. US Department of Homeland Security, "Fusion Centers," September 19, 2019, <https://www.dhs.gov/fusion-centers>.
10. FBI Directorate of Intelligence, "Field Intelligence Groups," November 11, 2021, https://www2.fbi.gov/intelligence/di_fig.htm.
11. US Department of Homeland Security, "Fusion Centers and RISS Centers," June 17, 2016, <https://www.dhs.gov/fusion-centers-and-riss-centers>.
12. US Department of Justice, "Regional Information Sharing Systems," November 11, 2021, <https://www.riss.net>.
13. NYPD, "Intelligence," <https://www1.nyc.gov/site/nypd/bureaus/investigative/intelligence.page>.
14. Jeff Stein, "NYPD Intelligence Detectives Go Their Own Way," *Washington Post*, November 10, 2010, http://voices.washingtonpost.com/spy-talk/2010/11/nypds_for_eign_cops_play_outsid.html.
15. Jim Garamone, "Combined Joint Operations Center Keeps Eyes on ISIL," *DoD News*, April 21, 2016, <https://www.defense.gov/News/Article/Article/740246/combined-joint-operations-center-keeps-eyes-on-isil/>.
16. ODNI, "Updated Assessment on COVID-19 Origins," <https://www.dni.gov/files/ODNI/documents/assessments/Declassified-Assessment-on-COVID-19-Origins.pdf>.
17. James Timbie, "Open Source Early Warning of the COVID-19 Outbreak," Hoover Institution, May 6, 2021, <https://www.hoover.org/research/open-source-early-warning-covid-19-outbreak>.
18. Thomas Fingar, "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, ed. Baruch Fischhoff and Cherie Chauvin (Washington, DC: National Academies Press, 2011), 22.
19. Ibid., 16.
20. Ibid.
21. Ibid.
22. Christopher Dickey, "The Spymaster of New York," *Newsweek*, January 31, 2009, <http://www.newsweek.com/2009/01/30/the-spymaster-of-new-york.html>.

7

THE INTELLIGENCE PRODUCT

Thus far we have introduced the nature of twenty-first-century conflicts, the process for conducting analysis, and the participants in the analytic network. Now we turn to the types of intelligence products that support customers—and some of the shaping factors, constraints, and pitfalls to watch out for.

Intelligence products are often described in categories, though overlap always occurs. Two useful ways to think about products concern purpose and time frame, again with the caveat that they are related. Intelligence can be characterized as descriptive, anticipatory, or prescriptive.¹ These categories have been explained as follows:

- *Descriptive intelligence* describes what has happened or is happening now. The analyst is tasked with identifying threats and opportunities of a current issue a customer (a decision maker) is grappling with. It typically requires looking at political, economic, and social factors, among others. In the military, descriptive intelligence is called situational awareness.
- *Anticipatory intelligence* is sometimes referred to as predictive. We really can't predict the future, though. There are many possible futures, after all. The analyst's goal is to identify the most probable alternatives. It typically requires examining the dominant forces or factors that could shape the future. That means in-depth research, and it results in several possible future scenarios. Because anticipatory products make use of the laws of probability, they are referred to as probabilistic.
- *Prescriptive intelligence* goes one step further than either descriptive or anticipatory; it recommends a course of action for a decision maker. In US national and military intelligence, analysts historically have been restricted from giving such advice; it's never been in the job description. That may be changing as intelligence analysts and customers collaborate more closely. And in local government, law enforcement, and business, such recommendations are sometimes welcomed and even expected.²

Intelligence products are also viewed as falling into one of three broad classes: intelligence research, current intelligence, or indications and warning. (Any of the three also can be characterized as descriptive, anticipatory, or prescriptive.) Let's look at each in turn. We'll start with intelligence research because it is critical to any analytic network. If you haven't done it, you won't perform well with the other two.

INTELLIGENCE RESEARCH

In this book, we occasionally refer to intelligence research (also called in-depth research) and strategic intelligence as though they are the same. They aren't—quite. Intelligence research involves answering a customer's question, working through the issue definition phase, planning the project, conducting research, and producing a finished report. Strategic intelligence is about the production of a specific type of intelligence required for forming policy, strategy, and plans in government, the military, law enforcement, and industry. Strategic intelligence is almost always a product of intelligence research, though, so the two concepts are closely related.

Intelligence research can be on almost any topic, so long as it is one where the customer needs an answer. The key is that the question cannot be answered *immediately*. A formal investigative process is required to make the assessment. Part II details that process.

CURRENT INTELLIGENCE

Much of this book describes how to handle in-depth research, comprising major analytic efforts that require creating target models; it can take days to weeks. Current intelligence deals with issues that require immediate attention. It usually is disseminated quickly, with a minimal level of evaluation or interpretation. The product goes through a similar, but abbreviated, process because it must proceed quickly and be cut to the essential message.

Intelligence research and strategic intelligence, as noted earlier, are similar concepts. The same is true of current and tactical intelligence; they are closely related but not the same. Both usually concern immediate events. But current intelligence can include anything that may inform the customer's decision making. Tactical intelligence is more specific; it provides information the customer needs to make decisions and take action within the immediate future.

Tactical intelligence often is thought of in the context of military actions, that is, responding to the needs of field commanders so that they can plan for and, if necessary, conduct combat operations. It actually is a much broader concept. Supporting trade negotiations, providing relief to flood or famine victims, enforcing laws, and stopping narcotics or clandestine arms shipments are all examples of the application of tactical intelligence.

At the tactical level, the intelligence process is often very fast. A general understanding of the target must already exist; ideally, it was created based on past intelligence research. Incoming intelligence is simply added to refine or update the understanding, and an analysis of changes is extracted and reported quickly.

Tactical intelligence must be highly reactive, and the customer wants specific details. A military commander doesn't need to be told, for example, what an enemy tank can do; that is a known fact. What the commander needs to know is where the

tank is and where it is going. At the tactical level in diplomacy, the diplomat worries less about negotiating strategy and more about an opponent's likely reaction to the diplomat's initiatives.

INDICATIONS AND WARNING

Indications and warning intelligence (commonly referred to as I&W) involves detecting and reporting (usually) time-sensitive information on foreign developments that threaten the country's military, political, or economic interests. It therefore is closely related to (and overlaps with) two other categories of intelligence: capabilities, plans, and intentions; and crisis management and operations support.

The original purpose of I&W was to provide warning of a conventional military attack. That required an intelligence unit to develop indicators, or norms, for military force deployments and activity. If a US I&W organization had existed in December 1941, it would have had the following indicators, enumerated by Harold Ford in his book *Estimative Intelligence*, about Japanese plans and intentions that year:

- A HUMINT report in January from Peru's minister in Tokyo stating that, in the event of trouble between the United States and Japan, the Japanese intended to begin with a surprise attack on Pearl Harbor.
- Intercepts of Japanese Foreign Ministry traffic on November 19 containing the message "East wind rain," which some US intelligence officers interpreted as indicating a decision for war in the near future.
- Notification from Foreign Minister Shigenori Togo on November 22, to Ambassador Nomura Kichisaburo in Washington, D.C., that negotiations had to be settled by November 29, stating, "after that things are going automatically to happen."
- In late November, the Japanese began padding their radio traffic with garbled or redundant messages—a classic tactic to defeat COMINT operations.
- At the beginning of December, the Japanese navy changed its ship call signs, deviating from its normal pattern of changing call signs every six months.
- On December 2, the Japanese Foreign Ministry ordered its embassies and consulates in London, Manila, Batavia, Singapore, Hong Kong, and Washington, D.C., to destroy most codes, ciphers, and classified documents.
- In early December, the locations of Japan's aircraft carriers and submarines were "lost" by US naval intelligence.
- Scattered reports came in of recent Japanese naval air practice torpedo runs against ships anchored in a southern Japanese harbor.³

In hindsight, these bits of intelligence together indicate an impending Japanese attack on Pearl Harbor. In practice, they would have formed a partial picture within a mass of conflicting and contradictory evidence, as Roberta Wohlstetter points out in her book *Pearl Harbor: Warning and Decision*.⁴ At best, a cautiously worded warning could have been issued as to the likelihood and nature of an attack within days. In 1941, however, no national I&W organization existed.

Since World War II, that has changed. Most countries of any size have created organizations to warn of pending military action that would pose a threat.

For the forty years between 1950 and 1990, US national I&W continued to be dominated by concern about military conflict—specifically a Soviet strategic nuclear strike. A secondary focus was persistent world hot spots: the likelihood of Arab-Israeli, India-Pakistan, or Korean conflict. National I&W for many Middle Eastern countries was dominated by the Arab-Israeli situation. But providing I&W on military threats to national security remained the highest-priority product. (It wasn't until the 9/11 attack in 2001 that I&W focus began to include unconventional threats, which we will return to in a moment.)

Despite some missteps (such as the Yom Kippur and Falkland Islands surprises mentioned in chapter 1), US I&W has performed reasonably well in warning against conventional military attacks.

I&W units can do that because they have compiled a set of indicators of conventional attack that can be observed in advance, as the Pearl Harbor example demonstrates. Sets of indicators are pulled together through experience and accumulated knowledge. Standard indicators of impending military attack, for example, are a stockpiling of whole blood, recall of diplomats, recall of military personnel on leave and canceling leave, threats made in the press, massing of troops near the border, and movement of warheads out of storage. Charlie Allen, CIA national intelligence officer for warning, used those indicators to issue a warning on July 25, 1990. He estimated a 60 percent chance of an Iraqi attack against Kuwait, more than a week before the invasion began.⁵ And in 2022, all of those indicators appear to have been present prior to the Russian invasion of Ukraine, allowing the United States to issue an unequivocal warning.

The failure to warn of 9/11 led to the most significant reorganization of US intelligence since 1947. But even prior to 2001, I&W had begun to take on a broader mission than simply warning of armed conflict. Its purpose today could be described as warning of a surprise that would damage the country's (or organization's) interests. That could include warning of imminent hostilities, enemy actions or intentions, insurgency, and terrorist attacks, of course. Today it also includes warnings of coups or civil disorder, economic threats, pandemics, and refugee surges, even though they may not immediately and directly affect the country making the assessment. In the fall of 2008, many governments focused their I&W intelligence efforts on a worldwide economic crisis. And beginning in early 2020, international I&W efforts were addressing the threat of COVID-19 outbreaks.

Whether focused on conventional military attack or on broader imminent hostilities, I&W typically has been treated as current or tactical intelligence. But in today's context, it can be strategic and not necessarily time sensitive. It now involves identifying and forecasting emerging threats. Warnings about instability or new defense technologies or breakthroughs that could significantly alter the relative advantages of opposing military forces are examples. Such warnings usually require in-depth research. And developing indicators for them is a challenge.

Warning norms for terrorism, instability, low-intensity conflict, and technological breakthroughs are much more difficult to spot. Furthermore, a warning system should be able to address the unconventional or extraordinary event. The tendency, though, is for intelligence services to "institutionalize" warning through an established set of indicators based on past experience. Such indicators are well established for conventional military attacks. They are more difficult to identify for a type of attack or an event that has never happened before, and the danger of missing the warning for such attacks or events is consequently high. New types of indicators, especially those drawn from social media, must be created to improve the chances of making such warnings. The point is that the indicators must exist for warning to be effective.

Also, the problem of pulling a coherent set of indicators out of the mass of available information has not become much easier since 1941. Many lists of the pre-9/11 evidence of an impending terrorist attack on the United States using airplanes have been compiled since the attacks on the Pentagon and World Trade Center. Like the Pearl Harbor evidence, they can be judged fairly only when placed among all of the conflicting, contradictory, and often false raw intelligence the US intelligence community received beforehand.

Finally, I&W indicators present a tradeoff problem. Analysts do not want to miss the indicators and fail to give a warning, a problem complicated by opposing expertise in denial and deception—the subject of chapter 13. By contrast, analysts become vulnerable to the "cry wolf syndrome" if the warning threshold is set too low and false alarms result. Customers become desensitized, and in a genuine crisis the alarm is ignored.⁶ A different type of desensitization happens when a situation worsens gradually over time, or when warning indications persist for some time without the event happening. This pattern occurs frequently enough that British author Michael Herman has given it a name—"alert fatigue."⁷ The trick is to have a set of indicators that is both necessary and sufficient, so that you can successfully navigate between the unfortunate outcomes of missed events and false alarms.

This section has focused on national intelligence I&W. Many commercial organizations also have an I&W effort assigned to their competitive intelligence unit. For them, the highest I&W priority is on significant threats to the organization's survival—impending alliances among competitors or a competitor's imminent product breakthrough, for example. But I&W has a broader role in competitive intelligence. Competitors often send out deliberate signals of their intentions. The competitive intelligence analyst must be attuned to these indicators and ensure that the customer is

aware of the signals.⁸ Analysis of the meaning of deliberate signals is a special skill that all analysts should possess, because governments send out deliberate signals, too.

WHAT SHOULD AN INTELLIGENCE UNIT PRODUCE?

A basic question that any analysis unit must consider is this: Should we produce intelligence research, current intelligence, or I&W intelligence? Or all three?

Customers want the latter two types—indeed, they *demand* I&W intelligence—but they often *need* the first type. Consequently, the analyst has a responsibility to persuade the customer to consider the strategic analysis product. A common approach is to produce both current intelligence and research, preferably in the same serial product. Customers read the current intelligence, and the in-depth research in the document just may catch their interest. This is the equivalent of the “teaser” that television news programs use: putting a high-interest item last in the program and telling viewers about it up-front—so that the viewers will watch the whole program.

Analytic managers, for their part, should take care not to send mixed signals to their analysts. It’s a recurring problem in intelligence organizations, and one where managers and analysts always seem to have different perspectives. Managers typically have a solid handle on the mission and goals. They believe that they’ve shared those goals with their team members. The analysts, in contrast, frequently claim to be uncertain about mission and goals.

A common source of the mixed signals comes from the tension between current and in-depth intelligence. Managers, for example, will conduct periodic analyst meetings that stress the need for in-depth research, but their day-to-day guidance is focused on responding to current priorities.

All three types of products have their proponents in intelligence organizations and among policymakers. It is not useful to think of them in either-or terms when allocating time and resources, because *all three are needed*. Current intelligence allows analysts to be in close touch with customers and facilitates better understanding between the two. Intelligence research provides the background that allows analysts to make credible judgments in current reporting. I&W intelligence is an absolute requirement and depends on the other two types being done well.

Which area to stress depends on the customers and where they are in operations. Almost all national leaders want current intelligence that is specific to their immediate interests.⁹ But as former CIA deputy director for intelligence Bruce Clarke once noted, “Intelligence research is putting money in the bank; current intelligence is making a withdrawal.”¹⁰ The problem with abandoning in-depth research is that eventually the intelligence models become irrelevant to the problem. Without a clear picture of long-term trends, you cannot make short-term predictions. The intelligence outfit becomes bankrupt. It not only cannot provide strategic intelligence; it cannot even produce good current intelligence.

Focusing too many resources on current intelligence engenders other problems. Discussing the failures of the US intelligence community in Iraq estimates during 2002 to 2004, Richard Kerr and others note,

In periods of crisis, when demands are high and response time is short, most written intelligence production is in the form of policy-driven memos and briefs and pieces written for daily publications. The result of this narrowly focused and piecemeal intelligence flow is that it neither fosters continuity of analysis nor provides a context within which to place seemingly unrelated information. In the case of Iraq, national intelligence did not provide a comprehensive picture of how the country functioned as a whole.¹¹

Nevertheless, several incentives favor the production of current intelligence, to the detriment of in-depth research. First, it's easier to do. Second, you have a customer set that depends on the information being delivered in a timely manner. Third, you get instant gratification from seeing results, a task completed, and a grateful customer. The most important customer in the US intelligence community is the president, and the premier intelligence product is current intelligence in the form of the President's Daily Brief.

If there are two tasks—an in-depth study that is not time sensitive, and a quick-reaction task—analysts will inevitably tackle the one that can be done quickly. That is true in any profession. However, there's always another time-sensitive action waiting when the first is done. Analysts will claim that they're fully loaded—but it's a load of choice. Any intelligence unit will always have more tasks waiting than resources to deal with them. Unless there is some incentive to tackle the tough tasks, a natural tendency is to gravitate to the easier ones. Analysts must fight that tendency. A first step is to recognize the tyranny of current intelligence, how it can dominate, and then find some way to compensate.

CONSTRAINTS ON THE INTELLIGENCE PRODUCT

All intelligence products are subject to constraints—factors that shape them. Analysis has limits, boundaries, and constraining pressures. Every analyst should understand what these are:

- *Limits*, in this definition, delineate the difference between what analysis can do and what it cannot.
- *Boundaries*, by contrast, delineate the things that intelligence should do and the things that intelligence should *not* do (even if it can).
- *Constraining pressures*, both internal and external, often shape the analysis product.

Let's examine each of these three.

Limits

Limits can be summed up nicely in a phrase attributed to a senior intelligence community official: “Intelligence does not do fortune-telling.” What that means is that an intelligence community can deal with secrets, but not with mysteries.

The contrast between secrets and mysteries was described by Robert Gates when he was deputy director of intelligence at the CIA. He observed that secrets are potentially knowable; mysteries are not. The intelligence community gets blamed unfairly because it is unable to predict outcomes that are mysteries even to the principals involved. Consider the following examples:

- *The fall of the Soviet Union.* Gorbachev, the Soviet Union’s president, didn’t see it coming. US intelligence identified the political and economic troubles in the Soviet system but did not predict the collapse.
- *Putin’s rise to power in Russia.* Putin himself appears not to have expected it (noted in chapter 16) until his popularity soared after he took responsibility for launching the second Chechen war.
- *The Tunisian, Libyan, and Egyptian revolutions of 2011.* The leaders, their security forces, the militaries, and the revolutionaries all were to varying degrees surprised by the outcome.

If the leaders in-country who are best positioned to know the situation are caught by surprise, how can intelligence services be expected to apprehend what is about to happen? The best intelligence can do is to say that conditions are favorable for an event.

A good analogy is the stock market. Research firms and brokerages spend vast sums trying to forecast how the stock market will behave. But how it actually will behave tomorrow depends on the individual decisions of a large number of people, and that is a mystery—though one that can be dealt with, to some degree, by probabilities.

In contrast, secrets can be discovered, and that is the job of intelligence. To cite some painful examples of failure:

- Egypt’s plan to attack Israel in 1973 (the Yom Kippur War) was a discoverable secret. One of Israel’s agents, Ashraf Marwan, actually provided the Israelis with advance warning of the attack, but his information was not acted upon.
- The 9/11 plot was discoverable, and the intelligence community’s part in the failure to provide warning resulted in a fundamental change in the way that the community does business today.

- The secret that Iraq did not have weapons of mass destruction prior to the 2003 war was discoverable.
- Iran's capabilities to produce nuclear weapons are discoverable, but whether the Iranians will do so appears to be a mystery. (Until the weapons are actually produced, a decision can be made at any time to halt the effort.)

Former director of the National Intelligence Council Fritz Ermath has identified a third distinct category—neither mystery nor secret—something he calls an “obscurity.”¹² This refers to the questions that a customer hasn't asked yet, but would if the customer had the required knowledge. Tom Fingar put it well when he said: “Sometimes the most important ‘answers’ are the ones provided by an analyst to questions that customers should have asked, but did not.”¹³

The “obscurity” is a limit of imagination or curiosity, and one that an intelligence analysis group therefore can overcome. But it requires the application of estimative methodologies, which are discussed in part III. Because the target-centric approach engages the customer, it helps address Ermath's “obscurity” premise by providing the customer with necessary knowledge. Sometimes, dealing with obscurities requires the creation of a separate unit dedicated to exploring the frontiers. In 1970, the CIA's Office of Scientific Intelligence created a separate branch dedicated to just such a mission. Called the Future Threats Branch, it identified likely developments that eventually became realities and issues of policymaker concern.

Boundaries

As noted earlier, there are few limits on what intelligence can do. In contrast, a number of boundaries define what intelligence should *not* do. They are, in most cases, flexible and sometimes circumvented, but it is important to recognize them nonetheless—and especially to recognize when you are crossing one. The boundaries also differ from one intelligence service to another. For example, the “Five Eyes” countries (the United States, the United Kingdom, Canada, Australia, and New Zealand) share intelligence and their intelligence services resemble each other, but their analysts abide by different boundaries. Following are a few examples, starting with the most important: the policy boundary.

The Policy Divide

In the United States, a boundary exists between providing intelligence and making policy recommendations. Analysts today are expected to do the former but not the latter.

A similar divide has long existed between intelligence and operational decisions. Military commanders welcome intelligence that identifies an opposing force's threats and vulnerabilities. But no military commander would encourage an intelligence

officer to say, “General, I think that you should deploy your armored units around the Fulda Gap.” Operational decisions are a commander’s prerogative, and rightly so; commanders usually have more experience and a better understanding of the capabilities of their own forces.

So the border between intelligence and policy or operational decisions is a firm one. Or is it? There is a contrary view—that the boundary is one that many analysts want to observe, but one that at least some policymakers or commanders want them to cross. That requires that the analyst provide *prescriptive intelligence*—a sensitive issue that we’ll revisit in chapter 22.

Furthermore, talented (and more adventurous) analysts have discovered how to make a policy or operational recommendation without really making one. For example, one might write something like this:

- “China greatly fears... [insert here a course of action that the analyst believes will succeed].”
- “India’s fear is that the United States would adopt policy *X* [where policy *X* is favored by the analyst].”
- “Indonesia’s reaction to [a possible US action] would be... [describe the outcome that would be beneficial or adverse to US interests].”

This is not a two-way boundary, in any case. Analysts generally don’t cross the intelligence-policy divide except by using the stratagem described above.

In the competitive intelligence world, the policy boundary is much more variable. Some business leaders welcome policy or operational advice—prescriptive intelligence—from their intelligence units. Some don’t.

All-Source versus Single-Source Intelligence

National intelligence collection organizations perform what is called *single-source analysis*, and their product is not referred to as “finished” intelligence. In the United States, all analysts in the National Security Agency, the National Geospatial-Intelligence Agency, and the Open Source Center (OSC), for example, are responsible for single-source analysis: Their job is to process, exploit, and analyze material collected from COMINT, IMINT, and OSINT, respectively. In the United Kingdom, the Government Communications Headquarters (GCHQ) does the same for COMINT. When we talk about the “collector” in this book, we usually are referring to these single-source analysts. They also have the job of identifying targets for their organization’s collection assets, based on the gaps in knowledge about those targets. This is a well-established role for COMINT and GEOINT analysts. And some HUMINT and measurements and signatures intelligence (MASINT) organizations now have *targeting analysts* who do the same job: identify issues and gaps in knowledge that their collection assets can help with.

In contrast, some national agencies are charged with all-source analysis: the CIA, the Defense Intelligence Agency, the Department of Homeland Security, the FBI,

the State Department, and the military services all have the responsibility to provide all-source analysis. They are the customers of the single-source analytic product, and their product is often described as “finished” intelligence.

Supposedly, a boundary exists between these two analysis types. It is a bureaucratic line that is frequently ignored in practice. Single-source analysis groups have to use extrinsic sources (collateral intelligence) to do their jobs, and the result is that they often produce all-source intelligence. Because US intelligence agencies have moved toward a target-centric approach, raw intelligence is now shared widely among collection organizations. So single-source analysts usually have the material needed to cross the boundary and therefore perform all-source analysis. And all-source analysts are known to do their own open-source research and to analyze raw imagery.

Domestic versus Foreign Intelligence

Originally, the United States maintained a divide between domestic and foreign intelligence, based on the organization collecting the intelligence and the uses to which the information was to be put. The CIA, DIA, and State Department collected foreign intelligence to support foreign policy actions. The FBI collected domestic intelligence, primarily to support law enforcement activity.

The divide was blurred by the passage of the USA PATRIOT Act in 2001. It is all now considered to be national intelligence. But some sort of boundary exists: Intelligence that is intended to support law enforcement must operate under different rules, to preserve its admissibility in a court of law.

The United Kingdom continues to have a division between the two: MI5 is concerned with domestic intelligence, and MI6 is responsible for foreign intelligence. Russia operates similarly: its Foreign Intelligence Service (SVR) and GRU concentrate on foreign matters, and the Federal Security Service (FSB) conducts domestic intelligence. The division is not as distinct for China: The Ministry of State Security handles both foreign and domestic intelligence, and the Ministry of Public Security handles domestic intelligence as well. The People’s Liberation Army handles foreign military intelligence.

Operational Information versus Intelligence

In the course of combat operations, friendly units are constantly observing enemy actions visually while using imagery and electronic means. This could be considered intelligence, or simply operational information. Consider these examples:

- A Predator video that is used for on-the-spot targeting could be considered intelligence but probably is more correctly considered operational information.
- Electronic intelligence (ELINT) intercepts that are used to geolocate enemy radars are referred to as operational ELINT (or OPELINT). Is this really intelligence or simply operational information? The US military uses the

term *electronic support measures* (ESM) for OPELINT that is used to support electronic and physical attack; a common belief is that the term was coined specifically to keep OPELINT out of intelligence budgets and away from intelligence management.

- A battlefield radar detects opposing forces' aircraft and helicopter movements. This usually would be considered operational information, but it might be intelligence also because such air movements often are used to warn of future actions of an opponent.

As the examples suggest, there may be a boundary, but it's a fuzzy one. The difference becomes important primarily when the United States goes through its annual funding exercise. A system that provides operational information goes into a different budget, requiring different approvals than one designated for intelligence use.

Constraining Pressures

We want our analysts to “tell it like it is,” to produce the best possible intelligence, uncolored by pressures to produce a specific outcome. In 1991 the Senate Select Committee on Intelligence conducted hearings on the confirmation of Robert Gates as the director of central intelligence. The standard of conduct was described by analysts testifying in those hearings as

a strong tradition among older CIA officers, one [that stressed] the need for integrity of judgment and action, a generation of officers raised on the need to tell it like it is, of going where the evidence takes one and then candidly so telling senior policymakers, whether they find such judgments congenial or not—the aim being to enlighten them about the true shape of the world, not to please them or cater to their preconceptions.¹⁴

This is the gold standard of intelligence analysis. It is a difficult one to reach consistently, because of pressures to shape the result. Pressures to have analysis produce a specific answer are not unique to intelligence. They are found in all fields of research. Complete analytic objectivity is an elusive goal in the basic sciences, social sciences, and, yes, in intelligence as well.

Unfortunately, pressures to conform analysis to the customer's desires do exist. They can come from inside the analyst's organization or from the outside, and they usually are very subtle. Let's take a look at some of them.

Internal

Jack Davis has highlighted four “key perils of analysis.” Two are tied to organizational culture: coordinating judgments with other analysts and managers within their organization and confronting organizational norms.

At the Gates confirmation hearings, analysts testified about internal pressures to “politicize” intelligence. Some cited the actions from fellow analysts who were concerned that policymakers did not like (or read) the analysis that the office had been producing. Others disagreed, arguing that politicization required more than simply creating an atmosphere; there had to be deliberate efforts to produce the desired assessment.¹⁵

Although analysts may disagree on the importance of subtle influences, most observers have concluded that organizational bias or predisposition can shape analysis.

When analysis affects the budget of the parent organization, there are powerful internal incentives to produce a budget-favorable result. These incentives exist for any organization, not just for those involved in defense. Law enforcement, homeland security, and CIA analysts have all felt the resulting pressure from time to time. It is unwise to place complete faith in any intelligence analysis if the product has an impact on the parent organization’s budget.

External

Jack Davis also described the external pressures that underlie politicization of intelligence and included the concept as one of his key perils. It concerns the times when, as Davis observed, “analysts whose ethic calls for substantive judgments uncolored by an administration’s foreign and domestic political agendas seek to assist clients professionally mandated to advance those agendas.”¹⁶

We tend to think of this as an external pressure, but it manifests itself internally. Most of the attention to this politicization problem has centered on the CIA, though it is a problem elsewhere. Analysts themselves have noted that politicization can take many forms and is very difficult to prove. They are seldom, if ever, told what to write or instructed to change their conclusions. But, as one analyst noted during the Gates hearings,

judgments might be reached that are not supported by the available evidence. Evidence that does not support the desired judgment might be ignored. The review process that finished analysis goes through might be skewed to produce a desired result. Personnel assigned to produce analysis might be known to favor the desired result. Managers might, by their actions, create a “politically charged” atmosphere—a fog, as one analyst testified—that permeates the entire workplace. “You cannot hold it in your hand or nail it to the wall,” the analyst said, “[but] it is real. It does exist. And it does affect people’s behavior.”¹⁷

Former national intelligence officer Paul Pillar provided an example of how policymakers exert this pressure, without ever saying anything like, “This is the conclusion I want to see.” In his book *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform*, Pillar details the subtle and not-so-subtle pressures that White

House staffers put on the US intelligence community to provide assessments linking Saddam Hussein's regime to Al Qaeda and to WMD.¹⁸

Analysts, in responding to these pressures, go through a delicate balancing act—being relevant to the policymaker's needs without being politicized. Jack Davis noted the well-known quote of former director of central intelligence James Schlesinger that “every American is entitled to his own opinion but not his own facts.”¹⁹ What policymakers often do, if given an opportunity, is just that: select the facts they like and ignore the facts they find unpleasant.

Unfortunately, politicization is a fact of life in the intelligence trade. That's true not just in the United States, but also in any country where the intelligence chiefs are subservient organizationally to policymakers and decision makers. Since intelligence chiefs are almost always in that position, some form of politicization will exist in every country. It may be subtle and indirect, as in the United States and in most European countries. Or it may be blatant, as it is today in dictatorial regimes.

In the end, though, as Davis pointed out, policymakers and military commanders must make the decisions. They are the ones who usually will be held responsible for the outcome. Policymakers step over the line when they pressure analysts to arrive at their preferred answer, as they did prior to the 2003 invasion of Iraq. But they always have the right to disregard the answers that analysts produce.

One source of external pressures is a result of the extensive US liaison relationships with other countries, especially within the Five Eyes relationship, described earlier, and the relationship with Israel. All these relationships introduce complications that can slant both the raw intelligence reporting and the resulting all-source analysis.

The “special relationships” that US intelligence has with some foreign governments or leaders also can cause problems in the policy-diplomatic sphere. Years ago, the CIA's Clandestine Service had a close working relationship with the Druze faction in Lebanon. This arguably made it more difficult for CIA analysts to produce objective assessments of the political situation, since a great deal of the raw reporting likely reflected the Druze viewpoint. It certainly complicated the State Department's efforts to craft a policy in Lebanon. As another example, a close CIA relationship existed with Iran under the Shah during the 1970s, and the result may have been to unduly shape conclusions about the likelihood of a successful Iranian revolution.

The Defense Analysis Challenge

The intelligence analyst in a defense organization deals with two distinctive challenges: the premium placed on warning, and the pressure to produce threat assessments that align with defense policy.

Defense analysts have a special obligation to give their leaders warning of hostile military actions. The failure to warn has more severe consequences than does excessive warning. As Michael Herman observed: “Underestimation is less readily forgiven than overestimation.”²⁰ And “it is more satisfying, safer professionally, and easier to live with oneself and one's colleagues as a military hawk than as a wimp.”²¹

Herman also observed that “threat assessments have always been one of the military cards in bargaining with treasures.”²² The URDF-3 (particle beam weapon) described in chapter 20 and the Backfire bomber case described in chapter 21 are examples of such threat assessments as bargaining tools. It was an art that Soviet intelligence services once excelled at, and the current Russian intelligence services appear to be equally adept at it. The tendency is to overstate the threat to justify funding or to support defense policy positions. The resulting concern, Herman noted, is that defense intelligence organizations “have always had fairly low esteem.”²³

Defense analysts are obligated to break away from the trap of aligning assessments with funding or policy decisions by providing objective analysis even when it runs contrary to the official position of their service or of the defense establishment. It would be disingenuous, however, to say that those who have done so have always fared well. Gordon Negus, former executive director of the DIA, told of how Major General Lincoln Faurer, while director of the DIA, dealt with pressure to conform intelligence analysis to funding. When Jimmy Carter was president, the White House was considering options for dealing with the Soviet Union’s improved air defense system. Two of the options were to build the B-1 bomber or to arm the existing B-52 fleet with cruise missiles. The US Air Force wanted the B-1. But the DIA’s intelligence indicated that the Soviets felt much more threatened by the cruise missile option, which would nullify their massive air defense investment. The Air Force chief of staff told Faurer, in unequivocal terms, to revise the DIA estimate to support the Air Force position. Faurer refused and was gone from the DIA within a month.²⁴

Although the pressure to conform estimates to funding or policy is high in the military, it is not unique to defense. Any analytic group closely connected to a policy group has to deal with the problem. Recall from chapter 1, the British Foreign and Commonwealth Office forced the intelligence process to its desired conclusion that Argentina would not attack the Falklands in 1982.

Temporal Pressures

If you drew a chart of confidence in analytic judgment over time, it would show a steadily increasing level of confidence. For this reason, analysts naturally want to wait for that one more tidbit of raw intelligence to clarify their judgments. But the customer can’t wait indefinitely. Customers must act, and they will do so with or without the final intelligence report.

There are few situations, fortunately, where there is no time to think about the problem or issue before providing an answer to a customer’s question or need. They are mostly tactical: tracking a fleeing terrorist or criminal; reacting to a new internet virus that is about to go global; discovering that a friendly aircraft is about to enter a threat area and be targeted for destruction. All these, and more, require immediate response. But in most cases, there is at least some time to consider the issue, even in current intelligence, and to produce a finished intelligence product. When that time frame is insufficient, though, the outcome can be as disastrous as the Iraqi WMD miscall, discussed

earlier and detailed in chapter 23. It illustrates the bad consequences of a short deadline. A flawed methodology was applied and some sources weren't thoroughly vetted, but the very short deadline imposed by Congress left analysis managers with no real options.

Contrast that failure with the multiyear collection and analysis effort that resulted in the death of Osama bin Laden. The bin Laden case is an excellent example of the target-centric approach at work. When intelligence is focused on a specific target with a high enough priority, time works in your favor. The bin Laden trackdown was a long-term effort; time was available for analysis, for following many leads, and for subsequent guidance to IMINT and HUMINT collectors. Such was not the case for the Iraq WMD national intelligence estimate.

SUMMARY

An all-source intelligence analyst must constantly think about questions such as: Who are my customers? And what do they need? With those questions answered, the next logical question is this: Do my customers need descriptive, anticipatory, or prescriptive intelligence? And finally, what form of intelligence should I provide them? Intelligence research? Current intelligence? Indications and warning (I&W) intelligence? Or all three?

Intelligence research resembles the research conducted in a university or a research laboratory. It looks to the long term, or it addresses a specific issue in depth. It often produces strategic intelligence that is used to make policy decisions and strategic plans. Current intelligence covers fast-breaking events or new developments, and it looks much like newspaper or television news reporting. It often produces tactical intelligence to support ongoing operations. Customers usually prefer current intelligence but often need the research product—though they do not always recognize that.

I&W intelligence really isn't a choice; all intelligence units must provide warning. The objective is to avoid a surprise that would damage the organization's or country's interests. I&W usually provides time-sensitive intelligence about immediate threats. But it also identifies long-term developments that pose a strategic threat.

Dealing with customers requires that analysts have an intuitive understanding of the limits and boundaries of analysis. Limits distinguish between what analysis can and cannot do. One limit is defined by the difference between secrets, which are potentially knowable and therefore a legitimate subject for analysis, and mysteries, which are not.

Boundaries differ from limits in that they define what analysis should do and what it should not do (even if it can). Boundaries include those things that analysts can do but are bureaucratically constrained from doing. Perhaps best known is the boundary between providing intelligence and making policy or operational recommendations; analysts traditionally are expected to do the former but not the latter, though that may be changing. Three other traditional boundaries are those between single-source

and all-source analysis, between domestic and foreign intelligence, and between operational information and intelligence. Analysts will inevitably encounter all these boundaries and must find ways to deal with them while preserving their independence and professional integrity.

Analysts must handle internal and external pressures that can shape the analysis product. Internal pressures tend to protect the parent organization's equities. External pressures tend to protect the equities of other organizations—conforming analysis to policy, for example, or protecting sensitive relationships with other countries. The pressure to provide analytic products on short deadlines can result in a flawed product.

Threat assessments that support an intelligence organization's funding or policies (or those of its parent department) are usually received with skepticism—and should be. The tendency to shape analysis to support funding has been a special problem for intelligence organizations in many countries and can damage their credibility.

CRITICAL THINKING QUESTIONS

1. Choose an example of an existing intelligence issue—national, military, homeland security, or law enforcement. Discuss the pressures (internal, external, and temporal) that an analyst might have to deal with in publishing an intelligence report on the issue.
2. This chapter addresses the conflict between producing current intelligence and in-depth research and the tyranny of current intelligence. Provide at least three substantive suggestions to ensure balance between the two.
3. From current national or international events, choose one issue where the answer appears to be a secret. Choose another issue (or an element of the same issue) where the answer appears to be a mystery. Discuss how you would go about finding the answer (for the secret) or providing the likely answer (for the mystery).

NOTES

1. David E. Bell, Howard Raffia, and Amos Tversky, *Decision Making: Descriptive, Normative, and Prescriptive Interactions* (Cambridge, UK: Cambridge University Press, 1988), 9–11.
2. Robert M. Clark, *Geospatial Intelligence: Origins and Evolution* (Washington, DC: Georgetown University Press, 2000), 4.
3. Harold P. Ford, *Estimative Intelligence* (Lanham, MD: University Press of America, 1993), 3–5.
4. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962). The difference between conflicting and contradictory evidence was discussed in chapter 9.

5. Michael R. Gordon and Bernard E. Trainor, *The General's War: The Inside Story of the Conflict in the Gulf* (London, UK: Little, Brown, 1996).
6. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington, DC: CQ Press, 2002), 87.
7. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 233.
8. Liam Fahey, *Competitors* (New York, NY: Wiley, 1999), 78.
9. Most national leaders do think about long-term strategy, but they seldom want the help of strategic intelligence. In contrast, they are usually avid consumers of tactical intelligence.
10. Comment made at a CIA Directorate of Intelligence symposium, circa 1972.
11. Richard Kerr, Thomas Wolfe, Rebecca Donegan, and Aris Pappas, "Collection and Analysis on Iraq," *Studies in Intelligence* 49, no. 3 (2007), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Collection_Analysis_Iraq_5.htm.
12. Jeffrey R. Cooper, *Curing Analytic Pathologies* (Washington, DC: CIA Center for the Study of Intelligence, December 2005), 48, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/curing-analytic-pathologies-pathways-to-improved-intelligence-analysis-1/index.html>.
13. Thomas Fingar, "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, ed. Baruch Fischhoff and Cherie Chauvin (Washington, DC: National Academies Press, 2011), 10.
14. L. Britt Snider, *The Agency and the Hill: CIA's Relationship with Congress, 1946–2004* (Washington, DC: CIA Center for the Study of Intelligence, 2008), 210.
15. Ibid., 211.
16. Jack Davis, "Why Bad Things Happen to Good Analysts," in *Analyzing Intelligence*, ed. Roger Z. George and James B. Bruce (Washington, DC: Georgetown University Press, 2008), 158.
17. Snider, *The Agency and the Hill*, 211.
18. Paul R. Pillar, *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform* (New York, NY: Columbia University Press, 2011).
19. Jack Davis, "Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence," in *The Sherman Kent Center for Intelligence Analysis Occasional Papers* 2, no. 2.
20. Herman, *Intelligence Power in Peace and War*, 247.
21. Ibid.
22. Ibid., 248.
23. Ibid., 240.
24. Gordon Negus, unpublished papers (2007).

THE ANALYSIS PROCESS

Chapter 8	The Intelligence Issue	121
Chapter 9	Target Models	143
Chapter 10	The Target Framework	161
Chapter 11	Analyzing Existing Intelligence	183
Chapter 12	The Information Sources	215
Chapter 13	Denial, Deception, and Signaling	237
Chapter 14	Gaining Customer Acceptance	259

The key to becoming a credible and valued analyst is your skill in working through the analysis process, bringing to bear all available tools and methods, including the proper conceptual framework. Part I (in chapter 3) presented an overview of that process. Part II addresses the details of it.

The analysis process depends on the use of *conceptual frameworks*. It is difficult to imagine how intelligence could be created without them. A conceptual framework is an organizing construct for any type of investigation. It consists of a set of concepts that are placed in a logical form and are interrelated, based on empirical observations, critical thinking, and intuition. The framework is always connected to a research purpose. It has been defined as a visual or written product, one that “explains, either graphically or in narrative form, the main things to be studied—the key factors, concepts, or variables—and the presumed relationships among them.”¹ Put simply, it is an organizing device for research.

Consider these examples of conceptual frameworks used outside the intelligence field:

- Economists use the conceptual framework of “supply and demand” to describe the behaviors and incentive systems that tie business firms and consumers together.
- “Balance of power” is a conceptual framework used by statesmen dating back to the Peloponnesian War. It describes a state of equilibrium among countries or alliances that prevents any one entity from becoming too strong and, thus, gaining the ability to enforce its will upon the rest.

Innumerable conceptual frameworks are used in the intelligence business. The sheer volume of information to be analyzed requires all sorts of them. Chapters 8, 9, and 10 in part II address the first phases that analysts engage in from the moment a customer’s question is presented to them. Included in the discussion are four standard conceptual frameworks: the issue definition, issue decomposition, target model, and target framework. Pay special attention to the issue decomposition and the target framework: Those two are revisited throughout the analytic process from start to finish. Indeed, the target framework is the fundamental organizing concept for intelligence analysis.

The remaining chapters of part II explain how the target framework is applied in analysis. Chapter 11 addresses the interactive process of using the target framework for evaluating and incorporating existing intelligence. Chapter 12 covers how to identify and fill gaps in knowledge of the target. Chapter 13 deals with the subject of denial and deception—a topic that always must be considered because, if it is successful, the result is a misleading picture of the target. Part II concludes with Chapter 14, by examining a most difficult and most important step in analysis: gaining customer acceptance of the intelligence product.

8

THE INTELLIGENCE ISSUE

For most targets, there are typically several people who are interested in receiving intelligence. These customers will have different interests or problems to which they want answers. The US Department of Energy might be interested in Iraqi oil well activity to estimate current production; a field military commander might be interested in the same oil well activity to prevent the wellheads from being sabotaged. Therefore, all intelligence analysis efforts start with some form of issue or problem definition that fits with the customer's interest about the target.

The initial guidance that customers give analysts about an issue almost always is incomplete, and it may even be unintentionally misleading. Tom Fingar, drawing on his experience as chairman of the National Intelligence Council, cites two examples of flawed issue statements:

- In one case, customers were monitoring the progress of a program to protect Iraqi oil pipelines. They were pleased to note that no attacks had occurred on one pipeline segment—until an intelligence analyst posed the question that should have been part of the problem statement: *Was that segment operational during the period in question?* It turned out that it had been out of commission.²
- In another case, Fingar received a request from the National Security Council staff for an update on political reconciliation, economic reconstruction, and public safety in Iraq. Probing for details about this seemingly straightforward request, Fingar found that the staff director really wanted to know whether an NSC assumption—that progress on political reconciliation would facilitate progress in other areas—was supported by the evidence. (It was not.)³

The first and most important step an analyst should take is to understand the issue in detail. You must determine why the analysis is being requested and what decisions the results will support. The success of your analysis depends on an accurate issue definition. As one senior policy customer noted in commenting on intelligence failures, “Sometimes, what they [the intelligence officers] think is important is not, and what they think is not important, is.”⁴ And, as one veteran intelligence officer observed,

It is also essential that the analyst think the problem through, going beyond a mere statement of the question. Although such an analysis may appear premature, it is imperative that the problem be mulled over thoroughly for disclosure of its implications and ramifications and that these be formulated in the shape of a preliminary outline of what is desired to be known about the subject.⁵

The poorly defined issue is so common that it has a name: the *framing effect*, introduced in chapter 4. It has been described as “the tendency to accept problems as they are presented, even when a logically equivalent reformulation would lead to diverse lines of inquiry not prompted by the original formulation.”⁶ We encounter this effect in many disciplines where the problem must be defined properly before it can be solved effectively. A classic example of framing was a 1982 study in which US doctors were presented with two different formulations for the outcome of an operation. One group was informed that the operation had a 93 percent survival rate; the other was told that the operation had a 7 percent mortality rate. Rationally, there should have been no difference in the doctors’ decisions since both statistics have the same meaning. But those who were quoted the mortality rate showed a definite preference not to operate.⁷ Intelligence analysts often run afoul of the framing effect—one of the best-known examples being the National Intelligence Council’s estimate on the Iraqi WMD program (discussed in detail in chapter 23).

For these reasons, veteran analysts go about the analysis process quite differently than do novices. At the beginning of a task, novices tend to attempt to solve the perceived customer problem immediately. Experienced analysts spend more time thinking about it to avoid the framing effect. They use their knowledge of previous cases as context for creating mental models to give them a head start in addressing the problem. They also are better able to recognize when they lack the information necessary to solve a problem,⁸ in part because they spend enough time at the beginning, in the problem definition phase. In the case of most twenty-first-century intelligence problems, issue definition should be a large part of an analyst’s work. Before we get to that point, though, there are some preliminary questions that need to be answered.

PRELIMINARY QUESTIONS

In the world of scientific research, certain guidelines are generally followed before beginning a new project. Three that are especially important are (a) the research effort should have “a reasonable expectation of results, (b) you should believe that someone will care about your results and that others will be able to build upon them, and (c) you should ensure that the problem is indeed open and underexplored.”⁹ Intelligence analysts should have similar goals in their profession. So, before beginning an intelligence research effort, you should answer these five questions:

1. *Who is the customer?* Identify your customers and try to understand their needs. The traditional process of communicating needs can involve several intermediaries, and the needs inevitably become distorted as they move through communications channels—an outcome that can be avoided by direct interaction with the customer, as discussed in chapter 3. Also, even when the intelligence effort is undertaken for a single customer, the results often go to many other recipients. It helps to keep in mind these second-order customers and their needs, as well.
2. *What is the purpose?* Intelligence efforts usually have one main purpose that should be clear to all participants (including the customer) when the effort begins. It also should be clear in the result. For instance, the purpose might be to provide intelligence to support trade negotiations between the United States and the European Union. A number of more specific intelligence purposes support this main one—such as identifying likely negotiating tactics and pinpointing issues that could split the opposing negotiators or undermine their popular support. Again, customer involvement helps to make the main purpose clear.
3. *What are the real questions?* Obtain as much background knowledge as possible about the problem *behind* the questions the customer asks and understand how the problem affects policy or operational decisions. A vaguely worded request for information is usually misleading, and the result will almost never be what the requester wanted.
4. *When is the answer needed?* Determine when the product must be delivered. (Usually, the customer wants the report yesterday.) In the traditional intelligence cycle, many reports were delivered too late—long after the decisions had been made that generated the need—in part because the customer was isolated from the process. The target-centric approach dramatically cuts the time required to get actionable intelligence to the customers because they are part of the process.
5. *What form of output or product will be most effective?* Written reports (in electronic form) are standard because they endure and can be distributed readily to multiple customers. When the result goes to a single customer or is extremely sensitive, a verbal briefing may be the form of output. Briefings have the advantage of customer interaction and feedback, along with a certainty that the intended recipient gets the message. Constant customer interaction with the intelligence team during the target-centric process positions the customer to understand and accept the message.

These five parameters establish the starting point for crafting a problem statement. On large (multiweek) intelligence projects, this statement will itself be a formal product. The issue definition product helps explain the real questions and related issues.

Once it is complete, you can focus more easily on answering the questions the customer wants answered. But a well-defined problem statement requires two next steps: issue definition and decomposition.

ISSUE DEFINITION

When analysts receive the initial tasking—whether directed or self-initiated—time pressures tempt them to give issue definition short shrift. But no amount of analysis can save you from an improperly defined issue. Customers rarely ask for what they *need* to know. Usually, they ask for what they *want* to know or, more likely, what they *think* they need to know. You must understand the difference between the two question types and give customers what they need to know to make a decision.

You also need to understand the gaps in knowledge that prevent customers from doing their jobs. They usually don't know what intelligence might be able to do for them, especially regarding sensitive special compartments.¹⁰ And the questions posed by customers often have implicit assumptions that need to be made explicit. Efficient analysts clarify the question, identify assumptions, and focus the question. We'll look at each of these steps but understand that you often will be doing all three at the same time. Issue definition is an iterative process.

Clarify the Question

When a customer poses a question, there are often ramifications surrounding it that the customer has not considered. The issue might in fact be broader than the question would suggest.

To begin with, if a question is worded in such a way that what the analyst would need to know to answer it definitively is not clear, then the meaning of the terms must be clarified—ideally with the customers themselves—until exactly what they are asking for is evident. However, analysts become aware after some experience that customers themselves sometimes do not know exactly what they are asking for. Often this happens when customers know that an issue has potentially important implications but are unsure what form they might take. Again, this underlines the importance of direct face-to-face engagement. Having insight into the customers' priorities means it will be easier to make valid assumptions about their requirements on other occasions when you cannot talk to them directly.

There often are important factors affecting the issue that the customer may not have thought about. Again, there likely are questions that the customer should have asked but didn't. So it's important to think through the different *perspectives* of an issue that may be critical. Two in particular can help with clarity: considering issue categories and using the PMESII view.

Issue Categories

The issue has many names in different intelligence organizations. It is also called the question, problem, need, or topic, to name a few. (In this book, they are used interchangeably.) Most intelligence issues that customers pose about a target fall into one of five categories:

- *Plans, intentions, and strategies.* Questions include concerns about motivation and doctrine; perceptions, priorities, and policies; and current intent.
- *Organizations and leaders.* Questions are usually about organizational structure; identities and purposes or roles of key persons; their responsibilities and the influence they exert on the organization or externally.
- *Operations.* Questions revolve around activities, methods, and tactics, usually having spatial and temporal components. In military operations, they include exercises and alerts.
- *Infrastructure.* Questions are about facilities of intelligence importance, their function, and their locations. They encompass factories, maintenance facilities, utilities, transportation networks, and technology. Military infrastructure issues may concern such facilities as garrisons, launch sites, command-and-control centers, and safe houses.
- *Systems acquisition and employment.* Questions about systems acquisition address research, development, training, and evaluation (RDT&E); production; and international transfers. Employment topics include capabilities, readiness, technical parameters, and vulnerabilities.

Though the customer's initial question likely will be framed in terms of one of these categories, an analyst must consider if it should be broadened to include one or more of the others. Suppose a policy customer poses a question about an adversary's plans, intentions, and strategies—for example, about its intent to invade a friendly country. While you might be able to discern that such intent exists, the customer should also want to be aware that the adversary has neither the infrastructure nor the weapons systems needed to be successful. Twenty-first-century intelligence issues most often cross several categories.

The PMESII Perspective

Chapter 2 introduced the instruments of national power—an *actions* view that defines the diplomatic, information, military, and economic (DIME) actions that policy-makers, military or law enforcement officers, and executives can take to deal with a situation.

The customer may have those four “levers” that can be exercised, but intelligence must be concerned with the *effects* of pulling the levers. Viewed from an effects perspective, there are usually six factors to consider: political, military, economic, social, infrastructure, and information, abbreviated *PMESII*. “Social” and “infrastructure” are not considered actions that can be taken but are in the category of *effects* of actions.¹¹ Which construct you use depends on whether the focus is on actions (DIME) or effects (PMESII). Policymakers and military commanders naturally tend to think about actions. Intelligence analysts must think about both the opponent’s actions and the effects of customer actions.

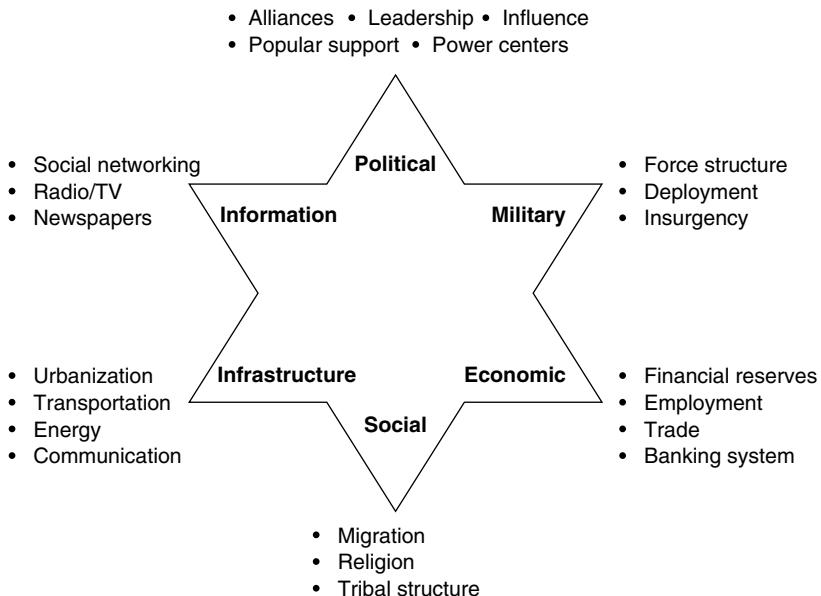
Figure 8.1 illustrates the PMESII view as a six-pointed star, with simple examples of factors that might be of intelligence interest within each point for a national government. (The examples in figure 8.1 are far from exhaustive for a government, and they would look somewhat different if the focus were on an insurgent group or a transnational criminal organization.) Following is a description of what each point of the star encompasses, with typical questions that might be asked of an analyst.

- *Political*. Describes the distribution of responsibility and power at all levels of governance—formally constituted authorities, as well as informal or covert political powers that exert influence. (Who are the tribal leaders in the village? Which political leaders have popular support? Who exercises decision-making or veto power in a government, an insurgent group, a criminal enterprise, or a commercial entity?)
- *Military*. Explores the military and/or paramilitary capabilities or other ability to exercise force of all relevant actors (enemy, friendly, and neutral) in a given region or for a given issue. (What is the force structure of the opponent? How good is their combat training? What weaponry does the insurgent group possess? What is the accuracy of the rockets that Hamas intends to use against Israel? What enforcement mechanisms are drug cartels using to protect their territories?)
- *Economic*. Encompasses individual and group behaviors related to producing, distributing, and consuming resources. (What is the unemployment rate? Which banks are supporting money laundering? What are Egypt’s financial reserves? What are the profit margins in the heroin trade?)
- *Social*. Describes the cultural, religious, and ethnic makeup within an area and the beliefs, values, customs, and behaviors of society members. (What is the ethnic composition of Nigeria? What religious factions exist there? What incentives does the gang MS-13 find most effective in attracting new recruits?)
- *Infrastructure*. Details the composition of the basic facilities, services, and installations needed for the functioning of a community, society, or business

enterprise in an area. (What are the key modes of transportation? Where are the electric power substations? Which roads are critical for food supplies?)¹²

- *Information.* Explains the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information. (How much access does the local population have to news media or the internet? What are the cyberattack and defense capabilities of the Saudi government? How effective would attack ads be in Japanese elections?)

FIGURE 8.1 ■ The PMESII View



The typical intelligence problem seldom deals with only one of these factors or systems. The Ukrainian crisis of 2014, the North Korean missile crisis of 2017–2018, the COVID-19 pandemic, the 2021 collapse of the Afghan government, and the 2022 events in Ukraine involved all the PMESII factors. The PMESII perspective is also relevant in issues that are not necessarily international. Law enforcement must deal with them all (in which case, “military” refers to the use of violence or armed force by criminal elements or police).

When a customer’s question touches on several factors, issue definition becomes tougher, and an analyst must have a systematic approach. As a conceptual framework, PMESII is one of the best. It results in the creation of several distinct models (the subject of chapter 9), as the following example illustrates.

Let's consider what a PMESII perspective might mean in an example where the issue is a country's ability to develop or acquire advanced conventional weapons. We'll use the government of Azerbaijan in this example and continue to use it later in this chapter and in chapter 10. To a novice analyst, this might seem to be only a military issue. But on closer investigation, the issue has all the PMESII elements. Following are some of the questions that could shape the analysis.

Political. What are Azerbaijan's plans to cooperate with other nations in developing or producing advanced weapons or technology?

Who are the key persons in advanced technology development? What is their influence on national decision makers, especially President Ilham Aliyev, concerning weapons or technology development, sale, and acquisition?

What drives Azerbaijan's desire to acquire advanced weapons? National ambitions and perceptions of regional balance of power, a regional arms race, a need to gain decisive military advantage over regional competitor states, or something else?

How are international or domestic disputes driving Azerbaijan's desire for missiles or advanced weapons and technology?

Military. What are Azerbaijan's plans to acquire, develop, buy, or sell advanced weapons or technology? Will their military make unexpected use of existing systems?

Where will advanced weapons be deployed? How will these weapons be integrated into existing Azeri military doctrine?

What are the performance parameters, vulnerabilities, and characteristics of the advanced weaponry they are contemplating acquiring?

Economic. What is the funding priority of advanced weapons systems? What is the Azeri military RDT&E budget, and how is it funded?

What are the economic trends (in Azeri growth, trade, stability, or unemployment) that shape decisions to sell or buy advanced weapons or technology?

What foreign aid or other support exists or is expected?

Social. How stable is the Azeri government?

How strong is popular support for the government's plans regarding advanced weaponry?

Infrastructure. Where are the advanced weapons or technologies facilities located (to include garrisons; launch sites; command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facilities; maintenance; logistics; training; decontamination; and safety)?

What are the transportation routes and critical nodes for importing or exporting advanced weapons and technology?

Identify and characterize Azeri research, development, testing, and production facilities involved in advanced weapons or technology development.

Information. What are the government's plans to conceal advanced weapons or technology production, testing, or proliferation activities? Do they have the capability to conduct cyber warfare, and if so, what are those capabilities? How do they intend to explain the new weaponry to their people?

A Check on Question Clarification

To determine whether you have sufficiently clarified the question, ask yourself this: Is it obvious what I would need to know to provide an answer (even if finding it out would be difficult)? If the answer is yes, then the focus shifts to identifying assumptions. If the answer is no, then you should spend more time on this step with the customer.

Identify Assumptions

Is the customer's question based on valid assumptions? That is the item every good analyst will examine next. If the question is closed (that is, it has a defined set of possible answers), then the customer may not have considered certain important factors and an open question is likely more appropriate. As with clarifying the question, identifying assumptions will involve dialogue in which you are looking to understand the "why" about what the customer needs to know regarding the question. This should expose any hidden assumptions and enable a more accurate reframing of the question.

This step also allows you to pinpoint assumptions that the customer does *not* want to have questioned—and that should set off alarm bells, as the following example illustrates.

BOX 8.1 THE LEBANON DEBACLE

Beginning in 1981, the Reagan administration became concerned that an ongoing conflict between Lebanese factions supported by Syria and Israel would escalate into an Arab-Israeli war. The concern was soon justified. Israel invaded Lebanon in 1982 and a Syrian-Israeli conflict ensued. The United States pushed for a cease-fire and attempted to negotiate a withdrawal of the Palestine Liberation Organization and Israeli and Syrian forces from the country. A US-led multinational force including French and Italian troops, along with the 32nd Marine Amphibious Unit, was deployed to the Beirut area as a peacekeeping force.

During 1983, the situation deteriorated steadily, and Syrian president Hafez al-Assad refused to consider withdrawal of his forces. US leaders based their policy decisions on a set of assumptions that the US intelligence community disagreed with (enumerated in chapter 10 as this case continues). Policymakers specifically did not want to hear from US intelligence that there was no reasonable way to force Assad to withdraw from Lebanon.¹³ They chose to ignore or discount intelligence indicating that US peacekeepers in the country were at risk.

This disconnect between intelligence and the customer resulted in worse than a foreign policy debacle for the United States. On October 23, 1983, terrorists blew up the US Marine barracks at Beirut International Airport with a truck bomb that killed 241 military personnel. The United States subsequently withdrew from Lebanon, its policy in tatters.

Policymakers sometimes choose not to be informed by intelligence on issues or to ignore challenges to assumptions, as they did in Lebanon. If the issue is important enough, though, the analyst must try to find a way to deal with those choices. Chapter 14 discusses how to respond when the customer is antipathetic to intelligence or is making questionable assumptions.

The Lebanon case is an unfortunate illustration of the need to validate assumptions as part of the issue definition. Always conduct a *key assumptions check* during the process. A key assumption is a hypothesis that (a) has been accepted as true and (b) will be a part of the problem definition or the final assessment product. A pitfall occurs when those assumptions are not questioned or doubted at the beginning of the analysis effort and become simply accepted as fact thereafter.

The purpose of the check is to identify key assumptions, question their validity and relevance, and state them explicitly only after they have been accepted. To be “key,” an assumption must be essential to the analytic reasoning that follows it. The method includes three basic steps: State the assumption, ask if it is valid and whether it remains valid in all circumstances, and check relevancy.

If the assumption turns out to be invalid, then the conclusions also probably are invalid. CIA’s *Tradecraft Primer* identifies several questions that should be asked about key assumptions:

- How much confidence exists that this assumption is correct?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or [a] key factor?
- Could the assumption have been true in the past but less so now?
- If the assumption proves to be wrong, would it significantly alter the analytic line? How?
- Has this process identified new factors that need further analysis?¹⁴

Questions about the future raise particular risks that customers are asking for something other than what they really are interested in. A question that asks for an unequivocal (yes or no) answer, such as

- Will Premier Jones still be in power in 2025? or
- Does Iran have a covert biological weapons program?

should (at least in presenting the answer) be treated as though the customer asked for the probabilities of those hypotheses being true. That avoids the inevitable customer

response if the yes-or-no answer is an unwelcome one: “prove to me that it’s so.” The better question to answer is this:

- How likely is it that Premier Jones will still be in power in 2025? or
- How likely is Iran to have a covert biological weapons program?

At this point, you should have a good idea what the customer is interested in knowing, and the assumptions behind the request. You should now be able to answer these three questions:

- Is the customer really interested in something else and has assumed that your question will provide the answer? (As in the question posed to Fingar about political reconciliation in Iraq.)
- Are there any hidden assumptions underlying the question? (As in the question to Fingar about oil pipeline attacks.)
- If the question asked is closed (a yes-or-no question):
 - Would the customer probably be disappointed with an answer of yes or no, or
 - Would you want to answer it “yes, but” or “no, but”?

If the answer to all of these considerations is no, then you can move to the next step—focusing the question. If the answer is yes, then reframe the question with the customer so that it covers the real object of interest or is an appropriately open question instead of a closed one.

Focus the Question

Clarifying the question causes us to consider whether the issue should be stated more broadly. Focusing does the opposite. Once you have established the customer’s parameters of interest (which may, as discussed, be wider than the original question implies) and identified key assumptions, it’s time to focus the question by finding out whether there are categories of answers within which the customer’s decision will not vary. Time is a relevant category, for example.

Always establish the time frame to which the question relates. For instance, a question such as “How would Iran respond to a naval blockade?” does not consider time. The question needs to be reframed to clearly state the time frame to be addressed: “How would Iran respond to a naval blockade during the next year?” But exercise caution: Ensure that the time scale chosen is not artificial, thus constraining a proper response.

The request also should be specific and stripped of unwanted excess. This entails focused (and perhaps repeated) interaction with the customer responsible for the original request—the policymaker, operations officer, or executive (or their staff). Ask whether the request is framed correctly. The time spent focusing the request saves much time later during collection and analysis.

Be particularly wary of a request that has come through several “nodes” in an organization. The layers of an organization, including those of an intelligence bureaucracy, will sometimes “load” a request as it passes through with additional guidance that may have no relevance to the original customer’s interests. A question that travels through several such layers can become cumbersome by the time it reaches the analyst. A question about the current Iranian balance of payments could wind up on your desk as instructions to prepare a complete assessment of the Iranian economy. In such situations, you must go back to the originator of the request and close the loop.

A key consideration in focusing the question is this: Does the customer’s decision depend on whether the answer meets a threshold or set of thresholds rather than a precise answer? If the answer is yes, reframe the question with the customer so that it covers the narrower issue of whether the threshold has been or will be met. For example, if a nonnuclear country were enriching U-235, small amounts would not be a matter of concern. But there exists a threshold quantity that, once reached, becomes a major concern for potential opponents. Common examples of questions that are posed broadly and potentially should be refocused concern quantities, probabilities, and capabilities. When faced with a question such as “What is the probability that North Korea will attack South Korea next year?” carefully consider whether the answer is that a strike is a realistic possibility or just likely. However, drilling down further with the customer might reveal that anything above “remote” is of sufficient concern that the decision (perhaps, to make detailed contingency plans) would be the same. In this case, focusing helps narrow the resulting issue definition (and subsequent analysis) to what is most important. Similar considerations might apply for questions such as these:

- How many nuclear warheads does North Korea have?
- When, if ever, will Iran have the capability to mate nuclear warheads to its missiles?

In both cases, the policy customer might actually be interested in only one aspect of the answer; for example, whether the number of North Korean warheads is above a certain figure or whether Iran will develop the capability before 2025. In these cases, the questions can be revised as follows:

- Is the number of North Korean nuclear warheads greater than ten?
- Will Iran develop the capability to mate nuclear warheads to its missiles before 2025?

Both revised questions should be more readily answerable. It is worth bearing in mind that customers are often reluctant to be pinned down in this way. There are good and bad reasons for this. It is normal for the customer's decision to depend on a multitude of factors that have nothing to do with what the intelligence assessment suggests. A decision might depend not just on the probability of an outcome but also on a host of as-yet-unknown factors relating to your country's current resources, the political mandate of the government, and so on.

Occasionally, it is appropriate for an intelligence requirement to be expressed as a closed question (or set of closed questions). In this case, it should be expressed in such a way that the possible answers are mutually exclusive. For example, the question "Is Iran pursuing a nuclear ballistic missile capability, or have they abandoned it?" implies that these are the only two options, which isn't true. There is at least one more possibility, which is that Iran is pursuing a nuclear capability, but not one involving ballistic missiles. This question should therefore be rephrased to capture precisely what it is the customer needs to know.

After clarifying the question, identifying assumptions, and focusing the question, the analyst should have a good definition of the problem at hand. It's time to move to the closely related topic of issue decomposition.

ISSUE DECOMPOSITION

Issue decomposition—defining a problem in detail—is a conceptual framework that has carried many names over the years. Nobel laureate Enrico Fermi championed the technique of taking a seemingly intractable problem and breaking it into a series of manageable sub-problems. The classic problem Fermi posed for his students was, "How many piano tuners are there in Chicago?" (This was, of course, before the internet.) The answer could be reached by using the sort of indirect approach common in the intelligence business: by estimating how many families were in the city, how many families in the city per piano, and how many pianos a tuner can tune per year.¹⁵ Glenn Kent of RAND Corporation uses the name *strategies-to-task* for a similar break-out of US Defense Department problems.¹⁶ Within the US intelligence community, it is sometimes referred to as *problem decomposition* or *decomposition and visualization*.

Whatever the name, the process is simple: Break down the highest-level abstraction of the issue into its lower-level constituent functions until you arrive at the lowest level of tasks that are to be performed or sub-issues to be dealt with. Start from the issue definition statement and provide more specific details about the problem. The process defines intelligence needs from the top level to the specific task level via *taxonomy*—a classification system in which objects are arranged into natural or related groups based on a factor common to each object. At the top level, the taxonomy reflects the policymaker's or decision maker's view. At the task level, the taxonomy represents the view of the collection and analysis team. These subtasks are called key intelligence questions

(KIQs) within the competitive intelligence community. The military typically calls them essential elements of information (EEI), which are defined as “those items of intelligence information about a foreign power, armed force, target, or physical environment that are absolutely vital for timely and accurate decision making.”¹⁷

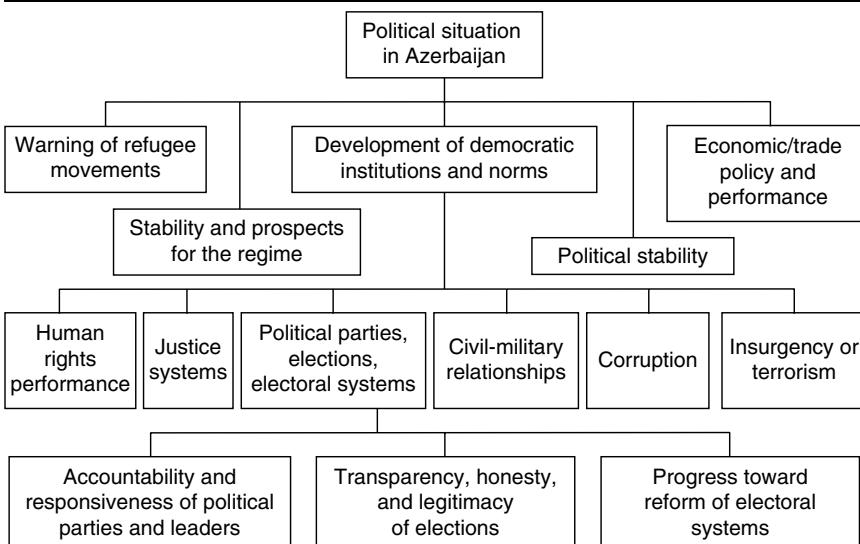
This approach has an instinctive appeal. Humans naturally tend to form hierarchical social arrangements and to think about issues hierarchically. Issue decomposition follows the classic method for problem solving. It results in a requirements hierarchy that is widely used in intelligence organizations. A few examples from different national policy problem sets will illustrate the technique.

Figure 8.2 shows part of a decomposition for the earlier example of the political situation in Azerbaijan. It illustrates the importance of taking the breakdown to the lowest appropriate level, though for simplicity, only one part of the breakdown is shown to the lowest level here.

The top-level question “What is the political situation in Azerbaijan?” is difficult to answer without first answering the more specific questions lower in the hierarchy, such as “What progress is being made toward reform of electoral systems?”

Another advantage of the hierarchical breakdown is that it can be used to evaluate how well intelligence has performed against specific issues or how future collection systems might perform. Again referring to figure 8.2, it is difficult to evaluate how well an intelligence organization is answering the question “What is the political situation in Azerbaijan?” It is much easier to evaluate the intelligence analyst’s performance in researching the transparency, honesty, and legitimacy of elections, because these are narrowly defined issues.

FIGURE 8.2 ■ Political Situation Issue Decomposition for Azerbaijan



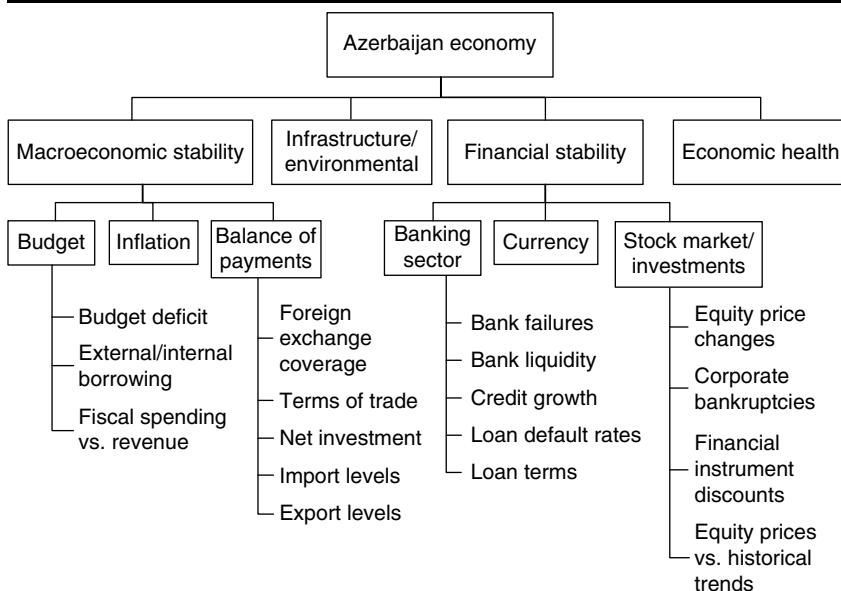
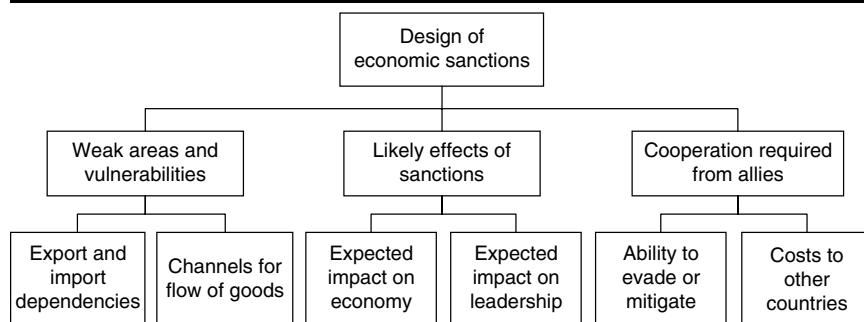
Several different issues can be associated with a given target or several different targets associated with a given issue. If the request is for an overall assessment of a country's economy, rather than its political situation, then the breakdown might look much like that shown in figure 8.3. Because of space limitations, the bottom of the figure shows only four of many question sets. At the bottom level, sub-issues such as terms of trade and corporate bankruptcies can be addressed with relative ease, compared with high-level questions such as "What is Azerbaijan's financial stability?"

To illustrate how this will subsequently be applied in analysis, let's use the issue decomposition of Azerbaijan's economy shown in figure 8.3 and focus on one part of the overall economy: the country's financial stability, specifically the stability of the banking sector. Five components contribute to an assessment of the banking sector: bank failures, bank liquidity, credit growth, loan default rates, and loan terms. The first four of these can be described by a simple type of model (discussed further in chapter 9): a temporal graphic. Using the available raw intelligence, the analyst would draw curves showing the following (these are hypothetical):

- Bank failures over the past three years (a flat curve)
- Bank liquidity over the same time period (decreasing steadily)
- Credit growth (rising sharply)
- Loan default rates (stable until last year, and then started increasing)

Combining these four factors into an overall picture, it's clear that although bank failures (the first factor) have been stable so far, the future does not look good. The other components of the model also show unfavorable trends. On the basis of your past experience as a financial analyst, you can analyze the four curves to create a predictive model, which indicates bank failures will rise dramatically in the near future and the banking sector of the Azerbaijan economy is headed for serious trouble.

Figures 8.2 and 8.3 are simplistic decomposition examples of the types of issues that analysts typically encounter about a target, and both are oriented to broad information needs (here, political and economic). But the decomposition can be much more specific and more oriented to the customer's options for attacking the problem. For example, Figure 8.4 illustrates intelligence support to the design of economic sanctions against a country, the type that might have been used against Iraq during the 1990s or against Iran in the 2000s. The policymaker may have stated the problem this way: "Tell me what I need to know to develop economic sanctions against Iran." A good analyst would create a decomposition of the issue to answer more specific questions such as "What impact would various types of sanctions have on Iran's economy?" and integrate the answers to those questions to provide an answer to the top-level question.

FIGURE 8.3 ■ Azerbaijan Economic Issue Decomposition**FIGURE 8.4 ■ Economic Sanctions Issue Decomposition**

No matter how narrow the top-level intelligence task, it usually can be broken into more specific questions. If the job is to assess the capabilities of an opponent's main battle tank, the tank's speed, range, armor, and firepower should be considered. Maintenance requirements, quality of crew training, logistics, and command and control supporting the tank should also be examined. Without these less obvious components, the tank is simply an expensive piece of metal and a threat to no one.

Complex Issue Decomposition

It's true that the most important step in the intelligence process is to understand the issue accurately and in detail. Equally true, however, is that intelligence problems

today are so complex they are described as nonlinear, or “wicked.” They are dynamic and evolving, and thus their solutions are, too. This makes them difficult to deal with—and almost impossible to address within the traditional intelligence cycle framework. A drug cartel is a wicked issue: The cartel itself is dynamic and evolving and so are the questions being posed by customers who have an interest in it. A cartel reflects real-world customer issues today, which present an analyst with the following challenges:¹⁸

- *It represents an evolving set of interlocking issues and constraints.* Only by working through the problem to get answers can one understand the ramifications. Often even when the project is complete, an analyst finds out that the customer didn’t fully appreciate the issues involved. Consider the constraints on possible solutions for defeating a cartel: Selectively introducing poison into the narcotics supply to frighten consumers and kill demand would reduce drug use, but it is not an acceptable option for the United States.
- *There are many stakeholders—people who care about or have something at stake in how the issue is resolved.* (Again, this makes the problem-solving process a fundamentally social one, in contrast to the antisocial traditional intelligence cycle.) Among the stakeholders trying to eliminate contraband narcotics are the Drug Enforcement Agency (DEA), law enforcement, US Customs and Border Patrol, the military, U.S. banks, and governments in drug-producing countries. And the stakeholders each have different perspectives. From the US point of view, the problem is to stem the flow of narcotics into the United States. From the foreign government’s point of view, the problems include corruption, intimidation, and assassinations created by the cartel.
- *The constraints on the solution, such as limited resources and political ramifications, change over time.* The target is changing constantly, and the customers (stakeholders) change their minds, fail to communicate, or otherwise change the rules of the game. The result is that the issue definition (and its decomposition) is dynamic; it cannot be created once and left unchanged. South American drug-producing countries usually don’t want *norteamericanos* to be visible in their counterdrug efforts, but that can change as the leaders gain confidence in their US partners.
- *Because there is no fixed issue definition, there is no definitive answer.* The intelligence process often ends when time runs out, and the customer must act on the most currently available information. Keeping customers in the loop means they have the most current assessment when they act.

Harvard professor David S. Landes summarized these challenges when he wrote, “The determinants of complex processes are invariably plural and interrelated.”¹⁹ Because wicked problems are an evolving set of interlocking issues and constraints, and

because the introduction of new constraints cannot be prevented, the decomposition also must be dynamic; it will change with time and circumstances. As intelligence customers learn more about the targets, their needs and interests will shift.

Ideally, a complex problem breakdown should be created as a network because of the interrelationship among the elements. Revisiting the political situation issue decomposition for Azerbaijan in figure 8.2 for a moment, we see the “Political stability” block is related to all three of the lowest blocks under “Political parties, elections, electoral systems,” though they all appear in different parts of the hierarchy. Political stability is enhanced, for example, when elections are transparent, honest, and legitimate. In figure 8.4, “Ability to evade or mitigate” sanctions is clearly related to “Expected impact on economy” or “Expected impact on leadership,” though they also are in distinct parts of the hierarchy.

Figure 8.4 illustrates that interrelationship in the earlier Iraq example. Iraq’s ability to evade or mitigate sanctions during the 1990s, and Iran’s ability to do so in the 2000s, was sufficient to minimize the impact on its leadership but insufficient to keep either economy healthy. If lines connected all the relationships that properly exist within these figures, they would show elaborate networks. The resulting dynamic network becomes quite intricate and admittedly a challenge to manage.

Although hierarchical decomposition may be less than ideal for complex problems, it works well enough if it is constantly reviewed and revised. It allows the analyst to define the issue in sufficient detail and with sufficient accuracy so that the rest of the process remains relevant. There may be redundancy in a linear hierarchy, but the human mind can usually recognize and deal with that. Fortunately, information technology developments evolve and improve to handle successive levels of complexity.

Structured Analytic Techniques for Issue Decomposition

We introduced structured analytic techniques in chapter 1. The key assumptions check is a SAT. And issue decomposition itself is a SAT. Another technique has been around for a long time and is valuable in decomposition: *brainstorming*.

Brainstorming is commonly used in problem solving to stimulate fresh thinking. In intelligence, it is most useful in the issue decomposition stage at the start of an analysis project to help generate a range of hypotheses.²⁰ A variant, called *starbursting*, is derived from the idea of a six-pointed star, each point labeled with one of the words *who, what, when, where, why, and how*. The technique is to brainstorm by asking questions about the issue that start with one of these six words.²¹

One caution about brainstorming, though: Texts on the subject usually warn not to allow criticism during the exercise. A flawed premise, which has been popular for over sixty years, is that criticism inhibits original thinking while brainstorming. Studies have shown that the opposite is true. More original ideas and fresh approaches come from team efforts when criticism is encouraged rather than suppressed.²² Whether criticism is allowed or not, the key is to create a climate up front in which participants

understand they are on the same team and that all ideas—including debate, no matter how seemingly far out—contribute to a better final product.

Brainstorming is supposed to be a group activity. But there should be no lower limit to the number of people in a brainstorming session. If it's difficult to pull together a group, it still can be an effective tactic with two people. Many a successful enterprise has begun when two people with a cocktail napkin start drawing models while they exchange ideas. And starbursting—asking the six questions—can be done by one person, if necessary.

The goal is to stimulate new thinking. Getting that result is more important than following a defined set of rules.

SUMMARY

Before beginning intelligence analysis, an analyst must fully understand the customer's issue. Ideally, this includes close interaction with the customer. You need to determine the purpose, the real questions (which may not be well stated in the initial customer request), when an answer is needed, and what type of analytic product to provide.

You also need to clarify the issue until it is apparent exactly what the customer needs to know. It helps to look at the issue from different perspectives. Issues, for example, typically fall into the categories of an opponent's plans, intentions, and strategies; organizations and leaders; operations; infrastructure; or systems acquisition and employment. You may also need to consider the effects of customer actions on an opponent. These effects fall into one or more of six factors: political, military, economic, social, infrastructure, and information, abbreviated *PMESII*:

- *Political*. The distribution of power and control at all levels of governance.
- *Military*. The ability of all relevant actors (enemy, friendly, and neutral) to exercise force.
- *Economic*. Behavior relating to producing, distributing, and consuming resources.
- *Social*. The cultural, religious, and ethnic composition of a region and the beliefs, values, customs, and behaviors of people.
- *Infrastructure*. The basic facilities, services, and installations needed for the functioning of a community or society.
- *Information*. The nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Next, identify the assumptions on which a customer's questions are based. Conduct a key assumptions check to identify and validate those assumptions essential to the

analytic reasoning and implicit in the questions. These are assumptions that, if not valid, will undermine the conclusions of the analytic effort. Explicitly state them, ask why they are relevant and valid, and determine whether they remain valid in all circumstances.

Focus or narrow the issue. A customer's initial question often is stated too broadly or contains elements that are not important to the customer. Questions about quantities, probabilities, capabilities, or time often are too broad; the customer may be interested only in a certain range of probabilities or increment of time, for example.

Once defined, the issue is broken down in a decomposition process to identify gaps in knowledge and collection efforts. Decomposition takes the form of a linear, hierarchical breakdown into sub-issues that can have several levels.

All significant intelligence issues are complex, characterized by a dynamic set of interlocking issues and constraints with many stakeholders and no definitive solution. Although the linear issue decomposition process is not an optimal way to approach such problems, it can work if it too is dynamic, meaning that it is reviewed and updated frequently during the analysis process.

Structured analytic techniques can be helpful throughout the analytic process. Two simple ones are the key assumptions check in issue definition and, for decomposition, brainstorming. Brainstorming stimulates fresh thinking about the issue. Its variant, starbursting, has participants ask questions that start with *who*, *what*, *when*, *where*, *why*, and *how*.

CRITICAL THINKING QUESTIONS

1. Choose one of the sub-issues at the bottom of figure 8.2 (accountability and responsiveness of political parties and leaders; transparency, honesty, and legitimacy of elections; or progress toward reform of electoral systems) and choose a country to apply the issue to.
 - a. Identify at least three assumptions that could be made for that country and issue.
 - b. Discuss at least three ways in which the issue might be clarified—that is, broadened to include PMESII factors—for that country.
 - c. Describe at least three ways that the issue might be focused—that is, reframed to be stated more narrowly.
2. Choose one of the five additional third-level sub-issues in figure 8.2 (human rights performance; justice systems; civil-military relationships; corruption; or insurgency or terrorism) and break it down into sub-issues for the country you selected, following the example shown for political parties, elections, and electoral systems.

3. Choose a country where information is available to answer one of the four bottom-level sub-issues shown in figure 8.3 (for example, budget deficit, external/internal borrowing, fiscal spending vs. revenue). Assess those sub-issues for that country. What conclusions can you draw about the higher level sub-issue (budget, in this example)?

NOTES

1. M. B. Miles and A. M. Huberman, *Qualitative Data Analysis*, 2nd ed. (Thousand Oaks, CA: Sage, 1994), 18.
2. Thomas Fingar, "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, ed. Baruch Fischhoff and Cherie Chauvin (Washington, DC: National Academies Press, 2011), 10.
3. Ibid.
4. Stew Magnuson, "Satellite Data Distribution Lagged, Improved in Afghanistan," *Space News*, September 2, 2002, 6.
5. Bernard Drell, "Intelligence Research—Some Suggested Approaches," CIA, September 22, 1993, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol1no4/html/v01i4a08p_0001.htm.
6. Matthew Herbert, "The Intelligence Analyst as Epistemologist," *International Journal of Intelligence and CounterIntelligence* 19, no. 4 (December 2006): 666–84.
7. Barbara J. McNeill, Stephen G. Paulker, and Amos Tversky, "On the Framing of Medical Decisions," in *Decision Making: Descriptive, Normative, and Prescriptive Interactions*, ed. David E. Bell, Howard Raiffa, and Amos Tversky (Cambridge, UK: Cambridge University Press, 1988), 562–68.
8. Rob Johnson, *Analytic Culture in the US Intelligence Community* (Washington, DC: Center for the Study of Intelligence, CIA, 2005), 64.
9. Robert W. Lucky, "In Research, the Problem Is the Problem," *IEEE Spectrum* (July 2011): 30.
10. For intelligence that requires extra protection from loss, compromise, or inadvertent disclosure, intelligence communities make use of compartmentation, where access to the material is limited to persons who are briefed on the special level of protection that it requires.
11. R. Hillson, "The DIME/PMESII Model Suite Requirements Project," *NRL Review* (2009): 235–39, https://www.nrl.navy.mil/content_images/09_Simulation_Hillson.pdf.
12. Expansion of a list contained in the US Army Training and Doctrine Command, "Operational Environments to 2028: The Strategic Environment for Unified Land Operations," August 2012, http://www.arcic.army.mil/app_Documents/TRADOC_Paper_Operational-Environments-to-2028-Strategic-Environment-for-Unified-Land-Operations_AUG2012.pdf.

13. David Kennedy and Leslie Brunetta, "Lebanon and the Intelligence Community," Case Study C15-88-859.0 (Cambridge, MA: Kennedy School of Government, Harvard University, 1988), 15.
14. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009), 7.
15. Hans Christian von Baeyer, *The Fermi Solution* (Portland, OR: Random House, 1993).
16. Glenn Kent and William Simon, *New Challenges for Defense Planning: Rethinking How Much Is Enough* (Santa Monica, CA: RAND, 1994).
17. See <https://www.britannica.com/topic/essential-elements-of-information>
18. E. Jeffrey Conklin, "Wicked Problems and Social Complexity," CogNexus Institute, 2010, www.cognexusorg/wpf/wickedproblems.pdf.
19. David S. Landes, *The Wealth and Poverty of Nations* (New York, NY: Norton, 1998), 577.
20. CIA, *A Tradecraft Primer*, 27.
21. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2011), 102.
22. Jonah Lehrer, "Groupthink," *New Yorker*, January 30, 2012, 22–27.

9

TARGET MODELS

Analysts who are armed with a well-defined intelligence issue and decomposition of it have a fighting chance. To address the issue, though, they need what Samuel Huntington referred to in his 1994 book *The Clash of Civilizations and the Remaking of World Order*. According to Huntington, “if we are to think seriously about the world, and act effectively in it, some sort of simplified map of reality, some theory, concept, model, paradigm, is necessary.”¹ He created such a map defining what he saw as the major world cultures that would be in conflict with each other during the coming century. While his theory has received criticism, most would agree with his statement that a guiding concept is needed.

Huntington’s “simplified map” is another name for a conceptual framework, introduced in Part II’s overview. Recall that creating one is the first step in most if not all types of research. Chapter 8 introduced the beginning conceptual frameworks for producing intelligence: the issue definition and decomposition. Chapter 10 concerns the conceptual framework for representing intelligence targets, which is almost always a model or a set of models. Before getting there, though, it’s worth going into some detail on just what constitutes a model—also a conceptual framework and the subject of this chapter.

MODELING THE INTELLIGENCE TARGET

Models are used so extensively in intelligence that analysts seldom give them much thought, even as they use them. Developing an assessment naturally leads to the creation of a model or set of models of the target. Simply stated, a model is a replica or representation of an idea, an object, or an actual system. Consider the following examples:

- Imagery analysts can instantly recognize a nuclear fuel reprocessing facility because they have a mental model of typical facility details, such as the use of heavy reinforced concrete to shield against intense gamma radiation.
- COMINT analysts recognize clandestine or covert radio communications because they fit a specific model: The signals are designed to avoid interception, such as communicating with very short (burst) transmissions or jumping rapidly from one radio frequency to another.
- Economic analysts recognize a deteriorating economy because they have a checklist (a simple form of model) of indicators, such as budget deficit, balance of payments, and inflation. The economic issue decomposition shown in chapter 8 (figure 8.3) illustrates such a checklist.

In a 2011 book titled *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform*, Paul Pillar described Huntington's simplified map of reality as the "guiding images" that policymakers rely on in making decisions.² In the previous chapter, we covered some guiding images that analysts use for issue definition and issue decomposition. One example is the PMESII concept that we'll soon return to in this chapter. They all are alternative forms of a map, theory, concept, or paradigm that in this book are merged into a single entity called a *model*.

As CIA's *Tradecraft Primer* puts it: "All individuals assimilate and evaluate information through the medium of 'mental models.'"³

Modeling is usually thought of as being quantitative and using computers. However, all models begin in the human mind. Modeling does not always require a computer, and many useful models exist only on paper. Models are used widely in fields such as operations research and systems analysis. With modeling, you can analyze, design, and operate complex systems. You can use simulation models to evaluate real-world processes that are too complex to analyze with spreadsheets or flowcharts (which are themselves models, of course); simulation models can test hypotheses at a fraction of the cost of undertaking the actual activities. And models are an efficient communication tool for showing how the target functions and for stimulating creative thinking about how to deal with an opponent.

All intelligence involves creating one or more models of the target and extracting knowledge from them. (So does all problem solving.) Without a device to capture the full range of thinking and creativity that occurs in the target-centric approach to intelligence, an analyst would have to keep in mind far too many details. Furthermore, in the target-centric approach, the intelligence customers are part of the collaborative process. Presented with a model as an organizing construct for thinking about the target, they can contribute pieces to the model from their own knowledge—pieces that an analyst might be unaware of. The primary suppliers of information (the collectors) can do likewise.

Because the concept is fundamental to everything in the analysis process that follows, a precise definition is important: A model, as used in intelligence, is an organizing constraint. It is a combination of facts, hypotheses, and assumptions about a target, created in a form that is useful for analyzing the target and for customer decision making (producing actionable intelligence). Let's distinguish critical terminology here:

- *Fact*. Something that is indisputably the case.
- *Hypothesis*. A proposition that is set forth to explain developments or observed phenomena. It can be posed as a conjecture to guide research (a *working hypothesis*) or accepted as a highly probable conclusion from established facts.
- *Assumption*. Something that is accepted as true, asserted without proof.

These are the elements that go into a target model. And it is essential to distinguish between them when you present the model. Customers should never wonder whether they are being presented with facts, hypotheses, or assumptions.

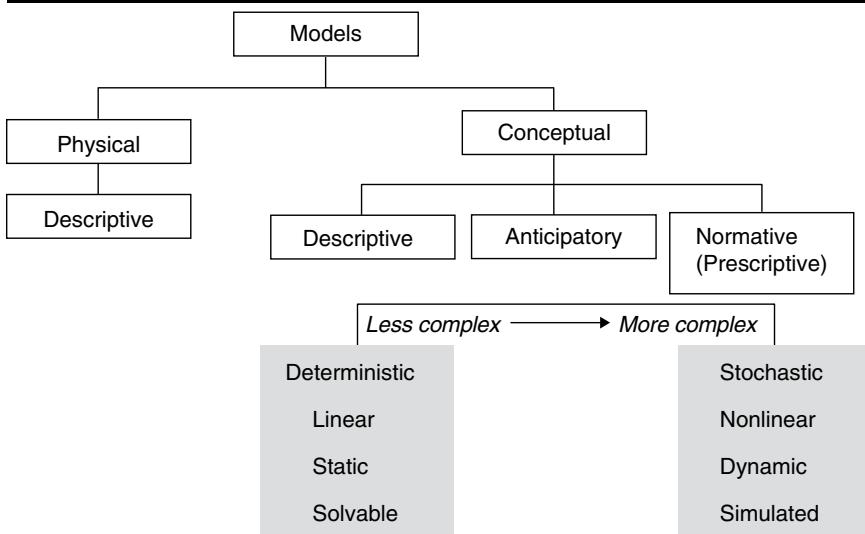
Models often describe how a system behaves. Instead of interacting with the real system, an analyst can create a model that corresponds in certain ways to the actual one. For example, results of a political poll are a model of how a population feels about a topic. Similarly, today's weather map is a model of how the weather is expected to behave.

Figure 9.1 shows a hierarchy of models and forms the basis for the discussion that follows. As the figure indicates, models can be classified as physical or conceptual (abstract).

A *physical model* is a tangible representation of something. A map, a globe, a calendar, and a clock are all physical models. The first two represent the Earth or parts of it, and the latter two represent time. Physical models are always descriptive.

Conceptual models—inventions of the mind—are essential to the analytic process. They allow the analyst to describe things or situations in abstract terms both for estimating current situations and for anticipating future ones. A conceptual model is not a tangible item, although it may be represented in tangible form. Mathematical models are conceptual; they can be created entirely in the mind. But they can be represented in tangible form by writing the equations on a sheet of paper. A conceptual model may be descriptive, describing what it represents in the present; anticipatory, identifying an expected future; or normative, prescribing what something should be. A normative model may contain descriptive segments, but its purpose is to show a best, or preferable, course of action. A decision-support model—that is, a model used to choose among competing alternatives—is normative. Normative models are used primarily for prescriptive intelligence, the subject of chapter 22.

FIGURE 9.1 ■ The Model Hierarchy



In intelligence analysis, as figure 9.1 implies, the models most commonly used are conceptual. Some general traits follow:

- *Conceptual models can be deterministic or stochastic.* In a deterministic model, the features and relationships are known and specified explicitly. A model that has uncertainty incorporated into it is a stochastic model (meaning that probabilities are involved), even though components of it may have deterministic properties.⁴ Consider the details surrounding the hunt for Osama bin Laden, described in chapter 3. A model of the compound in which bin Laden was located, and the security features it had, would have been deterministic—the details were known and specified exactly. A model of the people expected to be in the compound and their locations at the time of the attack would have been stochastic. The location of bin Laden and his guards could not be known in advance; it could only be estimated as a probability.
- *Conceptual models can be linear or nonlinear.* Linear models use only linear equations (for example, $y = Ax + B$) to describe relationships. It is not necessary that the situation itself be linear, only that it be capable of description by linear equations. The number of automobiles produced on an assembly line, for example, is a linear function of time. In contrast, nonlinear models use any type of mathematical function. Because they are more difficult to work with and are not always capable of being analyzed, the usual practice is to make some compromises so that a linear model can be used. It is important to be able to justify doing so, because most real-world intelligence targets are nonlinear. A combat simulation model is nonlinear: Interactions among the elements change in ways that cannot be described by linear equations. Attrition rates in combat, for example, vary with time and the status of remaining military forces. A model of an economy is inherently nonlinear, but the econometric models used to describe an economy are simplified to a set of linear equations to facilitate getting to an acceptable result.
- *Conceptual models can be static or dynamic.* A static model assumes that a specific time period is being analyzed and the state of nature is fixed for that time period. Static models ignore time-based variances. For example, you cannot use them to determine the impact of an event's timing in relation to other events. Returning to the example of a combat simulation, a snapshot of the combat that shows where opposing forces are located and their directions of movement at that instant is static. Static models do not take into account the synergy of the components of a system, where the actions of separate elements can have a different effect on the system than the sum of their individual effects would indicate. Spreadsheets and most relationship models are static.

A dynamic model, by contrast, considers several time periods and does not ignore the impact of an action in time period 1 on time period 2. A combat simulation model is dynamic; the loss of a combat unit in time period 1 affects all succeeding time periods. Dynamic modeling is a software representation of the time-based behavior of a system. Whereas a static model involves a single computation of an equation, a dynamic model is iterative; it constantly recomputes its equations as time changes. It can predict the outcomes of possible courses of action and can account for the effects of variances or randomness. One cannot control the occurrence of random events. One can, however, use dynamic modeling to predict the likelihood and the consequences of their occurring. Process models usually are dynamic because they envision flows of material, the passage of time, and feedback.

- *Conceptual models can be solvable or simulated.* A solvable model is one in which there is an analytic way of finding the answer. The performance of a radar, a missile, or a warhead can be determined by solving a set of equations. But other problems require such a complicated set of equations to describe them that there is no way to solve them. Worse still, complex problems typically cannot be described in a manageable set of equations. In those cases—such as the performance of an economy or a person—the analyst turns to simulation.

Simulation involves designing a computer model of a system and performing experiments on it. The purpose of these “what if” experiments is to determine how the real system is likely to perform and to predict the effect of changes to the system as time progresses. For example, you can use simulation modeling to answer questions such as “What is the expected balance of trade worldwide next year?” “What are the likely areas of deployment for mobile surface-to-air missiles in Iran?” “What is the expected yield of the nuclear warheads on North Korea’s newest long-range ballistic missile?” and “What is the likely cost to rebuild Mariupol, Ukraine?”

GENERAL TARGET MODELS

The preceding section introduced the concept of target models and why they are fundamental to analysis. Here, we review some general types of models widely used in analysis. (A number of specialized and more advanced target models are frequently used during in-depth research and anticipatory or prescriptive analysis. Part III details those: systems, relationship, geospatial, and simulation models.)

Models may begin in the mind, but they cannot remain there if they are to be shared. They must be expressed in tangible form, and there are several ways to do that. Almost any model can be described using written text. The CIA’s *World Fact Book* is an example of a set of textual models—actually a series of models (political, military,

economic, social, infrastructure, and information)—of a country. But, as noted previously, the models that have the most impact for analysts, collectors, and customers in facilitating understanding go beyond text. Visualization involves transforming raw or finished intelligence into graphic, pictorial, or multimedia forms so that our brains can process and understand large amounts of data more readily than is possible from simply reading text. Visualization allows us to deal with massive quantities of data and identify meaningful patterns and structures that otherwise would be incomprehensible.⁵

Comparative Models

Comparative techniques are a simple but useful form of modeling that typically does not require a simulation. They are used in government, mostly for weapons systems and technology analyses. Both governments and businesses use comparative models to evaluate a competitor's operational practices, products, systems, and technologies. The process is referred to as *benchmarking*. A powerful tool for analyzing a competitor's developments is to compare them with your own organization's developments. Your systems or technologies provide the benchmark for comparison. These simple models typically take the form of lists or matrices.

Lists. The most basic example of a model, Benjamin Franklin favored a “parallel list” for problem solving. He would list side by side the arguments pro and con on a topic, crossing off arguments on each side that held equal weight, to arrive at a decision. The list continues to be used by analysts today (digitally, of course) for much the same purpose—comparing alternatives. It works well on a wide range of topics and remains effective for conveying information to the customer. The parallel list also is often used in intelligence for comparative analysis—for example, comparing the performance of a Russian naval vessel with its US counterpart or contrasting characteristics of two cultures.

Matrices. A textual variant of the spreadsheet (discussed later) is the matrix, a valuable analytic tool for certain types of synthesis. It appears in various disciplines and under different names such as interaction, parametric, or traceability matrices.⁶ Table 9.1 is an intelligence matrix example. In 2005, four proposals were under consideration to be part of a South Asian gas pipeline project.⁷ The target matrix compares in simple form the costs and risks of each proposal. It's a concise and effective way to present the analysis results. Table 9.1 permits a view of the four proposals that facilitates comparison. (The actual pipeline wound up being none of the four, and the estimated cost has risen to approximately \$10 billion; the case is discussed in chapter 20.)

A matrix can be qualitative or quantitative; table 9.1 illustrates both features. A quantitative matrix naturally fits into many of the commercially available decision-support software packages. It is typically used to ensure that all possible alternatives are considered.

TABLE 9.1 ■ Target Matrix—Gas Pipeline Proposals

Pipeline Proposals	Cost	Supporters	Risks
From South Pars field, Iran, to Karachi	\$3 billion	Iran, Pakistan	Technical
From Iran to northern India	\$4–5 billion	Iran, India	Political, security, cost
From Turkmenistan's Dauletabad field to Pakistan	\$3.2 billion	Turkmenistan, Pakistan	Security
Underwater pipeline from Qatar to Pakistan	\$3 billion	Qatar, Pakistan	Political, technical

In economic intelligence and scientific and technical intelligence, it is often important to assess the impact of an industrial firm's efforts to acquire other companies. One model for assessing the likely outcome of a merger or acquisition uses the five criteria that Cisco Systems uses to evaluate possible acquisitions. The criteria are listed in the first column of table 9.2.⁸ In this matrix, the three candidates are ranked on how well they meet each criterion; the darker the shading, the higher the ranking. The model has potential applications outside the commercial world. In 1958, it would have been a useful tool, for example, to assess the prospects for success of the “merger” that year between Syria and Egypt that created the United Arab Republic. The proposed merger would not have fared well against any of the criteria in table 9.2 (even the one on similar cultures) and, in fact, the merger subsequently failed.

TABLE 9.2 ■ Matrix for Merger and Acquisition Analysis

Merger and Acquisition Criteria	Company A	Company B	Company C
Shared vision of where the industry is heading and complementary roles each company wants to play in it			
Similar cultures and chemistry			
A winning proposition for acquired employees, at least over the short term			
A winning proposition for shareholders, employees, customers, and business partners over the long term			
Geographic proximity, particularly for large acquisitions			

A Pitfall of Comparative Modeling

One pitfall of comparative modeling is *mirror imaging*: the inclination to rely on familiar models, such as your country's organizational or industrial process models, instead of those of the target country. This will lead to erroneous estimates (along with other pitfalls) and is discussed in chapter 18.

Comparative models must be culture specific. A classic example of a culture-specific organizational model is the *keiretsu*, which is unique to Japan, though similar organizational models exist elsewhere in Asia. A keiretsu is a network of businesses, usually in related industries, that have partial ownership of each other and board members in common as a means of mutual security. A network of essentially captive (because they are dependent on the keiretsu) suppliers provides the raw material for the keiretsu manufacturers, and the keiretsu trading companies and banks provide marketing services. Keiretsu have their roots in prewar Japan, which was dominated by four large conglomerates called *zaibatsu*: Mitsubishi, Mitsui, Sumitomo, and Yasuda. The zaibatsu were involved in areas such as steel, international trading, and banking and were controlled by a holding company. Six keiretsu—Dai-Ichi Kangyo Group, Fuyo, Mitsubishi, Mitsui, Sanwa, and Sumitomo—dominate Japan's economy today. Most of the hundred largest Japanese corporations are members of one or another of these “big six.”⁹

An intelligence analyst who mirror images Western business practices in assessing the keiretsu will underestimate the close cooperation between supplier and manufacturer and the advantages it gives in continual product development, quality improvements, and reductions in cost. But the analyst also might miss the weaknesses inherent in a dependency relationship that shields the partners from competitive pressures, which slows innovation and eventually erodes the market position of all the keiretsu parties.

To avoid the problem of mirror imaging, you should create parallel models, side by side, for comparative modeling. This exercise helps to highlight the differences between your own country or company model and that of the target, helping to catch potential areas of mirror imaging.

Profile Models

Profiles are models of individuals and groups—in national intelligence, of foreign government leaders and extremist groups; in competitive intelligence, of top executives in competing organizations; in law enforcement, of mob leaders, domestic terrorists, and serial criminals. The purpose of creating a profile is to help predict what the person or group will do in a given set of circumstances¹⁰ or to aid the customer in negotiating with the target. (Chapter 21 includes more advanced material on the use of profiles in predictive simulation.)

Profiles depend heavily on understanding the pattern of mental and behavioral traits shared by adult members of any given society—referred to as the society's *modal personality*. Several modal personality types may exist in a society, and their common

elements are often referred to as *national character*. A recurring quip that reflects widely held—though tongue-in-cheek—views of national character goes like this:

Paradise is where:

the cooks are French
the mechanics are German
the police are British
the lovers are Italian
and it is all organized by the Swiss.

Hell is where:

the cooks are British
the mechanics are French
the police are German
the lovers are Swiss
and it is all organized by the Italians.

US readers, after enjoying a laugh, might reflect that in many countries, common stereotypes of US national character include obese people gorging on fast food with one hand, toting a gun in the other, while arrogantly using up as many resources as possible in their materialistic quest for more and newer versions of everything.

Modal personality profiles are a starting point in comprehending the culture that a person comes from. But in intelligence we usually want to better understand a specific person. In national, military, and competitive intelligence, these are known individuals, and the person's background can be used to create a specific portrait. The profiles are often drawn from public information: observed behavior, biographical information, and speeches and writings.¹¹ Developing them is an art, and one of the best-known practitioners was Jerrold Post. Several decades ago, Post created and for twenty-one years ran the CIA's Center for the Analysis of Personality and Political Behavior. During his career, he developed profiles of Egypt's Anwar Sadat, Israel's Menachem Begin, Saudi Arabia's Osama bin Laden, Iraq's Saddam Hussein, Venezuela's Hugo Chávez, Iran's Mahmoud Ahmadinejad, and North Korea's Kim Jong-il, among many others.¹² Post described his modeling approach as based almost entirely on open-source and personal interviews with people who had dealt with the target individual:

In profiling a world leader, I try to discern his careerlong pattern of leadership and decision-making. I pay particular attention to first successes and first failures. Most official intelligence emphasizes what's happening right now. I look back—knowing that if something scarred the leader in the past, he'll avoid it in the future—and try to identify the issues that "hook" his political personality.¹³

Law enforcement encounters a completely different problem. More often the identity of the individual is unknown, and the analyst is doing behavioral profiling, also called criminal or offender profiling. The FBI operates behavioral analysis units that develop such profiles. Their work involves creating (as the name suggests) a behavioral model of the unknown target from available evidence. For example, in the online world it is done to predict the behavior of cyber criminals based on their online behavior. Detection systems that help build such models often create a normal online user profile and then identify users who deviate substantially. Cyber criminals, of course, know about such systems and keep finding clever ways to escape being profiled.

In searching for the perpetrators of the 2013 Boston Marathon bombing, investigators relied on a profile. When a bomb explodes, most people will panic and run from the scene. In videos of the blast scene, two spectators did neither, and investigators immediately zeroed in on one of them: Dzhokhar Tsarnaev, one of the two Boston Marathon bombers.

Mathematical Models

Some types of target models are represented by mathematical equations. Most problems in engineering or technical intelligence are single equations in a form such as

$$(x, y, z, t, \dots, a, b, c, \dots) = 0$$

or they are systems of equations in this form. Single equations are common in analyzing radar, communications, and ballistic missile targets; systems of equations are particularly prevalent in econometric models. Most such analysis involves fixing all of the variables and constants in such an equation or system of equations, except for two variables. The equation is then solved repetitively to obtain a graphic picture of one variable as a function of another.

Consider, for example, an equation that frustrates many economists because, while it works in practice, it has no apparent theoretical basis: the gravity model of international trade. The model says, quite simply, that the flow of international trade between two countries depends on the product of the sizes of their economy (usually measured in gross domestic product) divided by the distance between them; or in mathematical terms:

$$\text{Trade flow} = K \times (\text{GBP1})(\text{GDP2}) \div (\text{D12})$$

where K is a constant, GDP is gross domestic product, and D12 is the distance between the two countries. The model has been used successfully to assess the impact of trade agreements, treaties, and diplomatic agreements.

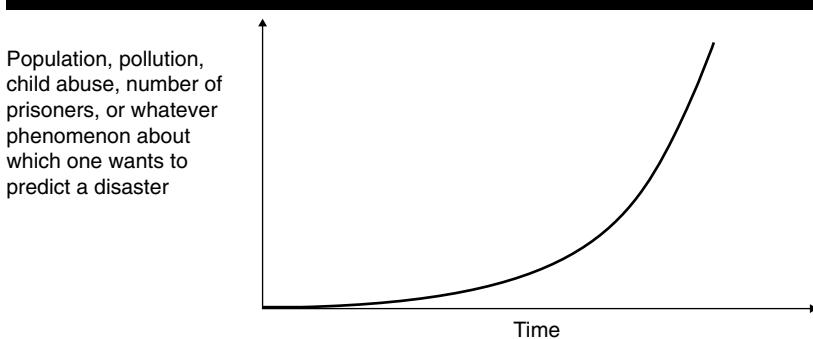
More complex mathematical models make use of spreadsheets and simulations:

- *Spreadsheets.* The computer is a powerful tool for handling the equation-solution type of problem. Spreadsheet software has made it easy to create equation-based models. The rich set of mathematical functions that can be incorporated into it, and its flexibility, make the spreadsheet a widely used model in intelligence. Its value for numerical data is that the software can be used for data visualization, discussed later. Spreadsheets show relationships at a basic level.
- *Simulations.* A simulation model is a mathematical model of a real object or system or an actual situation. It can be challenging to build. The main challenge usually is validation: determining that the model accurately represents what it is supposed to represent, under different input conditions. Simulation models are discussed in detail in chapter 21.

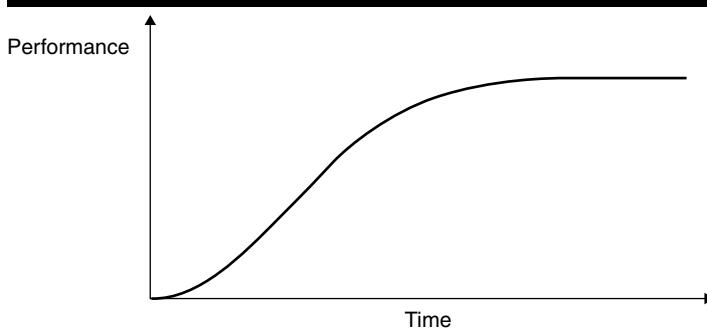
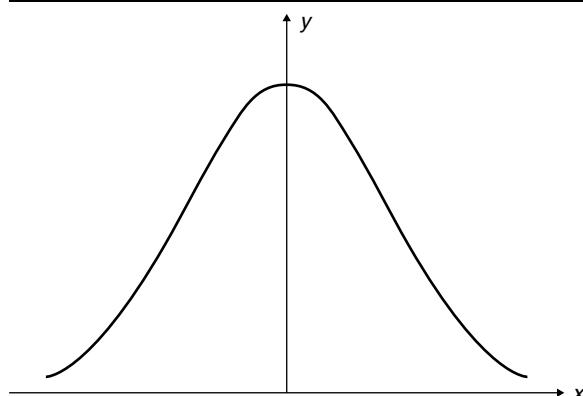
Mathematical models often are represented by graphic displays, typically in the form of curves. Curves are a simple type of model that can be created both for analysis and for presenting analytic results. More advanced curves are introduced and used in later chapters, but let's look at one of the most common: a curve that projects changes over time. When experts extrapolate into the future, they often concentrate on one (or a few) forces that affect an entity, such as the economy or the environment. That can lead them to posit some kind of disaster based on models that use the variables, leading to the *exponential* or *disaster curve* shown in figure 9.2.

Disaster curves tend to ignore or discount the ability of other variables, especially responsive or limiting factors such as human adaptivity and technology, to change at the same rate or faster. A classic example is the exponential extrapolation of growth in telephones, created about 1900, which predicted that by 1920 the entire US population would be working as telephone operators.* Of course, the disaster curve doesn't usually hold up. An opposing reaction, feedback, contamination, or some other countervailing force steps in and retards the exponential factor so that an *S curve* results (see figure 9.3). S curves are fairly common in predictive models.

Many phenomena can be modeled by the *Gaussian* or *normal curve*, shown in figure 9.4. The intelligence quotient of a population, variation in imagery quality, atmospheric dispersion of a chemical release, variation in securities pricing—all these and more can be represented by the normal curve. The quality of a photograph, for example, has an average value, indicated by the point where the curve in figure 9.4 peaks. But if many (say, two hundred) photographs of a scene are taken in rapid order with the same camera and their quality plotted, a curve of image quality like that in figure 9.4 results; a few photographs will be exceptional (falling on the far right side of the curve), and a few will be poor (falling on the far left side of the curve).

FIGURE 9.2 ■ The Exponential (or Disaster) Curve

* In one sense, this eventually turned out to be an accurate prediction. By the 1970s, almost all telephones were either dial or push-button operated. As a result, almost all Americans over the age of eight were part-time telephone "operators" in the sense of the original extrapolation.

FIGURE 9.3 ■ The S Curve**FIGURE 9.4 ■ The Normal Curve**

Pattern Models

Many target models fall under the broad category of *pattern models*. Pattern recognition is a critical element of all intelligence.¹⁴ Most national leaders, terrorists, and criminals have a modus operandi, or standard operational pattern. Most governmental and industrial organizations (and intelligence services) also prefer to stick with techniques that have been successful in the past. An important aspect of intelligence analysis, therefore, is recognizing patterns of activities and determining whether (a) the patterns represent a departure from what is known or expected and (b) the changes over time are significant enough to merit attention. The computer is a valuable ally here; it can display trends that allow an analyst to identify them. This capability is particularly useful when trends would be difficult or impossible to find by sorting through and mentally processing a large volume of data. Pattern analysis is one way to effectively handle complex issues, and current computer software programs have great capacity to sort through, find, and graphically display trends.

Pattern models rely heavily on statistics, and intelligence analysis deals with a wide variety of statistical modeling techniques. Some of the most useful are easy to learn and require no previous statistical training. Almost all statistical analysis now depends on software that provides both a broad range of statistical routines and a flexible data definition and management capability. Such software also includes basic graphics capabilities to display data visually as trend lines.

One of the most common pattern models in military and law enforcement intelligence is pattern-of-life (POL) modeling. It is a method of understanding the behavior of a single person or group by establishing a recurrent pattern of actions over time in a given situation. The resulting model can be used to assess future activity by the targets. POL analysis often uses video surveillance of individuals or groups, but it can be done entirely by nonvisual surveillance—focusing on internet browsing habits, telephone calls, or financial transactions, for example. In finance, POL analysis might identify patterns left by a particular kind of criminal. It is useful for white-collar crime analysis. For example, patterns of fraud such as embezzlement and insurance fraud are uncovered by application of POL techniques.¹⁵

One risk in creating a pattern model is that it can be tempting to settle on a pattern too quickly. Once a pattern has been identified, it is easy to emphasize evidence that seems to support it and to overlook or explain away evidence that might undermine it. That would be a mistake.

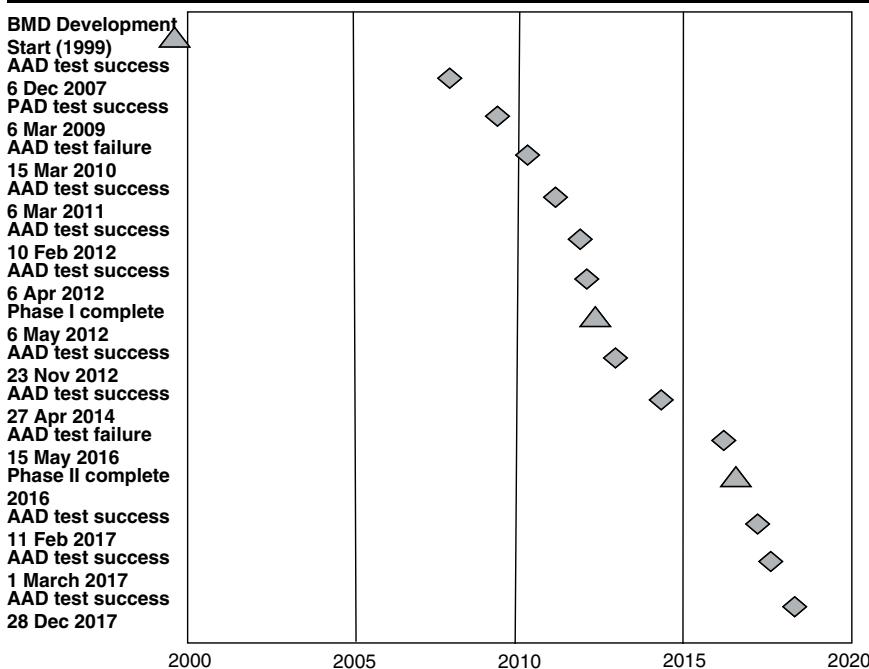
Most pattern models are temporal; they show patterns of activity over time. Pattern changes over time are often used to compare how things are going now with how they went last year (or last decade). Anticipatory analysis often relies on such chronological models. Timing shapes the consequences of planned events. In sales campaigns, military campaigns, and political campaigns, among others, timing is critical to making an impact. The importance of temporal models is illustrated in the Iranian nuclear negotiations example discussed in chapter 18.

Models that show patterns over both space and time are widely relied on in analysis. We typically want to observe activity in both space and time—sometimes over very short times. One example is the dynamic geospatial model (discussed in chapter 20). A few pattern models are purely temporal. Two of the most basic are timelines and histograms.

Timelines

An opponent's strategy often becomes apparent only when seemingly disparate events are placed on a timeline.¹⁶ Consider, for example, the model shown in figure 9.5. The timeline shows the testing chronology for India's Ashwin Advanced Air Defense (AAD) interceptor missile. For the analyst following India's Ballistic Missile Defense (BMD) program, the pattern of successes and failures over time tells a great deal about where India is in operational readiness to defend against ballistic missile attacks. And the variance in time between tests (illustrated in the figure) can be used to draw conclusions about the program. US intelligence has used similar timelines for decades to assess foreign weapons development trends.

FIGURE 9.5 ■ Chronological Model of Indian BMD Development



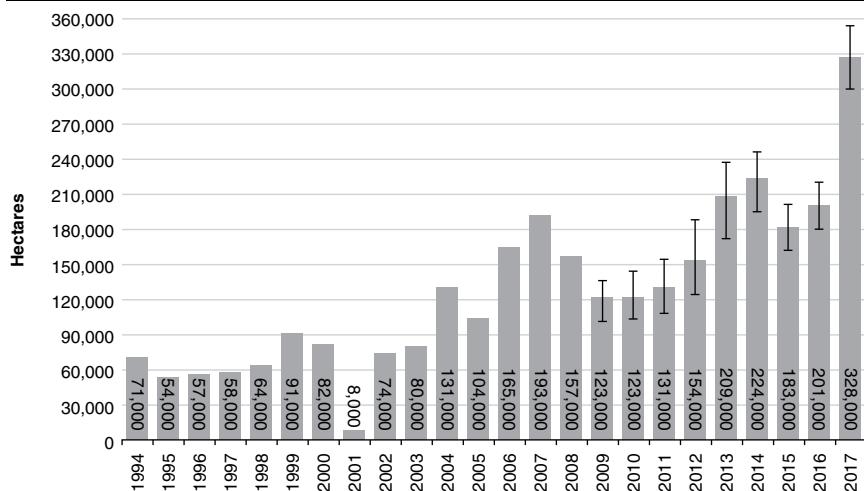
As another example, the activity patterns of a target network are useful in determining the best time to collect intelligence. An example is a plot of total telephone use over twenty-four hours—the plot peaks at about 11 a.m., which is the most likely time for a person in the network to be on the telephone.

Histograms

Histograms, which are bar charts that show a frequency distribution, are another example of a simple temporal pattern model.

A type of histogram that might be used in intelligence is shown in figure 9.6. The chart permits an analyst to examine patterns of opium production over time in Afghanistan and to correlate the changes with other events in the region, such as Taliban and government forces activities.

FIGURE 9.6 ■ Opium Production in Afghanistan, 1994–2017



Note: Bars from 2009 to 2017 indicate uncertainty in estimates.

Source: United Nations Office on Drugs and Crime Afghanistan Opium Survey.

This chapter covered the most basic model types, by way of an introduction to the subject. But a single target model of any given type seldom is sufficient in today's environment. You may need to create multiple models, as discussed in the next chapter.

SUMMARY

All intelligence involves creating one or more models of the target and extracting knowledge from them. The model is an organizing constraint: a combination of facts, hypotheses, and assumptions about a target, developed in a form that is useful for analyzing the target and for presenting the results for customer decision making. Intelligence models are typically conceptual. The easiest ones to work with are deterministic, linear, static, and solvable. Unfortunately, in the intelligence business, problems tend to require target models that are stochastic, nonlinear, dynamic, and simulated.

Lists are the simplest form of model. In intelligence, comparative models or benchmarks are often used; almost any type of model can be made comparative, typically by creating models of a similar known system side by side with the target system model or benchmarking.

Profiles of leaders and key executives are used to predict their likely decisions in given situations. Such models start with understanding the target culture's modal personality type. But most often, a specific profile is needed, based on analysis of the target individual's background. A different approach is required in law enforcement, where the usual challenge is to create behavioral profiles of unidentified individuals, based on their patterns of activity.

Mathematical models are commonly used in systems analysis to determine weapons performance. Economic intelligence depends on other types of mathematical models. These can be as simple as an equation or a spreadsheet, and as complex as a computer simulation. Graphic displays, in the form of curves, are commonly used to present the results of a mathematical model.

Pattern models depend on the natural tendency of humans to establish and repeat certain types of behavior. Behavior of individuals or groups over time can be represented by a specific type of model called a *pattern-of-life (POL) model*; it allows the behavior of a single person or group to be understood by establishing a recurrent pattern of actions in a given situation. Statistical information is most readily understood when presented graphically to display patterns.

Purely temporal models are used to address intelligence issues where timing is a critical factor—as it often is in military campaign planning and in assessing new systems development. The product often takes the form of a timeline. Over longer time frames, temporal models convey trends about topics such as population growth, pollution, climate change, and unemployment in a fashion that can be readily understood. Such chronological models allow intelligence customers to examine the timing of related events and, when warranted, to plan a way to change the course of these events.

CRITICAL THINKING QUESTIONS

1. Identify a social, political, military, or economic trend that might fit the exponential curve in figure 9.2. Identify restraining forces that are likely to keep the curve from growing exponentially. Try to use a restraining force other than those listed in the figure.
2. Consider the opium production histogram in figure 9.6. Can you explain the two outliers in the histogram (in 2001 and 2017)?

3. Pick two distinct national cultures—preferably non-US. Create a parallel list model that identifies contrasting features of the two cultures.
4. For the cultures that you selected in question 3, describe a scenario in which an intelligence analyst might mistakenly mirror image in reaching a conclusion.

NOTES

1. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York, NY: Simon & Schuster, 1996), 29.
2. Paul R. Pillar, *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform* (New York, NY: Columbia University Press, 2011).
3. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009).
4. A stochastic process is one in which the events of the process are determined by chance. Such processes are therefore analyzed using probability theory.
5. Peter Buxbaum, "Showing to Tell," *Geospatial Intelligence Forum Magazine*, October 2013.
6. Theodore J. Gordon and M. J. Raffensperger, "The Relevance Tree Method for Planning Basic Research," in *A Guide to Practical Technological Forecasting*, ed. J. R. Bright and M. E. F. Schoeman (Englewood Cliffs, NJ: Prentice Hall, 1980), 134.
7. Ian Gill, "Gas Pipeline Race," *ADB Review*, October 2005, Asian Development Bank, Manila, www.adb.org/Documents/Periodicals/ADB_Review/2005/vol37-5/gas-pipeline.asp.
8. Michelle Cook and Curtis Cook, "Anticipating Unconventional M&As: The Case of DaimlerChrysler," *Competitive Intelligence Magazine*, January–February 2001.
9. "Facts from the Corporate Planet: Ecology and Politics in the Age of Globalization," *Wired*, October 23, 2002, www.wired.com/news/business/0,1367,8918,00.html.
10. Carolyn M. Vella and John J. McGonagle, "Profiling in Competitive Analysis," *Competitive Intelligence Review* 11, no. 2 (2000): 20.
11. Benedict Carey, "Teasing Out Policy Insight from a Character Profile," *New York Times*, March 28, 2011, <http://www.nytimes.com/2011/03/29/science/29psych.html>.
12. Ken Adelman, "The Mind of a Leader," *Washingtonian*, November 1, 2007, <https://www.washingtonian.com/2007/11/01/the-mind-of-a-leader/>.
13. Ibid.
14. M. S. Loescher, C. Schroeder, and C. W. Thomas, *Proteus: Insights from 2020* (Utrecht, Netherlands: Copernicus Institute Press, 2000), 25.
15. Gabriel Miller, "Activity-Based Intelligence Uses Metadata to Map Adversary Networks," Defensenews.com, July 8, 2013, <http://archive.defensenews.com/print/article/20130708/C4ISR02/307010020/Activity-based-intelligence-uses-metadata-map-adversary-networks>.
16. Ibid., 24.

10

THE TARGET FRAMEWORK

Chapter 8 highlighted the value of issue decomposition as a conceptual framework to gain full understanding of the intelligence customer's issue. Chapter 9 described the central role of the target model in all analysis. This chapter is about developing a *target framework*: a conceptual framework specifically suited to strategic intelligence and in-depth research problems. It typically comprises multiple models, conceptually related to each other and to the issue, forming a set.

CREATING A TARGET FRAMEWORK

The first step in creating a target framework is to define the *system* that encompasses the intelligence issues of interest, so that the resulting target model set can be used to address them.

The system could be something as simple as a new fighter aircraft, a data processing center, an opium production operation, or a new oil pipeline. Many current or tactical intelligence questions can be that limited in scope. Recall the chapter 3 example of the BMP in Afghanistan: The analysis centered on the vehicle, its occupants, and the surrounding terrain. Problems coming into the Symantec war room (discussed in chapter 2) are usually narrowly focused on an immediate virus, hacker, or Trojan horse of concern; its source; and its victims. In contrast, few questions in strategic intelligence or in-depth research can be answered by addressing such a narrowly defined target.

Complex targets typical of in-depth research usually include a complete system, such as an air defense system that will use a new fighter aircraft; a narcotics growing, harvesting, processing, and distribution network, of which the opium poppy production operation is but a part; or an energy production system that goes from oil exploration through drilling, pumping, transportation (including the oil pipeline), refining, distribution, and retailing. In law enforcement, analysis of an organized crime syndicate involves consideration of people, funds, communications, operational practices, movement of goods, political relationships, and societal impact. Many intelligence problems will require consideration of related systems as well. The energy production system issue, for example, will give rise to intelligence questions about related governments, companies, suppliers and customers, and also nongovernmental organizations (such as environmental advocacy groups).

The second step is to select a *generic target framework* for the system. The target can be defined broadly, or narrowly. The goal is to define the *relevant* target: the one that will address the customer's specific intelligence issue. A major challenge is to use restraint. The definition must include *essential* elements but nothing more. Part of an analyst's skill lies in being able to include in a target framework all the relevant components, and only the relevant components, that will address the issue. The questions that customers pose should be answerable by reference only to the target framework, without the need to reach beyond it.

For many systems of intelligence interest, there are only a few generic target frameworks. Opium poppy processing, for example, is a narrowly defined target and has only a few generic target frameworks—depending on whether the desired final product is opium, morphine, or heroin. For broader and more complex targets, there may exist several generic target frameworks. A country's economy, for example, can be modeled as a market or socialist economy, or as a mixture of the two such as the Nordic model common in Scandinavian countries or the socialist market economy practiced in the People's Republic of China.

A system, as explained in chapter 3, can be examined structurally, functionally, or as a process. A systems model can therefore be represented as structural, functional, process, or any combination thereof; and there typically exist generic target frameworks for each representation. Structural models include actors, objects, and the organization of their relationships to each other. Functional models concentrate on the results achieved, for example, a simulation of the financial consequences of a proposed trade agreement. Process models focus on interactions and their dynamics.

The generic target framework for an intelligence issue is the starting point for any analysis. It usually already exists; few target classes have never been seen before, and when a new one does appear, it creates major analysis problems, as we'll see in chapters 18 and 20.

The generic framework is a set of target models, created in much the same fashion as the issue decomposition framework of chapter 8:

1. Begin from a top-level view of the target.
2. Next, parse (deconstruct) it into sub-categories and continue into lower-level sub-categories (all being models) as necessary.
3. The deconstruction leads you into the third step: make the generic target framework specific to the issue.

Why go through all of this? Because the detailed specific framework that results facilitates a comprehensive understanding of the target. Ideally, both the target and the issue are represented by a visual picture. The target picture always takes the form of a set of interrelated target models.

In the case of a network, the target picture includes understanding how the network functions and how the sub-elements of the network interact with each other.

Reconsider the basic cocaine trafficking network from chapter 3 (shown in figure 3.4). Fleshing out the network with additional components (suppliers, infrastructure details, names of key people) gives you the basis for conducting detailed analysis. In short, deconstruct and identify components and attributes of the target system, which are then deconstructed into further elements until a detailed picture of the target emerges.

Defining and deconstructing components into the lowest levels reveals what is known and unknown, what is assumed, and the critical gaps that exist. Chapters 11, 12, and 14 go into more depth on those topics, but a few examples will help illustrate the basic process for now.

Suppose that the customer has posed one of these three intelligence questions:

1. How effective is the ideology being promoted by the terrorist group al-Shabaab at attracting adherents?
2. What options for exerting influence on the government of Azerbaijan are likely to be successful?
3. What is the status of Monopolitania's biological warfare program, and what threat does it pose?

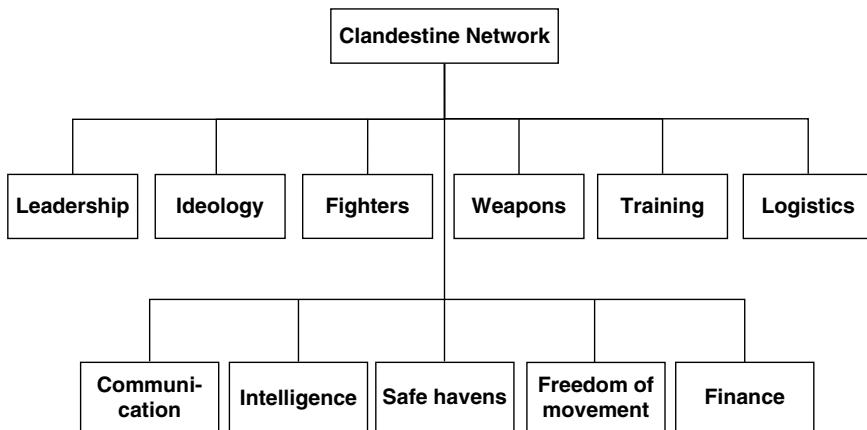
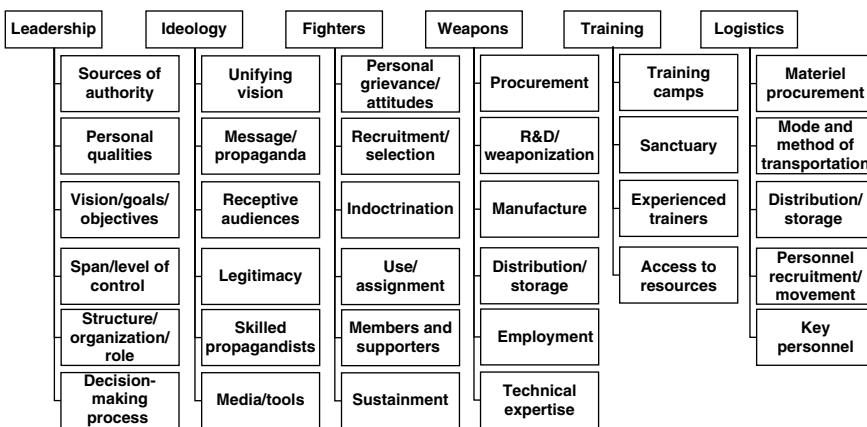
For each of these questions, we will begin with a generic target framework; then we'll *populate* the framework—the subject of chapters 11 and 12—in the process, making it specific to the target and the issue.

ISSUE 1: AL-SHABAAB IDEOLOGY

"How effective is the ideology being promoted by the terrorist group al-Shabaab at attracting adherents?" In this issue, the generic target is a clandestine network, typical of one that operates internationally. Similar networks engage in narcotics, weapons, or human trafficking. A top-level generic framework would look something like figure 10.1. As a terrorist network, al-Shabaab would have a structure much like the one shown in the figure. As the figure demonstrates, the targeting framework is intended to develop a simplified understanding of the target system, depicting the elements as a hierarchy.

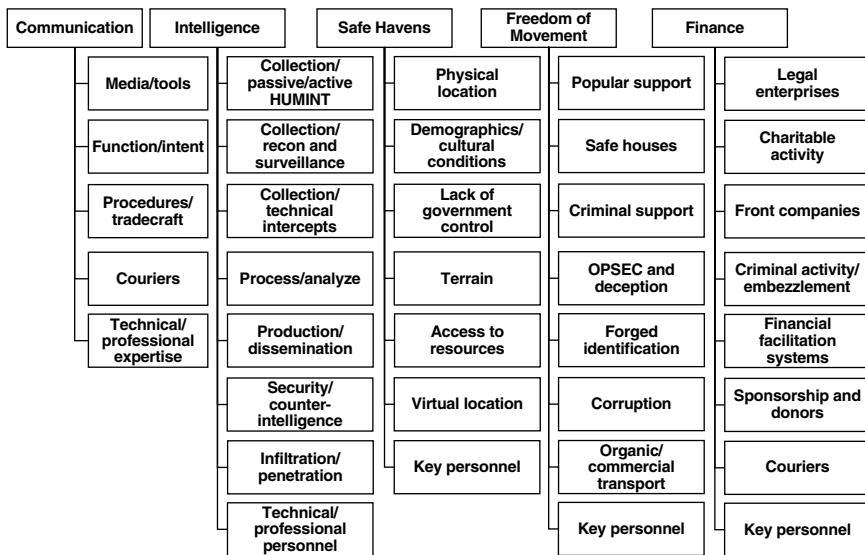
The deconstruction to a third level might result in the subordinate elements shown in figures 10.2 and 10.3. These were taken from the US Joint Forces Command publication *Commander's Handbook for Attack the Network*; in it they were applied to the example of an improvised explosive device network, but this generic target framework is broadly applicable to clandestine networks.¹

Let's apply this framework to a real target (al-Shabaab) to illustrate how it might be used, and to understand the importance of looking at the entire target deconstruction when addressing a customer's question.

FIGURE 10.1 ■ Clandestine Network Target Framework—Top Level**FIGURE 10.2 ■ Clandestine Network Target Framework Deconstruction I**

The customer's question is about ideology. A casual look at figures 10.2 and 10.3 naturally leads an analyst to focus on assessing the ideology breakdown block, and that's a good place to start. But it's not enough. Several other blocks in the two figures also shape the effectiveness of the ideology: sources of authority and personal qualities (leadership), personal grievance/attitudes and indoctrination (fighters), media/tools (communication), and charitable activity (finance), among others. The point is that the components in a target deconstruction differ from those in an issue decomposition. Of course, the two are inevitably interrelated. Target framework deconstruction, though, better helps the analyst to investigate interrelationships among the system's components.

FIGURE 10.3 ■ Clandestine Network Target Framework Deconstruction II



The al-Shabaab example illustrates the most common method of developing a target framework by deconstruction: a hierarchy. Issue 2 is a broader question, better served by using a different construct.

ISSUE 2: INFLUENCING AZERBAIJAN

“What options for exerting influence on the government of Azerbaijan are likely to be successful?” It is a topic that policymakers typically are very interested in hearing about for many countries.

In a 2013 paper, CIA analyst Jason Manosevitz presents a compelling case for the importance of conceptual frameworks. He illustrates the point using a generic conceptual framework to assess the influence that one country can exercise over another. He observes there are many ways to convey the idea of influence: persuasion, sway, manipulation, leverage, and pressure—that is, getting people or organizations to do something they would not otherwise do.² Manosevitz draws on the work of David Baldwin, who outlines four means of exerting influence: symbolic, economic, military, and diplomatic.³ If this sounds much like the DIME instruments introduced in chapter 2 (replacing “symbolic” with “information”), that’s no accident.

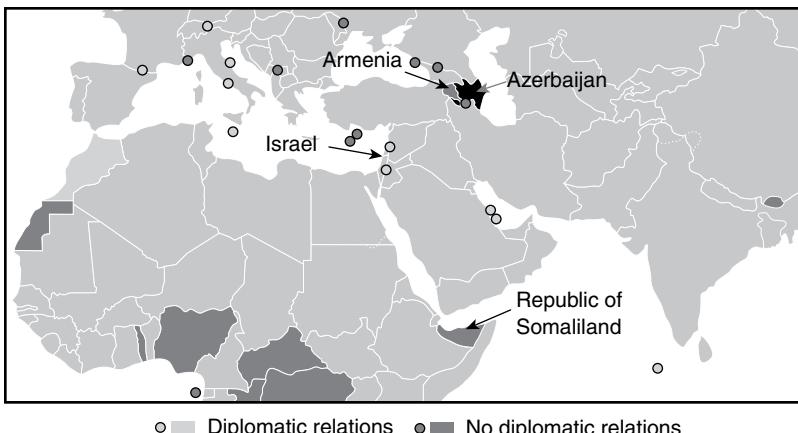
Some targets can best be deconstructed using the DIME view, but, again, in this book we use the more inclusive PMESII perspective introduced in chapter 8. The deconstruction in Issue 2 includes the six PMESII factors, two of which are not instruments. (In a moment it will be clear why those two should be part of the target

framework.) The set of models described here is far from complete, of course. Each example represents one likely sub-element of the top-level PMESII framework. We'll illustrate how the generic framework is populated with issue-specific submodels. Though we look at just one example for each factor, there are many possible submodels.

Political Model

The Azeri government eliminated presidential term limits in a 2009 referendum. President Ilham Aliyev today appears to be firmly in charge. An analyst could develop models of the political support that Aliyev has, his control over the judiciary and legislature, or government links with criminal elements, for example. To assess points of political influence, a useful model would be a display of Azerbaijan's diplomatic ties with other countries, shown in figure 10.4. It shows a few points of analytic interest: Azerbaijan does not have diplomatic relations with Armenia or the Republic of Somaliland, for example. (The small circles are countries too small to appear on the map.) That isn't greatly surprising; Azerbaijan has an unresolved conflict with Armenia over Nagorno-Karabakh, a primarily Armenian-populated region currently controlled by Azerbaijan. Armenia and Azerbaijan began fighting over the area in 1988, and a tenuous cease-fire has existed since 1994. And Somaliland is generally considered to be part of Somalia, not a separate country. More surprising is that Azerbaijan is one of the few majority-Muslim countries to have bilateral strategic and economic relations with Israel—a topic we revisit in the military model, next. The map shows that Azerbaijan has diplomatic relations with Tehran, but the relationships are strained because of Iran's support for the Armenians and Azerbaijan's connections to Israel.

FIGURE 10.4 ■ Countries Having Diplomatic Relations with Azerbaijan



Source: Adapted from "Azerbaijan Relations," Alinor at English Wikipedia. Licensed under CC BY-SA 3.0 via Wikimedia Commons, http://commons.wikimedia.org/wiki/File:Azerbaijan_relations.png#/media/File:Azerbaijan_relations.png.

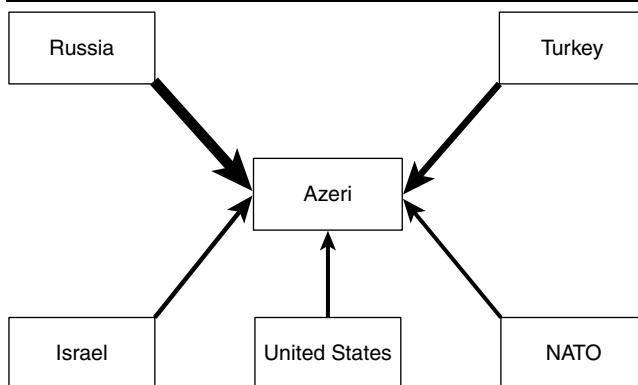
A more detailed analysis of Azerbaijan's political ties with other countries might indicate more areas of potential influence, but an obvious one is the relationship (or lack thereof) with Armenia. Azerbaijan would be very sensitive, for example, to any indication that the United States or Russia were becoming more favorably inclined to support Armenia in the unresolved conflict.

Military Model

Military models can describe deployments, mix of weaponry, or performance of weapons (aircraft, naval vessels, armored vehicles, artillery, air defense systems), and so on. Azerbaijan's military model is shaped by the unresolved conflict with Armenia mentioned earlier. Figure 10.5 specifically addresses the question of levers of influence. It shows the key cooperative relationships between Azeri military and other countries. In the figure, the thickness of the connection indicates the strength of the relationship:

- Russia is Azerbaijan's main arms supplier. Military and technical cooperation between the two is estimated to total about \$4 billion.
- Turkey has provided Azerbaijan with a mix of light weaponry and other military equipment along with professional training for the Azeri military. Turkey has agreed to provide troops, if necessary, in the event of a resumption of hostilities between Azerbaijan and Armenia over Nagorno-Karabakh.
- Azerbaijan and Israel cooperate in several areas of the defense industry, with Azerbaijan acquiring Israeli technology such as a capability to produce military UAVs.
- NATO assists Azerbaijan in defense organizational reforms.
- The United States has agreements providing for military cooperation with Azerbaijan, including special forces assistance.

FIGURE 10.5 ■ Cooperative Relationships of the Azeri Armed Forces

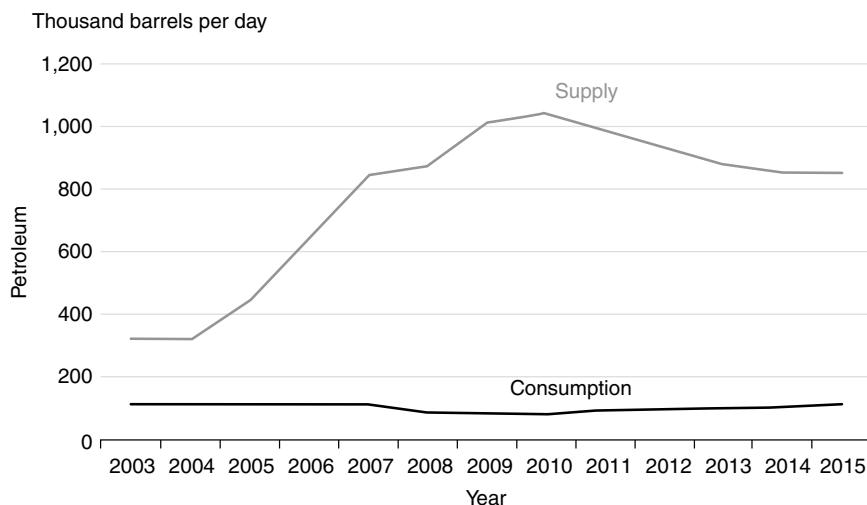


This example illustrates a point about the military instrument: Several countries could exert influence using it, with Russia and Turkey being in the best position to do so, but not by threatening to exert military force *against* Azerbaijan.

Economic Model

Azerbaijan experienced high economic growth in the first decade of the twenty-first century, thanks to large and growing oil and gas exports. The model in figure 10.6 illustrates this point and, in conjunction with the infrastructure model of figure 10.8, suggests possible points of economic influence. Note, for example, that while domestic consumption has not grown much, the supply has declined substantially since 2010, indicating possible problems for the Azeri economy. An analyst could model several of the nonexport sectors that have also experienced double-digit growth, including construction, banking, and real estate. Other economic models might track changes in GDP, unemployment, inflation rate, or public debt to identify areas in which economic influence might be applied.

FIGURE 10.6 ■ Petroleum Production and Consumption in Azerbaijan, 2003–2015



Source: "Azerbaijan: International Energy Data and Analysis," US Energy Information Administration, June 24, 2016, <https://www.eia.gov/beta/international/analysis.cfm?iso=AZE>.

Social Model

The social model is not an instrument that can be wielded, so it tends to get less attention than the four PMESII factors that are also DIME instruments.

But it can in fact be the most important factor. For example, in the 1960s and 1970s, in terms of political, economic, and military power, the United States was far superior to North Vietnam. That superiority had no bearing on the Vietnam War's outcome, according to David Baldwin:

*The United States may have been the greatest power in the history of the world, but it was ill equipped to fight a guerrilla war in a faraway land with language, culture and history that it understood poorly.*⁴

In other words, the social factor was the dominant one in that case. The USSR later encountered a similar result in Afghanistan. Its overwhelming military power did not translate to a victory. The Israelis, with a superior military force, had a similar outcome in Israel's 2006 conflict with Hezbollah in Lebanon. In his 1994 book, Samuel Huntington bases his primary thesis on the importance of the social factor: that twenty-first-century conflicts would be a matter of clashes between cultures.

But if the social factor isn't an instrument that policymakers could use, why include it? Because if it is well understood, then one or more of the four instruments—usually information—can be used to shape the social environment more favorably to your side's interests. And if it is understood, policymakers may be able to better anticipate and prepare for future events. US policymakers were reminded of that need, once again, in August 2021.

BOX 10.1 THE TALIBAN TAKE BACK AFGHANISTAN

The year 2021 saw one of the most dramatic failures of US policy in recent times: the rapid collapse of the Afghan government and the Taliban takeover of the country. The collapse itself was not a surprise; but the speed with which it happened during the last stages of US and allied force withdrawal from Afghanistan was. The result was both a humanitarian and a military disaster: panicked Afghans crowding around Kabul International Airport trying to flee, with US soldiers and Afghan civilians dying in a suicide bomb attack.

According to news reporting, four US intelligence agencies failed to predict the speed of the collapse.⁵ While we can only guess at the reasons for this reported failure, one factor seems apparent. The question requires a military assessment: relative combat effectiveness. The focus of all US policymaker assessments likely was on the Afghan army's military readiness. The United States and allies had spent the previous two decades equipping and training the Afghan military. On paper, the government's forces looked formidable, quite capable of holding off the Taliban for some time.

But the dominant factor was social. View the situation from the perspective of an Afghan soldier or his commander. The United States and allies are pulling out because they've said they can't win. If you couldn't win with their support, what chance do you have now? You are left to fight for a corrupt government, one that doesn't care about you, basically sacrificed to protect the foreigners' withdrawal.⁶ From that social perspective, was the collapse surprising?

The British government likely viewed its situation in Singapore in 1942 much like the US view in 2021: *Our forces outnumber the Japanese, and we're better equipped. We can hold the island.* But in Singapore, the defenders' point of view was quite different. They had suffered a series of demoralizing blows. Japanese Zeros quickly cleared the skies of the inferior Royal Air Force fighters. The British warships sent to support the city's defense, the HMS Repulse and HMS Prince of Wales, had been sunk by Japanese torpedo bombers on December 10, 1941. Then the Japanese commander ordered an invasion of the island that could have been repulsed but was not. The Singapore collapse has been summarized as a result of "poorly trained troops, deficient commanders, negligent preparation and government penny-pinching."⁷ But in Singapore, as in Afghanistan, more important was a lack of will to resist what appeared inevitable to the defenders.

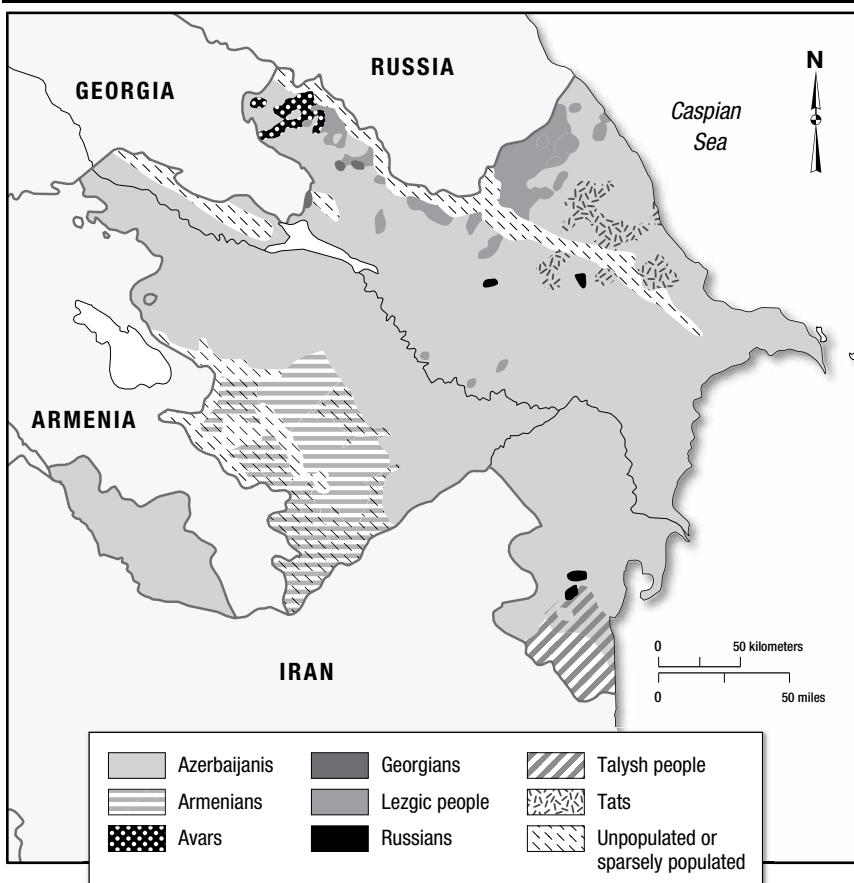
A similar outcome developed in the 2022 Russian invasion of Ukraine, except that it was the defenders that prevailed. Western military commentators predicted that Ukraine would be overrun within weeks because of superior Russian military prowess and numbers. Instead, the Russian forces encountered problems with poor leadership, supply mismanagement, and low troop morale. The assault on Kyiv was thrown back by a unified, determined, innovative, and well-led Ukrainian resistance. Again, observers missed the critical determinant in the conflict: the social factor.

How do such miscalls happen? One reason is that intelligence assessments naturally focus on the four instruments of national power, especially on the military and economic ones. Social factors do not intuitively present as decisive. But social factors can—and often do—prove more decisive than the military instrument. An astute observer of the Afghan situation summed it up this way: "No outside power can help a failed government that cannot help itself."⁸ In Singapore and Afghanistan, the attackers had that advantage. In Ukraine, the social unity advantage went to the defenders.

Returning to the Azerbaijan example: It is a nation with a majority-Turkic and majority-Shiite Muslim population. Several ethnic groups exist, as illustrated in figure 10.7. This particular model could be useful in assessing influence actions (information operations, for example) involving the Armenians, a persecuted group, or resistive groups such as the Talysh and Lezgins. A different social model might take into account religious entities that support or oppose the Azeri government; those entities would be potential targets for information operations also.

Infrastructure Model

Figure 10.6 illustrated the economic benefits of oil exports and their contributions to the GDP of Azerbaijan. Oil exports through several pipelines remain the main

FIGURE 10.7 ■ Ethnic Model of Azerbaijan

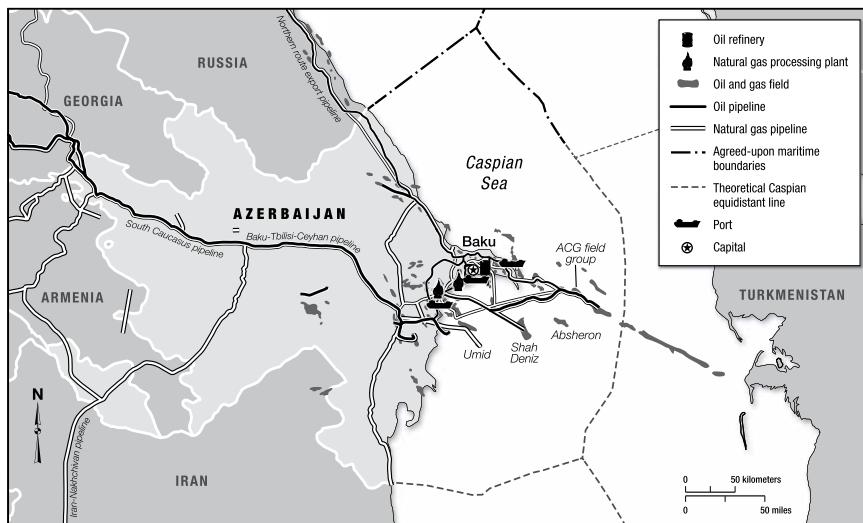
Source: Adapted from "Ethnographic Map of Azerbaijan, 2003," ©Yerevanci/Wikimedia Commons/CC-BY-SA-3.0. <http://creativecommons.org/licenses/by-sa/3.0/>

economic driver; these pipeline networks are illustrated in the infrastructure model of figure 10.8. Any occurrences that could disrupt these exports would be a major concern for the Azeri government and a factor to consider in looking at levers of influence.

Note that, like the social model, infrastructure is not an instrument that can be wielded. Instead, a policymaker would apply one or more of the four instruments—economic or information, for example—to exert influence using infrastructure. Cyber operations, for example, can be very effective in disrupting a country's infrastructure. A Russian hacker group demonstrated that fact on May 6, 2021, when it conducted a ransomware cyberattack on Colonial Pipeline, leading to the shutdown of gasoline and

jet fuel supplies to the southeastern United States. The shutdown caused panic buying and gas station closures across the region.

FIGURE 10.8 ■ Oil and Natural Gas Structure in Azerbaijan



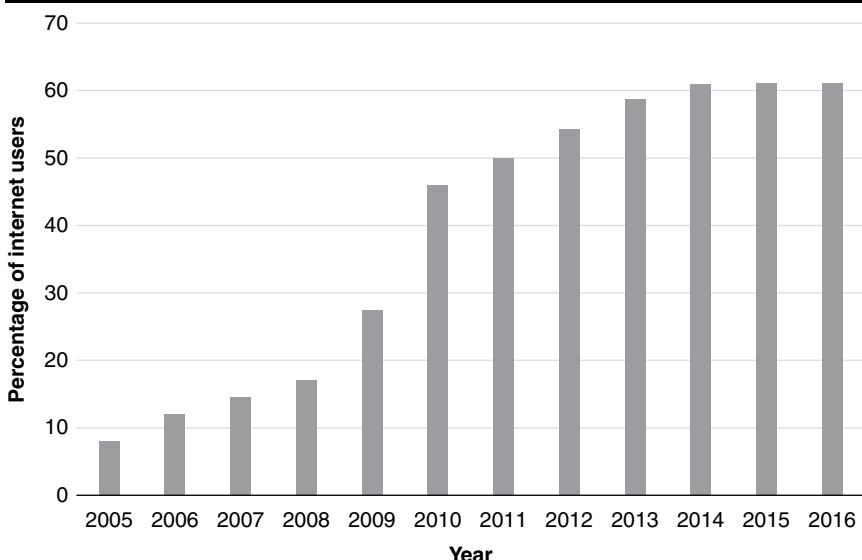
Source: "Azerbaijan: International Energy Data and Analysis," US Energy Information Administration, August 2014, https://www.eia.gov/beta/international/analysis_includes/countries_long/Azerbaijan/azerbaijan.exe.pdf; US Geological Survey, IHS EDIN.

Information Model

Figure 10.9 is an example of an information model. It shows the trend in internet access for Azerbaijan. Access was growing steadily until 2014, partly as a result of the country's national strategy: creating an information and communications technology hub for the Caucasus region. Consequently, the internet is mostly free from systematic government filtering or blocking. The government does not, however, tolerate political opposition postings online. The model is relevant in assessing the possible use of information operations as an information “lever” of influence—for example, in projecting a message to the Azeri leadership about the social or infrastructure factors discussed earlier.

These are straightforward, simplistic examples of a target model set that illustrate the use of modeling across all parts of a PMESII conceptual framework. Again, many more such models would be needed to provide a detailed picture to address the likely success of options for influencing the Azeri government.

A third way to create a framework is by deconstruction into a set of interrelated models such as process, temporal, or geospatial models, for example. Issue 3 illustrates that approach.

FIGURE 10.9 ■ Percentage of Internet Users in Azerbaijan by Year

Source: Created by the author from United Nations statistical reporting, http://data.un.org/Data.aspx?d=WDI&f=Indicator_Code%3AIT.NET.USER.P2.

ISSUE 3: THE MONOPOLITANIA BIOLOGICAL WARFARE THREAT

The issue here is to assess the ability of Monopolitania to produce, deploy, and use biological weapons for terror or combat purposes. An analyst might begin by synthesizing a generic process model, or model template, based on nothing more than general knowledge of what it takes to build and use biological weaponry. The model could apply to any BW program and would look like figure 10.10.⁹

From here, the model has to be expanded and made specific to the Monopolitania target, in an iterative modeling process involving the creation of a more detailed framework using *submodels* or *collateral models*.

Submodels

It is typical, for complex targets, to have many submodels of a target that provide succeeding levels of detail from the top-level model. Participants in the target-centric process then can reach into the model set to pull out the specific information they need. The collectors of information can drill down into more detail to refine collection targeting and fill specific gaps. The intelligence customer can do the same to answer questions, gain confidence in the picture of the target, and understand the limits of analytic work. The target submodel is a powerful collaborative tool.

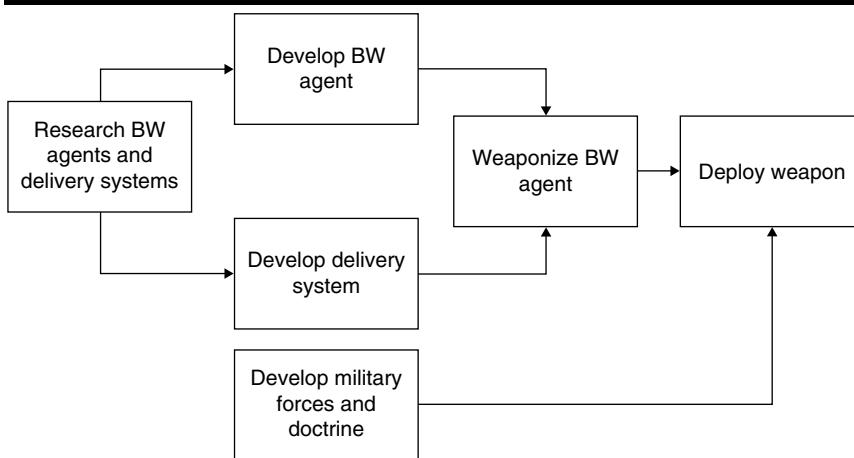
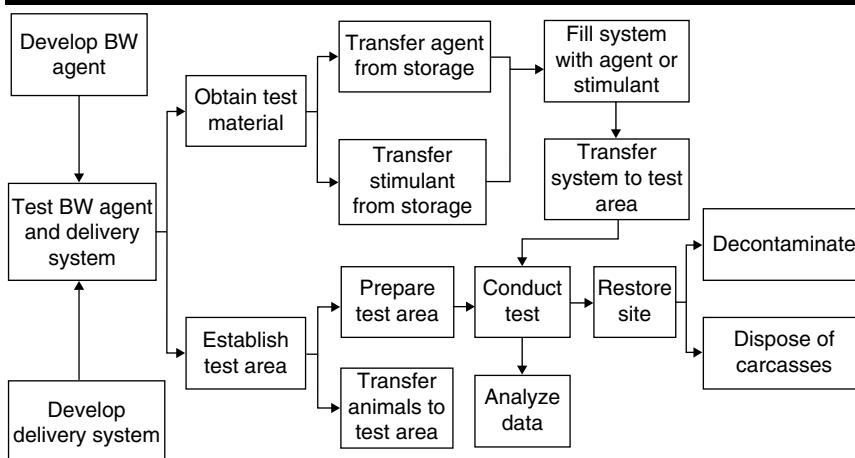
FIGURE 10.10 ■ Generic Biological Weapons System Process Model

Figure 10.11 illustrates a generic submodel of one part of the process shown in figure 10.10.¹⁰ In this scenario, as part of the development of the BW agent and delivery system, a test area has to be established and the agent must be tested on animals.

FIGURE 10.11 ■ Biological Weapons System Test Process Submodel

Collateral Models

A collateral model typically presents an alternative way of thinking about the target for a specific intelligence purpose. For example, suppose that as part of the issue decomposition, we have determined the customer needs to know how the Monopolitarian BW organization is managed, where the operations are located, and when the country might deploy biological weapons.

Figure 10.12 is a collateral model intended to answer the first question: How is the top level of the BW development organization managed? Like most organizational models, it is structural.

FIGURE 10.12 ■ Monopolitarian Biological Weapons Development Organizational Model

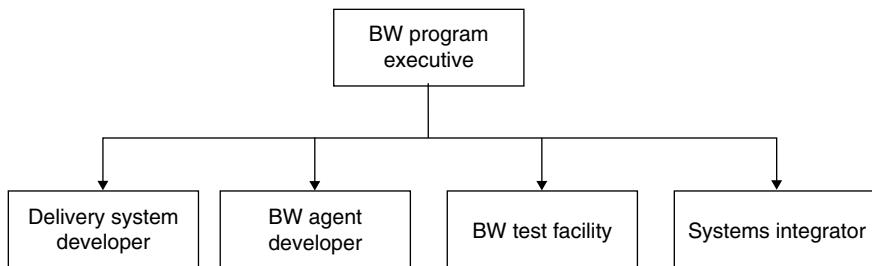
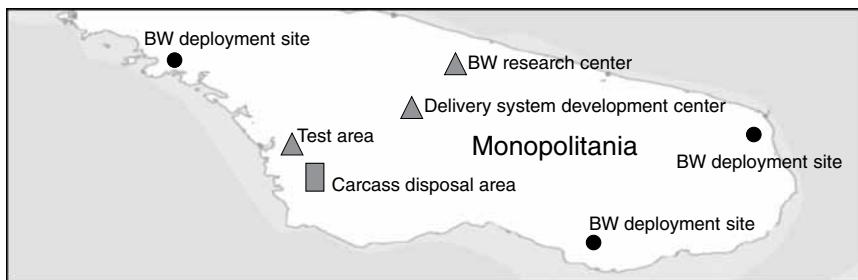


Figure 10.13 is a collateral spatial, or geographic, model of the BW target, answering the second question of where the BW operations are located. This type of model is most useful in collection planning.

FIGURE 10.13 ■ A Collateral Model of Monopolitarian Biological Weapons Facilities



A temporal (chronological) collateral model of the BW target is shown in figure 10.14. It is designed to answer the question of when the country will deploy biological weapons and also is of value to an intelligence collector for timing collection efforts.

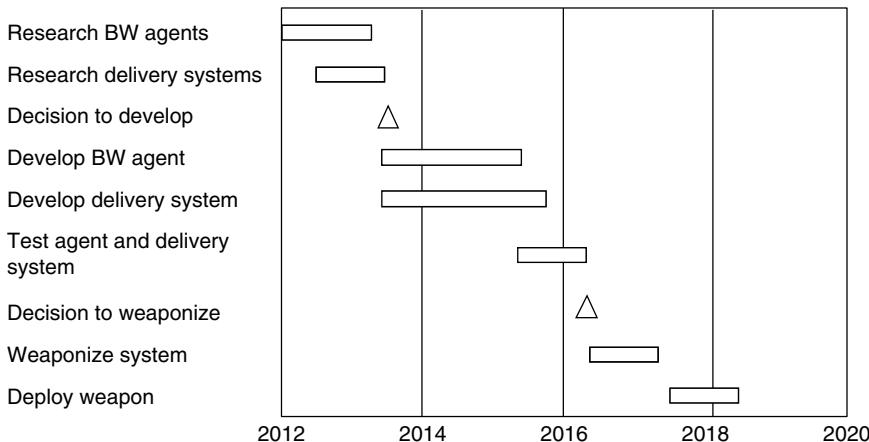
The collateral models in figures 10.12 through 10.14 are examples of the three general types—structural, functional, and process—used in systems analysis. Figure 10.12 is a structural model. Figure 10.13 has both structural and functional components. Figure 10.14 is both a process and a functional model. In analyzing complex systems, all three types are likely to be used.

These models, taken together, allow an analyst to answer the customer's original question. But they can also answer a wide range of customer questions. A model like the one in figure 10.13 can help determine the likely use and targets of the deployed

BW system. The model in figure 10.14 can help determine what stage the program is in and can help the customer with timing political, economic, or military action to halt the program or roll it back.

In practice, these models would be used together in an iterative analysis process (covered in chapters 11 and 12). But as a basic example of how the iterative approach works in filling knowledge gaps of the target, we can begin with the generic model in figure 10.10. From this starting point, an analyst might create the test process sub-model in figure 10.11. Prompted by the recognition that a BW testing program must have a test site, you would ask collectors to search for test areas having associated animal pens and certain patterns of biological sensor deployment nearby. The next logical request would be for collectors to search for a carcass disposal area. Assuming the effort is successful, you can create a collateral model—a map display like that shown in figure 10.13. Based on observation of activity at the test site and disposal area, the chronological model shown in figure 10.14 can be refined.

FIGURE 10.14 ■ Chronological Model of Monopolitarian Biological Weapons Development



ALTERNATIVE AND COMPETITIVE TARGET FRAMEWORKS

Alternative and competitive target frameworks are somewhat different things, though they are frequently confused with each other. Let's look at them in turn.

Alternative Frameworks

It is important to keep more than one target framework in mind, especially as conflicting or contradictory intelligence information is collected. The Iraqi WMD Commission noted, “The disciplined use of alternative hypotheses could have helped counter the natural cognitive tendency to force new information into existing

paradigms.”¹¹ As law professor David Schum writes, “The generation of new ideas in fact investigation usually rests upon arranging or juxtaposing our thoughts and evidence in different ways.”¹² Multiple alternative models accomplish that. And the more inclusive when defining alternative models (drawing in contributions from other stakeholders), the better.

In studies listing the analytic pitfalls that hampered past assessments, one of the most prevalent is failure to consider alternative scenarios, hypotheses, or models.¹³ Historically, three issues have been known to interfere with analysts developing alternative target frameworks:

- *Ego.* Former director of national intelligence Mike McConnell once observed that analysts inherently dislike alternative, dissenting, or competitive views.¹⁴
- *Time.* Analysts are usually facing tight deadlines. They must resist the temptation to go with the model that best fits the evidence without considering alternatives.
- *The customer.* When presented with two or more target frameworks, customers will tend to choose the one they like best, which may or may not be the most likely model.

The target-centric approach is intended to mitigate the effects of these issues. Ego is the easiest to deal with. From the beginning, analysts should understand that it’s not *their* model. It’s a shared model, to which all parties are expected to contribute, including suggesting alternative models. Moreover, as the facilitator of the process, it is the analyst’s responsibility to establish a tone of setting egos aside and of conveying to all participants, including the customer, that time spent up front developing alternative models is time saved at the end. It will keep them from committing to the wrong model in haste.

Time and tight deadlines become less of a problem when collectors are part of the team; and at all times, the customer has access to the most current models (including alternatives). Finally, the customer, having been involved in the process from the beginning, expects changes in the models to occur over time. (They may still choose the model they prefer over the most likely one, but they do so with more knowledge than if they had not been part of the process.)

A number of formal alternative analysis methodologies have been defined and given names such as “analysis of competing hypotheses” (see chapter 11), “argument mapping,” “signpost analysis,” and “challenge analysis.” These are discussed in detail in the book *Structured Analytic Techniques for Intelligence Analysis*, by Heuer and Pherson.¹⁵ Alternative analysis looks at a broader range of possible target frameworks and challenges the assumptions underlying a single model. We naturally tend to search for facts that confirm existing hypotheses and to prematurely discard alternatives. These formal methodologies challenge assumptions and hypotheses and identify alternative outcomes.¹⁶

Some organizations, in an effort to force alternative analysis, will set up separate teams to do “alternative analysis”—though, technically, that is competitive analysis (discussed next) done within the same organization.

Competitive Frameworks

It is well established in intelligence that, if you can afford the resources, you should have independent groups providing competing analyses. This is because intelligence deals with uncertainty. Different analysts, given the same set of facts, can come to different conclusions. The US intelligence community, as a result of its size and the presence of analysis groups in most of its sixteen members, has done competitive analysis for years. Chapter 6 described the Team A/Team B competitive national intelligence estimates that were clumsily executed in 1976. The 2021 *Global Trends* report cited in chapter 17 describes five competitive models of the future—only one of which (if any) could come true.

Sometimes the competitive framework is provided by the intelligence community in response to one created by the policymakers. That happened in the events leading up to the 1982 Lebanon debacle, described in chapter 8. As noted there, the Washington policymaking community was ignoring intelligence warnings about the dangerous situation in Lebanon. It envisioned Lebanon as a potential role model for future Middle East governments.¹⁷ Following that policy, the United States committed Marines to Lebanon in an ambitious attempt to end a civil war, to force occupying Israeli and Syrian armies out of Lebanon, and to establish a stable government. The policy was based on the target framework shown on the left side of table 10.1.

The intelligence community regarded the policymaker view not as an analysis to support policy decisions, but as a series of unverified assumptions. So it provided a competing framework, shown on the right in table 10.1. In contrast to the policymaker’s assumptions, this view was a series of analytic judgements based on facts.

Unfortunately, the policymaker view prevailed—for a time. Eighteen months later, the US administration withdrew from Lebanon, its policy discredited and its reputation damaged, with more than 250 Americans dead, most of them Marines killed in a terrorist bombing.

An analyst should at least consider all possible alternative or competitive target models—a point to which we’ll return in later chapters. The model of a situation that isn’t included may be the correct one. For instance, chapter 23 contains some alternative ones that were not considered in the October 2002 NIE on Iraq’s weapons of mass destruction. The NIE model was based on an invalid assumption: that because Saddam Hussein was stonewalling on inspections and concealing evidence of WMD, he must have WMD somewhere. The opposite possibility—that he *didn’t* have WMD and didn’t want his opponents in the region to know that fact—simply wasn’t considered.

TABLE 10.1 ■ Competitive Target Frameworks of the Lebanon Situation in 1982

Policymakers	Intelligence Analysts
We can negotiate speedy Israeli and Syrian withdrawals from Lebanon.	President Assad won't pull Syrian troops out unless convinced that he will be attacked militarily.
Lebanon can be unified under a stable government.	Lebanon in effect has no borders, and you can't say what a citizen is.
President Gemayel can influence events in Lebanon.	Gemayel doesn't control most of Beirut, and even the Christians aren't all behind him.
We have five military factions to deal with: Christian Phalange, Muslim militia, Syrian, Palestine Liberation Organization, and Israeli forces.	There are forty militias operating in West Beirut alone.
The Marines are peacekeepers.	The Marines are targets.

THE DYNAMIC FRAMEWORK

The target framework is dynamic. The issue usually changes over time, and target frameworks always do. As noted earlier, target deconstruction is an iterative process. It is seldom completely finished and will need to be revisited as new information comes to light. The situation in Lebanon has changed almost every year since 1982. Only one item in table 10.1 has stayed unchanged over those four decades: Lebanon *still* in effect has no borders, and you can't say what a citizen is.

SUMMARY

Creating a target framework begins with defining the relevant system. A system model can be a structural, functional, or process model, or any combination. The next step is to select generic models or model templates to populate with facts about the target. This set of models constitutes the target framework, a fundamental conceptual framework used in intelligence analysis, that relies on a deconstruction process. It resembles the issue decomposition process discussed in chapter 8, but it starts from a top-level view of the target, instead of the issue. Once the framework has been created, it is made specific by being populated with intelligence about the target.

Most target framework deconstructions take the form of a hierarchy: a structural or functional breakdown. A clandestine network, a facility, or a weapons system are examples. A hierarchy can begin from the instruments of national or organizational power and the effects of their use. Viewed from both the opponent's actions and the effects perspectives, there are usually six PMESII factors to consider. Target frameworks can be created by relying on any of those factors or can be a composite.

A target framework can comprise many different target models. Process models, which describe a sequence of events or activities that produce results, are often used to assess the progress of a political, military, economic, or social program. Submodels provide an in-depth look at parts of a target framework. Collateral models provide different perspectives of the target—structural, functional, or process views, for example.

Alternative and competitive target frameworks are an essential part of the process. Properly used, they help the analyst deal with uncertainty and the natural tendency to confirm existing hypotheses and prematurely discard alternatives. But they take time to create, analysts find it difficult to change or challenge existing judgments, and alternative models give policymakers the option to select the conclusion they prefer—which may or may not be the best choice. The target-centric approach specifically addresses these issues.

Having defined the intelligence issue and the relevant target, and constructed a target framework, the next question to address is this: "What do we need to learn about the target that our customers do not already know?" Answering that question involves doing some analysis, the subject of the next chapter.

CRITICAL THINKING QUESTIONS

1. Choose one of the six PMESII top-level models for Azerbaijan listed in this chapter and create a target deconstruction model for it (going down at least one level, two if possible).
2. Figure 10.9 shows that Azeri internet access grew steadily until 2014, when it suddenly hit a plateau. Can you determine why that happened, or develop one or two hypotheses as to why?
3. Generic target frameworks are commonly used in all types of analysis, even when not explicitly stated. There are instances, though, when all of the existing generic target frameworks don't apply, and using them can result in the wrong conclusion. Can you provide at least one example? Explain how using a generic framework would lead to an erroneous analysis for your example(s).

NOTES

1. US Joint Forces Command, *Commander's Handbook for Attack the Network* (Suffolk, VA: Joint Warfighting Center, 2011), III-5, http://www.dtic.mil/doctrine/doctrine/jwfc/atn_hbk.pdf.
2. Jason U. Manosevitz, "Needed: More Thinking about Conceptual Frameworks for Analysis—The Case of Influence," *Studies in Intelligence* 57, no. 4 (December 2013), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-57-no-4/pdfs/Manosevitz-Focusing Conceptual%20Frameworks-Dec2013.pdf>.
3. David A. Baldwin, "Power and International Relations," in *Handbook of International Relations*, ed. Walter Carlsnaes, Thomas Risse, and Beth A. Simmons (Newbury Park, CA: Sage, 2013), 275.
4. Ibid.
5. Vivian Salama and Warren P. Strobel, "Four U.S. Intelligence Agencies Produced Extensive Reports on Afghanistan, but All Failed to Predict Kabul's Rapid Collapse," *Wall Street Journal*, October 28, 2021, <https://www.wsj.com/articles/four-u-s-intelligence-agencies-produced-extensive-reports-on-afghanistan-but-all-failed-to-predict-kabuls-rapid-collapse-11635415201>.
6. Anthony H. Cordesman, "The Reasons for the Collapse of Afghan Forces," Center for Strategic and International Studies, August 17, 2021, <https://www.csis.org/analysis/reasons-collapse-afghan-forces>.
7. Michael Peck, "Singapore: The Battle That Destroyed the British Empire in Asia," *The National Interest*, February 17, 2017, <https://nationalinterest.org/blog/the-buzz/singapore-the-battle-destroyed-the-british-empire-asia-19482#:~:text=Perhaps%20the%20biggest%20consequence%20of%20the%20fall%20of,Asian%20guns%20left%20their%20mark%20on%20colonial%20subjects>.
8. Cordesman, "The Reasons for the Collapse of Afghan Forces."
9. Michael G. Archuleta, Michael S. Bland, Tsu-Pin Duann, and Alan B. Tucker, "Proliferation Profile Assessment of Emerging Biological Weapons Threats," Research Paper, Directorate of Research, Air Command and Staff College, April 1996.
10. Ibid.
11. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, chapter 1, https://fas.org/irp/offdocs/wmd_report.pdf.
12. David A. Schum, "On the Properties, Uses, Discovery, and Marshaling of Evidence in Intelligence Analysis," Lecture to the SRS Intelligence Analysis Seminar, Tucson, AZ, February 15, 2001.
13. Willis C. Armstrong, William Leonhart, William J. McCaffrey, and Herbert C. Rothenberg, "The Hazards of Single-Outcome Forecasting," in *Inside CIA's Private World*, ed. H. Bradford Westerfield (New Haven, CT: Yale University Press, 1995), 241–42.

14. William J. Lahneman, *The Future of Intelligence Analysis*, Center for International and Security Studies at Maryland, Final Report, vol. I [March 10, 2006], E-6.
15. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2011).
16. "Rethinking Alternative Analysis to Address Transnational Threats," *Kent School Occasional Papers* 3, no. 2 [October 2004].
17. David Kennedy and Leslie Brunetta, "Lebanon and the Intelligence Community," Case Study C15-88-859.0 (Cambridge, MA: Kennedy School of Government, Harvard University, 1988).

11

ANALYZING EXISTING INTELLIGENCE

Chapters 8, 9, and 10 addressed the importance of a well-defined issue and the use of conceptual frameworks for creating a target framework, beginning with a set of generic models. This chapter describes the next phase of analysis: populating the generic target model set with existing and incoming intelligence, a process sometimes called *collation*. We'll discuss the importance of existing pieces of intelligence, both *finished* and *raw*,¹ and how best to think about sources of new raw data. We'll talk about how credentials of evidence must be established, introduce widely used informal methods of combining evidence, and touch on structured argumentation as a formal methodology for that. Analysts need to be familiar with all of these concepts in order to handle the collation process.

In intelligence analysis, collation is the organizing of relevant information in a coherent way, taking source and context into consideration. It involves evaluating the information for *relevance* and *credibility*, and then incorporating it into the target model.

Analysts generally go through the actions described here, though they may not think about them as separate steps and aren't likely to do them in the order presented. They nevertheless almost always do the following:

- Review existing finished intelligence about the target and examine existing raw intelligence.
- Acquire new raw intelligence.
- Evaluate the new raw intelligence.
- Combine the intelligence from all sources into the generic target framework.

We'll go through each of these actions in turn.

REVIEWING EXISTING FINISHED INTELLIGENCE

There are few truly new issues. Before starting a collection effort, analysts should ensure they are aware of what has already been found on the issue. Information gathering to create or revise the initial target model begins with the existing knowledge base. The databases of all intelligence organizations include finished intelligence reports as well as many specialized data files on specific topics. Large commercial firms typically have comparable facilities in-house, or they depend on commercially available databases.

A literature search should be the analyst's first research activity. The purpose is both to establish the current state of knowledge—that is, to understand the existing model(s) of the target—and to identify controversies and disagreements surrounding the target model. This is an essential step, yet it can be a dangerous one for the novice analyst. The existing intelligence should not be accepted automatically as fact. The danger is that, in conducting the search, there is a natural tendency to adopt a preexisting target model.² In this case, premature closure, or a bias toward the status quo, can tempt a novice to keep the existing model even when evidence indicates that a different model may be more appropriate. Few experienced analysts would blithely accept the results of earlier studies on a topic, though they would know exactly what the studies found.

To counter the tendency toward premature closure, it's important to do a key assumptions check on the existing model(s). Much like the key assumptions check in defining the intelligence issue, here the analyst examines the target models focusing on somewhat different topics: Do the existing analytic conclusions about the target appear to be valid? What are the premises on which these conclusions rest, and do they appear to be valid as well? Has the underlying situation changed so that the premises may no longer apply?

Once the finished reports are in hand, an experienced analyst will next review all the relevant existing raw intelligence data. Few things can ruin an analyst's reputation faster than sending collectors after information that is already in the organization's files or, worse, is publicly available.

ACQUIRING RAW INTELLIGENCE

Most texts on intelligence sources, because of historical precedent, are organized around some version of the five major "INTs" perspective depicted in figure 11.1. The US intelligence community divided the collection methods using the "INT" (short for *intelligence*) disciplines to define the areas of responsibility of large collection organizations such as the National Geospatial-Intelligence Agency and the National Security Agency. As a result, INT names are the result of bureaucratic initiatives, which means there are varying opinions and quibbles about whether sources are properly named and, indeed, whether one source or another even should be termed an INT. Nevertheless, it's important to understand this division before we turn to a more helpful view that has more relevance for intelligence analysts.

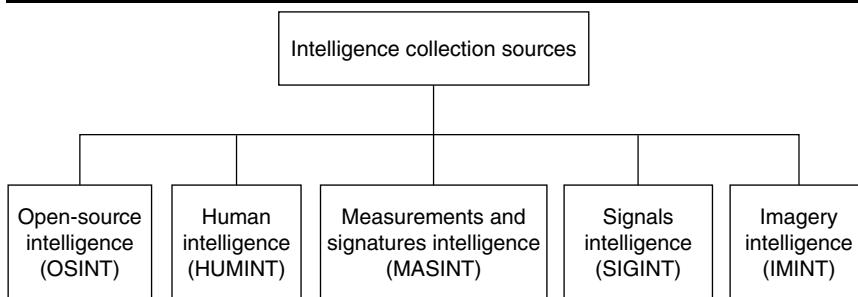
To recap, the standard definitions of each collection INT are as follows:

- *Open-source intelligence (OSINT)*. Intelligence derived from information openly available within the public domain
- *Human intelligence (HUMINT)*. Intelligence derived from information collected from and provided by human sources

- *Measurements and signatures intelligence (MASINT)*. Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angular, spatial, wavelength, time dependence, modulation, and hydromagnetic) derived from specific technical sensors
- *Signals intelligence (SIGINT)*. Intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence
- *Imagery intelligence (IMINT)*. Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electrooptics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced electronically on display devices or other media

Although not shown in the top-level taxonomy of figure 11.1, signals intelligence (SIGINT) is divided into three distinct “INTs”: communications intelligence (COMINT), electronics intelligence (ELINT), and telemetry interception; the latter is typically called *foreign instrumentation signals intelligence*, or FISINT. The lumping of COMINT, ELINT, and FISINT together as SIGINT is usually defended as logical because they have in common the interception of some kind of signal transmitted by the target. But some MASINT sensors rely on a signal transmitted by the target, as well. Plenty of observers would argue that SIGINT is in fact too general a term to use, when in most cases it means COMINT. Furthermore, it is common practice to have “GEOINT” instead of “IMINT” appear in the diagram. But as chapter 20 will point out, geospatial intelligence is an all-source technique for synthesizing and analyzing a target model, not a collection INT.

FIGURE 11.1 ■ The US Collection Taxonomy



You can begin to see the reasons for confusion and debates that occur among newly minted intelligence professionals surrounding the official collection paradigm. More in-depth and detailed discussions are contained in two companion books: Robert Clark’s *Intelligence Collection* (2014) and Mark Lowenthal and Robert Clark’s *The Five Disciplines of Intelligence Collection* (2015).

The taxonomy approach in this book is quite different. It strives for a breakout that focuses on the nature of the material collected and processed, rather than on the collection means. Figure 11.2 illustrates this view. It divides intelligence collection into two major source types: literal and nonliteral (including a prominent new form of literal intelligence: cyber collection).

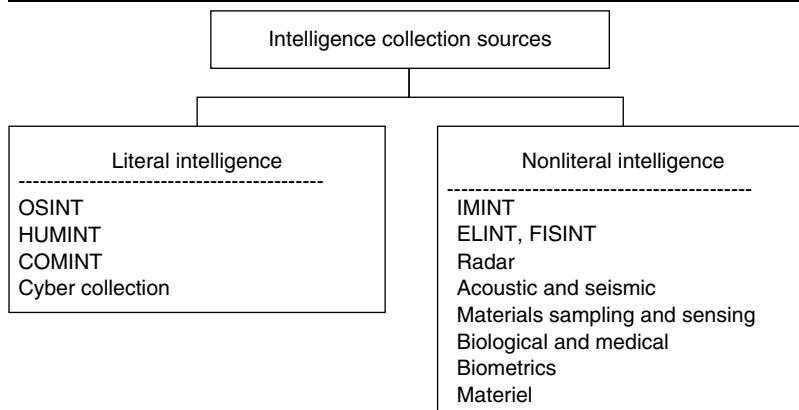
Traditional OSINT, HUMINT, and COMINT collection are concerned mainly with *literal* information, that is, information in a form that humans use for communication. The basic product and the general methods for collecting and analyzing literal information are usually well understood by intelligence analysts and their customers. The material requires no special exploitation after the processing step (language translation, for example) to be understood. It literally speaks for itself.

Nonliteral information, in contrast, usually requires special processing and exploitation in order for analysts and customers to make use of it.

The logic of this division has been affirmed by other intelligence writers. British author Michael Herman observed that there are two basic types of collection: One produces evidence in the form of observations and measurements of things (nonliteral), and one produces access to human thought processes (literal).³

It is not a completely “clean” separation. An important part of COMINT—traffic analysis—is not literal information; it depends on processing and interpretation. HUMINT sources are used in materials and materiel collection, which provides nonliteral intelligence. And cyber collection sometimes can provide nonliteral intelligence. Overlaps will occur no matter what boundaries are selected.

FIGURE 11.2 ■ An Analyst’s View of the Collection Taxonomy



Why use this division? Because analytic success requires understanding the sources of intelligence and the nature and limitations of the information available from them; as we’ll see, the limits and pitfalls differ substantially between literal and nonliteral intelligence. Raw intelligence must be treated differently, depending on which category it falls into. As a simple example, analysts and customers, if given access to the

original raw material (and with language and cultural expertise), can confirm or challenge the interpretation of OSINT, COMINT, HUMINT, and cyber collection. That is not true of nonliteral information where the same analysts and customers must rely on the processor/exploiter's judgment. There is some discomfort in that dependence. But interpreting a hyperspectral image or an ELINT recording takes special expertise that few of us have. The good news is that a single data source seldom provides everything needed to populate a model of a complex target. Rather, a wide range of sources must be called on—in part to reduce the chances of being misled by a single source.

One source of intelligence now dominates for most analysts. The amount of US intelligence derived from publicly available sources, or OSINT, has been estimated at around 80 percent.⁴ This is in no small part due to social media, so much so that it now is occasionally labeled as a separate INT, called SOCMINT.⁵

The automation of data handling has been a major boon to analysts. Information collected from around the globe arrives at their desks through the classified network or in electronic message form, ready for review and often presorted based on keyword searches. A downside of this, however, is the tendency to treat all information in the same way. In some cases, the analyst does not know what collection source provided the information; after all, everything looks alike on the display screen. And information must be treated differently depending on its source. Unclassified internet sources, for example, are notoriously unreliable. No matter the source, all information must be evaluated before it is synthesized into the target model—the subject to which we now turn.

EVALUATING EVIDENCE

The fundamental task in weighing evidence is determining its credibility—its completeness and soundness. In the end, this involves subjective judgments that the analyst usually has to make, often with help from collectors and customers. (Helpful insights on reliability are contained in the two texts on intelligence collection cited in the previous section.)

The CIA's *Tradecraft Primer* describes a methodology for evaluating information validity, called the *quality of information check*. Its purpose is described as follows:

Weighing the validity of sources is a key feature of any critical thinking. Moreover, establishing how much confidence one puts in analytic judgments should ultimately rest on how accurate and reliable the information base is. Hence, checking the quality of information used in intelligence analysis is an ongoing, continuous process. Having multiple sources on an issue is not a substitute for having good information that has been thoroughly examined. Analysts should perform periodic checks of the information base for their analytic judgments. Otherwise, important analytic judgments can become anchored to weak information, and any "caveats" attached to those judgments in the past can be forgotten or ignored over time.⁶

The quality of information check is described in more detail in the *Tradecraft Primer* and in other publications. Here, we discuss an alternative methodology for weighing evidence that entails three steps: evaluating the source, evaluating the communications channel through which the information arrives, and evaluating the evidence itself.

At the heart of the evaluation process is one of the oldest analytic principles, dating back to the fourteenth century, called Occam's razor. The name comes from William of Occam, who said, "It is vain to do with more what can be done with fewer."⁷ It requires explaining your observations with the fewest possible hypotheses. In other words, choose the simplest explanation that fits the facts at hand. In modern-day English, we know this as the KISS principle: Keep it simple, stupid! Possibly the most common example of Occam's razor is the advice given as the first remedy when a piece of electronic equipment doesn't work: Check to see if it is plugged in or if the battery is dead.

Occam's razor is not an infallible principle; occasionally the correct explanation for a given set of facts is complex or convoluted. And counterintelligence, especially denial and deception, is a possibility that the sciences tend not to have to contend with. However, it is possible to make data fit almost any desired conclusion, especially by selectively discarding inconvenient facts. So the razor is a basic but valuable part of the analyst's toolkit.

Evaluating the Source

Accept nothing at face value. Evaluate the origin of the evidence carefully and beware of potential motives. Evaluating the source involves answering three questions:

- Is the source competent (knowledgeable about the information being given)?
- Did the source have the access needed to get the information?
- Does the source have a vested interest or bias?

In the HUMINT business, this is called determining *bona fides* for human sources. Even when not dealing with HUMINT, these questions must be asked.

Competence

The Anglo-American judicial system deals effectively with competence: It allows witnesses to describe what they observed with their senses because, absent disability, people are presumed competent to sense things. The judicial system does not allow witnesses to *interpret* what they sensed unless they are qualified as experts in such interpretation.

Intelligence source evaluators must apply the same criteria. It is easy, in a raw intelligence report, to accept not only the source's observations but also the inferences the

source has drawn. Always ask: What was the basis for this conclusion? If no satisfactory answer comes forth, use the source's conclusions with caution or not at all.

A radar expert talking about an airborne intercept radar performance is credible. If he goes on to describe the aircraft performance, he is considerably less credible. An economist assessing inflation prospects in a country has credibility; if she goes on to assess the likely political impact of the inflation, the analyst should be skeptical.

Access

Access can be a critical issue in source evaluation. When there is any reason to be suspicious, check whether the source might not have had the claimed access. Lawyers know that rule well. In the legal world, checks on source access arise regularly in witness cross-examinations, as the next old but celebrated example illustrates.

BOX 11.1 THE ALMANAC TRIAL

The "Almanac Trial" of 1858 was so famous in the United States that there is a Norman Rockwell painting of the defense attorney in the Rockwell museum in Massachusetts. That attorney was Abraham Lincoln. It was the dying wish of an old friend that Lincoln represent his friend's son, Duff Armstrong, who was on trial for murder. Lincoln gave his client a tough, artful, and ultimately successful defense. But the trial's highlight came during cross-examination, when Lincoln consulted an almanac to discredit the prosecution witness who claimed that he saw the murder clearly because the moon was high in the sky. The 1857 almanac, which Lincoln held up for the jury, showed that the moon was lower on the horizon, and the witness's access—that is, his ability to see the murder—was called into question.⁸ The jury acquitted.

Sometimes the smallest distinction may matter when considering access. A now infamous mistake was made when CIA analysts prepared the NIE concerning possible Iraqi weapons of mass destruction in 2002. The source, codenamed Curveball (discussed in chapter 23) was assumed reliable because his knowledge was detailed and technically accurate, and part of it was corroborated by another source's reporting. But, as a CIA group chief later pointed out, the corroborating information simply established that Curveball had been to a given location, not that he had any knowledge of biological warfare activities being conducted there.⁹

Vested Interest or Bias

In HUMINT, analysts occasionally encounter the "professional source" who sells information to as many bidders as possible and has an incentive to make it as interesting as possible. Even the densest sources quickly realize that more interesting information gets them more money.

Official reports from government organizations have a similar vested interest problem. Instead of giving them automatic credibility, be skeptical of the information. One seldom finds outright lies in such reports, but officials may occasionally distort or conceal facts to support their policy positions or to protect their personal interests. On occasion, for example, US researchers have provided their government intelligence organizations with distorted information about their foreign contacts. The typical method is to exaggerate the importance of their foreign counterparts' work as a ploy to encourage more government funding for their own. A report does not necessarily have more validity simply because it came from a citizen of one's own country rather than from an international source. Vested interest and bias are also common problems for analysts who deal with experts in the comparative modeling and benchmarking techniques discussed next.

In assessing systems that use advanced technologies, test and evaluation results are especially important because many techniques work in theory but not in practice. The usual approach is to compare systems or technology performance against one's own results of test and evaluation programs.

However, an intelligence organization faces a problem in using its own parent organization's (or country's) test and evaluation results: the possibility of contamination. Sometimes the results contain distortions or omit key points; occasionally they are fabricated. Unfortunately, an honestly conducted, objective test may be a rarity. Several reasons for this exist. Tests are frequently conducted to prove or disprove a preconceived notion and thus are slanted unconsciously. Some results are fabricated because they would otherwise show the vulnerability or the ineffectiveness of a system and because future procurement decisions often depend on the test outcomes.

Although the majority of contaminated cases probably are never discovered, history provides many examples of this issue. Chapter 15 discusses the details of Sims's continuous aim naval gunnery system, wherein the US Navy tested a proposed new technique for naval gunnery. The test was designed to confirm the preconceived notion that the technique would not work, rather than to legitimately evaluate a concept.

In addition to recognizing that your own organization's (or country's) research or test results may be contaminated, an analyst also must deal with the parallel problem: The target organization may have distorted or fabricated its research or trial results for similar reasons. In examining any test or evaluation results, begin by asking two questions:

- Did the testing organization have a major stake in the outcome (such as the threat that a program would be canceled due to negative results or the possibility that it would profit from positive results)?
- Did the *reported* outcome support the organization's position or interests?

If the answer to either or both questions is yes, be wary of accepting the validity of the research or test. In the pharmaceutical testing industry, for example, tests

have been conducted fraudulently or the results skewed to support the regulatory approval of the pharmaceutical.¹⁰ The results can be similarly distorted in other industries. The lesson here is that it is unwise to rely on such reports alone. In a more general sense, if a government or an organization makes an unsubstantiated claim that furthers the government's or organization's interests, it should be regarded with skepticism.

A different type of bias can occur when collection is focused on a particular intelligence issue. It comes from the fact that, when people look for something, they may find it, whether or not it's there. The Baader-Meinhof phenomenon occurs due to selective attention and confirmation bias. When attuned to a topic of interest, a person's brain subconsciously seeks out more information (selective attention). Finding more examples of the information causes the same brain to infer proof that what it has been attuned to is actually there (confirmation). In investigating suspected Iraqi chemical facilities prior to 2003, analysts concluded from imagery reporting that the level of activity had increased at the facilities. But the appearance of an increase in activity may simply have been a result of an increase in imagery collection and the analysts' focus on searching for the evidence to support their belief.¹¹

This section has presented a basic, top-level view of source credibility. David Schum and Jon Morris's 2007 article on evaluating human sources of intelligence analysis goes further.¹² They pose a set of twenty-five questions divided into four categories: source competence, veracity, objectivity, and observational sensitivity. The questions cover in more explicit detail the three questions posed in this section about competence, access, and vested interest.

Evaluating the Communications Channel

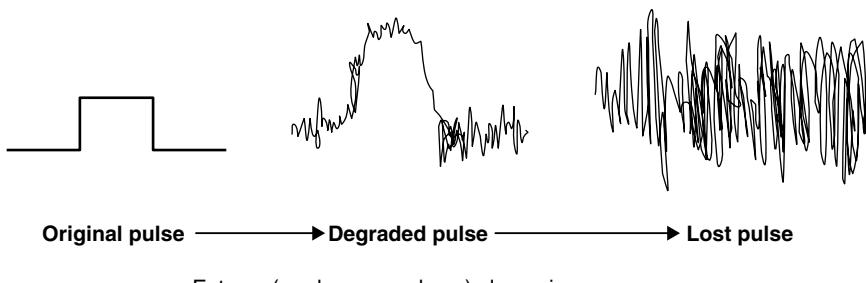
A second general rule of weighing evidence is to examine the communications channel through which the information arrives. In a large intelligence system, collection requirements move through a bureaucracy to a requirements officer, from there to a country desk, a field requirements officer, a SIGINT collector or a HUMINT case officer (for instance), then to an agent in the case of HUMINT; and the response then goes back through the reports chain. The message seldom gets through undistorted. This change is expressed in physics as the second law of thermodynamics. Entropy always increases with time. Simply stated, the degree of randomness increases steadily in any physical system. In intelligence, we consistently observe that the accuracy of a message through *any* communications system decreases with the length of the link or the number of intermediate nodes.

This same principle occurs in communications engineering; Claude Shannon describes it in his 1963 communications theory exposition.¹³ Just as heat always flows so that entropy (chaos, randomness) increases, on a digital communications line the originally crisp pulses will gradually lose their shape over distance and disappear into the noise, as illustrated in figure 11.3.

As is the case with an electronic communications channel being analyzed by applying Shannon's communications theory, some nodes in the intelligence communications channel contribute more "noise" than others. A message traveling down a noisy or distorted channel loses its original form and finally disappears in noise. The signal disappears completely or emerges as the wrong signal.

Many organizations have this problem. The result is often cited as "poor communication" and the effects can be observed in the large project curve (discussed in chapter 18). Over a long chain of human communication, the equivalent of figure 11.3 is this: The received message may bear little resemblance to what was originally sent. Informal gossip in any company makes an excellent illustration. What starts out as, "The company is considering new business strategies," down the line of twenty employees becomes, "everyone is getting fired and the doors to the company are closing."

FIGURE 11.3 ■ The Effect of Entropy on the Communications Channel



Entropy (randomness, chaos) always increases.

In the competitive intelligence world, analysts recognize the importance of the communications channel by using differentiating terms. *Primary sources* are for first-hand information, acquired through discussions or other interactions directly with a human source, and *secondary sources* refers to information learned through an intermediary, a publication, or online. This division does not consider the many gradations of reliability, and national intelligence organizations commonly do not differentiate between primary and secondary sources.

Rather, it is more important to consider the communications channel itself. Ask about the channel: What was it? Is this information being provided intentionally? If so, what part is true? Could it be deception or the sending of a message or signal? If it is a signal, what is the message, and what is the reason for it?

The communications channel is sometimes ignored in analyzing raw intelligence, but it is a critical piece of the reliability matrix. Part of the channel is the processing, exploitation, and analysis chain that raw intelligence goes through before reaching the analyst. It's not unheard of for the raw intelligence to be misinterpreted or misanalyzed as it passes through the chain. Organizational or personal biases can shape the interpretation and analysis, especially of literal intelligence. It's also possible for such biases to shape the analysis of nonliteral intelligence, but that is a more difficult product for all-source analysts and customers to challenge, as noted earlier.

The hearsay rule applied in judicial proceedings is a recognition of the application of Shannon's theory and of entropy in human affairs. Under the hearsay rule, a witness cannot testify about what a person said in order to prove the truth of what was said; in the court's view, the message has traveled through too many intermediate nodes to be credible. Entropy has an effect on the credibility of some intelligence, and the credibility degrades in direct proportion to the number of nodes traversed.

Entropy can have another effect in intelligence. An assertion that “*X* is a possibility” often, over time and through diverse communications channels, can become “*X* may be true,” then “*X* probably is the case,” and eventually “*X* is a fact,” without a shred of new evidence to support the assertion. We refer to this as the “creeping validity” problem. The Iraqi WMD Commission noted this as a major analytic failing; the premise that Iraq had hidden WMD became, over time, a presumption and eventually an unrebuttable conclusion.¹⁴

Earlier, we discussed bias in the source. Bias can also be a problem in the communications channel, as the following case illustrates.

BOX 11.2 THE FLAWED CHANNEL

Years ago, one US intelligence organization had the good fortune to obtain an audio tap into a highly classified foreign installation. The problem was that the audio was weak and not in English. One could barely discern that it was speech. One translator with very sharp ears was able to produce transcripts, however, and the product included exciting and particularly disturbing intelligence; several reports went to top levels of the US government.

The transcribed material was very good—too good, in fact, and technically inconsistent. It also presented a serious strategic problem: It indicated that a potential opponent had technical capabilities not previously known and well beyond what the United States could field in the event of a conflict.

When a target model conflicts with what is known, it's a clue that the model needs a closer look—which is exactly what was done. An investigation revealed that the translator wasn't translating; he was making it all up out of a fertile imagination and some knowledge of what was of current intelligence interest. The reports were withdrawn and the translator fired. On withdrawing the reports, the analytic community was reminded of a basic rule of intelligence: One of the best ways to get a customer to read a report is to retract it.

Evaluating the Credentials of Evidence

At the beginning of this chapter, we referred to evaluating information credibility and relevance as a collation activity. The credibility of tangible evidence depends on its authenticity and accuracy. For example, testimonial evidence credibility depends on the veracity, objectivity, memory, and observational competence of the testifier.¹⁵ Relevance means the information has value in answering a question or addressing an issue.

US government intelligence organizations have an established set of definitions to distinguish levels of credibility of intelligence:

- *Fact.* Verified information, something known to exist or to have happened
- *Direct information.* Information that is most likely factual because of the nature of the source (imagery, signal intercepts, and similar concrete observations)
- *Indirect information.* Information that may or may not be factual because of some doubt about the source's reliability, the source's lack of direct access, or the complex (nonconcrete) character of the contents (hearsay from clandestine sources, foreign government reports, or local media accounts)¹⁶

This division sounds suspiciously like the “primary” and “secondary” source construct used in competitive intelligence. It also downplays the real-world situation: that intelligence has a continuum of credibility, and that “direct information” such as signal intercepts or imagery can be misleading or false due to denial and deception (see chapter 13).

In weighing evidence, the usual approach is to ask three questions that are embedded in the oath that witnesses take before giving testimony in US courts:

- Is it true?
- Is it the whole truth?
- Is it nothing but the truth? (Is it relevant or significant?)

Is It True?

Is the evidence factual or opinion (someone else's analysis)? If it is opinion, question its validity unless the source quotes evidence to support it.

How does it fit with other evidence? The relating of evidence—how it fits in—is best determined in populating the target model. The data from different collection sources are most valuable when used together. The synergistic effect of combining data from many sources both strengthens the conclusions and increases the analyst's confidence in them. For example:

- HUMINT and COMINT data can be combined with ELINT data to yield a more complete picture of a radar.
- HUMINT and OSINT are often melded together to give a more comprehensive picture of people, programs, products, and facilities. This provides excellent background information to interpret data derived from COMINT and IMINT.

- Data on environmental conditions during weapons tests, acquired through specialized technical collection, can be used with ELINT and COMINT data obtained during the same test event to evaluate the capabilities of the opponent's systems.
- Identification of research institutes and their key scientists and researchers can be initially made through HUMINT, COMINT, or OSINT. Once the organization or individual has been identified by one intelligence collector, the other ones can often provide extensive additional information.
- Successful analysis of COMINT data may require correlating raw COMINT data with external information such as ELINT and IMINT, or with knowledge of operational or technical practices.

One of the best examples of synthesis comes from the extensive efforts used to assess the performance of ballistic missiles. Satellite photography of missiles on a launch pad is used to alert telemetry and COMINT collectors that a test is imminent so that they can start monitoring the test site. The same photography is compared with telemetry to check hypotheses about the weight and size of missiles. Radar tracking of the boost phase after launch is cross-checked with telemetry to determine booster performance, and the same cross-checks on reentry vehicles are used to estimate reentry vehicle size and weight more confidently.¹⁷

Is It the Whole Truth?

When asking this question, it is time to do source analysis. In HUMINT, this means looking at things such as past reporting history or a psychological profile (Is the source overly talkative? Failing to provide details when his story is challenged? Or weighing each word carefully?). We all have ad hoc profiles on the people we deal with based on first impressions or reputations, and so on. In intelligence, we usually need more—a personality profile of the sort discussed in chapter 9, for example.

An incomplete picture can mislead as much as an outright lie. An entertaining example occurred during the Cold War. Soviet missile guidance and control experts regularly visited their counterparts in the United States to do some informal elicitation. On one occasion, alerted to yet another impending Soviet visit, US intelligence, working with a leading outside expert, set up an elaborate display of a new and highly accurate missile guidance system in the expert's office. The Soviet visitors were impressed with the new technology, and the entire visit centered on the details of the guidance system, in particular, how it was manufactured. What the US expert did not mention was that for the system to work there were components that had to be machined to a precision beyond US or Soviet capabilities. It was a failed design. The problem would not become apparent until (as we heard later) the Soviets had spent many months and much money trying to replicate the design. The US expert told no lies—he simply omitted a critical truth.

Chapter 5 introduced the tension faced by investigative journalism, as exemplified by TV shows such as the long-running *60 Minutes*. A person or organization attempting to present an argument naturally tends *not* to present evidence for the counterargument. That's how advocacy works. Analysts often must take extra steps to find the missing evidence and complete the picture.

Is It Nothing but the Truth?

It is worthwhile here to distinguish between data and evidence. Data become evidence only when the data are relevant to the issue at hand. The simple test for relevance is whether it affects the likelihood of a hypothesis about the target. Does it help answer a question that has been asked? Or does it help answer a question that should be asked? As noted in chapter 8, the preliminary or initial guidance from customers seldom tells analysts what they really need to know—again, a primary reason to keep them in the loop through the target-centric process.

This relevance issue is the same as the “multiple pathologies” problem that doctors occasionally encounter: When two or more pathologies are present in a patient, the symptoms are mixed together, and diagnosing the separate illnesses becomes difficult.

As a simple example in intelligence, suppose the port authorities in Naples, Italy, discover a cache of arms and explosive devices in a cargo container on the docks. COMINT reporting later indicates that six members of a known terrorist group had met in a Naples harbor café on the day the illicit cargo was discovered. An analyst might be inclined to put the two facts together in the same target model of a planned terrorist act. But the two facts could be completely unrelated.

The converse mistake of force-fitting evidence into the model is the risk of discarding relevant evidence. Avoid discarding evidence simply because it doesn’t seem to fit the model. Such anomalies may indicate that something is wrong with the model, or that another model is more appropriate. Alternatively, as with the two-pathologies example, the evidence should be partitioned and fit into two distinct models.

Pitfalls in Evaluating Evidence

There are many pitfalls to avoid in weighing evidence. Seven that are especially important in intelligence follow:

Vividness Weighting

In general, the channel for communication of intelligence should be as short as possible, but could a short channel become a hazard? If the channel is too short, the result can be *vividness weighting*—the phenomenon in which evidence that is experienced directly is strongest (“seeing is believing”). Customers place the most weight on evidence they collect themselves—a dangerous trap that senior executives fall into repeatedly and that makes them vulnerable to deception. Strong and dynamic leaders are particularly susceptible: Franklin Roosevelt, Winston Churchill, and Henry Kissinger

are examples of statesmen who occasionally did their own collection and analysis, sometimes with unfortunate results. Michael Herman recounts how Churchill, reading Field Marshal Erwin Rommel's decrypted cables during World War II, concluded that the Germans were desperately short of supplies in North Africa. Basing his interpretation on this raw COMINT, Churchill pressed his generals to take the offensive against Rommel. Churchill did not realize what his own intelligence analysts could readily have told him: Rommel consistently exaggerated his shortages in order to bolster his demands for supplies and reinforcements.¹⁸

There is a danger in judging any evidence by its presentation. Statistics are the least persuasive form of evidence; abstract (general) text is next; concrete (specific, focused, exemplary) text is a more persuasive form still; and visual evidence, such as imagery or video, is the most persuasive. Of course, vividness can work to the advantage of a good analyst. Why not use the persuasive force of certain types of evidence to make the presentation of conclusions more effective with the customer?

Numerous examples exist of the powerful impact that vivid evidence can have. One such was the murder of *Wall Street Journal* reporter Daniel Pearl in Pakistan in February 2002. The video recording of the decapitation of Pearl evoked a strong public reaction. In August 2014, Daesh released videos of the beheading of US journalist James Foley; in January 2015, they released a video of the beheading of Japanese journalist Kenji Goto; and in February 2015, they broadcast the captured Jordanian pilot Muath al-Kasaesbeh being burned alive in a cage. All evoked strong reactions in the United States, Japan, Jordan, and other countries. Sometimes decision makers can be unduly affected by such vivid evidence. It can be argued that the subsequent measures several countries took against Daesh were harsher than would have been the case if the killings had not been presented by video.

Weighing Based on the Source

One of the most difficult traps for an analyst to avoid is weighing evidence based on its source. HUMINT operatives repeatedly value information gained from clandestine sources—the classic spy—above that from refugees, émigrés, and defectors. COMINT gained from an expensive emplaced telephone tap is valued (and protected from disclosure) above that gleaned from high-frequency radio communications (which almost anyone can monitor). The most common pitfall, however, is to devalue the significance of OSINT; being the most readily available, it is often deemed to be the least valuable. Using open sources well is a demanding analytic skill, and it can pay high dividends to those who have the patience to master it. It can provide warnings that one might not expect: The Open Source Center provided warning of the 2006 North Korean nuclear test based on openly available material.

It's easy to make the mistake of equating source with importance. If your organization has spent a sizable portion of its budget in collecting the material, you might be inclined to infer that its value can be measured by the cost of collecting it. But no competent analyst would ever make that mistake.

Favoring the Most Recent Evidence

Analysts often give the most recently acquired evidence the most weight—a phenomenon similar to vividness weighting. One caution on the danger of doing this is taken from the second law of thermodynamics, discussed earlier. For weighing evidence, it has a different slant. As figure 11.3 suggests, the value of information or the weight given it in a report tends to decrease with time. The freshest intelligence—crisp, clear, and the focus of an analyst’s attention—often has more influence than the fuzzy and half-remembered (but possibly more important) information that has traveled down the long lines of time. A good analyst must remember this tendency and compensate for it.

Favoring or Disfavoring the Unknown

It is hard to decide how much weight to give to answers when little or no information is available for or against each. Some analysts give an answer too much significance where evidence is absent; some give it too little. Former CIA analyst Richards Heuer Jr. cites this “absence of evidence” problem in the example of two groups of automobile mechanics who were given a choice of reasons why a car would not start, with the list of choices ending in “other.” The mechanics were told to estimate what percentage of failures was attributable to each reason. One group was given a list that omitted several of the reasons; they tended to over-weight the remaining reasons and under-weight the category “other.”¹⁹

Trusting Hearsay

A chief problem with much of HUMINT (though not including documents acquired through HUMINT) is that it is hearsay evidence; and as previously pointed out, the judiciary long ago learned to distrust hearsay for good reasons, including the biases of the source. Sources may deliberately distort or misinform because they want to influence policy or increase their value to the collector. Moreover, the analyst usually doesn’t have the nonverbal details of the conversation—the setting, the context, facial and body expressions—to aid judgment. The hearsay problem had severe consequences in the case of Curveball’s reporting on Iraqi biological weapons programs (detailed in chapter 23). US intelligence officers were not able to directly interrogate Curveball and observe his demeanor during interrogation. Had they been allowed to do so, they likely would have reached quite different conclusions about the validity of his reporting.

COMINT reporting, like HUMINT, is hearsay and has to be evaluated carefully for three reasons:

- Much interpretation goes into a COMINT report. The COMINT analyst who translates and interprets a conversation has to repeatedly make judgment calls about the material, based on past experience with the source and the culture. The analyst must, for example, consider that a message saying, “The semester begins in three more weeks. We’ve obtained 19 confirmations for

studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering”²⁰ may refer to a planned suicide attack by a terrorist group, not to the actual start of an academic semester.

- Some targets of COMINT know they are being monitored and deliberately use the collector as a conduit for deceptive information.
- Most important, people can be misinformed or lie. Saddam Hussein’s generals repeatedly lied to him about their military preparedness, and he in turn lied to them about WMD.²¹ COMINT can only report and interpret what people say, not the truth about what they say. Analysts have to use hearsay, but they must also weigh it accordingly.

Reliance on Expert Opinions

Expert opinion is often used as a tool for analyzing data and making estimates. Any intelligence community must often rely on its nation’s leading scientists, economists, and political and social scientists for insights into foreign developments. These authorities on a subject can and do make valuable contributions, and calls have been made to increase the US intelligence community’s use of outside expertise.²² But such expertise has to be used with caution, for a few reasons.

First, experts can have issues with objectivity. An analyst gets not only their expertise, but also their biases; there are those experts who have axes to grind or egos that convince them there is only one right answer (the one they have). British counterintelligence officer Peter Wright proffers an even more pessimistic opinion; he wrote that “on the big issues, the experts are very rarely right.”²³ They can be useful in pointing out flaws in logic; and their understanding of political, social, and economic situations in other countries often is superior to that of their intelligence community counterparts. But some studies have found that they are no better than simple statistical models at making predictions.²⁴

Also, more than a few scientific experts consulted by intelligence organizations have been guilty of report inflation at one time or another. When used as evaluators, the same can be true. Treat expert opinion as HUMINT and be wary when an expert makes extremely positive comments (“that foreign development is a stroke of genius!”) or extremely negative ones (“it can’t be done”). Similarly, in political, social, or economic analysis, experts may tend either to be overly impressed with or to disparage how another country or culture does something. In scientific and weapons intelligence, the negative comments often are tied to the idea of fundamental limits.

Fundamental limits are well known in physics: It is generally accepted that one can neither travel faster than the speed of light nor reduce the temperature of an object to absolute zero. Having tried an experiment or innovation and failed, a scientific expert is strongly tempted to conclude that “it can’t be done.” It is more reassuring to decide that something is impossible than to conclude that it is possible but that you failed to accomplish it.

British physicist R. V. Jones was the assistant director of Britain's Royal Air Force Intelligence Section during World War II and is widely regarded as the founder of the scientific intelligence discipline. During his tenure, Jones encountered several examples of the "it can't be done" syndrome from scientific experts. He called them "principles of impotence." Jones was told, for example, that "it is impossible to make a bulletproof fuel tank"; "radio waves cannot be generated in the centimeter band (above 3,000 MHz)"; and "photoconductive materials cannot be made to detect wavelengths longer than two microns."²⁵ All of these impossibilities later became realities. His most significant encounter with British scientific experts involved the V-2 rocket.

BOX 11.3 THE V-2 ROCKET

During 1943–1944, aerial photography of the German rocket test center at Peenemünde revealed the existence of a rocket about 45 feet long and 6 feet in diameter. As was the case with many other interesting analytic issues of World War II, this one fell to Jones to puzzle through.

British experts at the time were familiar only with rockets that burned cordite in a steel case. A simple calculation showed that a cordite-burning rocket of this size would weigh approximately 80 tons and would have to have a warhead weighing on the order of 10 tons to be worthwhile. To the British cabinet, the prospect of rockets as heavy as railroad locomotives carrying 10 tons of high explosives and landing on London was appalling.

In June 1944, a V-2 rocket crashed in Sweden, and British intelligence officers had an opportunity to examine the fragments. They reported that two liquids fueled the rocket and liquid oxygen was one of the fuels. Armed with this evidence, Jones was able to sort through the volume of conflicting HUMINT reports about the German rocket and to select the five reports that mentioned liquid oxygen. All five were consistent in attributing light weights to the rocket and warhead. Jones subsequently (and correctly) reported to the British war cabinet—over the objections of British rocket experts—that the V-2 weighed 12 tons and carried a 1-ton warhead.²⁶

Although experts have at times led us astray and generally fared poorly in this section, their contributions have value. Some say that they are harder to deceive. In the words of one author, "It is hard for one specialist to deceive another for very long."²⁷ By this view, deception (discussed in chapter 13) can be beaten more easily with expert help. Maybe. Many authorities in fields outside intelligence are not mentally prepared to look for deception. It is simply not part of their training.

One way to obviate issues with expert opinion is to tap more than one specialist. Using a panel of authorities to make analytic judgments is a common method of trying to reach conclusions or to sort through a complex array of interdisciplinary data. But

such panels have had mixed results. The quality of the conclusions reached depends on several variables, including the panel's

- Expertise
- Motivation to produce a quality product
- Understanding of the problem area to be addressed
- Effectiveness in working as a group

A major advantage of the target-centric approach is that it formalizes the process of obtaining independent opinions. It also lends itself readily to techniques, such as the *Delphi method*, for avoiding negative group dynamics. Delphi is a systematic version for reaching panel consensus by eliminating some of the traditional panel shortcomings. It uses anonymous inputs to help obtain an objective consensus from initially divergent expert opinion. One objective of the Delphi method is the encouragement, rather than the suppression, of conflicting or divergent opinions—specifically, the development of alternative target models. Participants explain their views, and others review these explanations absent the personality, status, and debating skills that are brought to bear in conferences. The Delphi method arrives at a consensus by pooling the two separate inputs to any estimate:

- Expert information or knowledge
- Good judgment, analysis, and reasoning

Although a Delphi participant may not initially be well informed on a given question, that person still can contribute judgment, analysis, and reasoning about the information and arguments that other respondents advance.

Where panels are used, several other techniques are available to make the input more effective. In general, the techniques apply whenever collaborative analytic efforts are used, as they inevitably are in the target-centric approach.

Premature Closure and Philosophical Predisposition

Premature closure contributed to each of the intelligence failures cited in chapter 1. It breaks several tenets of good problem solving, in particular the principle of postponing evaluation and judgment until all relevant data are available. Judicial systems have long recognized the importance of this principle; judges instruct jurors to wait until they have heard all the evidence, received final instructions, and discussed all the evidence among themselves before deciding the verdict. Both single-source and all-source analysts must guard against falling into the trap of reaching conclusions too early. For example, ELINT, COMINT, and GEOINT analysts can focus on one explanation for an intercept or an image and exclude others—fortunately, not a common occurrence, but it does happen.

Premature closure also has been described as “affirming conclusions,” based on the observation that people are inclined to verify or affirm their existing beliefs rather than modify or discredit them. One observer claims that “once the Intelligence Community becomes entrenched in its chosen frame, its conclusions are destined to be uncritically confirmed.”²⁸

The Iraqi WMD Commission identified what it described as a “textbook example” of premature closure. Iraq was attempting to acquire aluminum tubes, ostensibly for their Medusa rocket, and a CIA officer properly suggested that the CIA determine the precise rocket dimensions to determine if the tubes were in fact intended for Medusa. CIA management rejected the request because they had already concluded that Iraq was acquiring the tubes for gas centrifuges to support its nuclear weapons program.²⁹

The obvious danger of premature closure is that an analyst might make a bad assessment because the evidence is incomplete. But there is another critical danger: that when a situation is changing quickly or when a major, unprecedented event occurs, the analyst will become trapped by the judgments already made. It’s usually harder to revise an initial estimate than to make it. Intelligence analysts found that during the Cuban missile crisis in 1962 (a case continued in more detail in chapter 13).

BOX 11.4 THE CUBAN MISSILE CRISIS I

Few intelligence successes make headlines. Failures always do. One exception was the Cuban missile crisis, in which US intelligence services obtained information and made assessments that helped policymakers act in time to make a difference. The assessments would have been made sooner, however, except for the difficulty in changing a conclusion once it had been reached and the tendency to ignore the Cuban refugees who had “cried wolf” too often.

For some time before 1962, Cuban refugees had flooded Western intelligence services, embassies, and newspapers with stories of missiles being hidden in Cuba. When the reports about the deployment of medium-range ballistic missiles began to sift into the CIA and the Defense Intelligence Agency in 1962, they were by and large disregarded—intelligence analysts had heard such false reports too many times. One author has claimed that only as the weight of evidence from several independent sources, including photographic evidence and ship movement patterns, began to grow was it possible to change the collective mind of the intelligence community.³⁰

Though the potential of a nuclear war was averted, the Cuban missile crisis has occasionally been called an intelligence failure. After all, four times in the nine-month period leading up to the crisis, US NIEs assessed that Soviet activities in Cuba were meant to deter an American attack there, not to establish an offensive base in Cuba.³¹ But during that time, as Director of Central Intelligence John McCone later observed, the CIA had received 3,500 HUMINT reports, mostly from Cuban refugees claiming that Soviet missiles were on the island. A subsequent study by the President’s Foreign Intelligence Advisory Board concluded that only thirty-five of the reports were accurate. McCone himself estimated that only six of them were accurate.³²

The Cuban missile crisis illustrates the problem that Princeton University professor Klaus Knorr describes as “philosophical predisposition,” meaning a situation in which expectations fail to apply to the facts.³³ Before 1962, the Soviets had never deployed nuclear weapons outside their direct control, and US analysts assumed that they would not do so by deploying nuclear warhead–equipped missiles in Cuba. Thus, the analysts discounted information that contradicted this assumption. The counterintelligence technique of deception thrives on this tendency to ignore evidence that would disprove an existing assumption (a subject to which we return in chapter 13). Furthermore, once an intelligence agency makes a firm estimate, it has a propensity in future estimates to ignore or explain away conflicting information. This is why denial and deception succeed if one opponent can get the other to make an incorrect initial estimate.

Fortunately, several problem-solving approaches help to prevent premature closure and overcome the bias of philosophical predisposition in the sifting of data. Understanding the ways to combine different types of evidence, as discussed next, helps.

COMBINING THE EVIDENCE

In almost all cases, intelligence analysis involves combining disparate types of evidence. Analysts have to combine data to make qualitative judgments as to which conclusions the various data best support. Two common types are divergent and convergent evidence.

Divergent Evidence

Two items of evidence are said to be conflicting or *divergent* if one of them favors one conclusion and the other favors a different one.

Suppose that a HUMINT cable reports that the Chinese freighter *Kiang Kwan* left Shanghai bound for the Indian Ocean. A COMINT report on radio traffic from the *Kiang Kwan* as it left port states that the ship’s destination is Colombia. Ships seldom sail from Shanghai to Colombia via the Indian Ocean, so the two reports point to two different conclusions; they are divergent. Note that both items of divergent evidence can be true (for example, the ship could make an intermediate stop at an Indian Ocean port); they simply lead to differing conclusions. The evidence that Iraq was acquiring aluminum tubes that fit the dimensions of its Medusa rocket, cited earlier, diverged from the conclusion that the tubes were for gas centrifuges. But both conclusions nevertheless could have been true. The Iraqis could have purchased the tubes for both purposes.

In contrast, two items of evidence are *contradictory* if they say logically opposing things. A COMINT report says that the *Kiang Kwan* left Shanghai yesterday at 1800 hours; a HUMINT report says that the ship was in Singapore this morning. Given the distance between these ports and the maximum speed of merchant ships, only one report can be true.

Convergent Evidence

Two items of evidence are said to be *convergent* if they favor the same conclusion. A common type of convergent evidence is called *redundant*.

To understand the concept of redundancy, it helps to appreciate its importance in communications theory. Information comes to an analyst by several different channels. It often is incomplete, and it sometimes arrives in garbled form. And we know that entropy takes its toll on any information channel. In communications theory, redundancy is one way to improve the chances of getting the message right.

Redundant, or duplicative, evidence can have corroborative redundancy or cumulative redundancy. In both types, the weight of the evidence stacks up to reinforce a given conclusion. A simple example illustrates the distinction.

Corroborative Redundancy

Suppose an analyst is following clandestine arms transfer networks, and she receives two reports. A COMINT report indicates that a Chinese freighter carrying a contraband arms shipment will be at coordinates 05° 48' S, 39° 52' E on June 13 to transfer the arms to another ship. A separate HUMINT report says that the Chinese freighter *Kiang Kwan* will rendezvous for an arms transfer south of Pemba Island on June 13. Both reports say the same thing; a quick map check confirms that the coordinates lie near Pemba Island, off the Tanzanian coast. No new information (except the ship's name) is gained by the second report. The second report has value for corroboratory purposes and helps establish the validity of both sources of information.

The analogy in communications theory might occur when dealing with a noisy teletype channel. Message errors are not a concern when dealing with text only, because text has inherent redundancy: If “Chinese freighter will rendezvous” is sent, but the recipient gets the printout “Chinese frei3hter will rentezvous,” the message will probably be understood in spite of the errors. The coordinates of the rendezvous point, however, have less inherent redundancy. A message that has the coordinates “5 degrees 88 minutes South” clearly has an error, since minutes of latitude and longitude never exceed 59. However, it is unclear what the correct latitude should be. It is common practice to spell out or repeat numbers in such a message, or even to repeat the entire message, if a chance of a garble exists; that is, the sender introduces corroborative redundancy to ensure that the correct coordinates are received.

Cumulative Redundancy

Now, suppose instead that the HUMINT report in the previous example says that a Chinese freighter left port in Shanghai on May 21 carrying AK-47 rifles and ammunition destined for Tanzanian rebels. The report does not duplicate all the information contained in the COMINT report, but it adds credibility to both reports. Furthermore, it leads to a more detailed conclusion about the nature of the illicit arms transfer.

The HUMINT report, in this case, adds cumulative redundancy to the COMINT report. Both reports are given more weight, and a more complete estimate can be made than if only one report had been received.

Formal Methods for Evaluating and Combining Evidence

The preceding sections illustrate some ways of evaluating evidence. As evidence is evaluated, it must be combined and integrated into the target model. That usually is a straightforward process, learned through practice. But sometimes, it is important to demonstrate the logical process the analyst went through in reaching a conclusion based on the evidence.³⁴

The formal process of doing that is called *structured argumentation*. Formal structured argumentation approaches have been around at least since the seventeenth century. Two are discussed in the next section. (A number of other structured argumentation methods are used to produce anticipatory intelligence: Chapter 16 discusses influence trees and influence diagrams; scenario creation is covered in chapter 17.)

STRUCTURED ARGUMENTATION

Structured argumentation is an analytic methodology for both evaluating and combining evidence. It brings into the open and makes explicit the important steps in an argument and thereby makes it easier to evaluate the soundness of the conclusions reached.

The process begins with breaking down and organizing (decomposing) an issue into parts so that each one can be examined systematically, as discussed in earlier chapters. As analysts work through each part, they identify data requirements, state assumptions, define any terms or concepts, and collect and evaluate relevant information. Potential explanations or hypotheses are formulated and evaluated with empirical evidence, and information gaps are identified.

Perhaps the most popular structured argumentation method is analysis of competing hypotheses: identifying a set of hypotheses, and systematically evaluating raw intelligence for consistency or inconsistency with each hypothesis. Bayesian analysis is another, more complicated structured argumentation method, one that deals in the probabilities associated with observed events. Both methodologies help limit the potential for analytic miscalls. Both require some practice to master and can be time consuming to apply.

Analysis of Competing Hypotheses

Analysis of competing hypotheses (ACH) is one of the best-known structured argumentation techniques. It was developed by Richards Heuer Jr. during the 1970s and published in his book *Psychology of Intelligence Analysis*.

At any stage of the analysis process, it may become important to take a close look at competing hypotheses. These can arise in the issue definition phase, in developing the target model(s), or in identifying gaps in knowledge (discussed in chapter 12). ACH is a tool to aid judgment on important issues that require weighing of alternative explanations or conclusions. It helps overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult to achieve.

ACH is a simple model for how to think about a complex problem. It is an analytic process that identifies a complete (ideally, at least) set of hypotheses, systematically evaluates data that are consistent and inconsistent with each of them, and rejects those hypotheses that contain too much inconsistent data. The wrong way to go about the business is to pick out what appears to be the most likely hypothesis, then look at the available information from the point of view of whether or not it supports this hypothesis.

ACH is not appropriate for all types of analysis. It is most often used to analyze potential intelligence gaps about what is known, what is not known, and what the analyst still needs to know. The value of ACH is measured by the extent to which it helps the analyst to do the following:

- See the target from alternative perspectives.
- Look for additional relevant evidence that may not have initially seemed relevant.
- Question assumptions.
- Identify the most lucrative future areas of investigation.
- Generally stimulate systematic and creative thinking about the target.

To perform an ACH, Heuer recommends the following actions:

1. *Identify all possible hypotheses to be considered that answer your intelligence question. Use a group of analysts with different perspectives to brainstorm the possibilities.*
2. *List all significant evidence and arguments (including assumptions and logical deductions) for and against each hypothesis.*
3. *Prepare a matrix with hypotheses across the top and each piece of evidence on the side. Assess whether each piece of evidence is consistent, inconsistent, or not applicable to each hypothesis and its credibility and relevance to determine how much weight it should have in the analysis.*
4. *Refine the matrix and reconsider the hypotheses—in some cases, analysts will need to add new hypotheses and reexamine the information available. Identify gaps in the*

evidence that may need to be filled to refute hypotheses and consider the possibility of denial and deception.

5. Establish the relative likelihood of the hypotheses—those with the least number of inconsistent pieces of evidence should be considered most likely.
6. Analyze how sensitive the ACH results are to a few critical items of evidence. Consider how your conclusion would be affected if key evidence or arguments were wrong, misleading, or subject to a different interpretation. Double check the validity of key evidence and arguments that determine the outcome of your analysis.
7. Report conclusions. Include discussion of alternatives that were considered and why they were rejected.
8. Identify milestones for future observation that may indicate events are taking a different course than expected.³⁵

Bayesian Techniques for Combining Evidence

By the early part of the eighteenth century, mathematicians had solved what was called the “forward probability” problem: When all the facts about a situation are known, what is the probability of a given event happening? For example, if you know the number of black and white balls in a bag, it is easy to determine the probability of drawing a black ball out of the bag. In the middle of that century, British mathematician and Presbyterian minister Thomas Bayes dealt with the “inverse problem”: Given that an event has occurred, what can be determined about the situation that caused the event? Continuing the bag of balls example, if you draw three black balls and one white ball out of a bag, what estimate can you make about the relative number of black and white balls in the bag? And how does your estimate change if you then draw a white ball out? Intelligence analysts find this of far more interest than the forward probability problem, because they often must make judgments about an underlying situation from observing the events that the situation causes. Bayes developed a formula for the answer that bears his name: Bayes’ rule.

The application of Bayes’ rule is called, not surprisingly, *Bayesian analysis*. It uses incoming data to modify previously estimated probabilities. It therefore can be used to narrow the error bounds on estimates. Each new piece of information is evaluated and combined with prior historical or subjective assessments of the probability of an event to determine whether its occurrence has now been made more or less likely and by how much. Bayesian analysis can also be used to compute the likelihood that the observed data are attributable to particular causes. One advantage claimed for Bayesian analysis is its ability to blend the subjective probability judgments of experts with historical frequencies and the latest sample evidence.

While Bayesian analysis can be a powerful tool for fitting new intelligence into an existing target framework, it has been observed that it is neither easy to teach nor easy to apply in practice.³⁶ In the decade since that observation was made, software packages have become available that make Bayesian analysis more accessible. For those interested in learning more about it, an excellent introduction and tutorial has been prepared by Kristan Wheaton, Jennifer Lee, and Hemangini Deshmukh of Mercyhurst College.³⁷

A NOTE ABOUT THE ROLE OF INFORMATION TECHNOLOGY

It may be impossible for new analysts today to appreciate the markedly different work environment that their counterparts faced forty years ago. Incoming intelligence arrived at the analyst's desk in hard copy, to be scanned, marked up, and placed in file drawers. Details about intelligence targets—installations, persons, and organizations—were created in written form and often kept on 5" × 7" cards in card catalog boxes. Less tidy analysts “filed” their most interesting raw intelligence on the top of their desks and filing cabinets, sometimes in stacks over two feet high.

A major consequence of the information explosion is that analysts must handle “big data” in collating and analyzing intelligence. *Big data* is defined as “datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze.”³⁸ It is about more than just size, though. The challenge is to deal with datasets so large and complex that they become difficult to process using existing database management tools or traditional data processing applications.

Big data has been described as

*not a revolution but an evolution whose catalyst is the digitization of everything. Unfathomable amounts of resulting data must be stored and processed. And we are still using analytics to synthesize that data into information with meaning and value, just like we always have.*³⁹

For intelligence, it is more than just the “digitization of everything.” The new source material provided by social media, cell phone communications, and imaging systems, for example, has flooded intelligence data banks. Analysts have had to move from dealing primarily with structured data (tables, relational data) and unstructured data (raw text, images, video, and audio) to dealing with metadata (data about data). Although the flood is not readily addressed, the payoff is high. We can extract intelligence from these new sources that simply could not be acquired with the limited sources of previous years.

Analysts, inundated by the data deluge, have turned to information technology (IT) tools for extracting meaning from it. A wide range of such tools exists, including those for data visualization, pattern identification, statistical analysis, and simulation

modeling. Analysts with responsibility for counterterrorism, organized crime, counter narcotics, counterproliferation, or financial fraud can choose from commercially available tools such as Palantir, Analyst's Notebook, NetMap, Orion, or VisuaLinks to produce matrix and link diagrams, timeline charts, telephone toll charts, and similar pattern displays.⁴⁰ Tactical intelligence units, in both the military and law enforcement, find geospatial analysis tools to be essential.

Intelligence agencies also have in-house tools that replicate these capabilities. Depending on the analyst's specialty, some tools may be more relevant than others. All, though, have definite learning curves and their database structures are generally not compatible with each other. The result is that these tools are used less effectively than they might be, and the absence of a single standard platform hinders collaborative work across intelligence organizations.

In a completely different category are IT tools to support structured argumentation. Efforts have been made in recent years to incorporate a structured argumentation process into software to aid intelligence analysts. These promise to make structured argumentation useful for dealing with complex intelligence problems. Under Project GENOA, the Defense Advanced Research Projects Agency (DARPA) developed a tool named SEAS⁴¹ that was well conceived but did not gain wide acceptance. Subsequently, a proprietary tool to support the analysis of competing hypotheses, called ACH, was developed for the intelligence community. An open-source version of it, called Analysis of Competing Hypotheses, is available online.⁴²

SUMMARY

In gathering information for populating the target framework, analysts must start by reviewing existing finished and raw intelligence. This usually provides a picture of the current target model. A simple key assumptions check at this point is invaluable: Do the premises that underlie existing conclusions about the target seem to be valid?

Next, in a step often called collation, the analyst evaluates incoming raw intelligence and fits it into the target model. Raw intelligence is viewed and evaluated differently depending on whether it is literal or nonliteral. Literal sources include OSINT, COMINT, HUMINT, and cyber collection. Nonliteral sources involve several types of newer and highly focused collection techniques that depend heavily on processing, exploitation, and interpretation to turn the material into usable intelligence. Analysts and customers can independently assess literal source material, but nonliteral material requires judgments made by processors.

Fitting the information in requires a three-step process:

- Evaluating the source, by determining whether the source (a) is competent, that is, knowledgeable about the information being given; (b) had the access needed to get the information; and (c) has a vested interest or bias regarding the information provided.

- Evaluating the communications channel through which the information arrived. Information that passes through many intermediate points becomes distorted. Be aware of potential bias within the channel and also possible creeping validity.
- Evaluating the credentials of the evidence itself. This involves judging (a) the credibility of the evidence, based in part on the previously completed source and communications channel evaluations; and (b) the relevance of the evidence.

As evidence is evaluated, it must be combined and incorporated into the target framework. Multiple pieces of evidence can be divergent (favoring different conclusions and leading to alternative target models) or convergent (favoring the same conclusion). Convergent evidence can also be redundant (corroborative or cumulative), reinforcing a conclusion.

A large number of analytic methodologies for both evaluating and combining evidence are available to the analyst. One of the most powerful is structured argumentation: a formal process of examining and combining evidence graphically and/or numerically. Two such processes are analysis of competing hypotheses (ACH) and Bayesian analysis. ACH identifies a set of hypotheses, systematically evaluates data that are consistent and inconsistent with each of those and rejects those hypotheses that contain too much inconsistent data. Bayesian analysis uses the probabilities associated with observed events to revise conclusions.

Information technology tools to acquire, organize, search, store, and retrieve raw intelligence are widely available and boost analyst productivity. Tools to extract meaning from data, for example, by relationship, pattern, and geospatial analysis, are used where they add value that offsets the cost of “care and feeding” of the tool. Tools to support structured argumentation are available and can significantly improve the quality of the analytic product.

In the ongoing target-centric process, the picture will almost always be incomplete after the existing finished and raw intelligence are incorporated into the target framework. This means that gaps exist, and new collection must be undertaken to fill them. How that is done is the subject of chapter 12.

CRITICAL THINKING QUESTIONS

1. Select a news article about a current national issue or law enforcement incident. (Your instructor may provide a set of examples to choose from.) Perform an evidence evaluation on the item, conducting independent research as necessary. That is, evaluate the source and the communications channel. Evaluate the credentials of the article by answering the three questions: Is it true? Is it the whole truth? Is it nothing but the truth?

2. In the critical thinking questions for chapter 5, you were asked to develop a set of hypotheses for the alleged Cuban sonic attacks on US and Canadian diplomats in Havana.
 - a. Using those hypotheses, prepare an ACH matrix following the Heuer steps listed in this chapter.
 - b. Establish the relative likelihood of each hypothesis and explain how your conclusion would change if a particular key item of evidence or argument were invalid.
3. (Answer only after studying the article by Wheaton et al., on Bayesian analysis): You are a UK National Crime Agency intelligence analyst following the operations of the Sinaloa drug cartel. The cartel has been reported to be using a Romanian crime gang to smuggle cocaine through one of two UK ports: Felixstowe and Harwich. You have concluded, based on the evidence, that the probabilities for each port are even—50 percent likelihood that the port is being used to smuggle cocaine. You also conclude, based on past operations of Romanian gang members, that they will make regular visits to either port with a .3 probability if the port is not being used as a cocaine entry point, and that the probability of regular visits rises to .8 if the port is being used to smuggle in cocaine. Recent HUMINT reporting indicates that gang members are regularly traveling to Harwich. What is the new probability that Harwich is the entry port?
4. Chapter 2 included the case titled “Netwar I/II: Erdogan versus Gulen.” A number of sources are available online that present different perspectives on the case. (Some sources are included as endnotes in the case, but you are not limited to these.)
 - a. Which source would you consider most credible? What are your reasons?
 - b. Which do you believe is the least credible? What are your reasons?
 - c. Identify at least two examples of convergent or divergent evidence in the material that you used.

NOTES

1. We've mentioned raw and finished intelligence earlier. The distinction is this: Raw intelligence is information, generally from a single source, which has not been fully evaluated, integrated with other information, or interpreted and analyzed. Finished intelligence has gone through all of those steps, generally with an independent review, and is intended for intelligence customers.
2. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, CIA, 2005), 22.
3. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 82.

4. Christopher Eldridge, Christopher Hobbs, and Matthew Moran, "Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of 'Big Data,'" *Intelligence and National Security* 33, no. 3 (2018): 391–406.
5. Robert Dover, "SOCMINT: A Shifting Balance of Opportunity," *Intelligence and National Security* 35, no. 2 (2020): 216–32.
6. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009).
7. Bertrand Russell, *A History of Western Philosophy* (New York, NY: Simon & Schuster, 1945), 472.
8. John Evangelist Walsh, *Moonlight: Abraham Lincoln and the Almanac Trial* (New York, NY: St. Martin's Press, 2000).
9. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 97, https://fas.org/irp/offdocs/wmd_report.pdf.
10. John Braithwaite, *Corporate Crime in the Pharmaceutical Industry* (London, UK: Routledge and Kegan Paul, 1984).
11. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 125.
12. David A. Schum and Jon R. Morris, "Assessing the Competence and Credibility of Human Sources of Intelligence Evidence: Contributions from Law and Probability," *Law, Probability and Risk* 6, no. 1–4 (March 2007): 247–74.
13. Claude E. Shannon, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1963).
14. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 10, 49.
15. David A. Schum, "On the Properties, Uses, Discovery, and Marshaling of Evidence in Intelligence Analysis," Lecture to the SRS Intelligence Analysis Seminar, Tucson, AZ, February 15, 2001.
16. CIA Directorate of Intelligence, "A Compendium of Analytic Tradecraft Notes," February 1997, http://www.oss.net/dynamaster/file_archive/040319/cb27cc09c84d056b66616b4da5c02a4d/OSS2000-01-23.pdf.
17. John Prados, *The Soviet Estimate* (Princeton, NJ: Princeton University Press, 1987), 203.
18. Herman, *Intelligence Power in Peace and War*, 96.
19. Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (McLean, VA: CIA Center for the Study of Intelligence, 1999), 119.
20. United States Institute of Peace, "Terror on the Internet: Questions and Answers," <http://www.usip.org/publications-tools/terror-internet/terror-internet-questions-and-answers>.
21. Neil MacFarquhar, "Saddam Hussein, Defiant Dictator Who Ruled Iraq with Violence and Fear, Dies," *New York Times*, December 30, 2006, <https://www.nytimes.com/2006/12/30/world/middleeast/30saddam.html>.

22. William J. Lahneman, *The Future of Intelligence Analysis*, Center for International and Security Studies at Maryland, Final Report, vol. I (March 10, 2006), iii.
23. Peter Wright, *Spycatcher* (New York, NY: Viking Penguin, 1987), 12.
24. Johnson, *Analytic Culture in the U.S. Intelligence Community*, 64.
25. R. V. Jones, "Scientific Intelligence," *Research* 9 (September 1956): 350.
26. Ibid.
27. Roy Godson, *Intelligence Requirements for the 1990s* (Lanham, MD: Lexington Books, 1989), 17.
28. Matthew Herbert, "The Intelligence Analyst as Epistemologist," *International Journal of Intelligence and Counterintelligence*, 19 (2006): 678.
29. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 68.
30. Prados, *The Soviet Estimate*, 133.
31. Amy Zegart, "The Cuban Missile Crisis as Intelligence Failure," The Hoover Institution, October 2, 2012, <https://www.hoover.org/research/cuban-missile-crisis-intelligence-failure>.
32. Ibid.
33. Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics* 16 (April 1964): 455–67.
34. David A. Schum, *The Evidential Foundations of Probabilistic Reasoning* (Evanston, IL: Northwestern University Press, 1994), 161.
35. Heuer, *Psychology of Intelligence Analysis*, chapter 8.
36. Kristan J. Wheaton, Jennifer Lee, and Hemangini Deshmukh, "Teaching Bayesian Statistics to Intelligence Analysts: Lessons Learned," *Journal of Strategic Security* 2, no. 1 (2009): 39–58.
37. Ibid.
38. McKinsey Global Institute, "Big Data: The Next Frontier for Innovation, Competition, and Productivity," May 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.
39. David Williams, "If 'Big Data' Simply Meant Lots of Data, We Would Call It 'Lots of Data,'" *Forbes*, September 19, 2012, <http://www.forbes.com/sites/davidwilliams/2012/09/19/if-big-data-simply-meant-lots-of-data-we-would-call-it-lots-of-data/>.
40. Jennifer Schroeder, Jennifer Xu, Hsinchun Chen, and Michael Chau, "Automated Criminal Link Analysis Based on Domain Knowledge," *Journal of the American Society for Information Science and Technology* 56, no. 6 (2007): 842–55.
41. See the description of SEAS, the Structured Evidential Argumentation System, at SRI International's Artificial Intelligence Center, <http://www.ai.sri.com/project/GENOA>.
42. Visit Palo Alto Research Center, www2.parc.com/istl/projects/ach/ach.html, or Pherson Associates, www.pherson.org, to download a copy of the tool.

12

THE INFORMATION SOURCES

FILLING GAPS

Chapter 11 focused on the important analytic step of collation: fitting relevant, credible existing pieces of intelligence, both finished and raw, into the generic target framework. That process naturally makes apparent gaps in knowledge to be filled—the subject of this chapter. Here, collaboration can be an analyst's saving grace. The target-centric approach removes any temptation to simply sift through carefully kept files, add a few items within easy reach, and write a report. Having collectors and customers on the team helps guard against the natural tendency to draw conclusions from available information rather than attend to what gaps need to be filled and go after the needed material.

And what, exactly, is a gap? It is a missing item of knowledge that, if filled, allows an analyst to choose among alternative hypotheses and answer the customer's questions with greater confidence. These gaps always exist. Identifying them leads to developing a collection strategy and collection plan.

For straightforward collection problems, planning can be done quickly and efficiently by starting with a detailed issue decomposition and the target framework. The analyst, collectors, and customer working together then identify gaps in knowledge of the target that must be filled to satisfy the customer's needs. Armed with this information, after reviewing collection assets and capabilities, they are ready to define a collection strategy and ask specific collectors to go after the necessary elements.

As an introduction to collection strategies, let's look back at how Queen Elizabeth I's spymaster, Sir Francis Walsingham, planned for collection. His "Plat for Intelligence out of Spain" in preparation for the Spanish Armada reads:

1. *Sir Ed. Stafford to draw what he can from the Venetian Amb.*
2. *To procure some correspondence of the Fr. K. agent in Spain.*
3. *To take order with some in Rouen to have frequent advertisements from such as arrive out of Spain at Nantes, Newhaven (i.e., Le Havre) and Dieppe.*
4. *To make choice of two especial persons, French, Flemings, or Italians, to go along the coast to see what preparations are a making there. To furnish them with letters of credit.*
5. *To have two intelligencers in the court of Spain—one of Finale, another of Genoa. To have intelligence at Brussels, Leyden, Bar.¹*

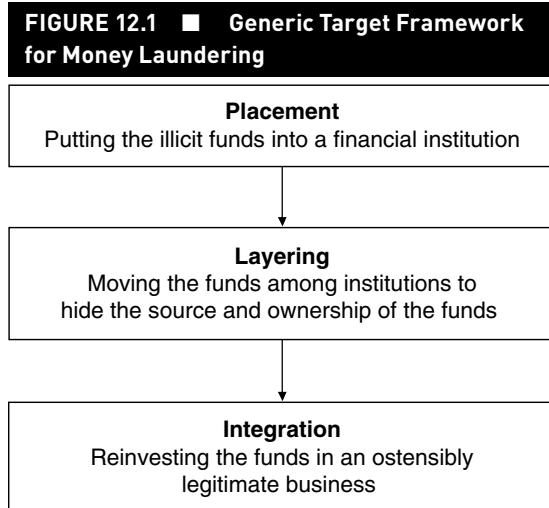
Clearly Walsingham had a thorough issue decomposition and a specific target framework, focused on England's most important strategic target: Spanish plans to attack England. He knew what the gaps were in his knowledge and what collection assets were available. So, he gave detailed, specific guidance on how to fill the gaps. Things were so simple then. (Walsingham's problem was not collection, his strong point; it was getting his leaders to believe his intelligence.)

USING THE ISSUE DECOMPOSITION AND TARGET FRAMEWORK

Everyone—including the analyst, collectors, and customer—needs to understand the relationship between the two. The issue decomposition helped ask the right questions. The existing target framework provides the context. At times the two may look almost identical, but they are separate models, and it's best to keep them that way. Why is that?

- *They come from different sources.* Each changes in different ways as new information comes in from two different directions. A customer's needs inevitably change with time, and the issue definition and decomposition must change accordingly. Also, new information from collection sources changes the target model.
- *An issue breakdown may look at only part of a target model or of several target models.* Let's revisit the political model in chapter 10 (figure 10.4). Most countries have diplomatic relations with Azerbaijan, as the model indicates. But only a few (Russia and Turkey, for example) are positioned to exert political influence and therefore are relevant to dealing with the issue.
- *Conversely, a target model may serve many issues.* Consider the economic target model in chapter 10 (figure 10.6): the trends in petroleum production and consumption in Azerbaijan. Our issue concerns the potential value of petroleum in influencing the Azeri government. Another analyst may have the issue of assessing worldwide oil production trends and would make use of the same model along with collateral models of other oil-producing countries.

To reiterate: The issue decomposition and the target framework are separate concepts and separate models, but the two are closely related. A simple example illustrates the relationship. Take the problem of money laundering—the movement of illicit proceeds into mainstream commerce and other funds transactions designed to conceal the source, ownership, or use of the funds. Criminal organizations, terrorist groups, and pariah states such as North Korea use the practice to evade international sanctions. It can be thought of as a process having three distinct stages—placement, followed by layering, followed by integration—as shown in the straightforward generic process model in figure 12.1.²



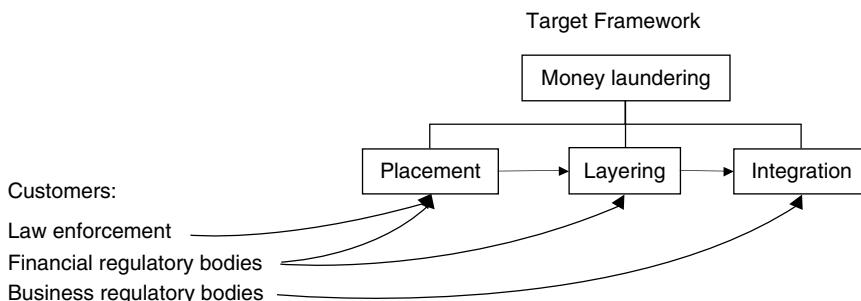
From the customer's point of view, a target's money laundering activities divide naturally into these three stages. But different intelligence customers will be interested in different stages. Consider these customers for such a target, and how their top-level issues might look:

- Law enforcement organizations, such as Interpol or the US Financial Crimes Enforcement Network, would focus on the placement stage. Countermeasures, it turns out, have been most effective when aimed at this stage. It is easier to identify and deal with money laundering then, so most law enforcement and regulatory work concentrates on detecting the placement of illicit funds.³
- Financial regulatory customers such as the United Kingdom's Financial Services Authority would address issues concerning both placement and layering, since they have oversight of the financial institutions involved.
- The US Securities and Exchange Commission or state regulatory agencies might center their attention on the integration stage, given their responsibilities for overseeing business activity—including businesses that handle integration.

As indicated in figure 12.2, each of these customers is focused on specific parts of the overall target framework. They likely would be interested in intelligence about all three steps in the process, of course.

Let's illustrate how an analyst gets from a specific target framework to a collection plan that fills gaps in knowledge, using a real-life example of money laundering. Box 12.1 introduces a network once run by Altaf Khanani. We will return to it throughout the chapter.

FIGURE 12.2 ■ Customers' Issue Connections to the Generic Target Framework



BOX 12.1 THE KHANANI NETWORK

In the mid-2000s, Pakistani money changer Altaf Khanani was one of the most successful practitioners in the clandestine business of laundering money. He had close ties to one of the world's wealthiest gangsters, Dawood Ibrahim, and his clients included Mexican, Chinese, and Colombian drug cartels and many terrorist organizations around the world. Through him massive volumes of hard currency flowed to heroin producers in Afghanistan. His business strategy was simple and effective: undercut your competitors. He offered commission rates as low as 3 percent and wound up laundering billions of dollars every year.⁴

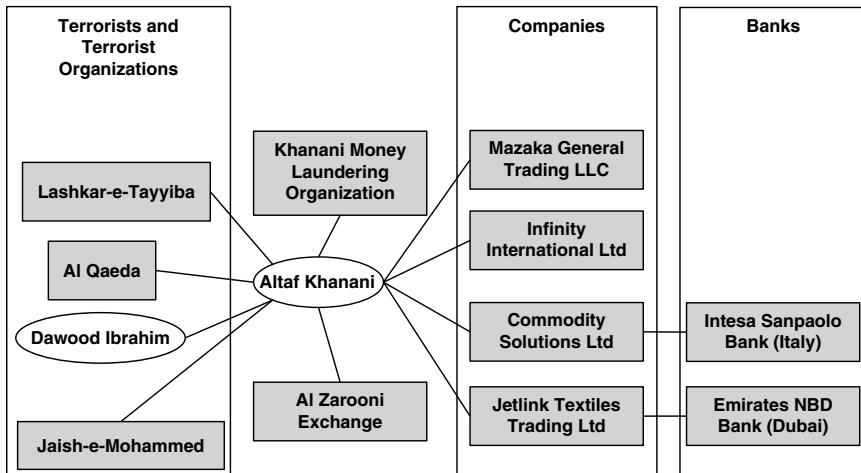
Khanani's run of good fortune ended in September 2015, when he was arrested in Panama in a US Drug Enforcement Administration (DEA)-led sting operation. The operation itself was a remarkable team effort by intelligence and law enforcement operatives of all the "Five Eyes" countries—who had been pursuing Khanani for years.⁵

After spending more than a year in a Miami jail, on March 29, 2017, Khanani was sentenced in a US district court in Florida to sixty-eight months in prison and a \$250,000 fine on one count of conspiracy to commit money laundering. The sentence was a light one, given the original 2015 indictment on fourteen counts of money laundering. Each count carried a maximum twenty-year prison term and \$250,000 fine. Khanani had pleaded guilty to one count, in exchange for his agreement to cooperate with investigators and the prosecution's dropping the remaining counts. The investigators who interviewed him were astonished at Khanani's ability to recall intricate details—phone numbers, bank accounts, and business names. It was a treasure trove for the Five Eyes intelligence agencies.⁶

Figure 12.3 illustrates part of a specific target framework that was drawn from the initial report of operations involving the Khanani money laundering organization.⁷ Note that this model includes more than just people; it also includes banks, terrorist

organizations, and companies—a point we'll return to in chapter 19, when we discuss target networks.

FIGURE 12.3 ■ The Altaf Khanani Network



Collectors might have used figure 12.1 as a starting point for collection against Altaf Khanani's network to get to the specific target framework shown in figure 12.3. HUMINT collection is likely to be most useful against the placement and integration stages, where well-placed human sources can monitor and report on unusual transactions. That's exactly what the Australians did, starting with couriers, which led them to brokers, which led them to the middlemen in the Khanani network.⁸ COMINT collection is well positioned to help in tracking the financial transactions associated with layering, because such transactions are typically made through international data transmission. OSINT can be useful in analyzing the business activities involving integration.

Given a cooperative source such as Altaf Khanani, investigators could obtain extensive intelligence about his network that would permit very focused targeting. And in the Khanani case, the prosecutors and the US Treasury Department apparently did just that, with assistance from Australian intelligence (which had provided the \$1 million in funds for the sting) among others.⁹ The Treasury Department, just prior to the plea deal, imposed sanctions on the companies and persons listed in table 12.1 and identified the associations shown, apparently based at least in part on information that Khanani provided.

But Khanani's network didn't end with Altaf Khanani's arrest; it simply reconfigured itself. That meant the Five Eyes investigators had a new target, with new gaps in knowledge. We'll revisit the case in the next section and use it as an illustration of identifying and filling knowledge gaps.

TABLE 12.1 ■ Khanani Money Laundering Organization Associations

Person or Company Name	Associations
Khanani, Hozaifa Javed	Kay Zone Builders & Developers; Unico Textiles; Altaf Khanani Money Laundering Organization
Khanani, Javed	Altaf Khanani Money Laundering Organization
Khanani, Obaid	Kay Zone General Trading LLC; Landtek Developers; Altaf Khanani Money Laundering Organization; Al Zarooni Exchange
Polani, Atif	Altaf Khanani Money Laundering Organization; Al Zarooni Exchange
Aydah Trading LLC	Altaf Khanani Money Laundering Organization
Jetlink Textiles Trading, Ltd.	Altaf Khanani Money Laundering Organization
Mazaka General Trading LLC	Altaf Khanani Money Laundering Organization
Seven Sea Golden General Trading LLC	Altaf Khanani Money Laundering Organization
Wadi al Afrah Trading LLC	Altaf Khanani Money Laundering Organization

IDENTIFYING GAPS

A target framework, after being populated with existing knowledge, is seldom complete enough to answer customer questions. It will become obvious that there are gaps in knowledge of the target. These gaps have to be made explicit, and intelligence collection has to close them.

Gaps are identified by asking these types of questions:

- How do we pull information out of the target model to address the problem?
- Does the target model, in its present form, include everything needed to address the customer's issue? (It does happen, though not often.)
- If not, where are the gaps in knowledge of the target, and how can they be filled?

Following is a formal process an analyst should go through in considering those questions. Veteran intelligence analysts follow the process described here, though they may do so intuitively.

Identifying data gaps is a continuous and iterative process—as new data come in and are fitted into the model, new gaps will be identified. Gap analysis is the process of

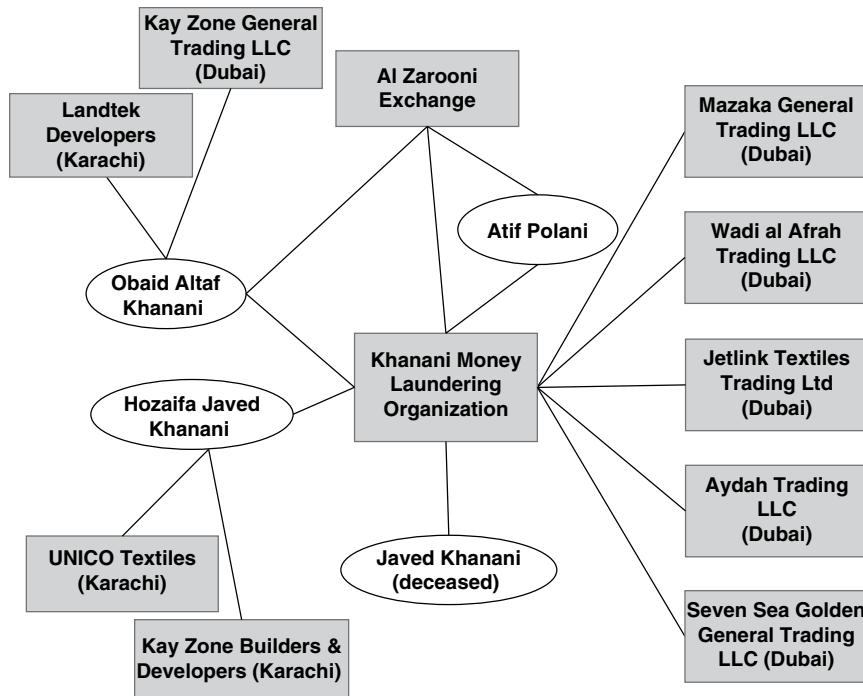
- Identifying and prioritizing gaps based on the importance of the underlying need and size of the gap.
- Classifying gaps as to their nature: Do they occur in collection, processing, analysis, or dissemination?
- Sorting gaps as either short term, for current collection systems “tuning,” or long term, for new capabilities development.

Consider some examples of gap analysis in a tactical situation. Take the example of the Afghan BMP, introduced in chapter 3, where the problem is to determine when the BMP would reach a village where Doctors Without Borders is working. If the analyst did not know how fast the BMP could travel on the road, that might be a collection gap to fill. Or it might be a dissemination gap: the information exists, but the analyst doesn't have it. In the Symantec war room example from chapter 2, analysts might have to deal with several gaps. They might come upon a familiar virus that could be easily countered but have a critical need to know where it started and what internet service provider (ISP) to call—a collection gap. In the process of defeating the virus, they would learn about a need to improve the collection system to identify the ISP more quickly—a long-term collection gap. They could also encounter a new type of virus, one that could not be examined effectively with their existing knowledge—an analysis gap.

Now let's return to the reconfigured Khanani network—the one that survived his arrest. Figure 12.4 is the partial network as it existed sometime afterward, drawn based on table 12.1. To avoid confusion, we'll refer to it subsequently as the Khanani Money Laundering Organization (MLO) network. In the continuing process of gathering intelligence about the new network, we'll refine both the generic money laundering model and the specific Khanani MLO target model.

A straightforward gap analysis can be done by comparing figure 12.4 with the original organization in figure 12.3. Knowledge gaps that become apparent include the following:

- What is the relationship between Obaid Altaf Khanani, Hozaifa Javed Khanani, and Atif Polani in the Khanani MLO? What role does each play, and what additional connections to organizations not shown in the figure exist for each?
- What connections now exist between the Khanani MLO and the terrorist organizations Lashkar-e-Tayyiba, Al Qaeda, Jaish-e-Mohammed, and terrorist/crime lord Dawood Ibrahim?
- Are the banks Intesa Sanpaolo (Italy) and Emirates NBD (Dubai) still part of the money laundering operation? What other banks are connected to the Khanani network?

FIGURE 12.4 ■ Khanani MLO Network¹⁰

DEVELOPING THE COLLECTION STRATEGY

At this point in the analysis process, the gaps in information about the target have been identified. However, now is not the time to rush ahead. Before designing a collection strategy to fill them, it is important to understand their nature. Not all are collection gaps. Some exist because analysis of the existing material has been nonexistent or inadequate, not because of lack of collection. Others need research to determine what part collection can play. Treating all of them as collection gaps means that the collector will simply collect again without solving the problem, in some cases compounding it by adding more unneeded data to be analyzed.

Only after true collection gaps have been defined is it time to plan for collection and offer guidance to collection sources and organizations. A rich set of collection INTs is available to help acquire the information.

Using Existing Collection Assets

Just as analysts first use existing intelligence to make a generic target model specific to their customer's problem, acquiring new data to fill gaps is a matter of making good use of existing collection assets. These are the agents already in place, the open literature

already coming in and being translated, the collection satellites or aircraft currently flying, and so on. The process of asking for use of these assets to fill gaps is called *tasking*.

Analysts rely on their judgment in designing the best collection strategy for tasking to fill gaps. They traditionally initiate the tasking and must pull together the incoming information to form a coherent picture. In the collaborative environment envisioned throughout this text, formulating a collection strategy is a team effort, with input from collectors and processors. The following describes how it should proceed.

Basic Collection Strategy Development

Most collection strategies are developed as a result of experience. Stated another way, most collection problems are old ones; only the specific questions to be answered are new. Begin by looking at what has succeeded in the past.

Start with a review of the previous collection strategies against similar targets and look at their results. Each specialized substantive area of intelligence has its own collection techniques that have been tested over many years. Political intelligence traditionally has relied on a combination of OSINT and HUMINT, with some COMINT. Military intelligence relies heavily on COMINT and IMINT, along with specialized technical collection. Weapons systems intelligence uses all sources but relies most heavily on technical collection, IMINT, and OSINT. Analyzing previous strategies and their results illuminates the prospects for future strategies.

Analysts cannot rely only on previous strategies, however. A predictable collection strategy can be defeated (a principle addressed in chapter 13). Also, simply shifting tasking from one target to another usually opens gaps in other areas.¹¹ Try to develop innovative approaches to using existing assets. Encourage collectors not to repeat collection that has not obtained the needed information but instead to try new ideas. For example, techniques that work in economic or political intelligence problems may be applied to issues in other areas, such as military or scientific and technical intelligence.

In developing collection strategies, be sure to distinguish collectors' current contributions from their potential contributions. In some cases, gaps can be closed by applying collection resources where they now contribute very little. A HUMINT source that reports on political affairs may also be able to obtain economic information. A COMINT source that provides order of battle information may also provide insights into the personalities of enemy field commanders.¹²

Let's illustrate how that can happen by returning to the Khanani MLO network. We earlier identified three potential gaps in knowledge concerning the network, based on a comparison of figures 12.3 and 12.4. A possible collection strategy against these gaps would be as follows:

- *What is the relationship between Obaid Altaf Khanani, Hozaifa Javed Khanani, and Atif Polani in the Khanani MLO? What role does each play, and what additional connections to organizations not shown in the figure exist for each?*

COMINT targeting, especially of their cell phones, is a likely starting point for collection. HUMINT targeting might be done indirectly, that is, targeting their associates for collection to develop leads for further COMINT or HUMINT collection. A number of the organizations listed in figure 12.4 are located in Dubai and would likely communicate via satellite communications or the internet with their Khanani contacts in Karachi, so those channels should be targeted as well.

- *What connections now exist between the Khanani MLO and the terrorist organizations Lashkar-e-Tayyiba, Al Qaeda, Jaish-e-Mohammed, and terrorist/crime lord Dawood Ibrahim?* These three organizations and Ibrahim should be targeted for collection, primarily by COMINT and HUMINT. But links to the Khanani MLO will probably be more active as new relationships are formed subsequent to Altaf Khanani's arrest, and that activity provides a collection opportunity.
- *Are the banks Intesa Sanpaolo (Italy) and Emirates NBD (Dubai) still part of the money laundering operation? What other banks are connected to the Khanani MLO?* COMINT, or HUMINT from a source in either bank, might provide leads. In the case of Intesa Sanpaolo, the interbank financial transaction service known as SWIFT could be targeted for cyber collection. The funds transfer between Karachi and Dubai (Emirates NBD) makes use of the hundi system—a financial instrument of Indian origin, similar to the hawala system that is used mostly in Muslim countries. Funds movement in this network could be more difficult to track, but both COMINT and HUMINT could be used to fill this gap in knowledge.

Good collection strategy requires that the request be timed so that collection occurs when the highest probability of getting desirable content will occur. In the Khanani MLO collection strategy above, two opportunities for COMINT and cyber collection timing were obvious. Important communications among all elements of the network were highly likely immediately following the announcement of Altaf Khanani's arrest in 2015, and again immediately after the Treasury Department announced sanctions in 2016.

Miscellaneous examples of strategic timing of collection include the following:

- Missile range testing has consistent patterns. When a pattern of vehicle deployments indicates that a missile test is about to take place, it is the right time to task collection assets.
- Individuals consistently use their cell phones heavily at certain times of day. Establish the target individuals' patterns and ask for COMINT collection during those times.

- Questioning technical staff at professional conferences elicits more useful information than questioning them at more formal venues.
- The Chinese intelligence service successfully applies an elicitation technique designed to leave visitors exhausted and off guard. It begins with a hectic day of tourism, followed by an evening cocktail reception. After a few cocktails, the visitor is approached by a “graduate student” seeking research assistance, usually on a topic that the visitor has previously been unwilling to discuss.¹³

You can also obtain synergistic benefits by intelligently timing collection of different resources. Coordinated collection by different INTs at the same time can yield insights that those INTs could not provide individually. In the missile range testing example above, IMINT collection of the missile on its launch pad should take place just before the telemetry collection of the missile in launch phase. Technical collection, such as radar collection of the missile in flight and during reentry, should be timed to follow the launch phase. The combination of these sources can tell far more about the missile’s performance than can any one of them alone.

Advanced Collection Strategy Development: Cost-Benefit Analysis

On more complex problems, the general approach is the same but a formal process may be needed to develop and compare alternative strategy packages. This is a resource allocation step—an effort to fill short-term gaps (immediate needs) by identifying possible collection mechanisms and selecting the most promising combination of assets.

The result of such an effort should be a “package”—a combination of strategies for closing the gaps. On very large and high-priority efforts, this means sorting through alternative combinations. This is seldom done in practice, because it takes much planning and a high level of understanding of the various available sources. Topics such as locating mobile ballistic missiles or searching for weapons of mass destruction, for example, are important enough to merit developing and comparing alternative strategies. The most straightforward and accepted comparative method is cost-benefit or cost-utility analysis, which involves these actions:

1. Estimate the benefit or utility of each strategy (option) and combination of options.
2. Estimate the costs or risks of each strategy and combination.
3. Select a package that has a high ratio of benefits (or utility) to costs (or risks).

Determining benefit or utility depends on answering some questions. What are the probabilities of success? Which asset or combination has the best chance to get the needed information? How can we increase the probability of success and maximize

the value of the information collected? How likely is the opponent to successfully use denial and deception?

As an example of a utility tradeoff: A broad area search for mobile missile sites has high payoff if a successful hit occurs, but success is stochastic (controlled by probabilities) and the probabilities are low. A fixed intercontinental ballistic missile site is an almost-certain hit for IMINT collection (assuming no cloud cover), since its location is known, but the value of the intelligence gathered is likely to be low; not much changes at such a site from day to day. In summary, the benefit or utility of using collection resources is based on the following:

- Importance of the requirement or specific task
- Value of the information collected, if successful
- Probability of success of the collection effort

Estimating the cost or risks can be done in several ways. One way is to produce a resource cost estimate that identifies the opportunity costs associated with using collection assets as proposed. The term *opportunity costs* means that if a collection asset is being used against one target, it usually is not available to use against other targets. Actual costs of collection may be difficult to come by; collection organizations guard such information zealously.

Also, risks may be more important than costs as a factor against which to measure benefit. For example, when the Eisenhower administration decided to conduct aerial reconnaissance over the Soviet Union during the 1950s, the costs of the U-2 program were a relatively minor factor in its decision-making process. A much larger factor was the risk of a shoot-down and of consequent damage to the United States' image and to US-Soviet relations. A U-2 was indeed shot down, and the subsequent political fallout reemphasized that risk was in fact a better measure than program cost.¹⁴

EXECUTING COLLECTION STRATEGIES

The previous sections have emphasized that collaborative efforts result in more effective collection strategies. But they aren't done routinely; too often collaboration is an informal or ad hoc matter. The US intelligence community periodically attempts to formalize this process. One such initiative in 2008 was called, not surprisingly, collaborative collection strategies (CCS). CCS was basically a renaming of traditional multi-INT collection, intended to have collectors and analysts formally collaborate throughout the intelligence process to support cross-discipline collection and analysis operations—from identification of the problem through the development and execution of the specific strategy. CCS operations started with SIGINT-IMINT collaboration, and attempts were made to include the other intelligence community disciplines.¹⁵

CCS was one of the early steps that the intelligence community took toward implementation of the target-centric approach.

In the past three decades, some intelligence organizations have defined a specialized career field called *targeting analyst* to develop and implement collection strategies. The “target” in “targeting analyst” has the same meaning as used throughout this text: people, networks, things, organizations, systems, or facilities. The job of the targeting analyst is to translate intelligence needs into potential targets, identify gaps in knowledge, identify collection assets that can be used against the target, and develop a collection plan. In essence, one analyst handles all these steps, working closely with all-source analysts (the customers) and with collectors. Targeting analysts clearly do not plan routine collection, such as IMINT or ELINT collection, which is best done by automated systems. They are more likely to be focused on a single target of very high intelligence value.

Where more formal collaborative collection strategy approaches are not available, US analysts sometimes prepare collection support briefs (CSBs). CSBs have been used for decades, primarily to provide collection guidance to HUMINT collectors. But they have been created for all collection INTs. They usually consist of tutorial information on more arcane topics, along with some detail on what is known and what knowledge gaps exist. So, again, they provide a target model for the benefit of collectors. Their primary limitation has been that, in order to be useful for HUMINT collectors, CSBs must have a relatively low classification (“Secret” or below) so that they can be shared in the field.

ANALYST-COLLECTOR INTERACTION

The preceding sections have emphasized the secret to success with any collection strategy: a close and enduring relationship between analysts and collectors. Simply writing collection requirements and “throwing them over the wall” seldom works. But when collectors have input, access to, and a good understanding of the issue decomposition and target framework, they can respond much more effectively than if they do not have knowledge of these elements.

It's important to ask the right questions.¹⁶ But how does the analyst know what the right questions are? Collectors have in-depth knowledge of their capabilities and may be able to do things that analysts cannot imagine. So they have to understand what analysts really want (and therefore they are in the same position with respect to analysts that analysts are with respect to the customer). Again, sharing the issue definition and target framework is the best way to start.

A consistent theme of this chapter is collaboration. But, where to begin when collectors have different cultures, different sensitivities, and different preferences in dealing with all-source analysts, all shaped by their previous experience? Clearly, it is worth developing a solid understanding of those cultures, sensitivities, and preferences. The

single-source analysts in collection organizations can do a better job of identifying collection opportunities once they understand the gaps, because of their thorough knowledge of what their assets can do. Following are a few general tips that may help, keyed to the national-level channels:

- *OSINT.* Open-source specialists typically are skilled in research and translation of material from specific countries or regions. They have access to sources that analysts would have difficulty locating on their own. They're usually very helpful in responding to specific requests, and appreciative that their material is valued and being used. (Translating can be very boring work when it can appear that no one cares about the product.) It's a good idea to provide feedback about how you use their translations.
- *HUMINT.* In large intelligence organizations, there are usually one or two intermediaries between the analyst and the case officer (the person out in the field who recruits and runs agents). Clandestine services want to protect their vulnerable sources, and analysts aren't likely to find out much detail about a source unless they are a part of a small trusted inner circle. Analysts who get a reputation for being careless with their material may find themselves cut off. If they happen to have a source with the needed access, HUMINT collectors can provide incredibly good material. If not—well, paraphrasing what a former secretary of defense once said, you go with the sources you have, not the sources you wish you had. It is usually necessary to elaborate on and explain the requirements in person, because often the officers who prepare HUMINT reporting have material they haven't published, simply because no one has explained its value. Small intelligence services usually have fewer case officers in the field, but they enjoy a closer relationship with analysts, so HUMINT collection targeting can be done more precisely.
- *COMINT.* Like OSINT collectors, COMINT collectors have a good understanding of available sources and fluency in their target languages. They share with HUMINT officers a concern about protection of their sources and must have a strong bond of trust to share details about them. COMINT collectors can be particularly sensitive about being "scooped" (that is, having their raw product used by all-source analysts before they have a chance to publish it) or seeing their material otherwise misinterpreted by all-source analysts (or by customers such as Winston Churchill, noted in chapter 11). US COMINT collectors have a number of legal restrictions concerning COMINT, and analysts should be aware of those. For example, collection against US persons and companies (which are "persons" under law) is forbidden in general and subject to severe restrictions where permitted at all.

- *IMINT.* In working with imagery collectors, it's relatively straightforward—and important—to develop a close personal relationship. US overhead and airborne imagery collection systems pull in a vast quantity of images each day. Imagery collectors are overwhelmed with the volume, and under pressure to produce GEOINT or activity-based intelligence, both being forms of all-source analysis. Analysts likely have the expertise to help them and will likely get attention to their targets of interest in return.
- *MASINT.* Much of this collection discipline could be described as “boutique” collection. That is, it's specialized; many of its subdisciplines have a relatively narrow customer set and require specific guidance on what to go after.
- *Cyber collection.* With a rich set of possible targets, cyber collectors need specific, detailed guidance, and tips on where material of interest might reside. Which organization an analyst deals with depends on the nature of the target. If it's accessible on the web, it's likely to be a COMINT organization. Stand-alone computer targets and intranets that don't connect to the web may require HUMINT-enabled collection.

Again, these informal tips apply to national-level channels. Military units in the field and local law enforcement typically have a closer and less formal relationship between collectors and analysts. But in all collection INTs and at all intelligence levels, product evaluation and feedback to the collector is important. It helps collectors to do a better job, and the professional recognition for providing a quality product encourages more of the same. Analysts depend on feedback from their customers; why not give it to collectors, as their customer?

EVALUATING COLLECTION

An issue that often comes up is how to measure the effectiveness of collection. Analysts view collection effectiveness in terms that are relevant to dealing with their issue. For example, they would want to answer questions such as these: Where are Iran's mobile ballistic missiles located? Where are the petroleum industry's planned oil exploration regions? What is the expected size of the 2023 opium crop in Pakistan, Laos, Mexico, Thailand, Afghanistan, and Burma? Where are the opium processing centers in these countries, and how much can they process? Where are the concealed WMD production centers in North Korea? All of these questions call for a combination of collection and analysis.

That view for evaluation doesn't work well for collectors. It emphasizes content and quality of the information gleaned, which is not readily measured. Collectors must view things differently. They have to focus on measures of collection *performance*,

which is not the same as collection effectiveness. For example, consider some measures of collection performance that are employed:

- *IMINT.* How much of the target area was searched in imagery at a given resolution?
- *COMINT.* How many hours of continuous copy of a high-priority communications channel were obtained?
- *HUMINT.* How many reports did the case officer submit?

These are all measurable, but they don't address effectiveness from the analytic standpoint. One hundred percent of a target area could be searched in imagery without turning up a single item of useful intelligence. Twenty-four hours of communications might be obtained from a high-priority channel, but no conversations of substance occurred on the channel during that time. And evaluating HUMINT performance rated by the number of reports submitted has the drawback of encouraging the submission of many short reports instead of a few detailed ones.

Measuring collection performance in those ways is not in itself bad; it just doesn't give a complete picture. Intelligence collectors now mostly take advantage of the feedback loops that exist with analysts to help in report evaluation. The target-centric approach encourages them to look at collection effectiveness as well as performance (that is, to focus on content and quality as well as traditional collection measures). It bears repeating that this means providing collectors with positive feedback on valuable reporting—something that veteran analysts know well.

COLLECTION REQUIREMENTS

This chapter began by citing Sir Francis Walsingham's collection strategy for dealing with the Spanish Armada. Contrast his plan with the collection challenges facing a large intelligence service that has many collection assets and many targets. (Walsingham really had just one target.) Management of information acquisition is a major effort in modern intelligence communities. These communities rely on a formalized process of defining requirements, needs, and information gaps.

Collection requirements form a hierarchy. Requirements hierarchies make use of the strategies-to-task approach (see chapter 8). Lower elements in the hierarchy are more specific and, in a well-drafted requirements hierarchy, are linked to the higher elements by measures that indicate their relative value in the overall scheme of things. The number of specific lower-level targets will be in the dozens for targeting a business firm, in the hundreds for even a small country or a consortium, and in the thousands for an illicit network target such as the Khanani network. A typical requirement at the lower levels might read, "Geolocate all armored vehicles in the battlefield area,"

“Obtain a copy of Ambassador Smythe’s negotiating notes for tomorrow’s trade negotiations,” or “Determine the intentions of the Cuban leadership on seaborne migration.”

The US collection requirements system stems in part from the success the intelligence community has had in developing collection assets. US intelligence collection capabilities are probably the best in the world. The intelligence community has the most resources and does the best systems planning. It innovates constantly and attempts things few other services would try. In breadth and depth of coverage, the United States remains unparalleled, and therein lies its problem. Because intelligence can do so much, it is asked to do too much. And expensive collection assets are used too often when less costly ones might suffice.

As a result, a prioritized intelligence requirements structure is necessary. But the US structure has received considerable criticism, and there have been repeated attempts to define a workable alternative over many years. One critic said of the requirements process three decades ago:

Analysts themselves often thought that too many people were employed and too much activity was oriented solely to generating “intelligence requirements”; a better job could probably have been done by a few experienced people, working with the available data, and therefore aware of what was missing. Instead intelligence requirements were the object of repeated studies and reorganization efforts.¹⁷

Since then, a wide array of tools and a more collaborative environment have improved the speed and effectiveness of the requirements systems. Even though they still encounter criticism, formal structures are necessary in dealing with high-volume IMINT, COMINT, and OSINT material, where a multitude of potential targets exist, and where an extensive customer suite with competing priorities wants more collection than could be accomplished with half of the national budget.

There continue to be issues with the requirements structure. Examples include the following:

- A reluctance to close legacy collection systems that have become less useful, since some customers continue to rely on the product. In the business world, companies keep close watch on overhead and cut low-payoff functions. Governments find that difficult to do.
- A tendency to forget that if information is available from unclassified sources, other intelligence collection assets should not be used to get it, except where cross-checking is essential—for example, in countering suspected deception (see chapter 13). Increasingly, commercial sources such as commercial imaging satellites can do collection that once required national intelligence assets, and can do it more cheaply.

- The size and formality of the system tends to make it cumbersome and slow, looking at present or even past rather than future needs—an issue that is not unique to the US system. Michael Herman observed that “a requirements system necessarily lags behind reality and following it is no guarantee of success.”¹⁸

When these problems are not addressed, the bulk of raw data collected has lower value than data from a more interactive (target-centric) system. For example, most new overhead imagery contains information that is already known; natural terrain features and fixed structures change little, if at all, over the course of a year. Most COMINT traffic, which consists of personal telephone conversations and unusable (unbreakably encrypted) traffic, must be discarded as irrelevant.

However, the collected data must be processed to some extent, and the handling of this volume of irrelevant data chokes the processing and exploitation systems and often chokes the analyst as well. The problem derives from trying to force a process that is based on the idea of an intelligence cycle instead of using a target-centric process. To come closer to the effectiveness of the target-centric paradigm, it is essential to make the requirements structure efficient and responsive.

SUMMARY

With a good understanding of the customer issue decomposition and having incorporated existing intelligence into the target framework, the analyst, collectors, and the customer are able to first identify gaps in knowledge, next develop collection strategies to fill the gaps, and later produce finished intelligence. Three steps are commonly used in developing collection strategies:

1. *Identify gaps in knowledge of the target.* The gaps usually become fairly obvious when the issue breakdown and target model are compared, but they have to be made explicit to enable collection planning. With input, access, and understanding of the issue decomposition and target model, collectors (and customers) collaborate in this process.
2. *Develop a collection strategy.* This step involves using existing assets to deal with the gaps. Past experience with collection against similar targets can help. Looking at the sources that were used in populating the existing target model can help to identify the sources that are best positioned to fill gaps. Having a good understanding of the target, so that collection can be timed, improves the chances the effort will obtain useful information. The most success in collection strategy comes from analysts having a close relationship with collectors. On large collection efforts against high-priority targets, it is worthwhile to develop and compare alternative strategies.

3. *Plan for future collection systems development.* This step involves assessing both existing and likely future needs and gaps, including planning to deal with denial and deception.

These steps form an iterative process. They are listed in sequential order to facilitate understanding, but in practice they are worked in varying orders, and several iterations of the process occur over time.

Executing a collection strategy is a matter of coordinating the efforts of all collectors so that their collection takes place against the right parts of a target at the right times. Some intelligence agencies rely on targeting analysts to handle the planning and coordination. Whoever handles the execution must have a close relationship with collectors and ensure that all collectors have access to the target framework. The exact nature of that relationship varies by collection type. OSINT analysts are usually overwhelmed with incoming material to translate, and IMINT analysts are flooded with imagery; both welcome specific guidance on what is important to concentrate on. COMINT analysts and HUMINT collectors of necessity must protect their sources, so they typically are cautious in discussing what they may be able to obtain. Cyber collectors are a composite of both groups; they have many possible targets and need guidance on what to go after but are very protective of their sources and methods. MASINT subdisciplines vary greatly; some have specific targets and a narrow customer set.

Collectors and analysts have different views in evaluating collection. Analysts care about how well collection helps them deal with the customer's issue. This view emphasizes content and quality of what is collected. Collectors have to look at measurable results, in terms of collection performance. A collaborative system that includes analyst feedback on useful reporting helps to bridge the gap between these two perspectives.

The US collection system is robust and provides a vast amount of raw intelligence about issues worldwide. But a large intelligence community experiences many challenges in planning for and managing collection. Although analytic shortfalls are blamed for most failures, analysts cannot analyze intelligence that they don't have. A large intelligence community needs a carefully planned set of collection strategies against high-priority targets. Analysts have to help make the collection process work effectively. They can do so by being heavily involved in developing collection strategies.

CRITICAL THINKING QUESTIONS

1. Which of the organizations or persons in figures 12.3 and 12.4 appear to be involved in the integration stage of money laundering? Which appear to be part of the layering stage? Which are in placement? Cite evidence or reasoning for your choices. (This may also require online research.)

2. Critical thinking question #3 in chapter 11 included a simplistic Bayesian exercise on the Sinaloa cartel’s shipments of cocaine into the United Kingdom, and the two ports likely to receive incoming shipments (see “Mexico’s Sinaloa Cartel Has Reportedly Teamed Up with a Romanian Gang to Ship Drugs to the UK” in *Business Insider* at <http://www.businessinsider.com/mexicos-sinaloa-cartel-work-with-romanian-gang-drugs-to-uk-2017-7>; other online sources may provide additional information). Revisit that exercise scenario and then answer the following questions:
 - a. What collection assets would you turn to for (1) obtaining warning of incoming shipments and (2) detecting the arrival of cocaine shipments in either port?
 - b. Identify specific targets for your collection assets, by type, location, or both.
3. Three knowledge gaps were identified in this chapter for the Khanani MLO network and, on the assumption that these were collection gaps, a collection strategy was suggested. Describe possible circumstances where these were *not* collection gaps. In such circumstances, how would you close the gaps?

NOTES

1. Stephen Budiansky, *Her Majesty’s Spymaster* (New York, NY: Viking, 2005), 199.
2. Joseph M. Myers, “International Strategies to Combat Money Laundering,” Speech to the International Symposium on the Prevention and Control of Financial Fraud, Beijing, October 19–22, 1998.
3. Ibid.
4. Anwar Iqbal, “Khanani Group Laundered Billions of Dollars: US Report,” *Dawn*, March 4, 2017, <https://www.dawn.com/news/1318333>.
5. Linton Besser, “Catching the Money Man,” ABC News, February 5, 2018, <https://www.abc.net.au/news/2018-02-05/the-billion-dollar-bust/9383890>.
6. Ibid.
7. Khurram Husain, “Khanani Gets 68 Months in US Prison,” *Dawn*, April 4, 2017, <https://www.dawn.com/news/1324717>.
8. Besser, “Catching the Money Man.”
9. Mark Schliebs, “Australian Intelligence Pinged Global Crime Boss,” *The Australian*, July 8, 2017, <http://www.theaustralian.com.au/national-affairs/foreign-affairs/australian-intelligence-pinged-global-crime-boss/news-story/4e9a80530febb05a95472e55a9a60358>.
10. In the figure, Javed Khanani, Altaf Khanani’s brother, is shown as “deceased.” He fell from a building under construction and died shortly after being named in the Treasury Department release. His family claimed it was a suicide.

11. In response to the attacks of 9/11, the United States shifted a large segment of its intelligence collection and analysis capability onto the terrorism target. The knowledge gaps that have been opened in other areas will take years to close. Unfortunately, the shifted resources could not be used efficiently for reasons that are explained by the Brooks curves (see chapter 18).
12. The Department of Defense defines *order of battle* as “the identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force.” See “DOD Dictionary of Military Terms,” April 10, 2003, <http://www.dtic.mil/doctrine/jel/doddict/>.
13. D. Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York, NY: Random House, 2002), 13.
14. John Prados, *The Soviet Estimate* (Princeton, NJ: Princeton University Press, 1987), 96–102.
15. Scott C. Poole, “Integrated Collection Management Accelerates Interagency Cooperation,” *NGA Pathfinder* 6, no. 3 (May/June 2008): 8, www.nga.mil/NGASiteContent/StaticFiles/OCR/mayjune08.pdf.
16. Steven D. Leavitt and Stephen J. Dubner, *Freakonomics* (New York, NY: HarperCollins, 2005), 89.
17. John Prados, *The Soviet Estimate* (Princeton, NJ: Princeton University Press, 1987), 181.
18. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 292.

13

DENIAL, DECEPTION, AND SIGNALING

Writers often use the analogy that intelligence analysis is like the medical profession.¹ Analysts and doctors weigh evidence and reach conclusions in much the same fashion. In fact, intelligence analysis, like medicine, is a combination of art, tradecraft, and science.² But intelligence analysts encounter a problem that physicians do not. A doctor does not routinely have to deal with denial and deception (D&D). Patients are not opponents. Though they may forget to mention certain symptoms, they are not trying to deny or deceive their doctor.³

An intelligence analyst within the context of D&D is more analogous to a professional poker player, especially in the games of Seven Card Stud or Texas Hold 'em. Other players *are* opponents. Some of their resources are in plain sight; some are hidden. They often depend on deception to win. Professional players must observe their opponents' actions (bets, timing, and facial expressions, all of which incorporate art and tradecraft) and do pattern analysis (using betting history, statistics, and other tools of science).

In fact, intelligence analysis and poker share a common underpinning: target models. For example, in a high-stakes competition, a player creates a profile model of her opponent based on observations of past behavior, a model of his current hand based on the profile model and evidence of current behavior, and a statistical analysis of tangible elements—the exposed cards on the table. That set of models guides the player's analytic judgments just as with intelligence analysts. In intelligence, though, the stakes are higher.

The concluding step in the intelligence process before the final assessment is to do a comprehensive denial and deception check. In a formal product review, steps such as peer review, red teams, and devil's advocacy are intended to help identify D&D (see chapter 14). But the analyst team should be the closest of all possible reviewers to the raw material and therefore best positioned to identify it. Even if the team has been diligent in looking for D&D at every analytic turn, when the analysis is finished and the conclusions are being prepared, this is the opportunity to avoid probably the most humiliating outcome an analyst can experience: being misled by an opponent's D&D.

It is a difficult thing to ask someone to do at the end of a long process: make a hard stop and take a fresh look at results. To perform some form of “sanity check” on every major hypothesis. The customer is waiting and, more than anything, you want to move on and get the report out of the way. But do you want to do that badly enough to present a flawed picture that results in a bad customer decision? That could be career ending.

In chapter 14, we'll describe the formal review process that typically occurs before the product of intelligence research goes out the door. But before that step, and especially in the case of current or indications and warning intelligence (which, because of time constraints, may receive only a light review), the commandment of all successful analysts should be: *One last time*: Could the results have been affected by an opponent's D&D operations?

To recognize possible deception, analysts must first understand how it works. Four fundamental factors have been identified as essential: truth, denial, deceit, and misdirection:⁴

- *Truth.* All deception works within the context of what is true. Truth establishes a foundation of perceptions and beliefs accepted by an opponent and can then be exploited in deception. Supplying the opponent with real data establishes the credibility of future communications the opponent then relies on.
- *Denial.* It's essential to deny the opponent access to some parts of the truth. Denial conceals aspects of what is true, such as real intentions and capabilities. Denial often is used when no deception is intended; that is, the end objective is simply to deny knowledge. Encryption, for example, denies access to a message. One can deny without intent to deceive, but not the converse.
- *Deceit.* Successful deception requires the practice of deceit: causing the opponent to accept as true or valid that which is false or invalid.
- *Misdirection.* Deception depends on manipulating the opponent's perceptions. The goal is to direct the opponent away from the truth and toward a false perception. In operations, a feint is used to redirect the adversary's attention away from where the real operation will occur.

The first three factors allow the deceiver to present an opponent with desirable, genuine data while reducing or eliminating signposts needed to form accurate perceptions. The fourth provides an attractive alternative that commands the opponent's attention.

It is essential that these four factors—truth, denial, deceit, and misdirection—be considered while creating the target model framework, to tip off the likelihood of deception.

A caveat before the discussion: Though this chapter treats D&D (as most texts do) as one topic, denial and deception are separate entities. Obviously the two are closely interrelated (thus the acronym) because deception requires denial. They also share a focus on collection means (or channels) and knowledge of an opponent's analytic methods.

DENIAL

The opposing side's objective in using deception is to provide a scenario that your organization will believe and act upon—to its detriment. To do that, the opponent has to deny accurate information to your organization, normally through concealing or camouflaging details of the truth. Methods of denial are straightforward, although they can be extensive and multifaceted, as illustrated in the Indian nuclear test case later in this chapter. Also consider Yamantau Mountain in the Urals, discussed further in chapter 20. The complex remains an enigma; in locating the massive facility in the side of a mountain and underground, the Russians have executed an effective denial.

Some other types of denial include the following:

- Communications are routinely denied to SIGINT by a number of operational practices. Encryption has been used to deny analysis of intercepted communications for more than a century—dating back to its use in telegraphy during the 1800s. Burying communications cable and using fiber-optic cable (which is hard to tap into) instead of radio is another useful technique for denial. Where radio must be used, technical approaches to shaping the transmission, known collectively as low-probability-of-intercept (LPI) techniques, are used to make the radio signal difficult for SIGINT receivers to detect.
- Denial against IMINT may take the form of camouflage netting, obscuring or masking techniques, or placing sensitive operations in underground facilities (protecting them against attack at the same time); blinding sensors with lasers; conducting operations during darkness or cloud cover to hide military force movements or illegal activity; and moving units frequently to prevent their being targeted.
- Governments secretly developing fissionable materials will thoroughly scrub their production facilities before an internationally mandated plant inspection, to remove traces of the fissile material (though it often doesn't work; minute traces are very difficult to remove).

DECEPTION

Deception techniques are limited only by our imagination. Passive deception is the least complex. It might include using decoys, as has been the case since the beginning of warfare. For example, dummy troops, ships, missiles, and tanks have been widely employed. Having the intelligence target emulate an activity that is not of intelligence

interest, such as making a chemical or biological weapons plant look like a medical drug production facility, qualifies as a passive deception. Denial of knowledge is a prerequisite for conducting deception. In using decoys, for example, the locations of the real objects must be concealed. In misrepresenting the function of the chemical or biological weapons plant, its actual function has to be concealed.

Active deception includes misinformation (false communications traffic, signals, stories, and documents), misleading activities, and double agents (agents who have been discovered and “turned” to work against their former employers), among others. The following case relied on many of those features.

BOX 13.1 THE MAN WHO NEVER WAS

During World War II, the British had a very good model of German intelligence, including an understanding of the German operations in Spain and the close linkages between German and Spanish intelligence. Armed with this knowledge, they were able to plant on the Spanish coastline the body of an apparent British staff officer carrying documents that indicated the targets of the next Allied invasion. The deception effort, nicknamed Operation Mincemeat, was first revealed in Ewen Montagu's book (later a movie) entitled *The Man Who Never Was*.⁵ It involved dressing a corpse as a British Royal Marines officer. To the corpse was attached a briefcase with documents indicating that the upcoming Allied invasion of southern Europe would take place in Greece, with the real target—Sicily—being a feint. The corpse was then released from a submarine near the coast of Spain, where the British expected it would be found and the briefcase's contents shared with German intelligence. The deception succeeded because the British had an excellent model of how the German and Spanish services worked together, and they knew what form of information the Germans were likely to believe. A fake operations plan probably would have aroused German suspicions. Instead, the key document was a masterpiece of subtlety, in the form of a personal letter hinting that the next invasions would hit Sardinia and Greece, and that Sicily (the actual invasion target) was a feint.

Nevertheless, the plan had a number of potentially serious flaws. Fortunately for the Allies, these were overlooked by both Spanish and German intelligence. The body was released in a coastal area known to have strong pro-Axis sentiments, but the documents wound up in the control of the Spanish Navy—the least pro-Axis of possible recipients. The Spanish coroner who examined the body was, contrary to British expectation, an expert pathologist who had long experience in examining drowning victims. He noticed several suspicious features about the body: no fish or crab bites, shiny instead of dull hair, and clothing that wasn't shapeless. These features indicated that the body had not been in the water as long as the briefcase's documents indicated, but the state of decay indicated that the body had been in the water longer than the documents indicated.⁶ Furthermore, a large number of people knew of the operation (apparently including the Soviets), increasing the chances of a leak.

The Operation Mincemeat case illustrates that deception efforts are difficult to pull off against a competent opponent, even with a good model of the opposing services such as the British had. In the end, the success of the British effort depended on a few lucky breaks.

In more recent times, nongovernmental entities have developed considerable talent in operating deceptions. Illicit arms traffickers (known as "gray arms traffickers") and narcotics traffickers have developed an extensive set of deceptive techniques to evade international restrictions. They use intermediaries to hide financial transactions. They use front companies and false end-user certificates for weapons trafficking.⁷ They change ship names or aircraft call signs en route to mislead law enforcement officials. One airline went so far as to change its corporate structure and name overnight when its name became linked to illicit activities.⁸ The following are some of the standard deception techniques that illicit arms carrier aircraft use:

- Registering the aircraft in one country, then chartering it by companies registered in another, with crews that are hired in yet other countries and basing the aircraft somewhere else
- Using another aircraft's call sign
- Flying into an airport with one registration number and then flying out with a different one
- Making an unscheduled landing on the way to the approved destination and unloading illicit cargo
- Making an unscheduled landing to load illicit cargo en route, and then shipping the additional load under cover of the legal cargo

In one instance, a pilot was told to give the destination of his aircraft as N'Djamena in Chad, and when he arrived in Cairo he was told to file a new flight plan giving his destination as Muscat, Oman. Once the plane was on its way to Oman, the crew were told to divert to Riyan Airport, near Mukalla, Yemen, and then to fly a specific, circuitous route over Saudi Arabian airspace.⁹

The information instrument has been used for centuries to conduct deception—long before the fake documents created for Operation Mincemeat. During the Cold War, the Soviets used it often and with effect against the United States in South Asia, Africa, and Latin America, planting disinformation such as forged documents portraying the United States as a greedy, malicious world power intent on overthrowing existing governments. But in recent decades, prevalence of media reporters in all conflicts has enhanced its use. Media disinformation was repeatedly used by opponents to portray US and allied actions as "atrocities" during military campaigns in Kosovo, Iraq, Afghanistan, and Syria. On one occasion, in Kosovo, the Serbs posted

dramatic photographs of the same blood-stained children's doll in their reporting of several different alleged atrocities in different locations. There were even attempts to create atrocities for the media: Taliban forces in Afghanistan once took journalists on a night convoy to an alleged mass casualty site while coalition airstrikes were ongoing in the area, apparently for the purpose of drawing coalition fire with resulting media casualties.¹⁰

In conflicts that characterize the age of contested norms and persistent disorder, the use of the information instrument to promote deception has become a fundamental part of netwar: Traditional and social media are applied to paint a misleading picture of adversaries. Nongovernmental opponents (insurgents and terrorists) are especially effective in social media. An effective approach has been to produce online videos designed to: increase hostility toward the West, facilitate recruitment of new members, incite sympathizers to act, or increase traditional media sympathy for their cause.

Deception using the information lever has become so common in the past few years that it's been taken to a new level: deception claiming that on-the-ground in-person news reporting is a hoax—in a sense, deception squared. As reports of civilian casualties mounted during the 2022 Ukraine invasion, Russian media countered with videos purporting to show that the atrocities were staged. One video showed fake blood being applied to the face of an actor. Another claimed that a victim of the Mariupol hospital bombing was a beauty blogger who faked her injuries. A third claimed that the massacre of civilians in Bucha was staged.

The Russian effort was crude. It used clips from previous unrelated events that were easily located and brought forth. Nevertheless, the Russian videos had been widely shared and the fact-checking reports that followed to refute them did not reach the same audience.

DEFENSE AGAINST DENIAL AND DECEPTION: PROTECTING INTELLIGENCE SOURCES AND METHODS

Defense against the sort of deception the British conducted in Operation Mincemeat starts with your own denial effort, that is, the protection of sources and methods of collecting and analyzing intelligence. In the intelligence business, it is axiomatic that if you need information, someone will try to keep it from you. A general rule is that an opponent who can model a system can defeat it. So the best defense is to deny your opponent an understanding of your intelligence capabilities. Without such understanding, the opponent cannot effectively conduct D&D.

For small governments, and in the competitive intelligence world, protection of sources and methods is relatively straightforward. Selective dissemination of and tight controls on intelligence information are possible. But a major government has too many customers to justify such tight restrictions. Thus, these bureaucracies have

established an elaborate system to simultaneously disseminate and protect intelligence information.

There are two levels of protection for intelligence information. The levels distinguish between the *product* of intelligence and the *sources and methods*. Usually the product is accorded less protection than the sources and methods. Why? The product, if lost, reveals only itself and not how it was obtained. Information about the product is typically classified “Secret” or below, though “Top Secret” reports are used to protect especially sensitive information.

Sources and methods, though, need special protection in addition to the markings “Secret” or “Top Secret.” Information that might reveal the identity of the source (such as the identity of an agent) requires it. Loss of this information often results in the person being imprisoned or killed. Using intelligence terms, the source is lost permanently, and other potential sources are discouraged from coming forward.

This additional protection is loosely called *compartmentation*, because it puts information in “compartments” and restricts access to the compartments. In the US intelligence community, it is called the sensitive compartmented information (SCI) system. The SCI system uses an extensive set of compartments to protect sources and methods. Only the collectors and processors have access to many of those materials.

Under the SCI system, protection is extremely high for two types of COMINT. Clandestine COMINT—usually acquired through taps on telecommunications systems—is heavily protected because it is expensive to set up, it provides high-quality intelligence, and its loss has a severe and often permanent impact. COMINT based on decryption is the second highly protected type. Successes at breaking encryption are tightly compartmented because an opponent can readily change the encryption code, and breaking the new code is laborious.

Most IMINT, by contrast, has no special controls, because the information needs to be made available quickly to field commanders. Very little protection of sources and methods is needed anyway, because when a reconnaissance aircraft flies overhead, it is obvious to an opponent that images are being collected. Most aerial photography is classified “Secret” or below, and a substantial amount of satellite photography is now unclassified. Compartmentation is reserved for the unusual IMINT—unique capabilities that an opponent would not expect.

OSINT enjoys little or no protection because the source material is unclassified. However, the techniques for exploiting open-source material, and the specific material of interest for exploitation, can tell an opponent much about an intelligence service’s targets. For this reason, agencies that translate open source often restrict its dissemination, using markings such as “Official Use Only.” While limiting use of the material, a restrictive marking also allows a government to avoid copyright laws. Corporations make use of similar restrictive markings on material that is translated or reproduced for in-house use for the same reasons—concealment of their interest and avoidance of copyright problems.

An important reason for protecting open-source methods is that if an opponent knows which materials are being targeted, it is easier to take deceptive countermeasures. For example, the United States has long been aware that many foreign intelligence services translate and avidly read *Aviation Week & Space Technology*. If the Defense Department wished to mislead or deceive another country about US aerospace capabilities and intentions, this magazine would be a logical place to plant a misleading story.

The protection given to specialized technical collection varies greatly across the many collection types. ELINT is classified “Secret” or below. When opponents use a radar, they have to assume that someone will intercept its signal, and denial is very difficult. In contrast, the value of FISINT depends on concealing any successes in identifying the purpose of each telemetry channel collected. FISINT therefore resembles COMINT—the processing part is accorded tight compartmentation protection. The results of cyber collection are given a high degree of protection for a similar reason; collection can be defeated or used in deception if its success is discovered.

Unfortunately, other intelligence services often learn of your collection capabilities through the actions of policymakers. Demarches¹² and public statements that are based on intelligence results inevitably reveal something about intelligence capabilities. India used such knowledge in developing a strategic D&D plan to cover its nuclear device test in 1998.

BOX 13.2 THE 1998 INDIAN NUCLEAR TEST

On May 11, 1998, the Indians conducted three underground nuclear tests at their Pokhran nuclear test site in the country’s northwestern desert. The tests came as a complete surprise to the US government.

The denial and deception plan succeeded because the Indian government had an excellent understanding of the keys that US imagery analysts used to detect test preparations. The US government had succeeded in deterring an earlier plan by India to stage the tests. In December 1995, reconnaissance satellites had observed test preparations at the Pokhran site, including the movement of vehicles and the deployment of testing equipment. The US ambassador to India showed the imagery to top Indian officials in a successful demarche to persuade them not to test.¹³ However, what happened next is illustrative of unintended consequences.

Using the knowledge they gained from the demarche, the Indians were able to plan an elaborate D&D campaign to conceal preparations for the 1998 tests. The denial campaign was many-faceted, aimed at protecting the operation from HUMINT and IMINT.¹⁴

- The effort was protected by extensive secrecy measures within the Indian government. Few knew of the plan; the decision to test was not disclosed even to senior cabinet ministers.
- Work was done at night, and heavy equipment was always returned to the same parking spot at dawn with no evidence it had been moved.

- Piles of dug-out sand were shaped to mimic the wind-aligned and wind-shaped dune forms in the desert area.
- Shafts were dug under a camouflage netting.
- When cables for sensors were laid, they were carefully covered with sand and native vegetation to conceal the digging.

The deception campaign had several elements, making it an excellent example of multi-INT deception:

- All technical staff at the range wore military fatigues, so that in satellite images they would appear as military personnel charged with maintenance of the test range.
- All scientists involved in the operation left in groups of two or three on the pretext of attending a seminar or a conference. Tickets were bought for some location other than Pokhran under false names, and after arriving at their destination, the group would secretly leave for Pokhran. After finishing their part of the work, the group would go back, retracing their path. Then another group would travel to the range, employing similar means to do their part of the work on the nuclear devices.
- The Indian government issued public statements just prior to the test, designed to reassure other governments that no nuclear test was contemplated. Indian diplomats also categorically told their US counterparts that “there would be no surprise testings.”
- At the same time, Indian leaders began a misdirection campaign to focus US attention elsewhere. They started preparations for what appeared to be a ballistic missile test at their Chandipur test range, more than a thousand miles from the Pokhran site. The Indians did test a Trishul surface-to-air missile (which was of relatively low intelligence interest), but they moved additional equipment into the test range, making the preparations appear to be for a test of the Agni intermediate-range ballistic missile (of high intelligence interest).¹⁵

The deception was quite a success. As a result, US reconnaissance satellites reportedly were focused on the Chandipur missile site, with only minimal coverage of the nuclear test site at the time of the test.¹⁶ The deception was helped along by the US government’s mindset that, since India wanted to improve trade relations, the country would not provoke a crisis by testing a nuclear weapon.¹⁷

A sophisticated deception must follow a careful path; it has to be very subtle (too-obvious clues are likely to tip off the deception) yet not so subtle that the opponent misses the point. D&D is commonly used in HUMINT, but today it frequently requires multi-INT participation or a “swarm” attack to be effective. Increasingly, carefully planned and elaborate multi-INT D&D is used by various countries. Such efforts, particularly in the political realm, have long had an elegant name—*perception management*—that focuses on the end result.

Perception management can be effective against an intelligence organization that, through hubris or bureaucratic politics, is reluctant to change its initial conclusions about a topic. As noted in chapter 11, if the opposing intelligence organization makes a wrong initial estimate, then long-term deception is much easier to pull off. If D&D is successful, the opposing organization faces an *unlearning* process: Its predispositions and settled conclusions must be discarded and replaced. Highly adaptive organizations have the capacity to unlearn and are therefore less vulnerable to D&D than are more structured organizations. Large, bureaucratic organizations find unlearning remarkably difficult.

The best perception management results from highly selective targeting, intended to get a specific message to a specific person or organization. This requires knowledge of that person's or organization's preferences in intelligence—a difficult feat to accomplish, but the payoff of a successful perception management effort is high. It can result in an opposing intelligence service making a miscall or causing it to develop a false sense of security. If you are armed with a well-developed model of a foreign intelligence service, an effective counterintelligence operation in the form of perception management or covert action is possible. The Cuban missile crisis case, introduced in chapter 11, illustrates this point.

BOX 13.3 THE CUBAN MISSILE CRISIS II

In early 1962, the Soviets decided to emplace nuclear-equipped SS-4 and SS-5 ballistic missiles in Cuba to counter the increasing US edge in ballistic missiles aimed at the Soviet Union. The result was the Cuban missile crisis of that year. While the attempt ultimately failed, the Soviet effort to conceal the deployment was well executed. The Soviets planned to hide their deployment from US intelligence with an elaborate perception management campaign that combined HUMINT, IMINT, OSINT, and diplomatic deception, along with denial:

- Soviet military units designated for the Cuban assignment were told that they were going to a cold region. They were outfitted with skis, felt boots, fleece-lined parkas, and other winter equipment.
- Officers and missile specialists traveled to Cuba as machine operators, irrigation specialists, and agricultural experts.
- Missiles were shipped from eight Soviet ports to hide the size of the effort; the missiles were loaded under cover of darkness. The missile crates and launchers were shielded with metal sheets to defeat infrared photography.
- Ordinary automobiles, tractors, and harvesters were placed on the top decks to convey the impression that the ships were carrying only agricultural equipment.
- The ships' captains made false declarations when exiting the Black Sea and the Bosphorus. They altered the cargo records and declared tonnage well below what was being carried. They often listed Conakry, Guinea, as their destination.

- In Cuba, anything that resembled agricultural equipment was unloaded in the daytime. Weaponry was unloaded only at night and moved directly to the missile bases along back roads before daybreak.
- Radio Moscow regularly reported that the Soviet Union was supplying Cuba with “machine tools, wheat, and agricultural machinery . . . and fertilizer.”
- During September, Soviet diplomats gave repeated assurances to top US officials (including President Kennedy) that they had no intention of putting offensive weaponry in Cuba.
- In what proved to be a brilliant move, the Soviets leaked accurate information about the deployment to mask it. They funneled accurate details through counterrevolutionary Cuban organizations in the United States. The CIA discounted the information because they did not regard the groups as credible, and dismissed the subsequent stream of reporting from Cubans, tourists, and foreign diplomats in Cuba—some of which were valid—as simply more of the same.¹⁸

The deception was not perfect. There were some slips:

- The Soviets used the freighter *Poltava* to carry missiles. Some US experts speculated that the ship might be carrying ballistic missiles, because the Soviets used large-hatch ships such as the *Poltava* to deliver such missiles.
- Had a vessel experienced mechanical failure en route, the captains were told to explain to any ships offering assistance that they were exporting automobiles. If such an encounter had occurred, it would have been a tipoff to analysts that something was amiss; the Soviet Union was not an automobile exporter at the time.
- Once deployed, the units were not well concealed from aerial reconnaissance. They had a characteristic imagery signature the Soviets did not change, and that led to the US discovery of the San Cristobal missile site in October—the beginning of the Cuban missile crisis.¹⁹

Though it didn’t accomplish its mission, the deception was a remarkably well-crafted multi-INT D&D effort that succeeded for a long time because the Soviets had a good understanding of US intelligence capabilities and predispositions. The United States, equipped with a similar knowledge of Soviet intelligence targets, returned the favor with its own deception twenty years later. We’ll visit that case shortly.

COUNTERING DENIAL AND DECEPTION

The introduction to this chapter noted similarities and differences between practicing medicine and analyzing intelligence. Another difference is that, in medicine, once doctors have a process for treating a pathology, it will in most cases work as expected. The human body doesn’t typically develop countermeasures to the treatment.²⁰ But in

intelligence, there is an opponent who may be able to identify the analysis process and counter it. The Soviet leak of accurate information illustrates another important point about protecting sources and methods: Analysis methods must be protected. If analysis becomes standardized, the opposing side can predict how you will analyze the available intelligence, and then D&D becomes much easier to pull off, as the Soviets did during the Cuban missile crisis.

The same rule applies to collection. When collection becomes too predictable—as can happen in large intelligence organizations—tactics for countering D&D no longer work. If opponents can model the collection process, they can defeat it. There is a tendency to believe that overhead (satellite) IMINT and SIGINT are less vulnerable to countermeasures. However, critics have pointed out that not only denial, but also effective deception, is possible against both IMINT and SIGINT if the opponent knows enough about the collection system.²¹ The effectiveness of hostile D&D is a direct reflection of the predictability of collection.

So both intelligence collection and analysis, by their nature, must evolve. Intelligence organizations cannot afford to establish a process and retain it indefinitely.

At one point in history, intelligence services were quite successful at both conducting and countering D&D because of a tight feedback loop. During World War II, intelligence analysts interacted continuously with HUMINT, IMINT, and SIGINT collectors and with customers to develop deception operations and countermeasures to the opponent's deception.

The target-centric approach models that process. Defeating D&D today depends, more than any other factor, on the strength of the relationships among the analyst, collectors, and the customer. Where a close working relationship exists among the players, the tiny inconsistencies or clues that signal D&D can be picked up and shared, exposing the fact that it is present. Though single-source and all-source analysts often are the focal points for identifying it, all stakeholders on the team have roles in defeating deception. Let's consider each.

The Analyst

In analysis, the first defense against D&D is maintaining alternative target models. Another important step is to continually develop new techniques for sensor fusion or synthesis of intelligence data. An analyst can often beat D&D simply by using several types of intelligence—HUMINT, COMINT, and so on—in combination, simultaneously, or successively. It is relatively easy to defeat one sensor or collection channel. It is more difficult to defeat all types of intelligence collection at the same time. Hyperspectral imaging, for example, is a valuable weapon against IMINT deception because it can be used to measure so many different aspects (signatures) of a target. Increasingly, opponents can be expected to use “swarm” D&D, targeting several INTs in a coordinated effort like that used by the Soviets in the Cuban missile crisis and the Indian government in the Pokhran deception. Such complex operations, however, as

in those examples, inevitably have their weak points. The analyst team has only to find them. The most effective weapon for countering D&D is an experienced and inquiring single-source or all-source analyst. One who also understands that success depends on two jobs: ensuring a close working relationship exists among all stakeholders, and considering the possibility of D&D at every turn in making judgments.

Collectors

Collectors make an important contribution to defeating D&D by making collection smarter and less predictable. There exist several tried-and-true strategies:

- *Don't optimize systems for quality and quantity; optimize for content.* One might, for example, move satellite-based collectors to less desirable orbits to achieve surprise or to keep opponents off balance. At the opposite extreme in sophistication, when collecting discarded papers (TRASHINT), don't keep coming back to the same dumpster every day at the same time.
- *Apply sensors in new ways.* Analysis groups often can help with new sensor approaches in their areas of responsibility. Also, techniques for defeating D&D that have been developed for one problem (counternarcotics, for example) may be applicable to others (weapons proliferation).
- *Consider provocative techniques against denial.* In the US Air Force airborne reconnaissance programs dating back to the 1950s, provocation was used effectively to overcome the practice of emissions control (EMCON) by the Soviets. In EMCON, one keeps all nonessential signals off the air until the SIGINT collector has left the area. The US response was to send an aircraft on a penetration course toward the Soviet border, for instance, and turn away at the last minute, after the Soviets had turned on their entire air defense network to deal with the threat—thereby providing the needed signals for collection. Probing an opponent's system and watching the response is a useful tactic for learning more about the system. Even so, probing can have undesirable consequences: The Soviets would occasionally chase and shoot down the reconnaissance aircraft to discourage the practice.
- *Hit collateral or inferential targets.* If an opponent engages in denial about a specific facility, supporting facilities may allow inferences to be made or expose any deception. Security measures around a facility and the nature and status of nearby communications, power, or transportation facilities may provide a more complete picture.
- *Consider that deception can be used offensively.* Military tacticians claim that the best weapon against a tank is another tank, and the best weapon against a submarine is another submarine. Likewise, the best weapon against D&D

is to mislead or confuse opponents about intelligence capabilities, disrupt their warning programs, and discredit their intelligence services. The Farewell Dossier case, discussed next, illustrates the offensive use of deception. It depended on the involvement of the third part of the counterdeception triad: the customer.

The Customer

As members of the team, customers may be able to identify a deception, based on their perspective and unique sources of knowledge. Also, customers typically have access to instruments that an intelligence community cannot easily use for both detecting and defeating deception. That sort of access turned out to be a critical factor in countering a Soviet deception and its associated covert action during the Cold War.

BOX 13.4 THE FAREWELL DOSSIER

In 1980, the French internal security service *Direction de la Surveillance du Territoire* (DST) recruited a KGB lieutenant colonel, Vladimir I. Vetrov, codenamed Farewell. Vetrov gave the French some four thousand documents, detailing an extensive KGB effort to clandestinely acquire technical know-how from the West, primarily from the United States. In 1981, French president François Mitterrand shared the source and the documents (which DST named the Farewell Dossier) with US president Ronald Reagan.

The documents revealed a far-reaching and successful intelligence operation that had already acquired highly sensitive military technology information about radars, computers, machine tools, nuclear weaponry, and manufacturing techniques. But the specific targets on the list provided the needed guidance for an effective counterstrike. And Gus Weiss knew exactly what to do with the list.

Weiss was a policymaker, serving on the staff of the National Security Council. Much of Weiss's government work had focused on technology transfers to communist countries. In contrast to many NSC members, he remained close to the intelligence community and especially to the CIA. He served on the Pentagon's Defense Science Board and the Signals Intelligence Committee of the US Intelligence Board. He frequented CIA headquarters, where he could often be found discussing Soviet economic and technical issues with analysts.

During the fall of 1981, Weiss was cleared to read the Farewell material. He devised an audacious plan: As he told an NSC associate, "Why not help the Soviets with their shopping? Now that we know what they want, we can help them get it." There would be just one catch: The CIA would add "extra ingredients" to the software and hardware on the KGB's shopping list. Weiss persuaded the director of central intelligence, William Casey, to take the idea to President Reagan, and the president directed Casey to make it happen.²²

In early 1982, the US Department of Defense, the FBI, and the CIA—with the help of industrial firms brought on board by Weiss and other NSC members—began developing a counterattack. Instead of simply improving US defenses

against the KGB efforts, the team used the KGB shopping list to feed back, through CIA-controlled channels, the items on it—augmented with “improvements” that were designed to pass acceptance testing but fail randomly in service. Flawed computer chips, turbines, and factory plans found their way into Soviet military and civilian factories and equipment. Misleading information on US stealth technology and space defense flowed into the Soviet intelligence reporting. The resulting failures were a severe setback for major segments of Soviet industry. The most dramatic single event resulted when the United States provided gas pipeline management software that was installed in the trans-Siberian gas pipeline. The software had a feature that would, at some point, cause the pressure to build up to a level far above the pipeline’s fracture pressure. The result was the Soviet gas pipeline explosion of 1982, described as the “most monumental non-nuclear explosion and fire ever seen from space.”²³

Mounting a counterdeception campaign (which the Farewell operation was) often requires extensive effort, but sometimes it is worth the payoff. The Farewell operation was expensive to run but produced many benefits; it may have hastened the end of the Cold War. But for the active support of the intelligence customer, it is unlikely that Farewell would have fared so well.

In many ways, the Farewell operation was the perfect counterintelligence response. Even its subsequent exposure did not reduce the effectiveness of the operation, since the exposure called into question all of the successful KGB technology acquisitions and discredited the KGB’s technology collection effort within the Soviet Union.²⁴ Detailed knowledge of an opponent is the key to successful counterintelligence, as the Farewell operation shows. The operation would not have been possible without the comprehensive details that Vetrov provided, which allowed the United States to create specific models of the KGB targets, the nature of the KGB operations, and the linkages—that is, the use of other Warsaw Pact country intelligence services in the technology acquisition effort.

Farewell was a model of collaboration, not only within US intelligence but also with allied governments and with industry. The operation would have been far less successful without the assistance provided by manufacturers in several countries. And it would probably never have happened if a customer—specifically, Gus Weiss—had not been part of the target-centric process.

A detailed discussion of methods for countering D&D is contained in Robert Clark and William Mitchell’s *Deception: Counterdeception and Counterintelligence* (2019). The book points out that analysts should be especially alert to deception when

- A potential deceiver has a history of conducting deception
- Key information is received at a critical time or from a source whose bona fides are questionable
- Analysis hinges on a single critical piece of information or reporting
- New information would require altering a key assumption or key judgment

- Accepting new information would cause the decision maker to expend or divert significant resources
- A potential deceiver may have a feedback channel to check on the success of deception²⁵

Finally, detecting deception depends on looking at all the ways in which information is reaching your network through both intelligence and nonintelligence channels, and identifying abnormal congruences and incongruences in the reporting.²⁶ These should be red flags that require a close investigation for possible deception.

SIGNALING

Like denial and deception, signaling relates to one intelligence service intentionally shaping what an opposing intelligence service sees. Also like D&D, its use depends on a good grasp of how the opposing intelligence service obtains and analyzes knowledge. For that reason, signals are addressed in this chapter.

The goal here is not to deny or deceive but just the opposite: to send a legitimate message about intentions. Depending on the situation, signals can be made verbally, by actions, displays, or subtle nuances that depend on the context. Recognizing and interpreting an opponent's signals is one of the more difficult challenges an analyst must face.

In negotiations, signals can be both verbal and nonverbal. True signals are used in place of open declarations, to provide information to the other side while preserving the right of deniability.

One signal that has gained use with the increase in satellite imagery is the purposeful display of items in an imaged area to send a message. Massing troops on a frontier as an intimidation tactic is an example. It is such a well-known maneuver that, in July 1990, Saddam Hussein's massing of troops on the Kuwaiti border initially was interpreted as such a signal, intended to put pressure on Kuwait in order to obtain economic concessions in upcoming negotiations. It was in fact something far less subtle—a preparation for invasion. The massing of Russian troops on the Ukrainian border in 2022 was also interpreted by some observers as an intimidation tactic. Only the United States and some European intelligence agencies recognized it as a precursor to invasion.

Analyzing signals requires examining the content of the signal and its context, timing, and source. Statements made to the press are quite different from statements made through diplomatic channels—the latter usually carry more weight. As an example of context, a statement made by the Egyptian ambassador to a US military attaché at an embassy social function could easily be a signal; the ambassador knows that he is speaking to an intelligence officer.

Signaling between members of the same culture can be subtle, with high success rates of the meaning being understood. Two US corporate executives can signal to each other with confidence; they both understand the rules. A US executive and an Indonesian executive would face far greater risks of misunderstanding each other's

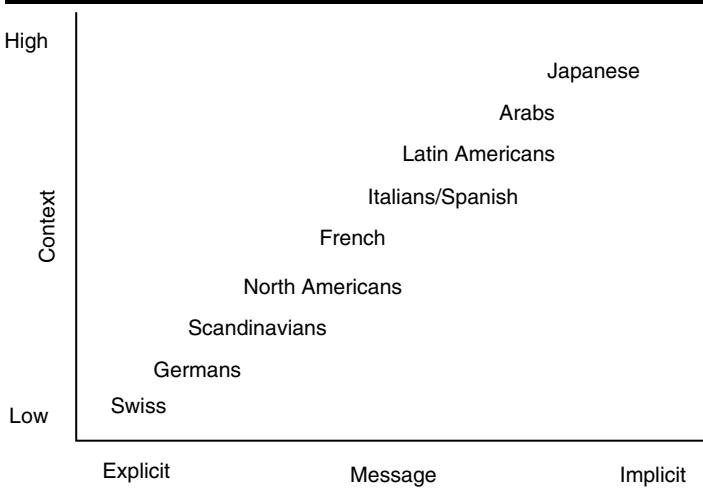
signals. The cultural differences in signaling can be substantial. For example, cultures differ in their reliance on verbal and nonverbal signals to communicate their messages. The more people rely on nonverbal or indirect verbal signals and on context, the higher the complexity. The Japanese, for instance, and the Chinese rely heavily on implicitly understood communications, and the context of any communication is also highly significant. As figure 13.1 indicates, the Swiss are at the opposite extreme; their messages are explicitly stated and often independent of context.

The importance of both implicit messages and context is illustrated in the final note submitted by Japanese diplomats to US Secretary of State Cordell Hull on December 7, 1941. Negotiations between the US and Japanese governments to resolve differences had reached an impasse, and the key parts of the note read as follows:

Hope to preserve and promote the peace of the Pacific through cooperation with the American Government has finally been lost . . . in view of the attitude of the American Government [Japan] cannot but consider that it is impossible to reach an agreement through further negotiations.²⁷

This was a *declaration of war*. But most Americans, less sensitive to context and more accustomed to explicit communication, would not read it as such. It might simply indicate a new phase in the negotiation, such as verbally upping the level of rhetoric. In no part of the message was the word *war* used. (To his credit, Secretary of State Hull did recognize the implications; he had considerable past experience in negotiating with the Japanese government.)

FIGURE 13.1 ■ Cultural Differences in Signaling



Source: Adapted from Edward T. Hall, *Beyond Culture* (New York, NY: Anchor, 1976).

Signaling is an art, and interpreting signals is an art. Failure to understand the signals can have severe consequences. In the Pearl Harbor case, Hull understood the signal, but nothing could be done. Because of an unexpected delay before Hull met with the Japanese ambassador, the attack was under way before he was presented with the note. Two brief examples illustrate the consequences of both failure to understand an opponent's signals and failure to understand that you are signaling the opponent:

- During the Korean War, as US and UN forces advanced north of the thirty-eighth parallel, China decided that a North Korean defeat was unacceptable. China's leaders moved aggressively on several fronts to signal their intention to intervene militarily if the advances continued. Diplomatic notes, press releases, and overt troop movements all were employed to send that signal. US policymakers and military leaders either dismissed or failed to understand the signals, and the Chinese intervention came as a surprise.²⁸
- In July 1990, the US State Department unintentionally sent several signals that Saddam Hussein apparently interpreted as a green light to attack Kuwait. State Department spokesperson Margaret Tutwiler had said, "We do not have any defense treaties with Kuwait." The next day, Ambassador April Glaspie told Saddam Hussein, "We have no opinion on Arab-Arab conflicts like your border disagreement with Kuwait." And two days before the invasion, Assistant Secretary of State John Kelly testified before the House Foreign Affairs Committee that there was no obligation on the United States's part to come to the defense of Kuwait if it were attacked.²⁹

The Iraq/Kuwait example illustrates the other side of signaling—and intelligence analysts can and should help their customers in this regard. Clearly, it is important to be able to tell a policymaker what the opponent's signals are and how to interpret them. But it is equally important to let policymakers know how their signals, whether intentional or not, are likely to be interpreted by the opponent.

SUMMARY

Intelligence analysis is a combination of art, tradecraft, and science. In large part, this is because analysts must constantly consider the possibility of denial and deception, which requires the artful application of tradecraft.

Many intelligence targets practice some form of denial. But in evaluating raw intelligence, analysts also must always be aware of the possibility that they may be seeing deceptive material deliberately provided by the opposing side to deceive. Deception—providing false information—takes more effort to execute, but it can have a big payoff.

When one intelligence service has extensive knowledge of another service's sources and methods, more ambitious and elaborate D&D efforts are possible. Often called *perception management*, these efforts involve developing a coordinated multi-INT campaign to get the opposing service to make a wrong initial estimate. Once this happens, that service faces an unlearning process, which is difficult. A high level of detailed knowledge also allows for covert actions to disrupt and discredit the opposing service.

Defense against D&D starts with the denial of your intelligence capabilities to opposing intelligence services. Some collection sources and methods have to be heavily protected, or they will become vulnerable to D&D. Names of HUMINT sources, the nature of COMINT or many types of technical collection, and the decryption of messages all fall into this category. In contrast, the information a source provides is accorded less protection than details about the source itself, because the information provided needs to go to many intelligence customers. IMINT and open sources usually receive less source protection than do HUMINT, COMINT, or specialized technical collection.

A collaborative target-centric process helps stymie D&D by bringing together different perspectives from the customer, collectors, and the analyst. Collectors can be more effective in a D&D environment with the help of analysts. Working as a team, they can make more use of deceptive, unpredictable, and provocative collection methods that have proven effective in defeating D&D.

The opposite of D&D, yet closely related, is the practice of signaling: deliberately sending a message to the opposing intelligence service while maintaining plausible deniability. Like D&D, its success depends on a good understanding of the opponent to whom a signal is sent. Signals can be verbal, or by actions or displays. Analysts have to be alert to the presence of signals and adept at interpreting their meaning. When signals must be sent between different cultures, it's important to recognize that they may be misinterpreted or missed altogether.

CRITICAL THINKING QUESTIONS

1. The literature has extensively documented many examples of successful deception. Operations Mincemeat, Bodyguard, and Fortitude are three notable ones that the Allies conducted during World War II. The Soviets had an initial success in the lead-up to the Cuban missile crisis. During the 1970s, the United States ran a deception to conceal attempts to recover a sunken Soviet submarine (Project Azorian). And the United States misled the Soviets in the Farewell Dossier case. Choose one of those cases (or one selected by your instructor) and consider the six factors (listed after the Farewell Dossier case in this chapter) that should alert an analyst to possible deception.

- a. Which factors could have provided an alert to the victim of the deception?
 - b. Justify your choice(s).
2. In dealing with the Farewell case material, the United States had other options than the one actually taken. The CIA had the specific target lists that the KGB was using. It had the identities of the KGB officers in Soviet embassies worldwide who were responsible for collection.
 - a. Describe some possible options for dealing with the threat, other than the one that was taken.
 - b. What disadvantages did those options have that likely led DCI Casey to choose the “contamination” option?
 3. This chapter discusses the four elements of deception: truth, denial, deceit, and misdirection. Identify the features of the Cuban missile crisis deception and the Indian nuclear test deception that fit each element. Your instructor may ask you to use additional resources.
 4. National leaders frequently signal their intentions to make a point or to gain an advantage. In current or recent world events, can you find an example of what appears to be signaling by a senior government official? Consider especially possible signals in the political, economic, or social arenas.

NOTES

1. Steven Marin, “Intelligence Analysis: Turning a Craft into a Profession,” https://analysis.mitre.org/proceedings/Final_Papers_Files/97_Camera_Ready_Paper.pdf.
2. Rob Johnson, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: CIA Center for the Study of Intelligence, 2005), 43.
3. Doctors must routinely deal with patients who conceal embarrassing information. But the patient seldom if ever is trying to lead the doctor to an incorrect diagnosis.
4. Edward Waltz and Michael Bennett, *Counterdeception Principles and Applications for National Security* (Boston, MA: Artech House, 2007).
5. Ewen Montagu, *The Man Who Never Was* (Annapolis, MD: Naval Institute Press, 1953).
6. Ben Macintyre, *Operation Mincemeat* (New York, NY: Harmony Books, 2010), 201–2.
7. International legal protocol surrounding the shipment of lethal weapons requires that the shipper have a certificate of “end use,” in which the buyer declares that the weapons are for its use only and will not be trans-shipped.
8. Brian Wood and Johan Peleman, *The Arms Fixers* (Oslo, Norway: International Peace Research Institute [PRIO], 1999), chapter 5, http://www.nisat.org/publications/arms_fixers.
9. Ibid.

10. US Department of Defense, "Background Briefing on Enemy Denial and Deception," October 24, 2001, <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2162>.
11. Amaury Murgado, "Drug Interdiction for Patrol," *Police Magazine*, September 5, 2012, <http://www.policemag.com/channel/careers-training/articles/2012/09/drug-interdiction-for-patrol.aspx>.
12. A démarche is a political or diplomatic step, such as a protest or diplomatic representation made to a foreign government.
13. Tim Weiner and James Risen, "Policy Makers, Diplomats, Intelligence Officers All Missed India's Intentions," *New York Times*, May 25, 1998.
14. Ibid.
15. "Strategic Deception at Pokhran Reported," *Delhi Indian Express* in English, May 15, 1998, 1.
16. Weiner and Risen, "Policy Makers, Diplomats, Intelligence Officers."
17. Ibid.
18. James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence* 46, no. 1 (2002), <http://www.cia.gov/csi/studies/vol46no1/article06.html>.
19. Ibid.
20. This analogy has its limits, of course; microbes do develop resistance to antibiotics over time.
21. Angelo Codevilla, *Informing Statecraft* (New York, NY: Free Press, 1992), 159–65.
22. Gus W. Weiss, "The Farewell Dossier," *Studies in Intelligence* 39, no. 5 (1996), www.cia.gov/csi/studies/96unclass.
23. Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (Novato, CA: Presidio Press, 2004).
24. Weiss, "The Farewell Dossier."
25. Robert M. Clark and William L. Mitchell, *Deception: Counterdeception and Counterintelligence* (Thousand Oaks, CA: Sage/CQ Press, 2019), 170.
26. Ibid., 174.
27. "Japanese Note to the United States, December 7, 1941," *Department of State Bulletin*, vol. V, no. 129 (Dec. 13, 1941), Yale Law School, <http://avalon.law.yale.edu/wwii/p3.asp>.
28. P. K. Rose, "Two Strategic Intelligence Mistakes in Korea, 1950," *Studies in Intelligence* (Fall/Winter 2001), http://www.cia.gov/csi/studies/fall_winter_2001/article06.html.
29. Jude Wanniski, "Where Did Saddam Hussein Come From?" *Wall Street Journal*, February 19, 1998.

Sherman Kent, often described as the “father of intelligence analysis,” wrote in 1949 that “intelligence cannot serve if it does not know the doers’ minds; it cannot serve if it has not their confidence; it cannot serve unless it can have the kind of guidance any professional man must have from his client.”¹ Getting intelligence to serve, to use Kent’s words, depends on having the customer involved—a key part of the target-centric approach. Once the customer is engaged in the process, communicating the results becomes much less difficult, and the customer is more likely to understand and use the intelligence. The British model introduced in chapter 5, of having analysts and customers work together on intelligence assessments, has demonstrated that the approach works.

This chapter discusses the process of preparing and delivering the intelligence product, which typically requires an analyst to work three steps:

1. Develop either a written or a verbal report (typically, a briefing).
2. Go through some form of product review.
3. Gain customer acceptance.

STRUCTURING THE MESSAGE

Throughout this book, we have emphasized the reasons analysts must learn effective communication skills, in both writing and speaking. Taking a broad view, there are procedures for writing a report or presenting a briefing, generally recognized across professions. Some are institution specific. Analysts should pay strict attention to their particular organization’s technical quality and style guidelines. Following the conventional standards for publications in the appropriate area and using terminology that customers understand will help ensure acceptance. In general, analysts should present results that

- Are forward looking, with predictions of future developments or of major trends in the subject area and descriptions of the factors driving those trends
- Contain clearly stated conclusions supported by research and technical reasoning
- Include clear explanations, at the customer’s level, of complex technical subjects

Moreover, it's essential to do all of this *succinctly*. One way to develop the analytic product is through a rapid prototyping approach that starts with the issue decomposition and expands a preliminary target model into a final report or briefing. In that process, you are continuing to update the issue definition as you develop the target model and draw or refine analytic conclusions. The advantage is that, at any point, you have available (and the rest of your network should also have access to) the most current picture of the issue and target.

The type and the format of the presentation are shaped by the preferences of the customer or customer class; generally, a short, to-the-point, graphically oriented presentation works best. Think of the types of one-liners that pop up online—whether as spam or as interesting headlines with pictures to entice clicks. Let's start with three basic rules that are essential to getting the message across.

Write for the Customer

Many—possibly most—customers have favorite INTs. That is, they have “personal and organizational preferences for, and biases against, specific intelligence collection disciplines, or ‘INTs.’”² British Prime Minister Winston Churchill, for example, especially trusted HUMINT and COMINT. His opponent, Adolf Hitler, relied primarily on OSINT, even though he had other, more reliable, sources. US president Jimmy Carter valued COMINT and IMINT but initially mistrusted HUMINT.³ Find out if the customer has such preferences and ensure that supporting arguments cite those “favorite” INTs where feasible.

You should also have a pretty good idea what presentation form will attract your customer's attention. For example, in the case of the premier US customer, the president, analysts have found that each president has a definite preference. Some prefer a carefully reasoned analytic approach in written form. Some want a verbal presentation, and a few like to see imagery or photographs. President Trump reportedly had a unique preference that intelligence officers adjusted to. According to White House officials, intelligence reports had to be on a single page, with as many pictures and maps as possible—which is not a new thing. But, more important, the president would pay attention only to those reports that mentioned his name. So the reporting that he received consistently included frequent references to him by name.⁴

Finally, consider the extent to which a decision maker is able or willing to act on the intelligence conclusions. That should not stop you from providing the assessment, but it should mitigate any surprise at the decision maker's later actions. If the report's conclusions are that important, be prepared to work to get buy-in, as discussed later in this chapter. As an example, US policymakers for six decades routinely “downplayed, deflected, or ignored” intelligence about Israeli, Pakistani, and North Korean nuclear weapons programs—either for political reasons or because they simply had no leverage over those governments. In contrast, the policymakers

had leverage, and used it, to stop nuclear weapons efforts in South Korea, Taiwan, and Libya.⁵

Support Every Analytic Conclusion

Whether a written report, an e-mail, or a verbal briefing, all conclusions must be clearly traceable to the results from the target framework and explained in the body of the presentation. Provide, explain, and emphasize key intelligence insights. The customer should be able to follow the reasoning at every turn. Highlight key words, phrases, or sentences to stress their importance.

The final written product should include a concise executive summary right up front to allow the busy reader to get “the bottom line” without poring through page after page of details. Limit the executive summary to one page. Follow that with a more detailed description for the decision maker’s staff and for fellow analysts. The description should contain enough detail to allow another analyst to duplicate the results.

Separate Facts from Analysis

Make it abundantly clear when moving from fact to analysis. Never cover up evidence with slick writing. As noted in chapter 11, analysts inevitably have to work with incomplete and conflicting information. For this reason, the finished presentation must clearly articulate what is known (the facts), how it is known (the sources), what drives the judgments (linchpin assumptions), the impact if these drivers change (alternative outcomes), and what remains unknown. Customers expect logical and objective arguments. Detailed evidence may or may not be appropriate, depending on the scope of the topic and the audience’s technical sophistication, interest, and need. But readers or listeners should never be in doubt about whether they are getting facts or analysis.

First, *state the facts*. A typical intelligence assessment includes a summarization or brief description of relevant information, written by answering these questions:

- Who?
- What?
- When?
- Where?
- How?

Occasionally, results conflict with what the customer wants to hear—for example, they may undercut existing policy. Facts become critical in such a case. The only chance to change a policy decision (and a slim chance, at that) is to present concrete, persuasive evidence, and solid factual evidence is the best kind.

Second, *analyze the facts*. The *who-what-when-where-how* questions usually elicit the facts of the situation, but answers to those questions normally require analysis. An intelligence assessment answers, typically, two other questions:

- Why?
- So what?

The *why?* and *so what?* questions require analysis that extends beyond the facts. *So what?* answers the customer's question of, "Why should I be concerned about this conclusion?" Both questions require an analytic opinion. At this point, analysts are no longer reciting certainties, or simply reporting; they are doing *analysis*. Answering these questions may also require a source reliability evaluation, using the guidelines established in chapter 11.

PRESENTING THE MESSAGE

Developing effective written reports and verbal briefings is time consuming. Each type has its advantages:

- The report gets wider circulation and typically has a longer life. Most analysis projects conclude with some type of written report.
- The briefing has the advantage of the customer providing direct and immediate feedback. Verbal briefings are probably the primary communication method for executives. Decision makers usually value the two-way exchange, and the analyst in turn should value the feedback.

The availability of secure electronic communication has opened up new forms of conveying intelligence assessments to customers at remote locations, and there is a definite trend to make these interactive. They can take the form of a hybrid written product and verbal briefing, for example.

Again, the important thing is to fit the presentation to the style of the key customer(s). Although most executives prefer briefings, some like written reports and an increasing number want electronic communication. If possible, conduct an intelligence effort on the key customer (which the customer's staff will usually cooperate in). Find out the customer's favorite way to get information. Some prefer more text; some want graphics. A few may want lots of supporting data in the form of facts and figures. But whatever the presentation format, the basic rules for engaging the customer remain the same. Some time-tested key principles are described in the sections that follow.

Get to the Point

Because most intelligence products provide information, customers expect to hear clear, concisely stated conclusions and projections at the beginning. This means writing with a purpose—which, if the issue has been defined properly, will be straightforward.

Plunge right in. Never build up to the main point. Put it in the beginning of each section. Give recommendations before justifications, answers before explanations, conclusions before details. Analysts are not in the business of writing mystery novels. Shorter is better. For written products, ten pages is reasonable; but two or three pages is the limit for a busy policymaker (and they all are busy). Ideally, keep everything that the policymaker needs to know on one page.

Beating around the bush irritates people. Don't do it.

Write or Brief to Inform, Not to Impress

The formal communication skills most students learned in academia involved presenting material to a professor. The main purpose was impressing upon someone who knew more than you did how well you, too, had mastered the subject area. The audience in a work environment is drastically different. Consequently, the style and technical content of the products should be too.

In intelligence work, the expert is the presenter, not the customer. Hence, the analyst must write to inform. The intended message needs to be as clear as possible and, again, tailored to the audience. Do not assume the customer will be familiar with technical jargon or with the consequences or implications of observations or calculations. To communicate effectively, use vocabulary familiar to both the intelligence community and the customer. To introduce new terms, start from common ground, some unified understanding. This shared understanding permits the introduction of something new. The new term or concept then becomes common and can be used in turn to introduce something else new. Work from old to new, and do so in a logical, easy-to-follow manner.

Make It Easy and Enjoyable to Read or Listen to

Statistics show that most intelligence customers look at the summary of a paper and a slight majority will read the preliminaries. Few will read the technical discussion or the appendices. Similarly, it is well known that audiences pay attention for about the first five minutes of a briefing; their attention drops off markedly thereafter. As a writer or briefer who has spent a great deal of effort on the body of the presentation, why not raise the odds of getting this portion of a paper read, or that part of the briefing absorbed? The best ways to do that are to make the prose fun to read, the briefing entertaining, and the message obvious. Practice empathy; look at the message from the

customer's perspective. If possible, tell a story. Most readers are captivated by stories, especially those having a human-interest theme.

Good writing is hard work. But hard work is necessary to make it easy for recipients to digest the intended message. It is a dangerous gamble to make them work unnecessarily. They always have the choice of not reading (or listening to) the analysis or not finishing it. It is essential therefore to make the product as easy and fruitful as possible to follow. If a written product is a struggle to read, chances are it won't be.

Standardize the products and the source information. Customers need to see a standard product line and know where to look to find information. For example, don't have both one- and two-column products. Also avoid continuous text; it is difficult to absorb. If longer text is necessary, break it up with formatting such as bold text, bullets, and text boxes. Except for this: An all-caps message is the worst. It universally frustrates readers.

Write as You Would Talk

Write as you would talk to someone directly. Use declarative sentences. Avoid the passive voice. Writing should not be as informal as conversation, however. And there is no place for "texting" norms. There are two extremes to avoid: stilted writing and the opposite—informality that detracts from the message or reduces its credibility.

The major challenge in presenting a written message is the need for precision of expression. It is obvious in scientific and technical intelligence, but it occurs across all disciplines in intelligence, for a good reason. Analysts often find that their words are interpreted (or misinterpreted) by policy customers to fit with the customers' preferred course of action. The response by analysts, especially in NIEs, is to make precise expression an art form that is studied and practiced. As Michael Herman noted, precision of expression is rated very highly by analysts and their managers in intelligence communities in both Britain and the United States.⁶ But it too often causes the customer to lose focus or discount the product.

In preparing written intelligence, there is always an easier way, a clearer way, a more accurate way to say something. Unfortunately, they are not the same way. It is almost axiomatic that if a scientific and technical intelligence report is readable and understandable, it is technically inaccurate. And it happens in other intelligence disciplines on occasion. Only a highly skilled analyst can achieve technical accuracy and readability in one document. The next two steps can be helpful.

Avoid Acronyms

Use acronyms only after defining them. Even standard acronyms in common use throughout an organization may cause problems for customers from the outside. It is acceptable to use a standard list of acronyms that are defined in an appendix or a glossary.

Present the Message Visually

Nonfiction text can be boring. And since intelligence is not about writing fiction, the best bet is to avoid using text alone. Rely on visual aids to illustrate points. In fact, a general rule is the more graphics, the better. They help to explain and support the text and summarize data; the adage that a single picture is worth a thousand words still holds. One of the most memorable intelligence graphics ever produced was prepared in 1971 by an engineer from outside the intelligence community—James Headrick of the Naval Research Laboratory. Intelligence analysts were assessing a new Russian radar that, at the time, had the most massive antenna in the world. Headrick used a picture of the National Mall in Washington and put in it a white block scaled to the size of the radar antenna. (He couldn't include a picture of the antenna itself; it was classified.) The white block filled the Mall and was taller than the Washington Monument. This graphic was greatly admired, and copies of it were widely circulated because it carried a clear and easily understood message: The Russians know how to build really big and powerful radars.

Annotated pictures and maps that include all the main points are always well received. As are video clips. The key is to liberally annotate (or add verbal commentary, for video) such that they are self-explanatory. Also, be sure to refer to every figure and table in the text. Probabilities and statistics are convincing, but never use numbers alone. Graphics that provide a tour of the conclusions are remembered; straight text is not. Finally, use multimedia freely.

REVIEWING THE ANALYTIC PRODUCT

In chapter 13, we referred to a “sanity check,” where the analyst takes a step back to review, one last time, the draft product of the analytic effort. After that action, it’s time to have an independent validation of the product. This usually will include peer and management review. These are positive steps, intended to help the final product; analysts should welcome them. Often, a red team analysis or the use of a devil’s advocate also is needed.

Peer Review

The results and conclusions of a study are clear to the person who is closest to the work; they are not so straightforward to someone not involved in the study. Furthermore, results and conclusions should be carefully scrubbed for both apparent and actual contradictions. So, the one collaborative mechanism that many intelligence units insist on is peer review. It can be formal or informal. But if no other review is done, the analyst should at least ask for an informal review by another analyst. That’s common practice in current intelligence. Take advantage of every opportunity for a peer review of the final product. Colleagues can provide excellent feedback on the flow, logic, and clarity of the message.

Some form of peer review is an essential part of in-depth analysis. Analysts make conclusions based on judgments; that requires going beyond the facts, and any two analysts are likely to come to different conclusions. Formal peer review provides a final check on conclusions and on the tradecraft used to reach them.

When done properly, peer review (informal or formal) is important for another reason: The criticism and consequent rethinking of issues consistently improves the final product. In chapter 8, we noted the flawed premise about criticism in brainstorming (that it inhibits original thinking). The same principle applies in peer review: Criticism produces original ideas and fresh approaches as well as identifies weaknesses in analytic arguments.

Management Review

Management review is also necessary, up to a point. One level of management review is almost mandatory in both all-source and single-source analysis. Even fusion center or current intelligence products usually have one level of management review. But it's also common for the analytic product to receive additional upper-level reviews. One pragmatic motivation for multiple management reviews is to protect the organization's reputation for quality analysis.

Whether the additional management reviews add value is a contentious issue. Analysts sometimes receive contradictory guidance from multilevel reviews. Studies of the problem have suggested that multiple reviews are frustrating for analysts without necessarily being worthwhile.⁷

A more formal type of review involves red teaming or the use of devil's advocacy.

Red Teams

Red teams are formed to look at the analytic product from an adversarial perspective. Red teaming is often used to analyze an opponent's decision making—which is likely to differ markedly from how we would expect someone from our own culture to decide in similar circumstances. It is also useful in assessing an opponent's likely strategies and tactics. For example, opponents will have

- *Different beliefs.* A government may have a radically different model of the world, which would impact its leader's decision making. An isolated despot, for instance, may believe that he is the target of a foreign conspiracy and act accordingly (consider North Korea's Kim Jong-un or Russia's Vladimir Putin).
- *Different objectives.* Democratic governments tend to pursue peace and economic stability because those are in their direct interests. But states can be motivated to encourage political and economic instability for reasons of international attention or ideological expansionism (again, consider North Korea and Russia).

- *Different capabilities.* The powers of Western governments are heavily constrained by legal and institutional factors, but states differ widely in this regard: An autocratic state may have less economic power but more ability to make and execute political and military actions without concerns about internal opposition (consider Russia's ongoing political and military support for repressive regimes in Belarus and Syria and its ability to disregard internal dissent during the 2022 Ukraine invasion).
- *Different moral constraints.* For a number of reasons, states and nonstate groups differ in the tradeoffs they are willing to make between the achievement of their objectives and the moral costs in battle casualties, human rights, and protection of the innocent (again, consider the Syrian government's actions against the rebels, resulting in the deaths of innocent civilians since 2011, and of Russian atrocities during 2022).

Red teaming also can be used in the early stages of analysis to help in issue definition, but it is particularly useful in evaluating the final product. If done well, red teaming produces helpful insights that differ from products that do not focus on foreign thinking and processes in the same critical fashion. It is also dependent on the red team having a high degree of subject matter expertise to provide inputs and involves a considerable amount of pre-event preparation and effort.

Devil's Advocate

Devil's advocates take a position they do not necessarily agree with in order to provoke a debate. In taking the position, an individual assuming the devil's advocate role seeks to engage others in an argumentative discussion process. The purpose in the analytic setting is to test the validity and quality of the product and to identify weaknesses in logic, assumptions, or conclusions.

Devil's advocacy can be effective at checking conventional wisdom and countering groupthink, but it's difficult to do well. Ideally, devil's advocates would honestly believe and strongly support the counterarguments they present. And the "mainstream" analysts would seriously reexamine their conclusions based on rational consideration of those counterarguments. It has been suggested, though, that poorly presented (or poorly received) contrary arguments may create antagonism and result in the mainstream analysts becoming entrenched in their positions.⁸

CUSTOMER INTERACTION

The intelligence assessment is finished, reviewed, and out the door. Is the analyst finished? NO. In the target-centric approach, the delivery of intelligence to the customer is also an interactive process. Feedback from the customer is part of that interaction.

This can be a challenge when there is more than one customer, and it is quite impractical when the customer set is large. But analysts should be able to obtain feedback from *some* of the customers in that case.

The traditional intelligence cycle diagram depicted in chapter 3 (figure 3.1) has a block labeled “dissemination.” It’s yet another indicator that the cycle doesn’t really work that way. The report doesn’t just go out the door and the analyst’s job is complete. Successful analysts know that the most brilliant piece of intelligence analysis may as well have gone into the trash if it is not read by the right people in time for them to act on it. Analysts using the target-centric approach make sure that the person who initiated the request sees their report or receives a briefing—ideally, both. They get copies to other people who may have an interest in the results. They ask for feedback from as many of them as possible. *They can do these things because the customer has been involved in the process from the start.*

Chapter 4 identified major intelligence customer sets and the importance of understanding their perspectives. Remember that (a) analysts have to enter the interaction at the customer’s level, which can be quite different when dealing with a president’s national security advisor, a combat commander, a police captain, or a chief executive officer, and (b) the effectiveness of this interaction depends critically on the level of mutual trust and confidence between the customer and analyst. But for policymakers, the road to trust is seldom easy. Military commanders and their intelligence officers can usually establish a high degree of mutual trust; they are working together for a common goal against a common enemy. Neither is much concerned the other will share their confidences with the enemy. But policymakers often must deal with people who leak information to derail their policies, so analysts must demonstrate their ability to protect shared confidences. And trust is a two-way street. Analysts have to have some confidence that their assessments will not be twisted or misconstrued to fit a policy preference.

Even when a level of trust has been established, the analyst’s next job can be difficult: getting buy-in. That is, helping the customer to accept the message and consider acting on it. It’s especially challenging if the message runs contrary to the customer’s mindset.

ANALYST AS ADVOCATE: GETTING BUY-IN

A major problem of intelligence in sixteenth-century Europe was that spies could readily acquire information, but governments lacked the breadth of understanding to readily grasp its significance and act accordingly.⁹ Governments today are more sophisticated, but the issues they face are much more complex. The challenge for analysts today is still to help customers grasp the significance of intelligence.

If analysis is conducted as it is promoted in this book, customers will usually accept and make use of the results. But if the customers have not been closely involved in the

process, then they are more likely to ignore or reject the results. When that happens, analysts must shift their interpersonal skills in the direction of advocacy and act as a spokesperson in support of the analytic conclusions. Difficult as it may be, it is time to set objectivity aside and assume the opposite role—that of persuader. Now is the time to turn toward getting the analytic product read or heard and understood.

At the beginning of the analysis project, determining requirements and needs is marketing—finding out what the customer wants. This section is about sales—getting the customer to want (and use) what you have produced. The proper analytic attitude is made clear throughout this text: one of objectivity. But once analysis is finished, analysts must sell the product because they quickly encounter one of the fundamental principles of physics that also is a fundamental principle in intelligence: Every action produces an equal and opposite reaction. Intelligence is often tasked for a report because there is disagreement about an issue among customers. It follows that the analyst's results, then, will be met with skepticism or outright opposition by some.

Recognize, however, that “selling” is a controversial recommendation. The Iraqi WMD Commission report criticized this tendency, noting, “In ways both subtle and not so subtle, the daily reports seemed to be ‘selling’ intelligence—in order to keep its customers, or at least the First Customer, interested.”¹⁰

Analysts nevertheless often have no choice but to advocate for the product. Ideally, intelligence would be a commodity like food—consumers buy it because they need it. In operations, especially in military operations, that tends to be the case. Unfortunately, in policy support, it is more like insurance: It has to be sold, and buyers have to be convinced that they are getting a good product. On being reminded by an analyst that he had been warned about the impending outbreak of a war, then-national security advisor Henry Kissinger reportedly said: “You warned me, but you didn’t convince me.”¹¹ The implication could not be clearer. If policymakers expect intelligence analysts to convince them, analysts have to persuade.

One problem with looking at intelligence as sales, especially in policy matters, is that it increases the danger of telling customers what they want to hear.¹² Another challenge is that the analyst needs a good sense of timing (as every salesperson knows).¹³ Nevertheless, veterans of the business have consistently noted the need to persuade. Customers in the policymaking realm often do not understand the analytic mission, values, or standards. They tend to be skeptical of intelligence, especially if they are new to the policymaking world. They formed their views about who we are, what we do, and how we do it from the same sources as most Americans: popular media, the press, and congressional reports—not always the most accurate or sophisticated of sources. As Martin Petersen, author and former CIA senior intelligence officer, observed, “The reality for intelligence officers is that we must woo them [policymakers], sell them on the need for our services, and demonstrate the value of our material daily through its timeliness and its sophistication.”¹⁴

Policymakers are remarkable clients for another reason: Many come from the legal community. Lawyers prefer to use intelligence experts as they would use scientific experts in a courtroom: receiving testimony on the facts and opinions, cross-examining, determining the key issues, and deciding. The existence of a controversy and of differing opinions is essential, in the attorney's view, to establishing the truth. Lawyers are uncomfortable with a single expert opinion and with the intelligence compartmentation system. To them, the intelligence community's traditional compartmentation system for protecting sources and methods is suspect because it tends to conceal evidence and is therefore inconsistent with the goal of the discovery process in civil litigation. In dealing with a customer who has a legal background, advocacy skills are invaluable.

Obtaining acceptance from any customer can also depend on reputation. A reputation for credibility and veracity among customers is the analyst's most valuable asset. It takes a long time to build and can be lost in a day. Or, as David Landes observes, "In the public domain, a reputation for veracity is worth more than valor and intelligence, and this especially in a world of ubiquitous guile and duplicity."¹⁵ It's important to get the customer to pay attention, but it's not worth sacrificing credibility or truth to do it. A few examples:

- The KGB was discredited in the eyes of Soviet leadership when the Farewell operation (see chapter 13) became public, and all of its materiel acquisition results thereafter were called into question.
- During the Vietnam War, the CIA discounted and underestimated the magnitude and significance of North Vietnamese support reaching the Viet Cong through Cambodia's port of Sihanoukville. Subsequent information from a newly recruited source in the Cambodian port showed that the agency's estimates were wrong and the military's were more accurate. Afterward, whenever the CIA disagreed with the Pentagon, White House staffers would ask the director of central intelligence, Richard Helms: "What about Sihanoukville?"¹⁶
- The Iraqi WMD miscall damaged the credibility of several intelligence community analysis groups, especially the CIA's. Though progress has been made, it will take decades to overcome the whole of that damage.

AFTERMATH: DEALING WITH UNEXPECTED OUTCOMES

No matter how well an analyst has crafted and delivered the assessment, sometimes the result isn't what was envisioned or expected. Sometimes, the customer simply doesn't appear to make use of the intelligence. Other times, the customer uses it in such a way as to make analytic predictions appear to be wrong. Let's look at these two possible outcomes.

As noted in chapter 7, policymakers may be aware of the threat, and may even accept the analytic conclusions, but for their own reasons choose to pursue a policy that does not deal with the threat. Heads of government are particularly prone to inexplicably bypass their analysts. In chapter 11, we touched on the problems caused by Winston Churchill's inclination to be his own analyst. Josef Stalin and Adolf Hitler were noted for doing their own intelligence analysis, and neither of them was particularly good at it. Hitler, in particular, had his intelligence services competing to curry favor with him by providing interesting tidbits of intelligence. His ineptness as an analyst was one of the reasons the British chose not to attempt an assassination during World War II; they feared that he might then be replaced by a more competent military leader.

Seldom has there been an example in the United States of customer disregard of intelligence to match that of Lyndon Johnson's administration during the Vietnam War. CIA analysts repeatedly told the administration during 1963 to 1965 that substantially increasing combat operations in Vietnam would not result in a victory; the war was essentially a political-military struggle to be won in the South and primarily by the South Vietnamese. Their conclusions were ignored. From 1967 to 1968, despite pressure from the White House, the US Embassy in Saigon, and the military leadership in Vietnam to provide a more favorable assessment, CIA analysts provided accurate assessments of enemy strength in South Vietnam, indicating it was about twice what the US military was willing to acknowledge. The military's own intelligence analysts in Vietnam also found their assessments of the deteriorating situation suppressed by their commanders.¹⁷

Previous chapters touched on Saddam Hussein's invasion of Kuwait, another example of customer disregard for intelligence. The US national intelligence officer (NIO) for warning had provided repeated warnings of the attack that were disregarded at the national policymaking levels in the days prior to the invasion. On July 25, 1990, the NIO issued a "warning of war" estimating the chances of an Iraqi incursion into Kuwait at 60 percent. Early on August 1, the NIO issued a "warning of attack," indicating that there would be no further warning. The warnings went to all senior policy officials in the Defense Department, the Joint Chiefs of Staff, and the White House. The next day, on August 2, Iraq attacked.¹⁸

A senior Pentagon official subsequently admitted that neither warning was taken seriously because senior US officials contacted a number of leaders in the Middle East and the Soviet Union about the possible attack. All those contacted were of the opinion that Hussein did not intend to attack.¹⁹ The incident illustrates a challenge that analysts must continue to deal with: Most customers have their own sources of information, and they may choose to believe those sources, even when they directly contradict the assessments of the customer's own intelligence service. A number of factors—political considerations or constraints the analyst is unaware of, for example—may drive the customer in another direction. And as observed previously, the customer always has the prerogative to take actions that are contraindicated by the intelligence.

This outcome—disregard—is far less likely to occur in a target-centric analysis process. The customer, having been involved in the process of drawing conclusions and having had a chance to make inputs to the target framework, is more strongly inclined to accept and use the results. And the analyst, having insights into the customer’s thinking and constraints, is better prepared to understand when the customer does not use the intelligence as expected.

The opposite situation can also occur in anticipatory analysis, the subject of part III: The customer (or someone else) acts on the intelligence and thereby changes the anticipated outcome. This happens frequently. The policymaker accepts the results and, based on the intelligence, takes actions that prevent a predicted undesirable outcome from happening. Or the intelligence prediction in some way becomes public, thereby changing the outcome. For example, when a 1980s CIA assessment of the Soviet economy became public, the Soviets took action to prevent the predicted outcome.²⁰ The breakup of Yugoslavia (see chapter 23) is an example of an opposite result; the breakup may have been helped along by the publication of the national intelligence estimate predicting it. In cases such as these, analysts have to be satisfied with the knowledge that their results were correct, understood, and clearly accepted—and move on.

SUMMARY

In preparing the analytic product, begin by understanding how the customer likes to receive intelligence, and do it that way. Clearly explain and support analytic conclusions. Separate facts from the analysis of those facts. Place main points at the beginning. Make the message understandable, and design it to capture the customer’s interest. If possible, tell a story, and rely on graphics, especially to make complex concepts understandable.

Just before the product is ready to go to the customer, conduct some form of review, even on items with short deadlines; this is a critical cross-check that the message will not be misunderstood. It also provides a last check on factual or analytic errors. Peer and management reviews, red teams, and devil’s advocacy all can be used to provide this final check.

In dealing with customers, analysts have two challenges: to get the customer, first, to understand the message and, second, to accept and make use of the analytic results.

Making intelligence understandable requires communication skills and empathy—the ability to put oneself in the place of the customer. Getting the customer to accept and make use of intelligence may require an analyst to become an advocate—a controversial step. Acceptance also depends on the customer’s view of the analyst’s reputation.

Despite an analyst's best efforts, an analytic effort can have an unexpected result. Intelligence is occasionally disregarded or misused. Occasionally, the unexpected outcome actually is a success: A policymaker takes action to prevent an undesirable result, or the intelligence analysis becomes public and others act to prevent the undesirable outcome from occurring.

CRITICAL THINKING QUESTIONS

1. The president is an impatient person, and your current assignment is to present the President's Daily Brief (PDB) to him. You are well aware of his strong preference for graphics and illustrations. He consistently refuses to read more than the first two sentences of the written material in the PDB, and expects only a few verbal comments on each topic—but you are unsure that he pays much attention to what you say, typically being absorbed in the graphical presentation. You have a significant new intelligence item to present today, with serious implications for national security. But it contains subtleties and nuances that can't be conveyed visually. Design a plan of options to ensure that the message gets through.
2. You have prepared an assessment of the likely impact on your country's trade balance if current trade negotiations are concluded based on draft agreements that have been unofficially provided to you by the Foreign Ministry staff. Because your assessment indicates a serious negative impact on your country's trade balance, you believe that it is critically important to have the foreign minister see your report. But you learn that her staff disagrees with your conclusions and has ensured that she did not get a copy.
 - a. What options do you have?
 - b. What are the potential consequences of each option?
3. You are a naval systems analyst with a network of customers and collectors. One of your customers is the chief of the naval intelligence service, whose COMINT unit has discovered and monitors a covert naval communications channel operated by a potential opponent. Because of its importance, all information indicating your country's knowledge of the channel has been classified "Top Secret/special access required." Then your HUMINT service interrogates a recent defector, a former submarine communications technician, who describes the covert channel in detail. A report is prepared on the interrogation results, classified "Secret" (the normal practice). Before the report is released, you provide an advance copy to the chief of the naval intelligence service. He is outraged that you intend to release the report to your other customers, and demands that the defector's reporting be suppressed completely, or at least reclassified in the Top

Secret/special access channel that he controls—to which your other customers have no access.

- a. What is your response, and what are its implications?
- b. How do you handle the defector afterward?

NOTES

1. Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949), 182.
2. John A. Gentry, "Favorite INTs: How They Develop, Why They Matter," *Intelligence and National Security* 33, no. 6 (2018): 822–38.
3. Ibid.
4. Andrew Griffin, "Officials Put Trump's Name in 'as Many Memo Paragraphs as We Can Because He Keeps Reading If He's Mentioned,'" *Independent*, May 17, 2017, <https://www.independent.co.uk/news/world/americas/donald-trump-intelligence-reports-white-house-read-them-mentioned-name-president-a7740726.html>.
5. Henry Sokolski, "Improving the Role of Intelligence in Counterproliferation Policymaking: Report of the 'Speaking Truth to Nonproliferation Project,' 2018," *Studies in Intelligence* 63, no. 1 (2019).
6. Michael Herman, *Intelligence Power in Peace and War* (Cambridge, UK: Cambridge University Press, 1996), 105.
7. Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security et al., *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences* (Washington, DC: National Academies Press, 2011), 77.
8. Eyal Pascovich, "The Devil's Advocate in Intelligence: The Israeli Experience," *Intelligence and National Security* 33, no. 6 (2018): 854–65.
9. Stephen Budiansky, *Her Majesty's Spymaster* (New York, NY: Viking, 2005), 213.
10. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 14, https://fas.org/irp/offdocs/wmd_report.pdf.
11. Roger Z. George and James B. Bruce, *Analyzing Intelligence* (Washington, DC: Georgetown University Press, 2008), 80, 113.
12. Douglas H. Dearth and R. Thomas Goodden, eds., *Strategic Intelligence: Theory and Application*, 2nd ed. (Carlisle, PA: US Army War College and Defense Intelligence Agency, 1995), 153.
13. Ibid., 156.
14. Martin Petersen, "What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers," *Studies in Intelligence* 55, no. 1 (March 2011).
15. David S. Landes, *The Wealth and Poverty of Nations* (New York, NY: Norton, 1998), 167.

16. David S. Robarge, "Richard Helms: The Intelligence Professional Personified," *Studies in Intelligence* 46, no. 4 [2007]: 35–43.
17. CIA Center for the Study of Intelligence, *CIA and the Vietnam Policymakers: Three Episodes 1962–1968* (Washington, DC: Author, March 19, 2007), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/cia-and-the-vietnam-policymakers-three-episodes-1962-1968/index.html>.
18. Charles E. Allen, "Warning and Iraq's Invasion of Kuwait: A Retrospective Look," *Defense Intelligence Journal* 7, no. 2 [1998]: 33–44.
19. Ibid.
20. James Noren, "CIA's Analysis of the Soviet Economy," in *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*, ed. Gerald K. Haines and Robert E. Leggett, CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, chapter II, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article02.html>.



ANTICIPATORY INTELLIGENCE

Chapter 15	Anticipatory Analysis: Forces	281
Chapter 16	Anticipatory Analysis: Methodology	297
Chapter 17	Scenarios	327
Chapter 18	Systems Modeling and Analysis	343
Chapter 19	Relationship Modeling and Analysis	363
Chapter 20	Geospatial Modeling and Analysis	387
Chapter 21	Simulation Modeling	407
Chapter 22	Prescriptive Intelligence	429
Chapter 23	Case Study: A Tale of Two NIEs	441

Part I of this book provided an overview of the analysis process and the target-centric approach. Part II detailed the steps, from issue definition to gaining customer acceptance of the analytic product. The product itself is assumed to be *descriptive*; that is, an assessment of the current situation, based on an existing target framework. Most customers ask for that, and the analysis to produce it can usually be done with confidence, if the analyst follows proper analytic process and has good sources. Paradoxically, customers don't always ask the question they really want answered: What will happen next? Anticipatory analysis is required to handle that type of problem.

Part III addresses the components (driving forces), the methodology (conceptual frameworks), and the resulting product (outcome scenarios) of anticipatory analysis in chapters 15, 16, and 17. The next four chapters, 18–21, describe specialized and

advanced model types used for in-depth analysis. Chapter 22 considers *prescriptive* analysis—a step beyond anticipatory. (Chapter 23, the capstone case titled "A Tale of Two NIEs," applies to the entire book.)

The US intelligence community regularly produces anticipatory intelligence in the form of national intelligence estimates; but day to day, customers focus their questions on the here and now or, at best, on the immediate future. Why? Like most people, their attention is consumed by current events.

Nonetheless, most intelligence communities encourage analysts to provide anticipatory analysis, both short and long term. When the stakes are especially high, governments demand it. Such analysis follows much the same pattern as described in part II, but because it goes beyond analysis of facts, an additional conceptual framework is required: probabilistic analysis. Estimating the future state of a target can only be done using probabilities. Consequently, the risk of a miscall is substantially greater than when an assessment relies on established facts.

This highest form of intelligence analysis results in a picture of what is likely to happen, in the form of an intelligence estimate. Until recently, the process of producing such an estimate was called estimative analysis. It was not called prediction¹ because, as distinguished author Mark Lowenthal has noted, "Estimates are not predictions of the future but rather considered judgments as to the likely course of events regarding an issue of importance to the nation. Sometimes, more than one possible outcome may be included in a single estimate."²

The term that has begun to replace *estimation* in intelligence circles is *anticipatory intelligence*. The US Office of the Director of National Intelligence has defined it this way:

Anticipatory intelligence focuses on characterizing and reducing uncertainty by providing decision makers with timely and accurate forecasts of significant global events.³

The term has also gained cachet in the business world, as reflected in this quote:

Anticipatory analysis helps decision-makers, and those who support decision-makers, by systematically illuminating the potential outcomes in the future. Reducing uncertainty can help mitigate the adverse effects of surprises, if not avoid them, and it can also highlight opportunities that can be leveraged to yield benefits. In today's fast paced world, reaction typically forces us to consider a narrower and costlier set of options vice anticipation, where a wider range of options comes into view. In other words, anticipatory analysis assists organizations navigate the future by bolstering their resiliency and adaptability.⁴

This text uses the terms *anticipatory intelligence* and *estimation* interchangeably and occasionally commits heresy by referring to *prediction*. Old habits die hard.

One of the major challenges in anticipatory intelligence is identifying the relevant target. We introduced chapter 1 by briefly examining five intelligence failures. Four of them—Operation Barbarossa, Yom Kippur, the fall of Singapore and the Falkland Islands invasion—were surprise attacks involving conventional military conflict. All the victims of surprise misread their opponents' intents and capabilities; but in those examples, the target was well defined, if poorly understood.

The Soviet failure in Afghanistan was different; it was not a surprise attack. The Soviet surprise was in what they encountered after sending troops into Afghanistan: an unexpected insurgency abetted by aid flowing from other Islamic states and from the US and China. It stemmed from a Soviet failure to consider all relevant aspects of the target. The Soviets viewed Afghanistan from a military perspective, instead of considering all the PMESII aspects—especially the social and informational ones. They expected to be welcomed as protectors of the government and were surprised to encounter a popular uprising by Afghans who saw them as invading infidels. The Russian government repeated that mistake in 2022 when it invaded Ukraine, expecting a relatively easy takeover amid minimal resistance.

Government intelligence services in many countries have encountered similar surprises in the past half century. The Iranian revolution in 1979, the Palestinian Intifada of 1987–1993, and the Arab Spring of 2010–2011 are all examples of spontaneous popular rebellions that were misread by every intelligence organization.

This type of intelligence failure has been described as a *diffused surprise*. It arises when intelligence lacks a “relevant perceptual framework” for analysis.⁵ Or, in terms used herein, a target that considers all relevant PMESII aspects. The analytic methodologies described in part III are applicable to both types of targets: the well-defined ones that sometimes result in conventional surprises, and the misapprehended ones that result in diffused surprises.

The future for all targets is shaped by the factors, or forces, acting upon them. We begin by characterizing those forces.

Anticipatory analysis requires taking a methodological step beyond analysis of present facts. Previous chapters focused mostly on developing models of the current target and situation. Now we turn to models of possible futures. The goal is to produce valuable insights that help prepare customers to deal with the future as it unfolds. As former national security advisor Brent Scowcroft once observed, “What intelligence estimates do for the policymaker is to remind him what forces are at work, what the trends are, and what some of the possibilities are that he has to consider.”⁶

While some types of customers welcome some types of anticipatory intelligence, policymakers (who need it the most) tend to be skeptical. They are prone to believe that their own opinions about the future are at least as good as those of intelligence analysts. So, an analyst who offers an estimate without a compelling supporting argument should not be surprised if the policymaker ignores it.

Policymakers and executives will, however, accept and make use of anticipatory analysis if it is well reasoned, and if they can follow its logical development. This implies a formal methodology, one that customers can understand, so that they can not only see the basis for the conclusions drawn but also contribute to their formulation. The first step in that process is to identify the forces present or likely to arise that affect the target.

All participants in the collaborative process described in parts I and II have roles to play, but the analyst will always be the closest to the issue and the target model. An analyst’s most important contribution at the start lies in the assessment of the forces or factors that will shape future events and the future state of the target model. If the forces are assessed accurately, the intelligence customer has been served well, even if the prediction derived from that assessment turns out to be wrong. Customers may draw their own conclusions anyway, but understanding the forces helps them to make a more reasoned assessment and to refine it as new events unfold. In the ideal case, mentioned at the close of chapter 14, an estimate will not come true because the customer will act on the intelligence to change the anticipated outcome to a more favorable one.

The driving forces vary from one intelligence problem to another, and there are too many to catalog here. This chapter identifies the most common forces and includes a few that are generally present but are not obvious and sometimes not considered.

The CIA’s *Tradecraft Primer* describes an analytic methodology appropriate for identifying and assessing forces. Called “outside in” thinking, the objective is to identify the critical external factors that could influence how a given situation will develop.

According to the tradecraft manual, the analyst should develop a generic description of the problem or the phenomenon under study. Then, do the following:

- *List all the key forces (social, technological, economic, environmental, and political) that could have an impact on the topic, but over which one can exert little influence (e.g., globalization, social stress, the Internet, or the global economy).*
- *Focus next on key factors over which an actor or policymaker can exert some influence. In the business world this might be the market size, customers, the competition, suppliers or partners; in the government domain it might include the policy actions or the behavior of allies or adversaries.*
- *Assess how each of these forces could affect the analytic problem.*
- *Determine whether these forces actually do have an impact on the particular issue based on the available evidence.⁷*

In this book, what the CIA manual calls a “generic description of the problem” is a combination of the issue decomposition and target frameworks covered in chapters 8 through 12.

While the CIA methodology is a good beginning, the paradigm we’ll introduce in chapters 16 and 17 depends on considering *all* forces or factors—those that cannot be influenced, and those that can. The ones that are difficult to influence, after all, are the ones that cause a diffused surprise. So in anticipatory analysis, the analyst must be able to assess the impact of *all* forces that will shape the future. But how to do that?

Begin by identifying six broad categories of forces that should be familiar by now: the PMESII factors. There can be many forces that fall into each of the six factors, for example:

- *Political.* The distribution of power within the government; the influence wielded by the legislature; regulatory and legal restrictions.
- *Military.* The weaponry, capabilities, strategies, and tactics that opponents have or will use to apply armed force.
- *Economic.* Macroeconomic trends and forces shaping the economy as a whole, such as international trade barriers and exchange rates, raw material costs, and economic sanctions.
- *Social.* Demographics and softer issues of values, lifestyle, or political activism.
- *Infrastructure.* Existing facilities, communications, and environmental matters apply here—though the term *environmental* can apply to any factor.
- *Information.* Targeted messaging, including state-sponsored outlets, mainstream news organizations, and social media.

These form a more inclusive set of forces to be considered.

Military factors are often the focus of attention in assessing the likely outcome of conflicts. But other forces can turn out to be dominant. A historical example illustrates the point. In the developing conflict between the United States and Japan in 1941, Japan had a military edge in the Pacific. But the United States had a substantial edge in other factors:

- *Political.* The United States could call on a substantial set of allies. Japan had Germany and Italy, and they were located a continent away.
- *Economic.* Japan lacked the natural resources that the United States and its allies controlled.
- *Social.* The United States had almost twice the population of Japan. Japan initially had an edge in the solidarity of its population in support of the government, but that was matched within the United States after Pearl Harbor.
- *Infrastructure.* The US manufacturing capability far exceeded that of Japan, and would be decisive in a prolonged conflict (as many Japanese military leaders foresaw).
- *Information.* The prewar information edge favored Japan, which had more control of its news media, while a segment of the US media strongly opposed involvement in war. That edge also evaporated after December 7, 1941.

Japan's military edge gave it an early advantage in the consequent war, but the economic and infrastructural factors shifted the military advantage to the United States within a year after December 7, 1941.

The forces in this example are straightforward to identify. But some forces are both broad and subtle; in a sense, they operate “behind the scenes” in most situations. These also need to be considered and are described in the next section.

BACKGROUND FORCES

Some forces can fit under any of the PMESII factors and should be taken into account in almost all analytic estimates. Mostly social or environmental, they tend to temper events and other forces to shape the future. Analysts should start an anticipatory effort by asking which are relevant to the problem. Four common background forces are inertia, opposition, contamination, and feedback.

Inertia

A powerful and often overlooked force is inertia, the tendency to stay on course and resist change. Newton's first law of motion—that bodies at rest tend to stay at rest,

and bodies in motion tend to remain in motion—applies to organizations across the spectrum.

Organizations and individuals don't deal well with change in any of the PMESII factors. Military organizations have a tendency to refight the last war. Religious (social) organizations have a history of referring to attempted changes in doctrine as heresy. It has been observed that

historical inertia is easily underrated. [T]he historical forces molding the outlook of Americans, Russians, and Chinese for centuries before the words capitalism and communism were invented are easy still to overlook.⁸

Opposition to change is a common reason for organizational and individual inertia. Opposition to technology in general, for example, is an inertial matter; it results from a desire of both workers and managers to preserve their work environment as it is, including its institutions and traditions. But there are costs associated with inertia. One price is illustrated in the history of the Bessemer steelmaking process in America.

BOX 15.1 CHANGING THE BESSEMER PROCESS

The Bessemer process was invented at about the same time by two men, each working independently—Henry Bessemer, an Englishman, and William Kelly, an American. It involved blowing air under pressure into the bottom of a crucible of molten iron. Within a few years, the Bessemer process almost completely replaced the conventional crucible method of steelmaking. It lowered the price of producing steel and was the basis for the modern steel industries. It was one of the foundations of the Industrial Revolution.

Between 1864 and 1871, ten companies in the United States began using the Bessemer process to make steel. But the US companies had a shortage of workers experienced with the process. All but one of them, the Cambria Iron Company, imported English workers familiar with the process. By 1871, Cambria dominated the industry. Although the company had begun at a disadvantage, its workers were able to adapt to changes and improvements that took place between 1864 and 1871. The British steel workers at the other companies, secure in the tradition of their craft, resented and resisted all change. Those companies did not adapt.

There have been numerous examples since 1871 of inertia toppling industrial giants and thereby affecting a country's infrastructure. Kodak's attachment to film photography, IBM's commitment to the mainframe computer, and Detroit's long love affair with large automobiles all led to companies losing market share to competitors. But all societies resist change to a certain extent, and it can affect militaries as well as civil industries. A textbook example of resistance to innovation is the story of the US Navy and Lieutenant William Sims.

BOX 15.2 IMPROVING NAVAL GUNNERY

More than a century ago, the standard gunnery method used a highly trained gun crew to manipulate the heavy set of gears that aimed naval guns at an opposing ship. Because both ships would be moving, and the gun platform would also move with the pitch and roll of the ship, naval gunnery was an art, and accuracy depended on professionalism and teamwork.

In the early 1900s, a young naval officer, Sims, developed a new method that made use of the ship's movement. He was able to simplify the aiming gear set and remove the gunnery sight from the gun's recoil so that the operator could keep his eye on the gunsight and move the gears at the same time. His tests demonstrated that the new method would markedly improve the accuracy of naval gunnery.

Sims attempted to attract the attention of US Navy headquarters and was told that the Navy was not interested. He persisted, and the Navy finally consented to a test with some conditions: Sims's aiming device had to be strapped to a solid block in the Washington Naval Yard. Deprived of the ship's movement, the device failed, proving to the Navy that continuous-aim firing was impractical.

Sims, however, was as tenacious and bold as the person he next contacted with his idea—President Theodore Roosevelt. Roosevelt forced the Navy to take the device and give it a fair test. Sims's device was subsequently adopted and significantly improved naval gunnery accuracy.⁹

The organizational resistance to change that Sims encountered is common in all organizations. The structure of the US Navy is that of a highly organized and tradition-oriented society, and Sims's innovation directly threatened the society by making some skills less essential. The Navy resisted his innovation, and it took someone outside the society—the president of the United States—to force the change. Organizations are societies, just as a ship's crew is a society. The members possess a basic antipathy to changes that threaten their structure. Many research and development groups restrict their members' freedom to innovate: Ideas that don't fit the mold of the group are unwelcome.

From an analyst's point of view, inertia is an important force in prediction. Established factories will continue to produce what they know how to produce. In the automobile industry, it is no great challenge to predict that next year's autos will look much like this year's. A naval power will continue to build ships for some time even after a large navy ceases to be useful.

Opposition

The concept of opposing forces is closely related to inertia: All forces are likely to have opposing or resistive forces that must be considered. All governments face some types of opposition. The principle is summarized well by another of Newton's laws of physics: For every action, there is an equal and opposite reaction.¹⁰

As a general rule, no entity (country, organization, initiative, or project) can expand unopposed. Opponents will always arise. Harvard historian David Landes wrote that “all innovations of thought and practice elicit an opposite if not always equal reaction.”¹¹

Applications of this principle are found in all organizations and groups, commercial, national, and ethnic. As Samuel P. Huntington notes, “We know who we are . . . often only when we know who we are against.”¹² The rallying cry of Japan’s Komatsu Corporation, and the definition of its being, was summed up in its slogan, “Beat Caterpillar”—Caterpillar Inc. being Komatsu’s chief competitor worldwide.

A predictive analysis will always be incomplete unless it identifies and assesses the opposing forces, because they always will exist, sooner or later. An effort to expand free trade inevitably arouses protectionist reactions. One country’s expansion of its military strength always causes its neighbors to react in some fashion.

Counterforces need not be of the same nature as the force they are countering. A prudent organization is not likely to play to its opponent’s strengths. Many of today’s threats to US national security are asymmetric. They typically take the form of an unconventional yet lethal attack by a loosely organized terrorist group or a “lone-wolf” supporter of terrorism, as the events of 9/11, the 2013 Boston Marathon bombing, and a number of attacks since then have demonstrated.¹³ Asymmetric counterforces are common in industry as well. Industrial organizations try to achieve cost asymmetry by using defensive tactics that have a large favorable cost differential between their organization and that of an opponent.¹⁴ Any intelligence assessment of the consequences of a policymaker’s or field commander’s decision should take into account countervailing forces, because the opponents will react and smart ones are likely to react asymmetrically.

Contamination

Contamination is the degradation of any of the six PMESII factors through an infection-like process. It could even take the form of an infection; the COVID-19 pandemic degraded the political, economic, and social climate in several countries. More generally, corruption is a form of political and social contamination. The result of propaganda and “fake news” is information contamination. Money laundering, tax evasion, and counterfeiting are forms of economic contamination. Gresham’s law of currency is perhaps the best-known example of economic contamination. The law is based on the observation that when currencies of different metallic content but the same face value are in circulation at the same time, people will hoard the currency that has more valuable metal in it, or use it for foreign purchases, leaving only the “bad” money in domestic circulation. The law explains a major disadvantage of a bimetallic currency system. Gresham’s law is generally summarized as “the bad drives out the good.”

Irving Langmuir describes the contamination phenomenon in this story about a glycerin refinery:

Glycerin is commonly known as a viscous liquid, even at low temperatures. Yet if crystals are once formed, they melt only at 64 degrees Fahrenheit. If a minute crystal of this kind is introduced into pure glycerin at temperatures below 64 degrees Fahrenheit, the entire liquid gradually solidifies.

A glycerin refinery in Canada had operated for many years without having any experience with crystalline glycerin. But during normal temperatures one winter, the pipe carrying the glycerin from one piece of apparatus to another suddenly froze up. The whole plant and even the dust on the ground became contaminated with nuclei, and although any part of the plant could be temporarily freed from crystals by heating above 64 degrees, it was found that whenever the temperature anywhere fell below 64 degrees crystals would begin forming. The whole plant had to be shut down for months until outdoor temperatures rose above 64 degrees.¹⁵

Contamination phenomena can be found throughout organizations as well as in the scientific and technical disciplines. Once such an infection starts, it is almost impossible to eradicate. It keeps poisoning its host, and there are too many little bits to stamp out entirely—like the crystals of glycerin or metastasizing cancerous cells. For example, in the US electronics industry, a company's microwave tube production line suddenly went bad. With no observable change in the process, the tubes no longer met specifications. Somehow, the line had become contaminated. Attempts to find or correct the problem failed, and the only solution was to close down the production line and rebuild it completely.

Contamination phenomena have analogies in the social sciences, organizational theory, and folklore. Folklore tells us that “one bad apple spoils the barrel.”

At some point in organizations, contamination can become so thorough that only drastic measures will help—such as shutting down the glycerin plant or rebuilding the microwave tube plant. Predictive intelligence has to consider the extent of such social contamination in organizations, because contamination is a strong restraining force on an organization’s ability to deal with change.

The effects of social contamination are hard to measure, but they are often highly visible in a country’s infrastructure. Large sectors of industry in Russia reached a high level of such contamination during the Soviet era, and recovery has proved to be very difficult. Indications of contamination can be seen in the production results, but there are also other visible symptoms. For example, most Japanese plants are clean and neat, with grass and flowers even in unlikely areas, such as underneath drying kilns. Even today a Russian factory is likely to have a dirty, cluttered environment; buildings with staggering losses of energy; and employees with chronic absenteeism and alcohol problems. The environment in the Japanese plant reflects the high level of

social cohesiveness and acceptance of social standards in that country and reinforces the positive image. The environment in the Russian plant reinforces and prolongs the contamination. Such contamination can be reversed—the cleanup of New York City in the 1990s is an example—but a reversal typically requires a massive effort.

Contamination occurs across the political, economic, and social spheres in the form of corruption. It has been a major factor in all of the former Soviet republics and remains a problem even among those that have been incorporated into the European Union.¹⁶

Even our language can become contaminated: A word that develops negative associations will be replaced by a succession of euphemisms. That can be a boon for the intelligence analyst in assessing the effectiveness of programs, whether social, political, or technical—and of hardware also. *We don't rename our successes.* Ford Motor Company since 1964 has kept the name “Mustang” for its most beloved automobile and, since 1948, “F-150” for its best-selling truck; but there will never be another Edsel or, for that matter, another Pinto. The renaming of a program or project is a good signal that the program or project is in trouble—especially in Washington, D.C., but the same rule holds in any culture. For a number of foreign infrastructure projects or weapons development efforts, the renaming of the program was the first visible indication that the program was encountering difficulties.

Finally, contamination can be a powerful weapon to use against an opponent—whether it is a contamination of ideas or of objects. The Farewell operation was effective because it didn’t attempt to block the illegal flow of technology into the USSR; instead, it contaminated the flow (see chapter 13). The result was that, when the operation was discovered, the Soviets were faced with a dilemma. They didn’t know which plans or equipment they had acquired were contaminated, and which were not.

Feedback

In examining any complex system or organization, it is important to evaluate the feedback mechanism. Feedback is the mechanism whereby the system or organization adapts—that is, learns and changes itself.

The Indian nuclear test deception, described in chapter 13, is an example of how feedback works in the world of national policy and intelligence. The US State Department’s demarche about India’s test preparation contained detailed (though unintended) feedback to New Delhi on how to prepare for a test the next time around. The Indian government altered its test process accordingly. The output (or result) was highly satisfactory for India but less so for the United States.

Anticipatory analysis is not complete until it includes the potential effects of feedback. This assessment requires estimating the nature and extent of feedback. Feedback can be positive and encourage more output, or it can be negative and encourage less output. It can also be strong and have a greater effect on output or be weak and have less of an effect. Finally, feedback can be immediate and thus reflected immediately in the

output, or its effect can be delayed, so that it changes the output at some future time. So the effect of feedback is determined by the factors of strength and nature (positive or negative) and timing.

When feedback is powerful enough, systems, organizations, and people are forced to adapt. In organizations or social systems generally, persons (including decision makers) will evaluate the feedback they receive according to its strength and adjust their behavior accordingly. The stronger the feedback (whether positive or negative), the more likely they are to act. In positive feedback systems, where perceived benefits outweigh costs, current behavior is reinforced, and output (current behavior) therefore tends to grow (become stronger) at a rate determined in part by the amount of positive feedback. In negative feedback systems, where costs are perceived to outweigh benefits, the result is to stabilize, decrease, or even stop the current output. Or as Jerrold Post observed in assessing foreign leadership (see chapter 9): “If something scarred the leader in the past, he’ll avoid it in the future.”

Organizations tend to act to reduce the strength of feedback in two ways.

- First, because few organizations can readily cope with the uncertainty that comes from adaptability, organizations try to hold things constant so that they can deal with them (the inertia factor, again). This tendency is a powerful constraint on feedback.¹⁷ Sims’s problem with introducing his gunnery innovation is one of many examples of that type of behavior.
- Second, feedback must reach decision makers or action takers to be effective. Only when it is accepted by the appropriate people in an organization can it shape future actions. But the organization itself—its administrative layers and staff—diffuses, weakens, misdirects, and delays feedback, effectively reducing its strength. A large bureaucratic organization or a centralized economy, with its relative inflexibility and numerous layers of administrators, keeps feedback at a feeble level. Funding is set through political processes that have only an indirect relation to previous industrial successes and failures. The market provides poor feedback in a centralized or command economy.

National leaders tend to react poorly when they receive negative feedback—for example, if their policies are not turning out well. In dictatorships, negative feedback tends not to reach the leader at all, or to be so attenuated as to be ignored. In contrast, all leaders, and especially dictators, welcome positive feedback. So it tends to reach them in full strength. This book contains several examples of leaders who didn’t get the negative feedback because they didn’t want to hear it. Lyndon Johnson, Adolf Hitler, Saddam Hussein, and a succession of Soviet leaders, beginning with Josef Stalin—all failed to receive the negative feedback that they needed at critical times.

Speed of feedback has an effect. Often, positive feedback comes more slowly than negative. So, in the early stages, the system may receive only negative feedback, though

more positive information may be coming later. The benefits of deregulation or free trade agreements, for example, may be much more difficult to identify and take longer to observe than the costs.

The opposite outcome is perhaps more common: Benefits are perceived more quickly than costs. The drug industry has provided examples of this phenomenon, one of the most dramatic of which occurred with the drug thalidomide. First introduced in Europe in 1956 for use as a sedative and to combat morning sickness in pregnant women, its benefits were realized quickly. But the costs were observed later on; thalidomide was withdrawn from the market in 1961 after it was found to have caused severe birth defects in thousands of infants.¹⁸

The delayed effects of environmental pollution have provided other examples of such “false positive” feedback. The nuclear power industry, however, has probably provided the most spectacular examples. This industry benefited for some years from extensive government-supported efforts to advance technology. The resulting pace of nuclear power technology development was too rapid to allow adequate mitigation of the risks.¹⁹ As a result, in 1979, the United States suffered from the Three Mile Island reactor incident that released radioactive material into the air near Harrisburg, Pennsylvania, creating widespread panic. In 1986, Russia had its Chernobyl disaster—a reactor meltdown that contaminated a wide area in Ukraine and caused numerous deaths. In 2011, the Fukushima, Japan, nuclear power plant was hit by a tsunami. The damage resulted in the meltdown of three of the plant’s nuclear reactors, releasing substantial amounts of radioactive contamination into the environment.

Genetic engineering is one example of a current technology-driven field that could result in major social disruptions worldwide during coming decades.

When considering the forces that go into anticipatory analysis, there exists another factor (not truly a force) that should always be considered: synergy.

SYNERGY

Anticipatory analysis almost always requires multidisciplinary understanding. Therefore, it is essential that you, as an analyst, develop the understanding of a broad range of concepts in order to function in a multidisciplinary environment. One of the most basic concepts is that of synergy: The whole can be more than the sum of its parts due to interactions among the parts. Synergy is, therefore, in some respects, the opposite of the countervailing (opposition) forces discussed earlier.

Synergy is not a force; it is the result of interaction of forces. Synergy can result from cooperative efforts and alliances among organizations (synergy on a large scale). It can be the consequence of a combination of social, economic, political, and technological forces on a grand scale, such as those that caused the Industrial Revolution.²⁰ Netwar, as discussed in chapter 2, is an application of synergy.

An example of synergy on a large scale comes from the fields of computers and communications. These once-distinct technical areas merged over several decades during the past century as engineers expanded the use of one to enhance performance of the other. Managing the merger of these two required technical knowledge in both, plus an understanding of political issues (regulation in communications), economic issues (cost-performance tradeoffs of central versus distributed computing), and social issues (willingness of large numbers of people to adopt advanced technologies, as people have in using networks such as the internet, social networking technologies, and cloud computing). The result? The smartphone and smartwatch, Facebook, Netflix, TikTok, and much more.

Synergy is the foundation of the “swarm” approach that military forces have applied for centuries—the coordinated application of overwhelming force. In chapter 18, we discuss the effectiveness of synergy in a plan for defeating the HIND helicopter during the Soviet incursion in Afghanistan. The solution that was used—a combination of several surface-to-air missiles and several heavy machine guns—was far more effective than any one of these weapons would have been alone. One of the more promising military developments today is the swarm of attack drones that operates as a predatory pack.

Synergy is equally effective in the commercial world. In planning a business strategy against a competitive threat, a company will often put into place several actions that would not succeed if each were taken alone. But the combination can be very effective. As a simple example, a company might use several tactics to cut sales of a competitor’s new product: start rumors of its own improved product release, circulate reports on the defects or expected obsolescence of the competitor’s product, raise buyers’ costs of switching to the competitor’s product, and tie up suppliers by using exclusive contracts. Each action, taken separately, might have little impact, but the synergy—the “swarm” effect of the actions taken in combination—might shatter the competitor’s market.

In intelligence support to policymakers, the same rule holds. A combination of policy actions may be much more effective than any single action. The policymaker or executive usually identifies the possible synergies and, in the end, selects a package. But the analyst potentially has a role in that selection—covered in chapter 22.

Most of the major innovations and changes that make straight-line extrapolations fail over the long term occur because of some form of synergy. It should be on your mind constantly as you evaluate the factors going into a forecast.

CAUSAL MODELS

In chapter 16, we’ll examine three basic methodologies for anticipatory analysis, summarized in the concepts of extrapolation, projection, and forecasting. But, to execute any of those three, we first have to have identified the key forces that are shaping a

future situation. There exists a general model framework for doing that, and it has variants and many names. The most general term for the framework is the *probabilistic graphical model*, but other widely used terms for it include *causal networks*, *causal models*, *belief networks*, and *Bayesian networks*. We'll use the name *causal model* here for convenience, recognizing that an analytic model can take any of those forms.

As used in intelligence, causal models depict both elements of the target and elements affecting the target and describe how those elements are related by probabilities. The key features of causal models are as follows:

- They are composed of nodes, which can represent objects, people, concepts, forces, systems, or events, and links that indicate relationships between the nodes.
- The nodes are usually variables, and they can be either independent or dependent. A dependent variable node typically is related (linked) to another node that it depends on or is affected by.
- The causal relationship between two nodes can be positive or negative—that is, a change in the independent variable node can cause the same or an opposite change (whether an increase or a decrease) in the dependent variable node.
- They make use of probability distributions and the laws of probability.

For a causal model to exist, there must be *causality*. Four things are required in order to establish causality:

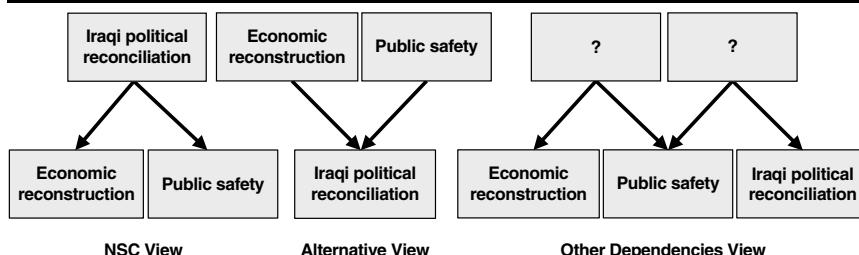
- *The time sequence must be proper.* The change or condition in the independent variable must always occur *before* the change or condition in the dependent variable.
- *The relationship cannot be spurious.* Correlation between two variables does not imply causation. There cannot be a third variable that is causing both the independent and dependent variables to change.
- *There must be covariation.* It is necessary to establish that as the independent variable changes, there is a corresponding change in the dependent variable.
- *There must be a theory of causality.* Empiricism alone cannot establish causality.

A recent example of a causal model is the argument that climate change—specifically global warming—causes an increase in terrorism. The argument was made in a 2014 US Defense Department report and repeated by President Barack Obama and candidate for the Democratic presidential nomination Bernie Sanders in 2015. It was repeated in 2015 by Britain's Prince Charles and in 2017 in a report commissioned by

the German foreign office. But causation is difficult to establish for this relationship, and the argument continues to be debated in the press.

For a more detailed example, let's revisit the request that Tom Fingar received, introduced in chapter 8. That case involved a National Security Council assumption that progress in Iraqi political reconciliation would have a positive influence on economic reconstruction and public safety; in other words, the causal model would look like the NSC view shown on the left in figure 15.1. In fact, the opposite could just as well be true: that progress in economic reconstruction and public safety would have a positive influence on Iraqi political reconciliation (the alternative view shown in the figure). And all three could instead depend on other undetermined events, actions, or changes in the political, economic, military, or social situations, as indicated on the right. In causal modeling terms, the relationships shown in the NSC and alternative views could be *spurious*.

FIGURE 15.1 ■ Views of Iraqi Situation Dependencies



In actuality, the Iraqi political reconciliation issue likely was shaped by three forces discussed in this chapter (among others):

- *Inertia*. The factions were constrained from working together by their established positions on issues.
- *Opposition*. Any initiative involving political reconciliation by one faction would likely meet opposition from other factions, and the Iraqis recognized that.
- *Contamination*. Public safety and economic reconstruction in Iraq were hampered by economic and political contamination: corruption in the government organizations responsible for those two functions. Social contamination took the form of continuing hostility between Sunni and Shiite factions.

We've introduced the idea that causal models are probabilistic. So where do the probabilities come in? The fact is that they're there, though not always obviously so. But we know that some outcomes will tend to occur more frequently when other

situations develop. Anticipatory analysis inevitably involves probabilities, even if they aren't explicitly stated or given a numerical value. The causal model is used widely in intelligence analysis, usually without giving it much thought; it is what we do naturally when trying to anticipate future developments. Often we mentally create the causal model, identify the dependent and independent variables, and assign probabilities in verbal terms (such as *probable*, *unlikely*, or *certain*).

Causal modeling is a powerful tool for identifying forces that shape a target's likely future state. The influence relationships between all of the nodes shown in figure 15.1, for example, represent forces. We'll briefly revisit causal modeling in chapter 16.

SUMMARY

Anticipatory analysis relies on assessing the impact of forces and factors that shape the target, lead to new developments, and motivate people and organizations to action. These generally fall into one or more of the PMESII categories. These shaping forces and factors should be a "first stop" in any estimative analysis about a target.

Some forces can fit under any of the PMESII factors and should be considered in almost all analytic estimates. These background forces tend to shape or temper events and other forces:

- *Inertia*, or resistance to change, is common in established organizations.
Organizations naturally seek to establish and maintain a stable state, and to keep doing what they've done in the past.
- *Opposing forces* will always arise to resist any significant force, and such countervailing forces may be of an asymmetric type.
- *Contamination* phenomena can adversely affect the PMESII assets of a state or organization.
- *Feedback* is an adaptive force that can be beneficial or detrimental, depending on the strength and time delay. Bad policy decisions can result when there are significant differences in time delays between positive and negative feedback.
- *Synergy*—the combination of forces to achieve unexpected results—is behind many social and technical advances. Synergy enables the effectiveness of the "swarm" attack that organizations increasingly use to win conflicts.

After identifying the forces affecting the target (including background forces), the question becomes: For a given issue and target, how do you identify the *key* forces and factors to consider? A method exists for doing that, referred to as causal modeling. It is a widely used analytic tool—an imperative one, in fact, for anticipatory analysis. Causal models, based on a model framework called the probabilistic graphical model, require the graphical portrayal of nodes (variables) and relationships among them. The

relationships have to involve causality: that is, proper time sequence of changes in the nodes, no spurious relationships, covariation of changes, and a theory of causality.

CRITICAL THINKING QUESTIONS

1. The contamination phenomenon is observed in many fields. One example is language, where words associated with something unpleasant over time are replaced with euphemisms—which then are replaced in their turn. Find three examples of euphemisms and trace their evolution as far back as possible. Consider the reasons for each successive iteration of the euphemism and provide an opinion on the probability of it changing again. Give an extended example of contamination in another field (not covered in this chapter).
2. In 2013, RAND Corporation published *Paths to Victory*, a set of case studies about forty-one insurgencies. It is accessible at https://www.rand.org/pubs/research_reports/RR291z2.html.²¹ Choose one case study from the set (your instructor may assign a subset to choose from). Then:
 - a. Describe the background forces (inertia, opposition, contamination, and feedback) that were involved on each side in the conflict.
 - b. Identify cases where synergy was present and affected the outcome.
3. The section on causal models includes the example of a hypothesized relationship between global warming and an increase in terrorism. Consider the four things that are required for causality to exist. For that example:
 - a. Which ones have been established?
 - b. Which have been negated?
 - c. Which remain undetermined?
4. In the Iraqi situation dependencies view of figure 15.1, the blocks marked “?” were left as an exercise. Identify one or more independent variables that could affect any or all of the variables (economic reconstruction, public safety, and Iraqi political reconciliation). Consider negative as well as positive influences. Develop a causal model that shows the relationships.

NOTES

1. The terms *predict*, *prediction*, and *predictive* still find wide use in the intelligence literature and in this book as well, in specific contexts.
2. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, DC: CQ Press, 2006), 133.
3. DNI, “Anticipatory Intelligence,” <https://www.iarpa.gov/index.php/about-iarpa/anticipatory-intelligence>.

4. Innovative Analytics and Training, "Anticipatory Analysis," <http://www.innovative-analytics.com/analytic-solutions/anticipatory-analysis/>.
5. Avner Barnea, "Strategic Intelligence: A Concentrated and Diffused Intelligence Model. *Intelligence and National Security* 35, no. 5 (2020): 701–16.
6. Quoted in Woodrow J. Kuhns, "Intelligence Failures: Forecasting and the Lessons of Epistemology," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael Handel*, ed. Richard K. Betts and Thomas G. Mahnken (London, UK: Frank Cass Publishers, 2003), 96.
7. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009), 30.
8. J. M. Roberts, *The Penguin History of the World* (London, UK: Penguin Books, 1995), xi–xii.
9. Elting Morrison, *Men, Machines, and Modern Times* (Cambridge, MA: MIT Press, 1966).
10. Sir Isaac Newton, *Philosophiae Naturalis Principia Mathematica* (July 5, 1687).
11. David S. Landes, *The Wealth and Poverty of Nations* (New York, NY: Norton, 1998), 201.
12. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York, NY: Simon & Schuster, 1996), 21.
- 13 Another thoughtful perspective on the use of asymmetric attack against the United States is presented in the book *Unrestricted Warfare* by Chinese People's Liberation Army colonels Qiao Liang and Wang Xiangsui.
- 14 Michael E. Porter, *Competitive Advantage* (New York, NY: Free Press, 1985), 500.
15. Irving Langmuir, "Science, Common Sense, and Decency," *Science* 97 (January 1943): 1–7.
16. Dan Goure, "Fighting Corruption in the Former Soviet Republics Is Critical to Western Security," *The National Interest*, October 6, 2019, <https://nationalinterest.org/blog/buzz/fighting-corruption-former-soviet-republics-critical-western-security-85846>.
- 17 Donald A. Schon, *Organizational Learning* (Boston, MA: Addison-Wesley, 1978).
- 18 Crohn's and Colitis Foundation of America, "Thalidomide and IBD," March 10, 2003, www.ccfa.org/weekly/wkly828.htm.
19. Ibid.
20. Landes, *The Wealth and Poverty of Nations*, chapters 13 and 14.
- 21 Christopher Paul, Colin P. Clarke, Beth Grill, and Molly Dunigan, *Paths to Victory: Detailed Insurgency Case Studies* (Santa Monica, CA: RAND Corporation, 2013), https://www.rand.org/pubs/research_reports/RR291z2.html.

16

ANTICIPATORY ANALYSIS: METHODOLOGY

Long-term predictions¹ are considerably more challenging to produce than current intelligence. As the span of time increases, the likelihood of encountering unforeseen (and unforeseeable) events also increases. And when a turning point, a major shift of some kind, is reached, the future becomes uncertain. As noted in chapter 14, to go beyond description to prediction, an analyst must be able to apply a proven methodology and bring multidisciplinary understanding to the problem. Expertise in a narrow technical specialty is useful for simple target modeling, but it is insufficient beyond that.

Another critical trait of a successful predictive analyst is the ability to put things within historical context. It is difficult to consider where something is going without understanding where it has been. Past models of the target are used to make an assessment about its future state. Analysts know this intuitively. When looking at a country's current trade pattern, they usually compare it to previous years to see if there's a trend. Threats made by a national leader are put in perspective by looking at whether the leader carried through on past threats. Similarly, North Korea's willingness to negotiate about its nuclear capabilities in 2018 had to be viewed within the context of its history of broken promises and failed commitments on that topic.²

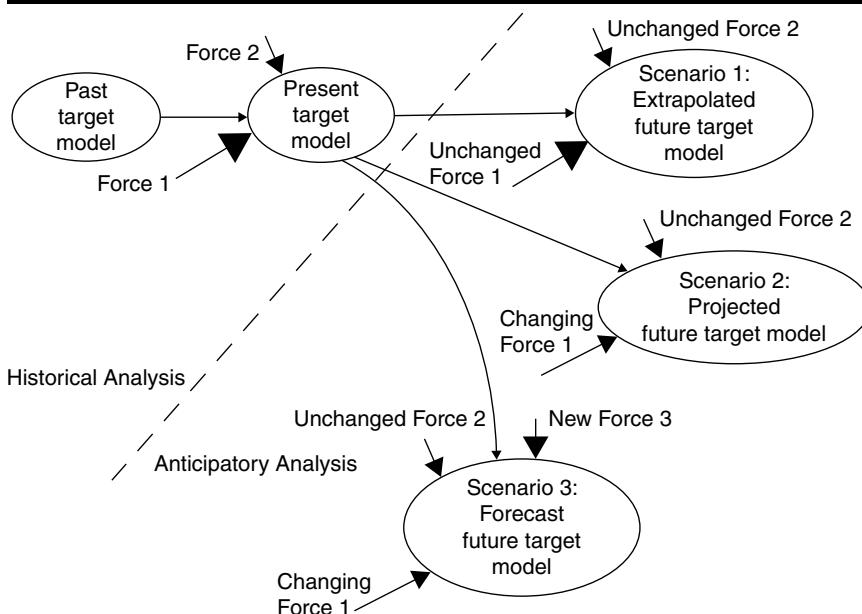
Estimates are as old as engineering. No large projects—temples, aqueducts, pyramids—were undertaken without some type of estimative process. Many estimative techniques have evolved over the past five centuries as mathematics and science have evolved.³ They frequently reappear with new names, though their underlying principles are centuries old.

The analysis process discussed in this chapter and the next is derived from an estimative approach that has been formalized in several professional disciplines. All those formalizations require combining data to estimate an entity's present state and evaluating the forces acting on the entity to predict its future state.

This concept—to identify the forces acting on an entity, to associate likely future forces, and to predict the likely changes in old and new forces over time, along with some indicator of confidence in these judgments—is the key to successful estimation. It takes into account redundant and conflicting data as well as the analyst's confidence in these data. It can be made quantitative if time permits and if confidence in the data can be quantified. But the technique can be applied qualitatively by subjectively assessing the forces acting on the entity. Figure 16.1 is an overview of the methodology. It assumes that the analyst has completed the target-centric analysis as described in part

II and, therefore, understands the target's history up to the present time. The next step is to identify one or more likely future models, using an analysis of the forces involved as a basis. Other texts on estimative analysis may describe these forces as issues, trends, factors, or drivers.⁴ Those terms have the same meaning: They are the entities that shape the future.⁵

FIGURE 16.1 ■ The Estimative Methodology



Note: Arrows vary in thickness to indicate the strength of their respective forces. Thicker arrows represent stronger forces; thinner arrows, weaker ones.

An important principle in making any estimate is to consider the phenomena that are involved, to determine whether anticipatory analysis is even possible.

CONVERGENT AND DIVERGENT PHENOMENA

Recall the discussion in chapter 11 of convergent and divergent evidence. Items of evidence were convergent if they tended to reinforce the same conclusion and divergent if they pointed to different conclusions. In examining trends and possible future events, the same terminology applies: Convergent phenomena make prediction possible; divergent phenomena frustrate it.

A basic question to ask at the outset of any predictive attempt is this: Does the principle of causality, discussed in chapter 15, apply? That is, are the relevant phenomena governed by the laws of cause and effect? One of the basic principles of classical

physics is that of causality. The behavior of any system can be predicted from the average behavior of its component parts if causality applies. Scientist and Nobel laureate Irving Langmuir defined such behavior as *convergent* phenomena.

The events leading up to World War I, which Barbara Tuchman superbly outlines in *The Guns of August*, had an inevitable quality about them, as befits convergent phenomena.⁶ World War I was predictable; many astute observers at the time saw it as almost certain. No one person or event actually “started” World War I; the assassination of Archduke Franz Ferdinand and his wife, Sophie, in Sarajevo merely triggered a process for which groundwork had been laid over many years.

Likewise, a war between the United States and Japan was predictable (and both sides foresaw it) throughout most of 1941. The Japanese aggression in China and Indochina, the consequent US imposition of a petroleum embargo on Japan, the freezing of funds by both sides, the steady deterioration in American-Japanese relations during the fall of 1941—all events converged toward war.⁷

Similarly, a pattern of continued Al Qaeda terrorist attacks on US interests worldwide was predictable and had been predicted before September 11, 2001, when terrorists flew three airplanes into the Pentagon and the World Trade Center. (The fourth airplane, bound for Washington, D.C., was brought down by passengers before it could hit its target.)

In the late 1940s, US ambassador George Kennan identified perhaps the most significant convergent phenomenon of the past century in defining his “containment” policy for the United States to pursue against the Soviet Union. He argued that, if contained, the Soviet Union would eventually collapse due to its overdeveloped military and underdeveloped economic system. It took over forty years for the collapse to occur, but successive US administrations had basically followed the containment policy.

In contrast to these examples, many phenomena are not governed by the laws of cause and effect. Quantum physics deals with the individual atom or basic particles and tells us that the behavior of such particles is as unpredictable as the toss of a coin; they can be dealt with only by the laws of probability.⁸ Such behavior can, from a small beginning, produce increasingly large effects—a nuclear chain reaction, for example. Irving Langmuir defined such phenomena as *divergent*. In chaos theory, such phenomena are the result of *strange attractors*—those creators of unpredictable patterns that emerge out of the behavior of purposeful actors.⁹ When dealing with divergent phenomena, making estimates is at the highest level of difficulty, or almost insurmountable.

To contrast the effect of the two types of phenomena, consider three major events that have occurred in Russia since 1997. CIA analysts warned policymakers of Russia’s looming economic crisis two months before the August 1998 ruble crash; they subsequently identified the economic rebound in the Russian economy long before business and academic experts did.¹⁰ Both events involved convergent phenomena and therefore were predictable. In contrast, the CIA was unable to predict the rise of Vladimir Putin to the Russian presidency until his handling of the Chechen war dramatically

increased his popularity. But in early 1999, Putin himself probably did not foresee this happening.¹¹ It was a divergent phenomenon. It will be an open question for some time to come whether a fourth major event, Russia's 2022 invasion of Ukraine, was due to convergent or divergent phenomena.

Assassinations, like that of Israeli prime minister Yitzhak Rabin in 1995, are not predictable. Specific terrorist acts, such as those on 9/11, similarly are not predictable in detail, though some kind of terrorist attempt was both predictable and predicted. In all such divergent cases, from the 1914 Sarajevo assassination of Archduke Franz Ferdinand to the 9/11 attack, a tactical warning might have been possible. An agent within the Serbian terrorist organization Black Hand could have warned of the Sarajevo assassination plan. An agent within Al Qaeda might have warned of the attack planned for 9/11. All such specific events can be described by probabilities but not predicted in the same fashion as the larger events they are immersed in—in these examples, World War I and the increasing conflict between the United States and Al Qaeda.

Let's look at an example of divergent phenomena from the business world.

BOX 16.1 THE OPERATING SYSTEM THAT MIGHT HAVE BEEN

One of the watershed moments in personal computing history was clearly a divergent phenomenon. In 1980, IBM was searching for software to run on its planned revolutionary Personal Computer (PC) and had zeroed in on a small startup company named Microsoft Corporation, located in Bellevue, Washington. Microsoft could provide the languages that programmers would use to write software for the PC, but IBM wanted more; it needed an operating system. Microsoft did not have an operating system and was not positioned to write one, so Bill Gates, Microsoft's president, steered IBM to Intergalactic Digital Research (later known as DRI).

An intelligence analyst assessing the likely future of personal computing in 1980 would have placed all bets on DRI. DRI built the CP/M operating system, at that time the most popular operating system for computers using the Intel processor. It had all the basic features IBM needed. Gates arranged an appointment between the IBM team and Gary Kildall, DRI's president, in Pacific Grove, California.

Instead of meeting with the IBM team, however, Kildall chose to take a flight in his new airplane. Miffed, the IBM team told Gates to find or write an operating system himself. Gates found one from a small software company in the Seattle area and called it the Disk Operating System (DOS), which later became the most widely used personal computer operating system and a major contributor to Microsoft's dominance of the personal computing business. A single event, a decision made to not keep an appointment, shaped the future of personal computing worldwide.¹²

In summary, the principle of causality applies to convergent phenomena, and estimates are made possible. Divergent phenomena, such as the actions of an individual person, are not truly predictable and must be handled using different techniques, such as those of probability theory or high-impact/low-probability analysis, discussed later

in this chapter. But where estimation is possible, analysts examine the convergent forces involved.

THE ESTIMATIVE APPROACH

The methodology (or conceptual framework) of anticipatory intelligence relies on three predictive mechanisms: extrapolation, projection, and forecasting. Those components and the general approach are defined here; later in the chapter, we delve deeper into “how-to” details of each. All three involve assessing forces that act on the target. An extrapolation assumes that these forces do not change between the present and future states, a projection assumes they do change, and a forecast assumes they change because, in addition to changing forces, new forces are added. In most cases, the future target models will be in the form of scenarios (the topic of chapter 17), as figure 16.1 indicates. The target analysis follows these steps:

1. Determine at least one past state and the present state of the target—for example, a terrorist organization, a government, a clandestine trade network, an industry, a technology, or a ballistic missile.
2. Determine the forces that acted on the entity to bring it to its present state. In figure 16.1, these forces (Forces 1 and 2) are shown, using the thickness of the arrow to indicate strength.
3. To make an extrapolation, assume that these same forces will continue unchanged; the result is the future state shown as Scenario 1.
4. To make a projection, estimate the changes in existing forces that are likely to occur. In the figure, a decrease in one of the existing forces (Force 1) is shown as causing a projected future state, different from the extrapolation (Scenario 2).
5. To make a forecast, start from either the extrapolation or the projection, identify the new forces that may act on the target, and incorporate their effect. In the figure, one new force is shown as coming to bear, resulting in a forecast future state that differs from both the extrapolated and the projected future states (Scenario 3).
6. Determine the likely future state of the target, based on an assessment of the forces. Strong and certain forces are weighed most heavily in this assessment. Weak forces, and those in which the analyst lacks confidence (high uncertainty about the nature or effect of the force), are weighed least.

Figure 16.2 shows how the process of figure 16.1 works in practice: It is iterative. This figure concerns a target (technology, system, person, organization, country, situation, industry, or some combination) that changes over time. The task is to describe or

characterize the entity at some future point. For example, the goal might be to establish the future performance of an aircraft or a missile, the future state of a country's economy, the future morale and effectiveness of a terrorist organization, or the future economic health of an industry. The models are created in succession, each one building on the results of the previous ones.¹³

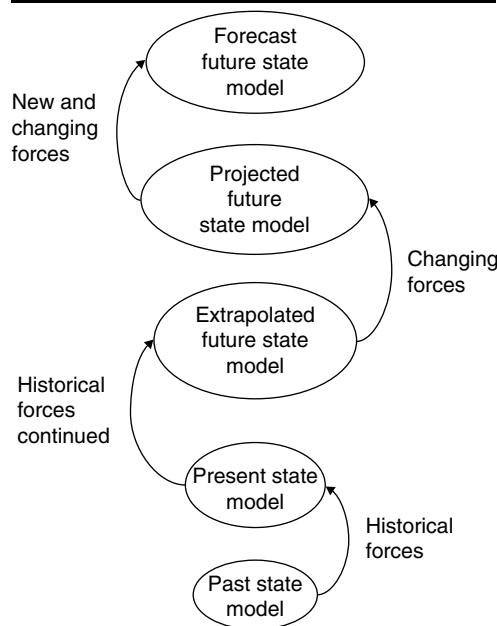
Designing good predictive scenarios requires such a process. In fact, iteration is the key to dealing with complex patterns and complex models.¹⁴ Again, the basic analytic paradigm is to start from the current assessment of the target and its history and, from that, to develop alternative models of its possible future states, usually created in scenario form. Following are two brief historical anecdotes illustrating outcomes of the process:

- The CIA's Office of Soviet Analysis in late 1987 estimated that Moscow could not effectively counter the US Strategic Defense Initiative (SDI) without severely straining the Soviet economy, discounting Moscow's assertions that it could do so quickly and cheaply. The estimate was based on a straightforward extrapolation of the state of the Soviet economy without Soviet attempts to counter SDI. It concluded that the Soviets had no margin for increased rates of investment in the economy. That estimate was followed by a forecast (adding in a new force—the burden on the economy of countering SDI). The analysts correctly predicted the alternative outcome: that Moscow instead would push arms control measures to gain US concessions on SDI.¹⁵
- A CIA assessment of Mikhail Gorbachev's economic reforms in 1985–1987 correctly estimated that his proposed reforms risked “confusion, economic disruption, and worker discontent” that could embolden potential rivals to his power.¹⁶ This projection was based on assessing the changing forces in Soviet society along with the inertial forces that would resist change.

The process used in these examples has many names—*force field analysis* and *system dynamics* are two.¹⁷ It involves finding out what the existing forces are, how they are changing, in what direction, and how rapidly. Then, for forecasting, the analyst must identify new forces that are likely to come into play. (Chapter 17 focuses on identifying and measuring these forces.) One of the most important forces comes from the feedback mechanism, as discussed in chapter 15. An analyst must ensure that all forces are given fair consideration. Concentrating on some and ignoring or downplaying others can improperly shape the assessment.

Force field analysis is an ancient predictive technique. Successful generals have practiced it in warfare for thousands of years, and one of its earliest known proponents was Sun Tzu. He described the art of war as being controlled by five factors, or forces, all of which must be taken into account in predicting the outcome of an engagement. He called the five factors Moral Law, Heaven, Earth, the Commander, and Method

FIGURE 16.2 ■ Applying an Iterative Approach to the Methodology



and Discipline. In modern terms, the five would be called social, environmental, geo-spatial, leadership, and organizational factors.

The simplest approach to both projection and forecasting is to use force field analysis qualitatively. That is, an analyst begins the process by answering the following questions:

1. What forces have affected this target (organization, situation, industry, technical area) over the past several years?¹⁸
2. Which five or six forces had more impact than others?
3. What forces are expected to affect this target over the next several years?
4. Which five or six forces are likely to have more impact than others?
5. What are the fundamental differences between the answers to questions 2 and 4?
6. What are the implications of these differences for the target being analyzed?

The answers to those questions shape the changes in direction of the extrapolation or the projection shown earlier in Figure 16.1. At more sophisticated levels of qualitative synthesis and analysis, the analyst might examine adaptive forces (feedback forces) and their changes over time.

It is also possible to create a projection or forecast quantitatively. The methodology in fact has been implemented using simulation models. One example, described in chapter 21, is a model based on game theory and developed by New York University professor Bruce Bueno de Mesquita. He has successfully used it to develop projections (based on changing forces) and forecasts (identifying emerging forces) of political developments in several countries.

High-Impact/Low-Probability Analysis

Projections and forecasts focus on the most likely outcomes. But customers also need to be aware of unlikely outcomes that could have severe adverse effects. Creating such awareness is the objective of high-impact/low-probability analysis. It is useful for sensitizing both customers and analysts to think about the consequences of unlikely developments—events that typically arise from the divergent phenomena discussed in chapter 11 and earlier in this chapter. These are typically unexpected and come as unpleasant surprises—to some customers, at least. The events of the Arab Spring in 2011, the rise of Daesh in Iraq and Syria, and the 2014 Russian incursion into Crimea are events that fit into this category. Possible but unlikely future events that could fit into this category are the implosion of China or Iran; an India-Pakistan nuclear exchange; or the release of a genetically engineered, lethal, and highly contagious disease organism.

The analysis requires describing how such a development might plausibly begin and considering its consequences. This provides indicators that can be monitored to warn that the development actually may occur. It therefore takes the form of a scenario (the subject of chapter 17). The CIA's *Tradecraft Primer* describes the analytic process as follows:

- Define the high-impact outcome clearly. This definition will justify examining what most analysts believe to be a very unlikely development.
- Devise one or more plausible explanations for or “pathways” to the low-probability outcome. This should be as precise as possible, as it can help identify possible indicators for later monitoring.
- Insert possible triggers or changes in momentum if appropriate. These can be natural disasters, sudden health problems of key leaders, or new economic or political shocks that might have occurred historically or in other parts of the world.
- Brainstorm with analysts having a broad set of experiences to aid the development of plausible but unpredictable triggers of sudden change.
- Identify for each pathway a set of indicators or “observables” that would help you anticipate that events were beginning to play out this way.
- Identify factors that would deflect a bad outcome or encourage a positive outcome.¹⁹

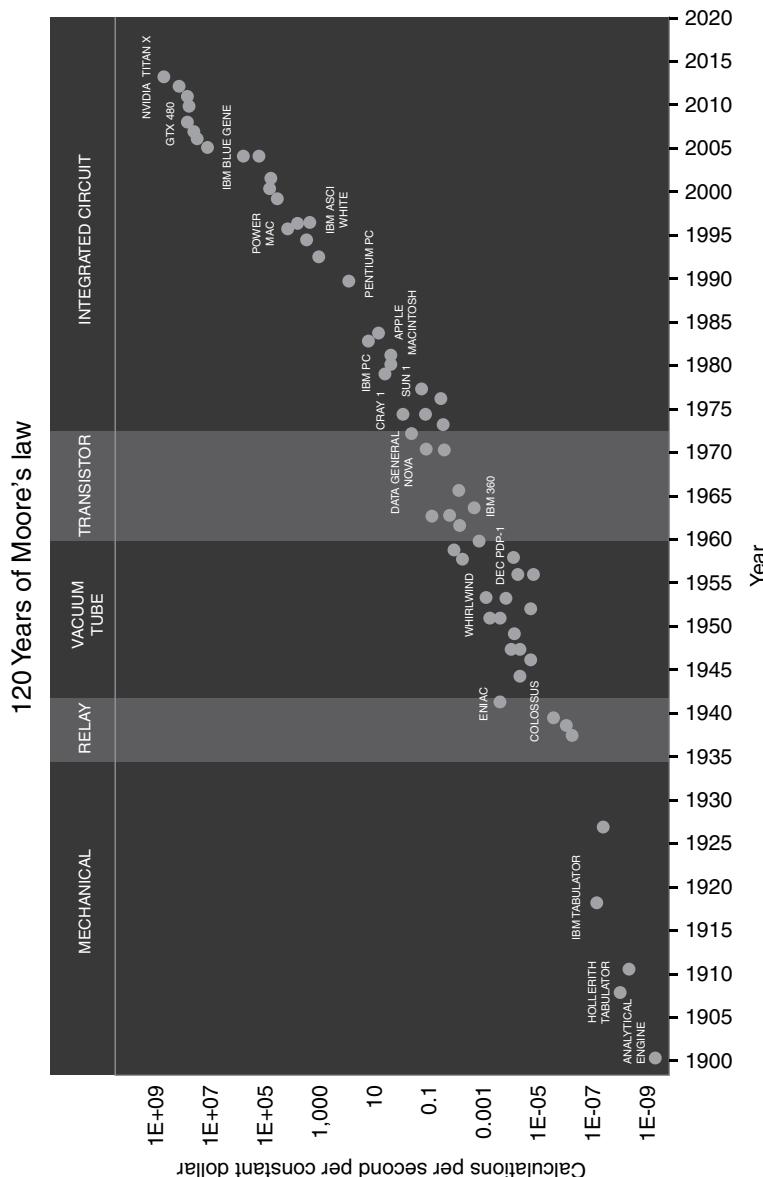
The product of high-impact/low-probability analysis is called a *demonstration scenario*, discussed in more detail in chapter 22.

With this background, we can visit in more detail the three approaches introduced earlier for predicting the future state of a target: extrapolation, projection, and forecasting. Different terms for the three approaches are used in different books. Liam Fahey uses the term *simple projection* to refer to extrapolation, and *complex projection* to refer to both projection and forecasting.²⁰ Projection and forecasting are addressed separately in this text, to emphasize that different forces are involved. To reiterate: An extrapolation predicts future events by assuming that the *current* forces influencing the target go unchanged; it does not consider new forces. A projection assumes current forces will change. A forecast typically begins from a projection and considers what *new* forces may come to bear.

Extrapolation

An extrapolation is a statement, based only on past observations, of what is expected to happen. It is the most conservative method of estimating. In its simplest form, an extrapolation, using historical performance as the basis, extends a curve on a graph to show future direction. When there is little uncertainty about the present state of a target model, and when the analyst is confident about what forces are acting on the target, the estimate begins from the present and propagates forward along the direction of an unchanged system (straight-line extrapolation). In this low-uncertainty, high-confidence situation, new information is given relatively low weight. But when uncertainty about the state of the model is high, new information is accorded a higher value. And when uncertainty about the forces acting on the target is high, uncertainty about the answer is high. Extrapolation is usually accurate in the short run, assuming an accurate starting point and a reasonably accurate understanding of the direction of movement. The assumption is that the forces acting on the target do not change. Inertia is what typically causes a straight-line extrapolation to work. Where inertial effects are weak, extrapolation has a shorter “lifetime” of accuracy. Where they are strong, extrapolation can give good results over time.

Let’s look at some examples of extrapolation. Technophiles in the digital age are familiar with one of the best-known examples, called Moore’s law—the observation that, over the history of computing hardware, the number of transistors that can be placed in an integrated circuit has doubled approximately every two years. American inventor and futurist Ray Kurzweil extended the basic idea of Moore’s law backward in time, by plotting the speed (in calculations per second) per dollar (in constant dollars) of forty-nine well-known calculators and computers spanning the twentieth century.²¹ The result, updated in 2016, is shown in figure 16.3.

FIGURE 16.3 ■ Kurzweil's Extrapolation of Moore's Law


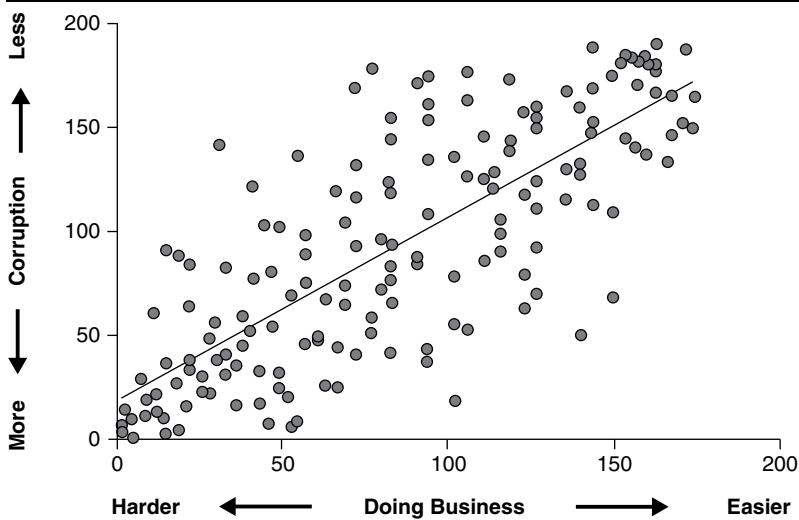
Source: "120 Years of Moore's Law," courtesy of Ray Kurzweil and Kurzweil Technologies, Inc. <https://www.flickr.com/photos/jurvetson/31409423572/>.

The graph illustrates this point: While extrapolations *usually* have relatively short time frames of validity, that's not always the case. Moore's law has been useful to electronics manufacturers for decades; they can plan for future hardware with confidence.

that more powerful computers will be available when they are needed. But it also illustrates a danger in relying on trend extrapolation. The apparent exponential growth shown in figure 16.3 is actually the early part of an S curve (discussed in chapter 9). S curves do not continue to climb indefinitely but eventually level off. By 2020, industry observers generally had concluded that was exactly what was happening.²²

Figure 16.4 illustrates the use of correlation to support extrapolation. It is based on the argument that corruption is strongly correlated with the existence of excessive business regulation. The figure shows the rankings for 175 countries using Transparency International's Corruption Perceptions Index (CPI) versus the World Bank's rankings on ease of doing business (DB 2014). High CPI scores indicate less corruption; high DB 2014 scores indicate a favorable business climate. As the figure indicates, the more bureaucracy and red tape involved in doing business, the more corruption is likely in the country. The correlation coefficient is nearly 0.80, indicating a high level of correlation. Graphics such as this are useful in extrapolating the effects of government actions, for example, the likely reduction in corruption that would result from a government's easing restrictions on doing business.

FIGURE 16.4 ■ Correlation of Perceived Corruption with Ease of Doing Business²³



Source: Augusto Lopez-Claros, "What Are the Sources of Corruption," retrieved from https://www.transparency.org/news/feature/corruption_perceptions_index_2017.

Extrapolation often is a valuable predictive methodology. But its limitations must be recognized, and it must be used properly. First, it usually is inaccurate in the long run because it is narrowly focused and assumes the static forces that operate on the model will continue unchanged, with no new forces being added. As noted earlier, the

method depends on inertia. Second, if the extrapolation starts from the wrong point, it will almost certainly be even farther off as it is extended forward in time. Both problems were present in the NIEs predicting the future development of Soviet military forces from 1974 to 1986. They overestimated the rate at which Moscow would modernize its strategic forces.²⁴ All these estimates relied on extrapolation, without fully considering restraining forces, and they used starting points that were, at best, shaky.

Projection

Before moving on to projection and forecasting, it is worth reinforcing the differentiation from extrapolation. An extrapolation is a simple assertion about what a future scenario will look like. In contrast, either a projection or a forecast is a *probabilistic* statement about a future scenario. The underlying form of such a statement is, “If *A* occurs (plus some allowance for unknown or unknowable factors), then we can expect *B* or something very much like *B* to occur, or at least *B* will become more probable.”

Projection is more accurate over the long term than extrapolation. It predicts a range of likely futures based on the assumption that forces that have operated in the past will change. The changing forces produce a deviation from the extrapolation line, as previously shown by figure 16.1.

Projection makes use of two major analytic techniques. One technique, discussed earlier, is *force analysis*. After a qualitative force analysis has been completed, the second technique is to apply *probabilistic reasoning* to it. Probabilistic reasoning is a systematic attempt to make subjective estimates of probabilities more explicit and consistent. It can be used at any of several levels of complexity (each successive level of sophistication adds new capability and completeness). But even the simplest level of generating alternatives, discussed next, helps to prevent premature closure and adds structure to complicated problems.

Generating Alternatives

The first step to probabilistic reasoning is no more complicated than stating formally that more than one outcome is possible. The analyst generates alternatives simply by listing all possible outcomes to the issue under consideration. The possible outcomes can be defined as alternative scenarios.

Ideally the alternatives should be mutually exclusive (only one can occur, not two or more simultaneously) and exhaustive (nothing else can happen; one of the listed alternatives must occur).²⁵

Let's look at a current example. Suppose that a customer asks for an estimate of the outcome of the ongoing al-Shabaab insurgency in Somalia. This seemingly intractable conflict has been ongoing throughout the twenty-first century. There are three obvious possible outcomes: The insurgency will be crushed, al-Shabaab will succeed in taking control of the country, or there will be a continuing stalemate. (Other outcomes may be possible, but let's assume that they are highly unlikely, and the customer didn't

request a high-impact/low probability analysis.) The three outcomes for the influence diagram are as follows:

- Regime wins
- Insurgency wins
- Stalemate

This list is mutually exclusive and exhaustive. If a fourth option, “The Regime wins initially, but it engenders a new insurgency” were added, the mutually exclusive principle will have been violated.

The key is to list all outcomes that are meaningful. It is far easier to combine multiple outcomes than it is to think of something new that wasn’t listed or to think of separating one combined-event outcome into its subcomponents. The list can serve both as a reminder that multiple outcomes can occur and as a checklist to decide how any item of new intelligence might affect an assessment of the relative likelihoods of the diverse outcomes listed. The mere act of generating a complete, detailed list often provides a useful perspective on a problem.

When generating a set of possible outcomes, the analyst should beware of using generic terms (such as *other*). As the anecdote of the automobile mechanics in chapter 11 illustrates, we do not easily recall the vast number of things that could fall under that seemingly simple label. A catchall outcome label should be included only when a complete list of alternatives cannot be generated first. Also, the possibility of nothing happening should not be overlooked. For instance, when creating a list of the things the French government might do regarding a tariff issue, one item should be “Nothing at all.”

Influence Trees or Diagrams

A list of alternative outcomes is the first step. But for more rigorous analysis, the next step typically is to identify the forces that shape those alternative outcomes and indicate their interrelationships. This process can be done by using an influence tree. Influence trees and diagrams represent a systematic approach to force analysis. They also are a special form of a causal model.

Let’s illustrate that process by continuing the Somalia example: During 2017 and again in 2020, economic conditions deteriorated and the country was in a pre-famine condition. As of 2022, the economy appeared to be improving. Who wins the conflict may depend on whether economic conditions remain the same, improve, or become worse over the next few years. It also may be affected by the success of an ongoing internationally funded poverty relief program. The assumptions that these two are “driver” events, factors, or forces in the outcome are often described as *linchpin premises* in US intelligence practice.²⁶

After listing the two forces, focus on these two questions next:

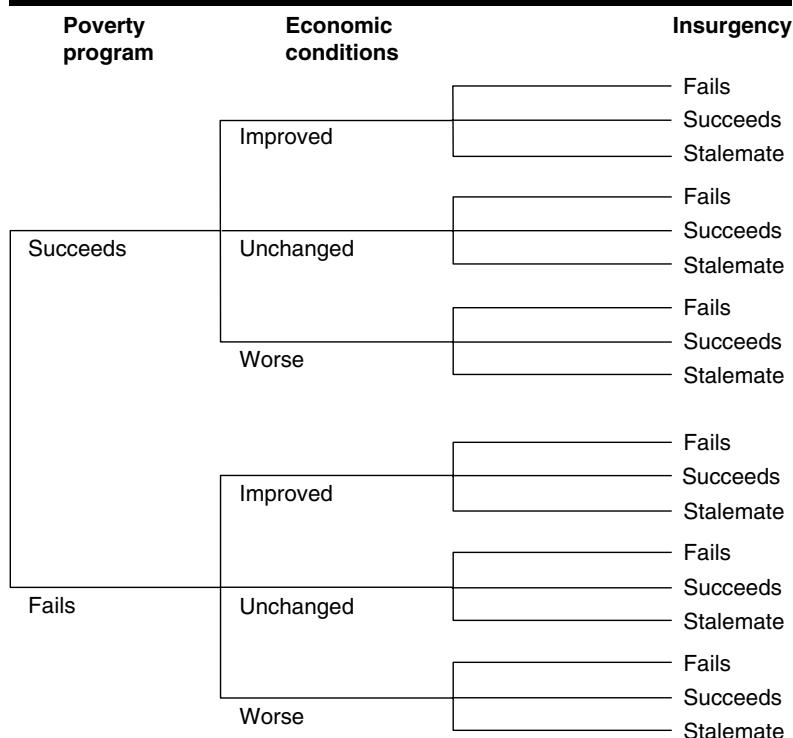
- Do either of these forces influence the other?
- Is it possible to assess the relative likelihood of these forces directly, or do the outcomes depend in turn on other forces and their outcomes?

If the answer to the first question is yes—the forces impact each other—the analyst must define the direction of impact. In the case at hand, there are two influencing forces—economic conditions and the poverty relief program. It is likely that each force affects the other to some extent, but it seems reasonable that the poverty relief program will have more influence on economic conditions than the converse. So an analyst is left with the following relationship:

The poverty relief program influences economic conditions, which influence the outcome of the insurgency.

Having established the uncertain forces that affect the outcome, proceed to the first stage of an influence tree, depicted in figure 16.5. This tree simply shows all the different outcomes in the hierarchy of dependency.

FIGURE 16.5 ■ An Influence Tree for the al-Shabaab Insurgency



Merely generating the list of influencing forces and their outcomes is useful for several reasons. The required thought process helps identify and document factors relevant to judging whether an alternative outcome is likely to occur. In fact, documenting the process (creating an audit trail) is particularly useful in showing colleagues and customers what the analytic thinking has been. It's especially helpful when asking others to contribute to improving the diagram with anything that may have been overlooked. Fortunately, software packages for creating influence trees allow the inclusion of notes that create an automatic audit trail.

In the process of generating the alternatives, analysts must address the issue of whether the force (and its outcome) will make a difference in the assessment of the relative likelihood of the outcomes of any of the other forces listed. For instance, in the economics example, if it would make no difference to the success of the insurgency whether economic conditions improve, remain the same, or worsen, then there would be no need to differentiate these as three separate outcomes. Instead, simplify the diagram.

The second question concerns the need to add influencing forces to the tree. This has to be done only for essential uncertain driving forces; each such addition at least doubles the number of possible outcomes, and the influence tree can quickly become unmanageable.

The thought process also should help identify those forces that contain no uncertainty. For example, the African Union has a peacekeeping force in the country, and the United States supplies arms to the government and supports government forces by conducting airstrikes against al-Shabaab units. Al-Shabaab, for its part, finances its insurgency from external sources, by taxing residents and businesses in areas that it controls and by smuggling goods through Kenya. All these forces will influence the outcomes. We assume that, in this problem, *these are not uncertain outcomes* because intelligence officers have high confidence in their estimates of the forces and effects. They are not linchpins. They have to be taken into account. In fact, they would be used to assess the relative likelihoods of the main event (insurgency) outcome, which will be done next. But the information does not need to be included in the diagram of uncertain forces.

Probabilistic reasoning is used to evaluate outcome scenarios. A relative likelihood must be assigned to each possible outcome in the influence tree in figure 16.5. We do this by starting at the left and estimating the likelihood of the outcome, given that all previous outcomes in that branch of the tree have occurred. This is a subjective process, done by evaluating the evidence for and against each outcome using the evaluative techniques discussed in chapter 11. Figure 16.6 shows the result, *using hypothetical (not actual) estimates*. Note that the sum of the likelihoods for each branch in the tree equals 1.00, and that the cumulative likelihood of a particular outcome (on the far right) is the product of the probabilities in the branches that reach that point. (For example, the outcome probability of the poverty program succeeding, economic conditions improving, and the insurgency failing is $0.224 = 0.7 \times 0.4 \times 0.8$.)

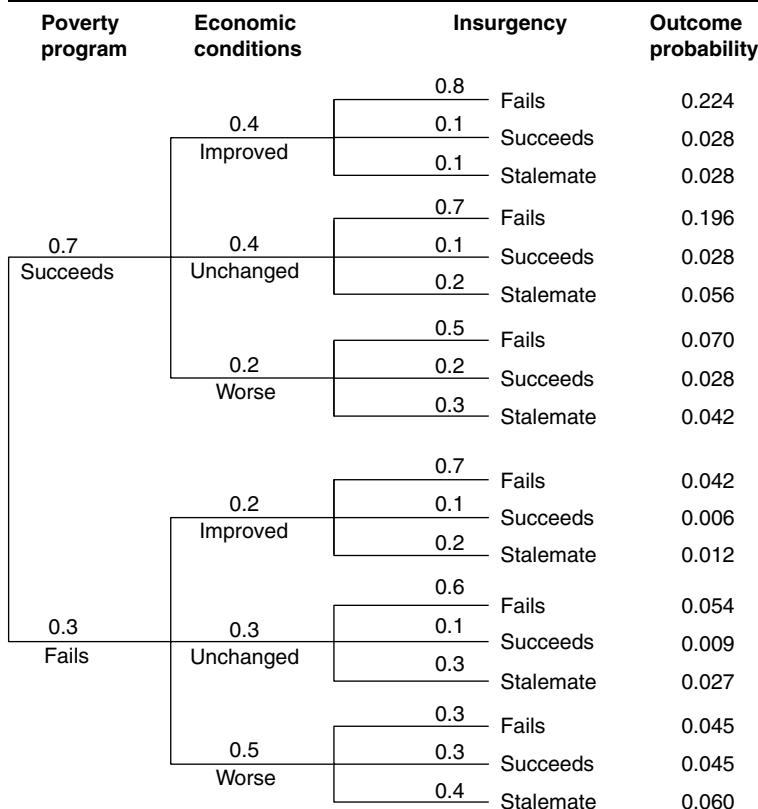
The final step in the evaluation is to total the probabilities on the right in figure 16.6 for each outcome: fails, succeeds, and stalemate. When we do this, we find the following probabilities:

Insurgency fails 0.631

Insurgency succeeds 0.144

Stalemate 0.225

FIGURE 16.6 ■ Influence Tree for the al-Shabaab Insurgency with Probabilities



Note: All values are notional.

This influence tree approach to evaluating possible outcomes is more convincing to customers than would be an unsupported analytic judgment about the prospects for the insurgency. Human beings tend to do poorly with such complex assessments when they are approached in an unaided, subjective manner; that is, by the analyst mentally combining the force assessments in an unstructured way. Conversely, though,

numerical methods such as the influence tree have the inherent disadvantage of implying a false degree of accuracy merely because numbers are used. The numbers are precise and unambiguous in meaning, but customers should be made aware that the numbers are no more accurate than the subjective judgments they represent.

The probability calculations and tree structuring techniques require that feedback loops do not exist, or that the feedback is so small that it can be ignored. A feedback loop would exist if, for example, the economic conditions significantly affect the poverty relief program, or if a continuing insurgency stalemate affects economic conditions. If feedback loops emerge and are needed in influence diagrams, the analyst will have to use techniques designed to handle dynamic feedback situations, such as simulation modeling (described in chapter 21).

Influence Nets

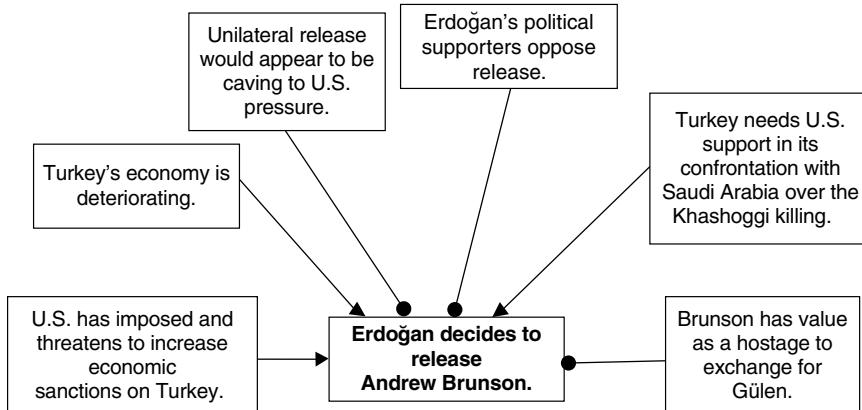
Influence net modeling is a simpler and less mathematical alternative to the influence tree. It is a powerful tool for projection of complex target models where the influence tree would be too cumbersome for practical use—that is, when there are too many uncertain forces to include in the tree. Influence net modeling is a combination of two established methods of decision analysis: Bayesian inference net analysis, originally employed by the mathematical community; and influence diagramming techniques, such as used in the al-Shabaab insurgency example, originally employed by operations researchers. Influence net modeling is an intuitive, graphical technique.

To create an influence net, the analyst defines *influence nodes*, which depict events that are part of cause-and-effect relationships within the target model. The analyst also creates *influence links* between the cause and effect that graphically illustrate the causal relation between the connected pair of events. The influence can be either positive (supporting a given decision) or negative (decreasing the likelihood of the decision), as identified by the link *terminator*. The terminator is either an arrowhead (positive influence) or a filled circle (negative influence). The resulting graphical illustration is called the *influence net topology*. An example topology, drawn from a follow-up to the Erdogan versus Gülen case of chapter 2, is shown in figure 16.7. That case described how in October 2016, Andrew Brunson, an American Presbyterian pastor working as a missionary in Turkey, was arrested and charged with collaborating with terrorists. Brunson's arrest and subsequent incarceration caused a disruption in already-strained US-Turkey relations. Figure 16.7 includes two seemingly unrelated events:

- Relations between the United States and Turkey worsened in 2018 when President Trump imposed economic sanctions on Turkey and reports surfaced of Turkish attempts to exchange Brunson for Gülen.
- On October 2, 2018, Saudi dissident Jamal Khashoggi, a critic of the Saudi government, was assassinated and dismembered after he entered the Saudi embassy in Ankara. The killing is suspected to have been ordered by the

Saudi royal family. It resulted in considerable economic and political pressure from Turkey, the United States, and several European countries to hold the perpetrators accountable.

FIGURE 16.7 ■ An Example Influence Net Model



Note: The arrows come from boxes that support the decision for Erdoğan to release Brunson. The filled dots come from boxes that do not support the decision.

Ten days after Khashoggi's killing, on October 12, a Turkish court ordered Brunson's release, following US negotiations with Erdoğan. Figure 16.7 shows influencing forces that most likely shaped Erdoğan's decision. Note the three factors that weigh against releasing Brunson were present prior to 2018, while the three factors supporting Erdoğan's decision occurred during 2018. The timing of the release also would suggest that one factor in the figure was the deciding one: a sudden need for US support in Turkey's confrontation with Saudi Arabia.

The influence net is one of the most important tools in implementing the target-centric approach. It can be shared with customers and encourages them to provide feedback from their knowledge of the target—adding influencing factors and increasing or decreasing the influence of existing factors in the diagram. (A useful variant for this purpose is to make the influence link lines larger or smaller to indicate the weight given to each factor.)

Note that both influence trees and influence nets are graphical representations of causal models. In some cases, we choose to make the probabilities associated with these models explicit, but it can involve a lot of effort. The influence tree for the al-Shabaab insurgency contained explicit probabilities. It showed that the success of an internationally funded poverty relief program increased the chances that economic conditions would improve; an improvement in the economic situation decreased the chances that the insurgency would succeed.

Methods for Probabilistic Projection

Probabilistic projection methods are used to predict the probability of future events for some time-dependent random process, such as the health of the Japanese economy. A number of probabilistic techniques are used in industry for projection. Two are commonly used in intelligence analysis as follows:

- *Point and interval estimation.* This method attempts to describe the probability of outcomes for a single event using either a most likely number (point estimate) or a range of numbers (interval estimate). An example would be a country's economic growth rate, and the event of concern might be an economic depression (the point where the growth rate drops below a certain level). In this example, a point estimation gives a specific number such as "a growth rate below 3 percent will trigger a depression." An interval estimate would read, "a growth rate below the range of 2 to 4 percent will trigger a depression." NIE estimates frequently make use of interval estimation, though usually by using the standard terms discussed in chapter 5 (such as *very likely* and *remote*) instead of using a numerical range, reflecting the uncertainty that is always present in such estimates.
- *Monte Carlo simulation.* This method simulates all or part of a process by running a sequence of events repeatedly, with random combinations of values, until sufficient statistical material is accumulated to determine the probability distribution of the outcome. Monte Carlo simulations are revisited in chapter 21.

Most of the anticipatory problems in intelligence call for subjective probability estimates. They are routinely used in dealing with broad issues for which no objective estimate is feasible. An estimate about the probability of a major terrorist attack occurring somewhere in the United Kingdom next week, for example, would inevitably be subjective; there would not be enough hard data to make a formal quantitative estimate. In contrast, a prediction of the probability that the Japanese economy will grow by more than 5 percent next year could be made by using formal quantitative techniques (in which case, either a point estimation or Monte Carlo simulation could be used), because quantitative data are available.

Even if a formal probability estimate is used, it will always have a subjective element. A subjective component is incorporated into every estimate of future probability; it is the basis for the weighting of respective outcomes to which no numerical basis can be assigned.

Sensitivity Analysis

When a probabilistic projection is made, it is sometimes worthwhile to conduct a sensitivity analysis on the result. The purpose of sensitivity analysis is to evaluate the relative

importance or impact of changes in the values assigned to influencing event outcomes. The inputs to the estimate are varied in a systematic manner to evaluate their effect on possible outcomes. This process lets an analyst identify variables whose variation has little or no effect on possible outcomes.

A number of tools and techniques are available for sensitivity analysis. Most of them are best displayed and examined graphically. Let's return to the al-Shabaab insurgency for an example of sensitivity analysis. This time we'll address the issue of al-Shabaab financing.

Since it lost control of the port of Kismayo, Somalia, in 2012, al-Shabaab has relied on smuggling through Kenya, abetted by bribes to a few Kenyan authorities. The customer relied on a previous report of the port's importance in supporting the combined attack by the Somali military and African Union forces that retook control of the port. The customer now is concerned about recent reporting on the smuggling through Kenya. She has asked for an assessment of the outcome if she pressures the Kenyan government to rein in the smuggling activities.

There are three possible outcomes: The existing route continues to be the primary (or only) route; al-Shabaab develops a new smuggling route; and al-Shabaab develops a new route, while the Kenyan route becomes secondary. Figure 16.8 shows an analysis of each likelihood, as a function of the probability that the Kenyan government, in response to pressure, will attempt to shut down the smuggling. These three possibilities add up to a likelihood of 1.0 at any point on figure 16.8.

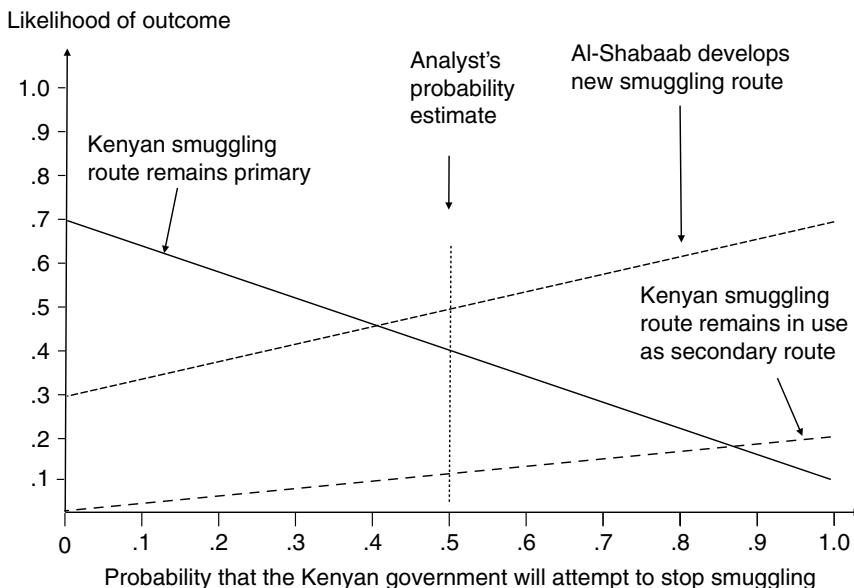
The sensitivity analysis indicates that government action increases the likelihood that al-Shabaab will develop an alternative route. It also indicates that such action strongly decreases the likelihood that the Kenyan route will remain primary but that use of the route in a secondary role is relatively insensitive to the likelihood that the Kenyan government will act. The chart is simplistic, of course; in fact, the straight lines would typically be curves with sharp "knees" at points where the probabilities start changing at different rates.

To complete the analysis, the analyst would estimate the likelihood that the Kenyan government will respond by attempting to stop the smuggling. Based on the estimate of a 50 percent probability that the Kenyan government will respond favorably to the pressure (the vertical line in figure 16.8), there is less than an even chance the Kenyan route will remain the primary route and an even chance that al-Shabaab will develop a new route. (Analysts usually don't give percentages to the customer in an assessment like this one; it implies a level of accuracy that's simply not justified.)

Forecasting

Projections often work out better than extrapolations over the medium term. But even the best-prepared projections can seem conservative when compared to reality years later. New political, economic, social, technological, or military developments will create results that were not foreseen even by experts in a field. Typically, these

FIGURE 16.8 ■ Sensitivity Analysis for al-Shabaab Smuggling through Kenya



new developments are described as disruptive technologies or disruptive events. To take these groundbreaking developments into account, analysts are forced to move to forecasting techniques. Forecasting uses many of the same tools that projection relies on—force analysis and probabilistic reasoning, for example. But it presents a stressful intellectual challenge, because of the difficulty in identifying and assessing the effect of potential new forces. Customers generally prefer to have this highest level of anticipatory analysis so that they can be aware of possible outcomes for a situation and the forces driving toward those outcomes.

A major objective of intelligence forecasting is to define alternative futures of the target framework, not just the most likely. It is essential for effective strategic decision making. Since there is no single predictable future, customers need to formulate strategy within the context of alternative future states of the target. To this end, it is necessary to develop a framework that will make it possible to show systematically the interrelationships of the individually forecast trends and events. A forecast attempts to identify new forces that will affect a target—to consider the possible effects of new developments in distantly related fields, such as new technologies in the realm of artificial intelligence, or new constraints posed by the sociological impact of pollution, or new forms of life created through genetic engineering—and to present them to the customer as possibilities. In all anticipatory analysis, but especially in forecasting, analysts still must consider background forces such as inertia, opposition, contamination, feedback, and synergy—covered in chapter 15.

The Nonlinear Approach to Forecasting

Forecasting methodology requires analytic tools or principles, of course. But for any forecasting methodology to be successful, analysts who have significant understanding of many PMESII factors and the ability to think about issues in a nonlinear fashion are also required. Just as the intelligence process is not linear, an analyst cannot effectively approach forecasting in a linear manner—gathering data, analyzing it, and formulating a solution. Such a mechanistic view of the universe has never served well for forecasting, and it is inappropriate for dealing with complex targets. But, as one study asserted, US intelligence community analysts are not well positioned to grapple with complexity and nonlinearity.

Futuristic thinking flows across many disciplines that have their own order and patterns. In predictive analysis, a good analyst may seem to wander about, making only halting progress toward the solution. This nonlinear process is not a flaw; rather, it is the hallmark of a natural learning process when dealing with complex and nonlinear matters. The natural pattern of thinking about the future appears chaotic on the surface, but it is chaos with a purpose.

The sort of person who can do multidisciplinary analysis of what is likely to happen in the future has a broad understanding of the principles that cause a physical phenomenon, a chemical reaction, or a social backlash to occur. Analysts who are multidisciplinary in their knowledge and thinking can pull together concepts from several fields and assess political, economic, and social, as well as technical, factors. Such breadth of understanding recognizes the similarity of principles and the underlying forces that make them work. It might also be called “applied common sense,” and it is not very common. Out of necessity, analysts instead tend to specialize, because in-depth expertise is highly valued by both intelligence management and intelligence customers. The CIA, for example, once had a Soviet canned-goods analyst and a Soviet timber analyst.²⁷

The failure to do multidisciplinary analysis is often tied closely to mindset. Examples from chapter 1 illustrated this relationship in the cases of the Yom Kippur War and the Soviet incursion into Afghanistan. The mindset of the Israeli and Soviet leadership constrained their consideration of the broader forces acting on Egyptian president Anwar Sadat and in Afghan society.

Similarly, in 1950, US intelligence had two major failures in anticipatory analysis within six months, as a result of a combination of mindset and failure to do multidisciplinary analysis. On June 25 of that year, the North Korean People’s Army invaded South Korea. The UN forces intervened to defend South Korea and pushed the invading forces back into the North. In October and November, responding to the impending defeat of the North Koreans, the Chinese People’s Liberation Army (PLA) attacked and drove UN forces back into South Korea. Both the North Korean and the Chinese attacks were surprises to US leadership.

The belief in Washington that permeated political, military, and intelligence thinking at the time cast the Soviet Union as the dominant communist state, exercising near-absolute authority over other communist states. The resulting perception was that only the Soviet Union could order an invasion by its “client” states, and that such an act would be a prelude to a world war. Washington was confident that Moscow was not ready to take such a step, so no attack was expected. This mindset persisted after the invasion, with the *CIA Daily Summary* reporting the invasion was a “clear-cut Soviet challenge to the United States.” As evidence mounted of a subsequent Chinese intervention, CIA analyses continued to insist that the Soviets would have to approve any Chinese action in Korea.²⁸

In fact, quite the opposite was true. Moscow opposed Chinese intervention, fearing that it could lead to a general war involving the Soviet Union. The US mindset of Soviet decision-making supremacy was abetted by the failure of the CIA to consider the multidisciplinary factors that led to both invasions. Cultural, historic, and nationalistic factors in fact dominated the North Korean and Chinese decision-making processes. Kim Il-sung, North Korea’s leader, was determined to unify Korea under his leadership; he apparently believed that the South Korean population would rise up to support the invasion and the United States would not intervene.²⁹ After the UN advance into North Korea, China’s strategic interests were threatened by the possibility of a hostile Korea on its border. Unfortunately, the CIA analyses took none of this into account.

Techniques and Analytic Tools of Forecasting

The tools described in this and succeeding chapters are used for both projection and forecasting. Chapter 9 introduced the idea of conceptual models. The conceptual model on which projection and forecasting are based is the assessment of the dynamic forces acting on the target. Forecasting is based on a number of assumptions, among them the following:

- The future cannot be predicted, but by taking explicit account of uncertainty, one can make probabilistic forecasts.
- Forecasts must take into account possible future developments in such areas as organizational changes, demography, lifestyles, technology, economics, and regulation.³⁰

For policymakers and executives, the aim of defining alternative futures is to try to determine how to create a better future than the one that would materialize if we merely keep doing what we’re currently doing. Intelligence analysis contributes to this definition of alternative futures, with emphasis on the likely actions of others—allies, neutrals, and opponents.

Forecasting starts with examination of the changing political, military, economic, and social environments. We first select issues or concerns that require attention. These issues and concerns have component forces that can be identified using a combination of the strategies-to-task methodology and causal modeling. Forecasts of changes to these forces (mostly in the form of trends and events) are generated and subsequently interrelated through techniques such as cross-impact analysis. The result is a “most likely” forecast future created in a scenario format from the trend and event forecasts.

If the forecast is done well, these scenarios stimulate the customer of intelligence—the executive—to make decisions that are appropriate for each scenario. The purpose is to help the customer make a set of decisions that will work in as many scenarios as possible.³¹

Evaluating Forecasts

Forecasts are judged on the following criteria:

- *Clarity.* Can customers understand the forecast and the forces involved? Is the forecast clear enough to be useful? For example, particular customers may not be able to accurately define “gross national product” or “the strategic nuclear balance,” but they still can deal with forecasts on these subjects.
- *Credibility.* Do the results make sense to customers? Do the results appear valid on the basis of common sense?
- *Plausibility.* Are the results consistent with what customers know about the world outside the scenario and how this world really works or is likely to work in the future?
- *Relevance.* To what extent will the forecast affect the successful achievement of customers’ mission?
- *Urgency.* To what extent does the forecast indicate that, if action is required, time is of the essence in developing and implementing the necessary changes?
- *Comparative advantage.* To what extent do the results provide a basis for customer decision making, compared with other sources available to customers?
- *Technical quality.* Was the process that produced the forecast technically sound? Are alternative forecasts internally consistent?³²

A “good” forecast meets all or most of these criteria. A “bad” forecast does not. Analysts have to make clear to customers that forecasts are transitory and need constant adjustment to be helpful in guiding thought and action. Customers typically have common complaints about forecasts. For example—the forecast is obvious; it states nothing new; it is too optimistic, pessimistic, or naïve; or it is not credible because it

overlooks obvious trends, events, causes, or consequences. Such objections are desirable; they help to improve the product. There are a number of appropriate responses to these objections: If something important is missing, add it. If something unimportant is included, get rid of it. If the forecast seems either obvious or counterintuitive, probe the underlying logic and revise the forecast as necessary.

UNINTENDED CONSEQUENCES

Policy customers are likely to use the conclusions of an estimate if it identifies specific forces that they can exert influence on. But when an organization or person acts, they often focus on solving the highly visible problem and fail to recognize possible adverse consequences of the selected solution. This is particularly common in national governments. In part because of slower feedback processes and a more cumbersome structure, governments are generally not as quick on their feet as the nongovernmental opponents they often deal with. And in intervention, governments continually encounter the law of unintended consequences: Actions taken to change a complex system will have unintended, and usually adverse, consequences. Like synergy, this is not so much a force as it is a result from the action of other forces.

A classic illustration of the law of unintended consequences dates back to Tudor England. In England before 1535, real property passed by descent to the oldest son upon his father's death. At that transfer, a tax was owed to the king. Over the years, feudal lawyers created a device called the *Use* that allowed trustees to hold legal title to land in trust for the true owner so that, unless all the trustees died at once, the land could be passed repeatedly from father to son without the requirement that a tax be paid.

The story goes that as his financial needs increased, King Henry VIII "contemplated the state of his exchequer with great dismay."³³ A survey of the kingdom's assets revealed to Henry how England's landowners were avoiding his taxes through the device of the Use. In 1535, Henry prevailed upon a reluctant Parliament to pass the Statute of Uses.³⁴ The statute was simple and direct: It vested legal title in the land's true owner, not in the trustee, so that taxes would be due upon the death of the true owner.

The statute is remarkable for two reasons:

- It totally failed in its revenue-raising purpose. Within a few years the British lawyers, who were no less clever than tax lawyers are today, had found enough loopholes in the statute to thwart it.
- The *unintended* consequences of this tax-raising statute were vast, so that it has been called the most important single piece of legislation in the Anglo-American law of property. Specifically, the law gave rise to the modern law of trusts and to the modern methods of transferring real estate. The British Parliament's reaction to the Statute of Uses also led to the law of wills as we know it.

The Statute of Uses also is one of the few known exceptions to the rule that unintended consequences are usually undesirable. It later had highly beneficial results for the general public, though not for Henry VIII.

The law of unintended consequences has an analogy in the world of data processing. In a modern distributed processing network, or in a complex software package, one cannot predict all the effects of changes. But it is predictable that most of the unintended consequences—system crashes, lockouts, vulnerability to malware, and so forth—will be undesirable ones.

The law of unintended consequences may be merely an elegant expression of Murphy's law (that anything that can go wrong, will) or simply an expression of human inability to foretell the outcome of a complex social process. One facet of the law has been described as “counterintuitiveness.” For example, a generic model of a welfare system demonstrated that expanding a welfare system to reduce the number of poor families in a community actually (and counterintuitively) increased their numbers.³⁵ Another model indicated that making drugs illegal as a way to curb drug abuse and reduce other societal problems had the opposite effect.³⁶

There are many historical examples of this law in action in international affairs:

- The harsh terms that the allies imposed on Germany after World War I were one of the root causes of World War II.
- Soviet secrecy during the Cold War forced US defense planners to assume the worst-case scenario and provoked a military buildup that the Soviets did not want.
- Many governments and commercial entities pay ransom for the return of hostages or of ships seized by pirates. But the practice simply provides an incentive for more kidnappings and piracy, the reason the US government policy is to not pay.

Intelligence analysts have an important role to play in dealing with this particular force. They are well positioned to understand how intelligence targets will react to customers' actions and so to identify possible unintended consequences of those actions.

SUMMARY

Intelligence analysis, to be useful, must be anticipatory. Some events or future states of a target are predictable because they are driven by convergent phenomena. Some are not because they are controlled by divergent phenomena.

Intelligence estimates may not come true. But a good estimate—one that accurately describes the forces acting on a target model and the assumptions about those forces—has lasting value for the intelligence customer. As a situation

develops, the customer can revise the assessment if the intelligence analyst gets the forces right.

Analysis involves estimating the future state of a target by using one of three means—extrapolation (unchanging forces), projection (changing forces), and forecasting (both changing and new forces). The task is to assess, from the present and past states of the intelligence target, the transition process that takes the target to its future state and the forces that shape the transition.

Extrapolation is the easiest of the three methods, because it simply assumes the existing forces will not change. Over the short term, extrapolation is usually reliable, but it seldom gives an accurate picture over the medium to long term, because forces do tend to change. Extrapolation can be used to anticipate both straight-line and cyclic trends. Correlation is a frequently used type of extrapolation.

For analysts estimating systems developments in the near term, extrapolations work reasonably well; for those looking farther into the future, projections usually fare better. Projection assumes a probability that the forces will change, and it uses several techniques to evaluate the probabilities and the effects of such changes. This probabilistic reasoning relies on techniques such as influence trees and influence nets. Sensitivity analysis can help the customer to identify the significance of changes in the probabilities that inform a projection.

Forecasting is the most difficult estimative technique. It must include the probabilities of changing forces, as projection does. But it must also identify possible new forces from across the political, economic, social, and technical arenas and assess their likely impact. Because of the resulting complexity, most forecasting relies on the use of scenarios. Forecasting, like projection, also takes into account the effects of shaping forces, discussed in chapter 15.

Unintended consequences—a factor to be considered in all anticipatory intelligence—often result from actions by organizations and individuals. An important role of the intelligence analyst is to identify possible unintended consequences for the customer before any action is taken.

CRITICAL THINKING QUESTIONS

1. The 2022 invasion of Ukraine has been documented extensively, and intelligence reporting about it has been publicly released by the US and NATO governments. Drawing on that material, answer the following questions:
 - a. Could the invasion be characterized as a convergent or divergent phenomenon? Justify your answer.
 - b. The invasion was clearly a high-impact event. At what time prior to the Russian attack on February 24, 2022, could it also be characterized as a low-probability event? Why?

2. The second critical thinking question in chapter 15 made use of the case studies in the 2013 RAND Corporation report *Paths to Victory*, accessible at https://www.rand.org/pubs/research_reports/RR291z2.html.³⁷ Consider again the case that you used there (your instructor may assign a different case):
 - a. Identify the forces that were dominant in the insurgency (aim for four to seven).
 - b. Create an influence tree for the outcome of the insurgency. Include uncertain forces in their order of influence. (In figure 16.5, the order is this: poverty program influences economic conditions.)
 - c. Draw an influence net model for all the dominant forces you have identified, using the diagramming conventions of figure 16.7. Adjust the thickness of the connecting lines to indicate your estimate of the strength of the influencing force.
 - d. If you were creating a sensitivity analysis diagram like figure 16.8 on some uncertain forces, what would its components be (that is, how would you label the two axes and the lines in the diagram)? Do not attempt to draw the diagram.
 - e. Were there any unintended consequences of either side's actions? If so, what were they? Could they have been avoided, and if so, how, and to what effect?
3. Figure 16.8 contains one or more flaws in assumptions or logic (or both). Can you identify it (or them)?
4. In the example problem of al-Shabaab smuggling, suppose you subsequently discover factual evidence that al-Shabaab has developed an alternative smuggling route. Describe how you would revise figure 16.8.

NOTES

1. Throughout this chapter and the next, we'll frequently use terms such as *prediction* and *estimate* as alternatives for *anticipatory analysis*.
2. Reuters Staff, "History of Failure: Efforts to Negotiate on North Korean Disarmament," *Reuters World News*, March 6, 2018, <https://www.reuters.com/article/us-northkorea-missiles-talks-factbox/factbox-history-of-failure-efforts-to-negotiate-on-north-korean-disarmament-idUSKCN1GI2PQ>.
3. George Likourezos, "Prologue to Image Enhanced Estimation Methods," *Proceedings of the IEEE* 18 (June 1993): 796.
4. M. S. Loescher, C. Schroeder, and C. W. Thomas, *Proteus: Insights from 2020* (Utrecht, Netherlands: The Copernicus Institute Press, 2000), A-iv.

5. Andrew Sleigh, ed., *Project Insight* (Farnborough, UK: Centre for Defence Analysis, Defence Evaluation and Research Agency, 1996), 17.
6. Barbara W. Tuchman, *The Guns of August* (New York, NY: Random House, 1962).
7. Roberta Wholstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).
8. Irving Langmuir, "Science, Common Sense, and Decency," *Science* 97 (January 1943): 1–7.
9. Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity* (Boston, MA: Butterworth-Heinemann, 1999), 52.
10. James Noren, "CIA's Analysis of the Soviet Economy," in *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*, ed. Gerald K. Haines and Robert E. Leggett, CIA Center for the Study of Intelligence Conference, Princeton University, March 2001, 11, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article02.html>.
11. Ibid.
12. Paul Carroll, *Big Blues* (New York, NY: Crown Publishers, 1993), 18.
13. Figure 16.2 assumes that the existing forces change to produce a projection. It is possible that existing forces don't change, and that only new forces come into play. In that case, you would iterate directly from the extrapolation to the forecast.
14. Gharajedaghi, *Systems Thinking*, 51.
15. Noren, "CIA's Analysis of the Soviet Economy."
16. Ibid.
17. Gharajedaghi, *Systems Thinking*, 122.
18. The time frame for most predictions extends over years. On a fast-developing situation, the appropriate time frame for force analysis may be months or even days, not years.
19. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009), 22, <https://www.cia.gov/resources/csi/books-monographs/a-tradecraft-primer/>.
20. Liam Fahey, *Competitors* (New York, NY: Wiley, 1999), 448.
21. Ray Kurzweil, "The Law of Accelerating Returns," March 7, 2001, <http://www.kurzweilai.net/the-law-of-accelerating-returns>.
22. David Rotman, "We're not prepared for the end of Moore's Law," *MIT Technology Review* 123, no. 1 (2020): 61.
23. Augusto Lopez-Claros, "What Are the Sources of Corruption," The World Bank, February 10, 2014, <http://blogs.worldbank.org/futuredevelopment/what-are-sources-corruption>. The World Bank authorizes the use of this material subject to the terms and conditions on its website, <http://www.worldbank.org/terms>.
24. Noren, "CIA's Analysis of the Soviet Economy," 5.

25. This will permit later extension to more sophisticated analyses, such as Bayesian analysis, discussed in chapter 11.
26. Jack Davis, *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence* (Washington, DC: CIA, 1995), 8.
27. Noren, "CIA's Analysis of the Soviet Economy," 7.
28. P. K. Rose, "Two Strategic Intelligence Mistakes in Korea, 1950," *Studies in Intelligence* (Fall/Winter 2001), http://www.cis.gov/csi/studies/fall_winter_2001/article06.html.
29. William Stueck, *The Korean War: An International History* (Princeton, NJ: Princeton University Press, 1995).
30. James L. Morrison and Thomas V. Mecca, "Managing Uncertainty: Environmental Analysis/Forecasting in Academic Planning," January 12, 2003, <http://horizon.unc.edu/courses/papers/Mang.asp>.
31. Ibid.
32. W. I. Boucher, *Technical Advisors' Final Report: Chapters Prepared by Benton International, Inc.*, prepared for the Futures Team of the Professional Development of Officers Study (PDOS), Office of US Army Chief of Staff (Torrance, CA: Benton International, 1984).
33. John E. Cribbet, *Principles of the Law of Property* (St. Paul, MN: Foundation Press, 1975).
34. Ibid.
35. Gharajedaghi, *Systems Thinking*, 49.
36. Ibid., 48.
37. Christopher Paul, Colin P. Clarke, Beth Grill, and Molly Dunigan, *Paths to Victory: Detailed Insurgency Case Studies* (Santa Monica, CA: RAND Corporation, 2013), https://www.rand.org/pubs/research_reports/RR291z2.html.

17

SCENARIOS

Chapters 15 and 16 established that doing anticipatory analysis, where uncertainty is at its highest level, is not for the timid. Doing it well requires an analyst to reach outside the established fact set of the current target framework and to consider future states using multidisciplinary, historical, and futuristic perspectives. The analyst must identify all relevant forces and factors (including those in the background) that could affect future developments. Next, the analyst isolates, analyzes, and ranks the potential impact of key and dominant driving forces using systematic, probabilistic methodologies. And finally, the subject of this chapter, the analyst conveys possible courses of events that may be hard to fathom and far afield from anything the customer can typically envision. There is a product for doing that: the outcome scenario.

Most anticipatory analysis results in some form of scenario—a specially constructed vignette that describes the future state of the target in story form. Because it is impossible to know the future precisely, the solution is to create several scenarios about what events may lie ahead, each one modeling a distinct potential outcome or plausible picture. The resulting set of scenarios establishes the boundaries of the customer's uncertainty and the limits to credible futures. It is used primarily for planning and decision making. In the past, scenarios took the form of written narratives in story form. Today, they are increasingly produced as augmented reality or virtual reality models; an interactive simulation is a powerful way to convey intelligence. Being immersed in what looks and feels like a real-world situation can be very persuasive. Think of virtual worlds such as Minecraft or massively multiplayer online role-playing games such as World of Warcraft.

Veteran analyst and writer Randolph Pherson observed that the objective of anticipatory analysis, or as he describes it, "foresight analysis," is "not to predict the future, but to generate a solid set of scenarios that can bound the range of plausible alternative futures—and sometimes even speculate on the potential emergence of possible scenarios.¹⁵" Pherson observed that scenarios can take several forms:

- *Expected Future Scenario. The future we expect will happen by making a straight-line extrapolation from current trends.*
- *Probable Future Scenarios. A set of scenarios that describe familiar variations on what is likely to happen given current trends.*

- *Plausible Future Scenarios.* A set of scenarios that could happen based on what we know today but are sufficiently different from what we ordinarily would expect.
- *Possible Future Scenarios.* A much larger set of scenarios capturing all that we can imagine could happen even though they may rely on disruptive technology that humanity does not yet possess.
- *Preferred Future Scenario.* What the decision-maker would most like to see emerge—and might even act in order to help make that happen.²

The preferred future scenario is a special type used in prescriptive intelligence, the subject of chapter 22.

WHY USE SCENARIOS?

The purpose of scenarios is to highlight or emphasize major forces that could shape the future. Scenario development makes the forces visible, so that as they begin to make an impact, an analyst will at least recognize them.³ Scenario planning thereby helps both the analyst and the customer to anticipate the future and better respond to subsequent events.

Scenarios have great power to communicate the sense or feel of situations that do not currently and may never exist. They give decision makers a feel for what might happen if they pursue a certain course of action in a complex situation that cannot be quantified. CIA's *Tradecraft Primer* refers to the methodology as *alternative futures analysis*.⁴ Every four years since 1997, the CIA and subsequently the DNI's National Intelligence Council has published a *Global Trends* report. These reports, primarily intended to inform policymakers in an incoming presidential administration, provide scenarios about the future global environment. To create the scenarios, the NIC draws on expertise from outside government on issues such as emerging transnational threats, demography, the environment, and globalization. Consider these synopses of five scenarios, taken from the introductory section, "Alternative Scenarios for 2040," provided in the 2021 report:

In Renaissance of Democracies, the world is in the midst of a resurgence of open democracies led by the United States and its allies. Rapid technological advancements fostered by public-private partnerships in the United States and other democratic societies are transforming the global economy, raising incomes, and improving the quality of life for millions around the globe. The rising tide of economic growth and technological achievement enables responses to global challenges, eases societal divisions, and renews public trust in democratic institutions. In contrast, years of increasing societal controls and monitoring in China and Russia have stifled innovation as leading scientists and entrepreneurs have sought asylum in the United States and Europe.

In A World Adrift, the international system is directionless, chaotic, and volatile as international rules and institutions are largely ignored by major powers like China,

regional players, and nonstate actors. Organization for Economic Cooperation and Development (OECD) countries are plagued by slower economic growth, widening societal divisions, and political paralysis. China is taking advantage of the West's troubles to expand its international influence, especially in Asia, but Beijing lacks the will and military might to take on global leadership, leaving many global challenges, such as climate change and instability in developing countries, largely unaddressed.

In Competitive Coexistence, the United States and China have prioritized economic growth and restored a robust trading relationship, but this economic interdependence exists alongside competition over political influence, governance models, technological dominance, and strategic advantage. The risk of major war is low, and international cooperation and technological innovation make global problems manageable over the near term for advanced economies, but longer term climate challenges remain.

In Separate Silos, the world is fragmented into several economic and security blocs of varying size and strength, centered on the United States, China, the European Union (EU), Russia, and a couple of regional powers; these blocs are focused on self-sufficiency, resiliency, and defense. Information flows within separate cyber-sovereign enclaves, supply chains are reoriented, and international trade is disrupted. Vulnerable developing countries are caught in the middle with some on the verge of becoming failed states. Global problems, notably climate change, are spottily addressed, if at all.

In Tragedy and Mobilization, a global coalition, led by the EU and China working with nongovernmental organizations and revitalized multilateral institutions, is implementing far-reaching changes designed to address climate change, resource depletion, and poverty following a global food catastrophe caused by climate events and environmental degradation. Richer countries shift to help poorer ones manage the crisis and then transition to low carbon economies through broad aid programs and transfers of advanced energy technologies, recognizing how rapidly these global challenges spread across borders.⁵

These are compelling summaries that point to current concerns in world affairs that everyday people (much less decision makers) discuss in coffee shops or around the kitchen table.

A narrower example scenario might be one that describes the likely pattern of daily life in the future under specified assumptions about nuclear power plant regulation. Depending on the views of the planner, the scenario could be used to support or oppose increased regulation. A supporter would likely develop scenarios that include a series of Chernobyl- or Fukushima-type disasters absent regulation. An opponent would be more likely to devise scenarios that show a world of high electric power costs, atmospheric pollution due to coal-burning power plants, and declining economies due to the increasing energy costs of regulation. Of course, an intelligence analyst's job is to maintain the objectivity to avoid such slanted treatment.

Scenarios are used in strategic planning—for instance, in business—to examine merger candidates or consider a new product line. They are used also in tactical or operational planning—for example, for interdicting illicit traffic such as narcotics. In interdiction, the scenarios would include a geospatial target model of coca crop-growing

and narcotics-processing areas and drug trans-shipment routes, possibly with time-line models showing when trans-shipments take place. For operational planning, they would be modified to show the effect of specific narcotics interdiction actions—for example, deployment of radar surveillance aircraft into the Caribbean or a program to pay farmers not to grow the coca crop. Knowledge of the target makes the analyst (along with the customer) a key player in incorporating such components into the scenario.

In an alternative future as depicted by a scenario, a decision maker should be able to make decisions and develop strategies by identifying the following:

- Relationships among forces
- The probable impacts of those forces on an organization or a situation
- The key decision points for taking action

To do this, the decision maker needs to have available a set of alternative scenarios that reflects a realistic range of possibilities. Predicting the future in detail is no more possible than predicting the weather in detail. The details tend to be controlled by divergent phenomena, such as an assassination in Sarajevo. But the dominant forces and trends tend to be convergent phenomena that allow the creation of a few “most likely” outcome scenarios, with indicators that point to which outcome is more likely.

Once scenarios are created, the intelligence analyst turns to tracking indicators that point toward a specific scenario (for example, favorable consumer reaction to the new product line or the increased flow of narcotics through a specific location). The methodology for doing that is discussed later in this chapter.

TYPES OF SCENARIOS

Three basic types of scenarios are used in intelligence.⁶ Each moves through time, enabling the customer to understand the forces and decision points that lead to the final “scene” of the scenario. Two of the three, the *driving-force* and *system-change* scenarios, are most commonly used and are covered here. The third, the *demonstration* scenario, is explained in chapter 22 because of its use in prescriptive intelligence.

Driving-Force Scenario

The driving-force scenario is an implementation of the estimative approach for projection, described in chapter 16. The analyst examines the major forces acting on the target and determines how they are changing. These forces are used to produce the projected future scenario.

The usual method is to create multiple driving-force scenarios (alternative outcomes). The analyst does the following:

- Identifies the key *uncertain* factors or forces that will shape the outcomes
- Identifies the alternative levels of change for each factor or force
- Develops a matrix or influence tree showing the outcomes for each assumed combination of the factors or forces

An example of this scenario development process is the influence tree reflecting the ongoing al-Shabaab insurgency in Somalia, described in chapter 16 (see figure 16.5). Three possible outcomes are postulated: regime wins, insurgency wins, and stalemate. Two uncertain forces are identified as shaping the outcome: a poverty program that could either succeed or fail, and economic conditions that could remain unchanged, improve, or worsen. The result is a set of six possible combinations of the two forces, which in turn leads to a set of probabilities for the three possible outcomes.

Some driving-force scenario combinations choose to emphasize a single dominant force for each alternative scenario. This path was taken in *Proteus*, a book of possible future scenarios sponsored by the US National Reconnaissance Office. In *Proteus*, for example, the scenario “Amazon.plague” has a single dominant force: a series of highly contagious, deadly viruses that sweep the globe.⁷ The *Global Trends* scenarios from their beginning have considered alternative dominant forces.

Driving-force scenarios allow the analyst to describe the effects of changing forces, with a caveat. Once they are selected, the alternative force levels are assumed to remain constant. This assumption is consciously made in order to simplify the problem, but it ignores potential events that would affect the strength of forces or introduce new ones. In the insurgency influence tree of figure 16.5, for example, there is no provision for a poverty program that initially does nothing, then gradually succeeds or—alternatively and more likely—initially succeeds and then runs into problems due to corruption.

System-Change Scenario

The system-change scenario is a variant of the driving-force scenario. The difference is that system-change scenarios must consider all PMESII forces that could have a significant impact. System-change scenarios also deal with the caveat identified previously. They account for both changes in existing forces and the introduction of new ones. One method of creating the system-change scenario relies on cross-impact analysis (discussed later in this chapter) to identify interactions among events or developments (such as synergy), and then from these interactions to develop alternative outcomes. This is an especially difficult scenario to develop because of the need to examine interrelationships among forces.

SCENARIO PERSPECTIVES

The scenario usually begins in the present and unfolds to some future time. The simplest is the straight-line extrapolation scenario; it assumes that only current forces and policy choices will be felt in the future (no technological discoveries or revolutions, for example, are permitted). These extrapolation scenarios are “momentum” scenarios—they are dominated by inertia, and no countervailing forces arise to slow the observed trend.⁸ Most China scenarios tend to be momentum scenarios based on the country’s consistently spectacular growth. They don’t contemplate a weak divided China of the future (for example, a China ruled by economic or military warlords) in spite of the Soviet example and of Chinese history. Scenarios about Japan’s economy created in the early 1980s had a similar momentum pattern and proved to be inaccurate. Because momentum scenarios are straight-line extrapolations, it is prudent not to use them for long-term assessments. The analyst can start with extrapolation but should then look at new and changing forces that create projection and forecast scenarios.

HOW TO CONSTRUCT SCENARIOS

Scenario planning is really a branch of the well-known modeling, simulation, and gaming methodologies. As such, it is an art as much as it is a standardized or systematic methodology. Nevertheless, it’s wise to begin with a straightforward framework.

Peter Schwartz, former head of global planning for Royal Dutch Shell and a highly regarded authority on scenario development, describes a straightforward process of scenario construction. He includes eight steps:

1. *Identify focal issue or decision*
2. *Key forces in the local environment*
3. *Driving forces*
4. *Rank by importance and uncertainty*
5. *Selecting scenario logics*
6. *Fleshing out the scenarios*
7. *Implications*
8. *Selection of leading indicators and signposts*⁹

Schwartz’s steps are based on the use of scenarios for business decision making. We’ll discuss the same elements but use an example relevant to intelligence.

Shell Energy Scenario

In 2018, Shell completed three scenarios that envisioned alternative energy futures and global average temperature change. Following is a brief description of each.

Scenario One: Mountains. This scenario anticipates a world of moderate economic development, with policy playing an important role in shaping the global energy system and environmental pathway. These policy measures result in more compact cities and transform the global transport network. Cleaner-burning natural gas becomes the backbone of the world's energy system. Global demand for oil peaks in about 2035, with electricity and hydrogen dominating for cars and trucks by the end of the century. Technology to capture carbon dioxide emissions aids in reducing CO₂ emissions from the power sector to zero by 2060. While greenhouse gas emissions begin to fall after 2030, they remain on trajectory to overshoot the target of limiting global temperature rise to 2 degrees Celsius.

Scenario Two: Oceans. This scenario envisions a prosperous, but also volatile world. The global energy system is shaped more by market forces and civil society than government policy. Both nuclear power and natural gas growth are limited outside North America by public resistance and slow adoption of policies and technologies, with oil and coal remaining significant forces in the worldwide energy system. Lacking legal and financial support, carbon catching and storage lags, capturing roughly 10% of emissions by mid-century. As a result, electricity generation takes about 30 years longer to become carbon neutral in the Oceans scenario vice Mountains. Hard-to-reach oil resources are developed due to high energy prices and a surge in energy demand, though oil demand plateaus around 2040. These high energy prices encourage improvements in efficiency and also solar power, with solar becoming the largest primary source of energy by the 2060s.

Scenario Three: Sky. This scenario brings further to the surface the emerging possibility of multi-lateral collaboration to tackle climate and air-quality issues. It combines the most progressive elements of both Mountains and Oceans. In Sky, governments respond positively to the rapid cycle of assessment, review, and improvement of national contributions, as set up under the 2016 Paris Agreement. Peer pressure, emerging from the Paris transparency framework, provides an additional push.

At the national level in Sky, governments implement legislative frameworks to drive efficiency and rapidly reduce CO₂ emissions, both through forcing out older energy technologies and by promoting competition to deploy new technologies as they reach cost effectiveness. Government-led carbon pricing emerges in Sky as a suite of taxes, levies, and market mechanisms. By 2030, a common understanding is reached between governments as to the appropriate level of the cost of emissions.¹⁰

Figure 17.1 illustrates a simplistic summary of major driving forces in the three Shell scenarios, with a fourth one added by this author: a momentum scenario, which currently appears to be the likely one—or in Pherson's terminology, the probable scenario, the other three being plausible scenarios.

Most scenarios are more detailed and broken down to lower levels than those illustrated in figure 17.1. For example, they might describe relationships among objects or entities (tanks, missiles, airplanes, and units in a military scenario; governments, companies, technologies, and weapons systems in a nonproliferation scenario; governments, farmers, drug cartels, banks, and drug users in a counternarcotics scenario). In a dynamic scenario, the objects must then change in space and time according to known rules (patterns of business competition; military doctrine in military scenarios; past patterns of clandestine trade and of systems development in a nonproliferation scenario). A military scenario, which can be well defined by existing scenario development tools, is quite different from a nonproliferation or counternarcotics scenario. It is not the same in format, content, event descriptions, or types of objects being manipulated. However, the basics remain the same; relationship analysis, for example, is much the same in all scenarios.

FIGURE 17.1 ■ Four Global Energy Scenario Logics

Mountains <ul style="list-style-type: none"> • Government policies dominate • Moderate economic future • Primary energy source: natural gas • CO₂ capture 	Sky <ul style="list-style-type: none"> • Government policies dominate • Prosperous economic future • Primary energy source: electricity • CO₂ capture
Momentum <ul style="list-style-type: none"> • Market forces dominate • Moderate economic future • Primary energy sources: oil and natural gas • Little or no CO₂ capture 	Oceans <ul style="list-style-type: none"> • Market forces dominate • Prosperous economic future • Primary energy source: oil • Little or no CO₂ capture

Note that this figure has the elements of a system-change scenario. It takes into account all the PMESII forces that could have a significant impact. It also includes both existing forces and possible new forces. Using the explanation of model types from chapter 9, it is a *descriptive* scenario, not *normative*; it does not specify a recommended set of actions for policymakers to take—though many would consider the Sky scenario the most attractive one to strive for.

To produce the scenario logics, the analyst has to work with the issues, the targets, and the forces, reshaping and reframing them and drawing out their less obvious elements until a pattern emerges about which two or three key or driving forces will make a difference in the outcome. These are the scenario drivers. This step involves differentiating the scenarios: identifying inconsistencies, finding underlying similarities, and eliminating scenarios that are redundant or implausible.

Let's look at each of Schwartz's steps in the context of the Shell scenarios.

1. Define the Issue and the Target Framework

We addressed this step in chapters 8 through 10. Lawrence Wilkinson, one of Schwartz's former partners, explains the relationship, the importance of issue definition, and the target framework this way:

Scenario planning begins by identifying the focal issue or decision. Rather than trying to explore the entire future, ask yourself, "What question am I trying to answer?"¹¹

In the Shell scenario set, the likely question could be either "What is the world's likely energy future?" or "What are the expected futures for global temperature change?"

2. Identify and Rank the Driving Forces or Factors

These actions correlate to Schwartz's steps 2, 3, and 4. The analyst first identifies the key forces that will shape the scenario. Attempting to identify the primary driving forces at work in the present leads to understanding the dynamics shaping the future. Pherson explains one of the tools for doing that—*horizon scanning*—as a systematic exploratory technique designed to identify and evaluate emerging trends, issues, and signals of all kinds that are likely to play an important role in how the future will unfold.¹² While we do not detail it here, the methodology is akin to the target-centric analysis process in that it relies on engaging decision makers as integral to achieving successful results.

Next, the analyst isolates the driving forces. Which ones are critical to the outcome? Focus also should be on any asymmetric forces present. Most companies, for instance, are driven by the need to cut costs and incorporate new technologies. Unless one of the target organizations is markedly better or worse than others at doing these things, the differences will not affect the end result. Thus, the two forces would not need to be included.

The next action is to rank the isolated driving forces by importance and uncertainty. Some carry more consequences than others. In the Shell scenarios, market forces and government policies have significant impact but are uncertain. In contrast, population growth is fairly predictable and over the coming decades will have a similar effect in any scenario. And oil and gas reserves are well known today and change slowly with new discoveries; but the rate of draw-down for both is uncertain. In contrast, some questions are highly uncertain. Both the economic future and the availability and effectiveness of CO₂ capture technology are examples. The driving forces to be considered will be those that are both very important (high consequences) and highly uncertain.¹³

3. Select the Scenario Logics

This is arguably the most important step. The goal is to finish with a scenario set—typically four or fewer—that provides your customer with a basis for decision making. The scenarios therefore must be derived from a few fundamental differences, or what Schwartz calls “scenario drivers.” Figure 17.1 illustrates the meaning of the term. The fundamental differences are clear, shown in a matrix drawn by placing the mutually exclusive factors opposite each other. Either government policies or market forces; either a prosperous or moderate economic future; either a vigorous or moderate technology development (specifically, energy and CO₂ capture technologies); and either open, cooperative governments or closed, conflictual ones dominate.

4. Flesh Out the Scenarios

Finally, go back to all the isolated driving forces and trends from step 2 and use these to flesh out the scenarios. In the Shell scenarios, degree of risk, ability of governments to act cooperatively, and ability to muster popular support are all critical in some and not so important in others.

There are two commonly used techniques for fleshing out scenarios: case-based models and cross-impact analysis.

Case-Based Models

Case-based models are the foundation for an analytic method called case-based reasoning. The technique is sometimes called reasoning by analogy or reasoning by history.

Case-based reasoning is about using previous experiences to understand and solve new problems. This can mean adapting old solutions to meet new demands, using old cases to help explain current situations or to critique new solutions, or reasoning from precedents to interpret a new situation (much as lawyers do) or to create an equitable solution to a new problem (much as labor mediators do).¹⁴ Intelligence analysts often work a new problem by remembering a previous similar situation (a similar target model) and then applying information and knowledge from that situation (duplicating the model).

A few typical situations having intelligence implications can illustrate how case-based reasoning should work:

- The French loss in Vietnam in the 1950s should have warned the United States of a possible adverse outcome scenario for intervening in Vietnam in the 1960s. The US outcome in Vietnam should have cautioned the USSR about a possible failure when invading Afghanistan in the 1980s. All of those should have been a warning flag for the Israelis in considering outcome scenarios before invading Lebanon in 1982.

- The 2002–2004 SARS outbreak; the 2009 H1N1 pandemic; the 2012 Middle East respiratory syndrome (MERS); the 2014 Ebola outbreak; and Zika in 2015—all provided illustrative cases about a pandemic’s origin and spread that could have assisted in planning to manage and contain the COVID-19 pandemic that started in 2020.

A caution on case-based reasoning, however. Future scenarios seldom (if ever) exactly follow the patterns of past ones.

Cross-Impact Analysis

Cross-impact analysis supports system-change scenarios. It usually shows interactions among events or developments, specifying how one will influence the likelihood, timing, and mode of impact of another in a different but associated field. As a simple example, the development of the Global Positioning System enabled the development of relatively inexpensive yet highly precise munitions (bombs and missiles). These developments in turn required increased emphasis on providing the military with precise real-time geospatial intelligence, driving a demand for continuous battlefield reconnaissance from, for example, UAVs. And the combination of all of these developments forced opposing military organizations to create highly mobile force units that move constantly during combat to avoid being hit.

The Shell scenarios are all the product of cross-impact analysis. Both government policies and market forces, after all, affect the economy, the selection of energy sources, and the advancement of CO₂ capture technology.

Cross-impact analysis has been used extensively to model the interaction between trends and future events. In the 1970s, the Futures Group developed a version of it called *trend impact analysis* that became well established and is still in use.¹⁵ Network analysis methodologies, described in chapter 19, naturally support cross-impact analysis.

This is a brief introduction to creating and fleshing out scenario plots. Jay Ogilvy and Peter Schwartz provide a more detailed step-by-step explanation, available online.¹⁶

5. Draw Out the Implications

This is Schwartz’s step seven. Having built a set of potential future scenarios, the analyst now assesses the implications in relation to the original question. Does the idea of paying farmers not to grow coca crops, introduced earlier, imply favorable outcomes in the counternarcotics scenarios? Perhaps a common result in the scenarios would be that new groups of farmers start growing coca crops in order to qualify for the payments, or a bidding war starts between the drug cartels and the government. (Both of these outcomes, of course, are unintended consequences, as discussed in chapter 16.) The customer of intelligence, the policymakers who are informed by the

scenarios, need to understand these possible implications and develop their options accordingly.

Implications are clearly drawn in the Shell scenarios. In Mountains, global demand for oil peaks in 2035, and greenhouse gas emissions start to decline in 2030. In Oceans, oil plateaus in 2040, and greenhouse gas emissions take longer to start a decline.

6. Identify and Monitor Indicators

The job of the intelligence analyst (and the customer) in Schwartz's final step is monitoring. What are the leading indicators that would tell which scenario—or which combination of scenarios—is actually taking place? As Liam Fahey points out, indicators will also give important insights into what scenarios are *not* taking place.¹⁷

The monitoring work may involve watching trends. An analyst might track demographic and economic trends, spread of infectious diseases, changes in pollution levels, or proliferation of terrorist cells. A political or economic analyst might look at the questions that opponents ask and the positions they take in trade negotiations. A military intelligence analyst would monitor troop movements and radio traffic for signals as to which scenario is developing. These types of indicators suggest movement toward a particular scenario.¹⁸ They provide a means to decide which options should be the focus of a customer's decisions. Specifically, they help identify which outcomes should be prepared for, possibly by use of some of the instruments of national power, and which potential outcomes can be disregarded.

The US intelligence community has developed a formal methodology for monitoring indicators, or what it terms “indicators or signposts of change.” It is described in the CIA’s *Tradecraft Primer* as “periodically review a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change.”¹⁹ It depends on the analyst’s identifying and listing the observable events that would indicate a particular scenario is becoming more or less likely, regularly reviewing all of the lists (one for each scenario) against incoming intelligence, and selecting the scenario that appears most likely to be developing.²⁰

The indicators in the Shell scenarios are mostly trends rather than specific events: trends in oil, natural gas, and coal usage, along with progress in CO₂ capture technology and usage. CO₂ capture technology, though, could advance suddenly and dramatically with an engineering breakthrough. And the patterns of energy usage envisioned in the Shell scenarios almost certainly will be disrupted in the wake of the 2022 Russian invasion, with its consequences in oil and gas embargoes on Russia and Western searches for both alternative supplies and new energy sources.

SUMMARY

Most anticipatory analysis results in some form of scenario—a description of the future state of the target. Typically, the analyst will create a set of alternative scenarios based on different assumptions about the forces involved. Two often used in intelligence

are the driving-force, a type of projection, and the system-change, a forecast. A driving-force scenario identifies and assesses the uncertain factors or forces that shape the future, often representing them in matrix or influence tree form. System-change scenarios are especially demanding to construct because they consider all PMESII factors and they require cross-impact analysis—that is, looking at how events or developments in one area will affect events or developments in a different area.

Analysts seldom create a single scenario; there are always alternative futures, and the need is to capture the most likely outcomes. Creating scenarios can be an art, but there is a logical framework to work from.

Creating an intelligence scenario involves six steps:

1. *Define the issue and the target.* The purpose here is to create a scenario that will be useful to the intelligence customer.
2. *Identify and rank the driving forces or factors.* Focus attention on those driving forces or factors that are both important and highly uncertain. They are the ones that are most likely to shape future developments.
3. *Select the scenario logics.* The final scenarios should be few in number and span the range of likely outcomes based on the dominant driving forces and factors.
4. *Flesh out the scenarios.* Expand and provide details about the scenario logics. Explain why the selected driving forces are likely to dominate and what their effects are likely to be.
5. *Draw out the implications.* Look back at the original question to ensure the scenarios give the customer needed insights into likely future developments, and identify likely unintended consequences of customer actions.
6. *Identify and monitor indicators.* Monitor incoming intelligence for indicators that help determine which scenario appears to be developing. These will tell which—if any—of the scenarios is actually taking place, as far in advance as possible.

CRITICAL THINKING QUESTIONS

For the first six questions, select one of the five scenarios excerpted early in this chapter from *Global Trends: A More Contested World*. Read the full scenario in the NIC report, rather than relying on only the synopsis from “Alternative Scenarios for 2040” (see the source note in the text to access the report).

1. What forces are at play to create the scenario? Include the forces opposing the development of that scenario. Identify forces that are neglected or minimized in the scenario.
2. Which type of scenario (driving-force or system-change) is it? Is it a combination of these?

3. Is the scenario normative, descriptive, or some combination?
4. Identify the assumptions behind the scenario. Do any of them seem flawed? Which ones?
5. To what extent is the scenario an extrapolation? A projection? A forecast? Identify specific forces, trends, or factors that fall into each of these three categories. (Reminder: An unchanging force or trend typifies extrapolation; a changing force indicates projection; a new force characterizes forecast.)
6. Identify examples of the use of case-based models or cross-impact analysis in the scenario. Describe how the technique is applied.
7. Although five explicit scenarios are cited here, the report actually contains a number of future scenarios on specific topics such as climate change. Scenarios often reflect the point of view, or bias, of the preparer. It's difficult to avoid. Can you identify any estimates in the *Global Trends* report that appear to reflect a particular point of view—that is, any that are less than completely objective? Identify the reasons for your choice. (This question is not limited to the five scenarios—any number of estimates in the report can be considered.)

NOTES

1. Randolph H. Pherson, "Leveraging the Future with Foresight Analysis," *International Journal of Intelligence, Security, and Public Affairs* 20, no. 2 (2018): 102–31.
2. Ibid.
3. T. F. Mandel, "Futures Scenarios and Their Use in Corporate Strategy," in *The Strategic Management Handbook*, ed. K. J. Albert (New York, NY: McGraw-Hill, 1983), 10–21.
4. CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: Author, March 2009), 34, <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tra decraft%20Primer-apr09.pdf>.
5. National Intelligence Council, *Global Trends: A More Contested World* (Washington, DC: March 2021), 8–9, <https://www.dni.gov/index.php/gt2040-home/gt2040-media-and-downloads>.
6. W. I. Boucher, "Scenario and Scenario Writing," in *Nonextrapolative Methods in Business Forecasting*, ed. J. S. Mendell (Westport, CT: Quorum Books, 1985), 47–60.
7. M. S. Loescher, C. Schroeder, and C. W. Thomas, *Proteus: Insights from 2020* (Utrecht, Netherlands: The Copernicus Institute Press, 2000).
8. Inertia and countervailing forces are discussed in detail in chapter 15.
9. Peter Schwartz, *The Art of the Long View* (New York, NY: Currency Doubleday, 1996).
10. Shell Corporation, "Shell Scenarios," <https://www.shell.com/energy-and-innovation/the-energy-future/scenarios.html>.

11. Lawrence Wilkinson, "How to Build Scenarios," *Wired*, February 12, 2002, <http://www.wired.com/wired/scenarios/build.html>.
12. Pherson, "Leveraging the Future with Foresight Analysis."
13. Liam Fahey, *Competitors* (New York, NY: Wiley, 1999), 452.
14. Janet L. Kolodner, "An Introduction to Case-Based Reasoning," *Artificial Intelligence Review* 6 (1992): 3–34.
15. T. J. Gordon, "The Nature of Unforeseen Developments," in *The Study of the Future*, ed. W. I. Boucher (Washington, DC: US Government Printing Office, 1977), 42–43.
16. Jay Ogilvy and Peter Schwartz, "Plotting Your Scenarios," Global Business Network, 2004, http://www.meadowlark.co/plotting_your_scenarios.pdf.
17. Fahey, *Competitors*, 415.
18. Andrew Sleigh, ed., *Project Insight* (Farnborough, UK: Centre for Defence Analysis, Defence Evaluation and Research Agency, 1996), 13.
19. CIA, *A Tradecraft Primer*, 12.
20. Ibid.

18

SYSTEMS MODELING AND ANALYSIS

The target framework models introduced in earlier chapters are mostly straightforward and relatively easy for analysts to create. Intelligence also makes use of four specialized target-model types in preparing finished intelligence. They can describe current situations, but as is the case with scenarios, their real value is in enabling anticipatory and prescriptive intelligence. We'll briefly introduce them here:

- *Systems models* are used extensively in assessing military weaponry but also have wide uses in the social sciences. This chapter goes into detail on systems models.
- *Relationship models*, of which network models are the most important in intelligence, are discussed in chapter 19.
- *Geospatial models* rely on a combination of maps and all intelligence sources (of which IMINT is the most widely used). See chapter 20.
- *Simulation models* have become more useful in intelligence with the ready availability of powerful computing capabilities. Simulation is addressed in chapter 21.

One of the tools for developing scenarios involves creating systems models and analyzing them. Throughout this text, we have described the typical intelligence target as three things: as a complex system, as a network, and as having temporal and spatial attributes. In this chapter, we focus on modeling the target as a system. Any entity having the attributes of structure, function, and process can be described and analyzed as a system. Air defense systems, antisubmarine weaponry, transportation networks, welfare systems—all of these and many others are objects of systems modeling and analysis. And systems analysis can be applied to analyze both existing systems and those under development. Even when the model is of an existing system, it is intended to answer a question about the future. Typically, that question is this: *What sort of threat will the system pose?* Or, as in the first example below, *how effective will the system be?* In all the examples in this chapter, the systems model is created and analyzed for anticipatory purposes.

Creating a systems model requires an understanding of the system, developed by examining the linkages and interactions between the elements that compose the system as a whole. As stressed throughout this book,

- A system has *structure*. It is composed of parts that are related (directly or indirectly). It has a defined boundary physically, temporally, and spatially, though it can overlap with or be a part of a larger system.
- A system has a *function*. It receives inputs from, and sends outputs into, an outside environment. It is autonomous in fulfilling its function. A main battle tank standing alone is *not* a system. A tank with a crew, fuel, ammunition, and a communications subsystem *is* a system.
- A system has a *process* that performs its function by transforming inputs into outputs.

An insurgency can be considered a system and analyzed by creating structural, functional, and process models. The following example from the Soviet-Afghan war illustrates the point. It also reveals the importance of considering the system from a broad perspective and the necessity of analyzing the performance of an existing system before considering alternative future ones.

BOX 18.1 THE MUJAHEDDEEN INSURGENCY

During the 1980s, the CIA engaged in a covert operation to supply the Afghans with resources to fight the Soviet occupation of Afghanistan. The agency planned to supply a stockpile of rifles to the mujahedeen who were leading the insurgency. A military systems analyst with the program, Michael Vickers, analyzed the total Afghan resistance effort. Vickers argued that supplying rifles alone would be counterproductive. The Afghans didn't have enough ammunition for the rifles they already had. Unless the CIA could supply a very high volume of ammunition, more rifles would hinder, not help, the resistance. The real problem was that the insurgents had to feed their families and care for their wounded, and that hindered their ability to put pressure on the Soviet forces. Based on his performance analysis of the insurgency, Vickers put together a complete systems package that included ammunition, food for the families, and medical kits to keep the mujahedeen in the field year-round.¹

Vickers's second brilliant performance analysis achievement came in assessing the mix of weapons needed to defeat the Soviet HIND attack helicopter, which was the most effective and feared weapon against mujahedeen fighters. US House representative Charlie Wilson, the covert action's key supporter, intended to supply Swiss Oerlikon heavy machine guns for the mujahedeen to use against the HIND. Vickers told Wilson that this was the wrong way to look at the problem. The Oerlikon was too heavy to be moved around in large parts of Afghanistan. And a single weapon can be defeated, as in this case, by tactics. But the proper mix of antiair weaponry could not. The mix here included surface-to-air missiles (SA-7s, British

Blowpipes, and Stinger missiles) and machine guns (Oerlikons and captured Soviet Dashika machine guns). The Soviet helicopter operators could defend against some of these, but not all simultaneously. SA-7s were vulnerable to flares; Blowpipes were not. The HINDs could stay out of range of the Dashikas, but then they would be at an effective range for the Oerlikons.² Unable to know what they might be hit with, Soviet pilots were likely to avoid attacking or rely on defensive maneuvers that would make them almost ineffective—which is exactly what happened.

Vickers's Afghan resistance assessment illustrates a key point about systems analysis: Analysis of any complex system is, of necessity, multidisciplinary. Systems analysts often struggle with multidisciplinary aspects; they are more comfortable with the technical aspects, primarily performance analysis. In its national intelligence estimate on Iraqi weapons of mass destruction, the WMD Commission observed, "The October 2002 NIE contained an extensive technical analysis . . . but little serious analysis of the socio-political situation in Iraq, or the motives and intentions of the Iraqi leadership. . . . [T]hose turn out to be the questions that could have led the Intelligence Community closer to the truth."³ That criticism is frequently valid; technical analysis of complex systems is often done in a vacuum, without consideration of political, economic, and social factors. Such was not the case with the Vickers analysis, and success is always more likely when the customer and the analyst work in collaboration, as happened here.

SYSTEMS ANALYSIS METHODOLOGY

The mujahedeen example concerned systems analysis of an existing system—the mujahedeen insurgency. Customers also are concerned about systems being built, such as the Turkmenistan-Afghanistan-Pakistan-India natural gas pipeline introduced in chapter 9. Most systems analysis issues in national intelligence, though, concern the possible threats posed by future foreign weapons systems; a great deal of security surrounds such developments. The first step usually is to identify the system under development. During this step, details on how it may operate are not as important as its general characteristics and capabilities and a fairly accurate time scale.⁴

Three logical thinking approaches were discussed in chapter 5: deductive, inductive, and abductive. As applied to developmental systems analysis, they can be described this way:

- The deductive approach to prediction is to postulate the opponent's desired objectives; identify the system requirements; and search the incoming intelligence for evidence of work on the systems, subsystems, components, devices, and basic research and development (R&D) required for the opponent to reach those objectives. In more general terms, the analyst fits the evidence into an existing model template.

- The opposite, an inductive or synthesis approach, is to begin by looking at the evidence of development work and then synthesize the advances in systems, subsystems, and devices that are likely to follow.⁵ Here, again, in general terms, the analyst uses the evidence to create a new model.
- Abduction is the inductive approach plus an analyst's insights and instincts borne from experience and staying with problems.

If only one system is being built, it is not too difficult to identify the corresponding R&D pattern and the indicators in the available information, and from that to synthesize the resulting systems development; deduction works well. The problem arises when two or more systems are under development at the same time. Each will have its own R&D process, and it can be difficult to separate the processes out of the mass of incoming raw intelligence. Induction—or, better still, abduction—is likely to work better.

Once a system has been identified as being in development, analysis proceeds to the second step: answering customers' questions about it. These usually are about the system's functional, structural, and process characteristics—that is, about performance, schedule, risk, and cost.

As the system comes closer to completion, a wider group of customers will want to know what specific purposes the system has been designed to address (targets, for example, in the case of weapons systems), in what circumstances it will be used, and what its effectiveness will be. These matters typically require analysis of four aspects of the system:

- Performance, including its suitability for operating in its environment or in accomplishing the mission for which it has been designed
- Process
- Associated risks
- Cost of development and deployment

Let's consider each.

PERFORMANCE

Performance analyses are done on a wide range of targets, varying from simple to highly complex multidisciplinary systems. Determining the performance of a narrowly defined target, such as a surface-to-air missile, is straightforward. More challenging is assessing the performance of a complex system such as a social welfare system or a narcotics distribution network.

Two techniques are frequently used to assess systems performance: comparative modeling and simulation; sometimes they are used together. Let's look at the more straightforward method of comparative modeling, introduced in chapter 9. Simulation is the subject of chapter 21.

Comparative Modeling

Recall from chapter 9 that comparative modeling is one of the most valued tools of competitive intelligence analysts. They examine their company's products and technologies to see how those of their competitors compare with that benchmark. The method is used on the national intelligence level for policymakers and the military, usually focused on systems performance, especially weapons performance.

Comparing the performance of your country's or organization's systems with those of an opponent can involve four distinct fact patterns. Each poses challenges the analyst must deal with. The first possible pattern is that country *A* has developed a certain systems capability and so has opponent country *B*. In this case, the analyst from country *A* has the job of comparing the two countries' capabilities. The other three possible patterns are that country *A* has developed a particular capability, but country *B* has not; that country *A* has not developed a particular capability, but country *B* has; or that neither country has developed the capability. In short, the possibilities can be described as follows:

- We did it—they did it.
- We did it—they didn't do it.
- We didn't do it—they did it.
- We didn't do it—they didn't do it.

There are many examples of the “we did it—they did it” intelligence problem, especially in arenas in which competitors typically develop similar products. The United States developed intercontinental ballistic missiles (ICBMs); the Russians developed ICBMs. Both sides developed antiballistic missile systems and missile-firing submarines. Many countries build aircraft, cruise missiles, tanks, electric power distribution systems, computers, and so on. In these cases, the analysis problem is not so difficult because analysts turn to their own country's or organization's experts on that particular system or product for help. But analysts have to reserve final judgment based on their level of understanding of the opponent, as the next example illustrates.

BOX 18.2 THE WÜRBZBURG RADAR

In World War II, both the British and the Germans developed and used radar. So, when in 1941 British reconnaissance aircraft brought back photographs of bowl-shaped antennas scattered along the French coast, British intelligence could determine that a new type of radar had been developed. Because the radar, which was later nicknamed the Würzburg, posed a threat to British aircraft attacks on Germany, the British undertook rather direct materiel collection means to gather additional information about it. They assembled a company of paratroops to make

an airborne assault on one of the Würzburgs located near Bruneval, France. The assault team made off with the feed antenna for the radar dish, the receiver, and display equipment. From those items, along with the reconnaissance photographs, the British were able to create a fairly accurate model of the radar.

The subsequent analysis of the Würzburg provides a good example of the mirror-imaging problem that can exist when a country uses its own experts (described in more depth in the next section). The Würzburgs were typically deployed in pairs (though only one was at Bruneval); one radar in a pair had one to three searchlights collocated with it. British radar experts believed that the second radar was a spare, to be used when the first radar was inoperative, since this was the normal British practice. British intelligence officer R. V. Jones, however, argued that the Würzburg with searchlights was intended to track bombers, whereas the second radar had the job of tracking fighters that would be guided to the bomber. British radar experts disagreed, since this would require a level of performance (accuracy in coordinate transformation) that was beyond their technical skill at the time. They failed to appreciate the accuracy with which German radars performed as a matter of course. As it turned out, Jones, armed with a better understanding of the German way of building defense systems, was correct.

In the second case, “we did it—they didn’t do it,” analysts run into a real problem: It is almost impossible to prove a negative in intelligence. The fact that no intelligence information exists about an opponent’s development cannot be used to show that no such development exists.

For example, after the British created the magnetron (a microwave transmitter tube widely used in radar) and discovered what wonders it could do for a radar system, their constant worry was that the Germans would make a similar discovery. If that happened, the British would have to face radars with performance equal to their own. In fact, the Germans learned about the magnetron only when they captured one from a downed British aircraft late in the war, but the threat kept British intelligence on edge.

The third pattern, “we didn’t do it—they did it,” is the most dangerous type analysts encounter. Here they have to overcome opposition from skeptics from within, because there is no generic target framework (in chapter 9) to use for comparison. R. V. Jones faced a case like this when he pieced together the operating principles of a new German aircraft navigation system called Knickebein.

BOX 18.3 KNICKEBEIN

Knickebein was a radio beam system that the Germans used during World War II to guide their bombers at night to their bomb drop point (usually London). It featured two widely separated transmitters located in France, the Netherlands, or Denmark, both of which aimed their beams toward the intended target in the United Kingdom. A bomber crew would tune its radio to receive the signal from both beams, and then

travel along one beam toward the target. When it received a signal from the second beam, the aircrew knew it was at the intersection of the two beams and would release its bomb load onto the target.

R. V. Jones, armed with both HUMINT and technical intelligence about the existence of a blind bombing system, tried to convince top government officials to send radio-equipped aircraft aloft to search for the Knickebein signal. His idea was opposed by Frederick Lindemann, the government's leading scientific advisor. Lindemann argued that the system couldn't perform at such long ranges; radio waves would not follow the Earth's curvature and so would not be observable beyond line of sight, that is, over London. Nevertheless, Churchill ordered the ELINT search aircraft aloft to search for Knickebein, and the aircrew's ELINT receiver was able to collect the signal. (Lindemann was partially right: The signal did not follow the Earth's curvature, but the German targets in the United Kingdom were not beyond line of sight at the bomber's altitude.)

The central premise of the novel and later movie *The Hunt for Red October* is a fictional example of this type. According to the plot, the Soviets had developed a low-noise caterpillar drive for their submarine, the *Red October*, making it almost undetectable when under way. In the movie, the United States had no equivalent development, so understanding the submarine's quiet performance was difficult. Ironically, at the time, the reality was quite the opposite: The US Navy had the technology while the Russians did not.

This third case presents analysts with another challenge: the opportunity to go off in the wrong direction. Such was the case in assessing the mission and performance of the Caspian Sea Monster.

BOX 18.4 THE CASPIAN SEA MONSTER

In the 1960s, US intelligence analysts obtained satellite imagery of a massive aircraft in the Caspian Sea near the port of Kaspisysk. Nearly 100 meters in length, it was the largest aircraft in the world at the time and was promptly nicknamed the Caspian Sea Monster. The vehicle appeared to be a seaplane, but it quickly posed problems for the analysts trying to identify its mission and performance. Its short, stubby wings could not support it as an aircraft in conventional flight. After much system performance modeling and simulation, analysts concluded that it was a "ground effect" or "wing in ground effect" vehicle, designed to fly a short distance above the water to take advantage of the additional lift provided by flying close to the surface.

The question of the monster's mission remained. Analysis focused on what the United States would do with such a craft—classic mirror imaging—and the major candidates for a mission were off the mark. The answer came many years later. The craft was originally intended as a high-speed transport for troops and military equipment—a mission the United States had no requirement for.

Flying close to the water is of course a risky affair, and the original monster crashed on takeoff in 1980. The vehicle was too heavy to be recovered from its watery graveyard. A smaller variant later was developed to carry antiship cruise missiles; it now sits rusting in the water at the Kaspiysk naval base.

“We didn’t do it—they didn’t do it” seems to be a ridiculous case. After all, if we haven’t developed a weapon and they haven’t developed a weapon, who cares? The answer is that people do care, and intelligence analysts spend a great deal of their time doing performance assessments on just this sort of problem. One historical example is the case of the German engine killer.

BOX 18.5 THE GERMAN ENGINE KILLER

During World War II, British intelligence received reports about classified testing taking place at a secret installation inside Germany. According to the reports, automobiles driving near this installation would suddenly stall and could not be started again. After a while a German sentry would step out of the nearby woods, tell the automobile drivers they could proceed, and the automobiles would start again and run normally.

As one might imagine, the thought of a weapon that could stall internal combustion engines caused British intelligence considerable concern, since British tanks, trucks, and airplanes relied on such engines. While the threat was a continuing concern to British intelligence, in the postwar period it was found that the order of events had become transposed in reports. What actually happened is that the Germans were testing very sensitive radio equipment that was vulnerable to automobile ignition noise. When testing was under way, German sentries throughout the area around the plant would force all motorists to stop and shut down their automobile engines until testing was over.

This sort of transposition of cause and effect is not uncommon in human source reporting. Part of the skill required of analysts is to avoid the trap of taking sources too literally. Occasionally, they must spend time on problems that are even more fantastic or improbable than that of the German engine killer. In chapter 20, we discuss the particle beam weapon scare of the 1970s. The particle beam weapon appears to have been a classic case of “we didn’t do it—they didn’t do it.” The United States didn’t build one and neither did the Soviets; in fact, no one could.

The Mirror-Imaging Challenge

A primary risk in all systems analysis is mirror imaging. It’s much the same as the cultural mirror-imaging issue in decision making introduced in chapter 9. Comparative modeling and simulation increase the need to be wary of it. The opponent’s system

or product (such as an airplane, a missile, a tank, or a supercomputer) is designed within the constraints of that country's engineering expertise, manufacturing processes, resource issues, and so on. The system or product might be developed to perform different operations or serve an unexpected market. More than once, US analysts of Soviet military developments made poor analytic assessments regarding weapons systems performance during the Cold War years as a result of mirror imaging. A few examples follow.

Unexpected Simplicity. In effect, the Soviets applied a version of Occam's razor in their industrial practice. Because they were cautious in adopting new technology, they tended to keep everything as simple as possible. They liked straightforward, proven designs. When they copied a design, they simplified it in obvious ways and didn't include the extra features the United States tends to put on its weapons systems. The Soviets made maintenance as easy as possible, because the hardware was going to be maintained by people who did not have extensive training. US analysts, however, tended to assume that a copied design would cost much the same as, and function much like, the US version. Often, that was not the case. The Soviet version's cost was frequently much lower and its performance was not likely to be as good, though maintenance would be easier because of its lack of complexity.

A Narrowly Defined Mission. The Soviets built their systems to perform specific, relatively narrow functions. The MiG-25 is an example of an aircraft built this way—overweight and inefficient by US standards but simple and effective for its intended mission as a high-speed interceptor. The United States tends to optimize its weapons systems for a broad range of missions. Consequently, in a textbook case of mirror imaging, analysts originally gave the MiG-25 credit for performance in dogfights that a similar US fighter would have—far better than the actual MiG-25 performance in such situations.

Quantity May Replace Quality. US analysts occasionally underestimated the number of units of a weapons system that the Soviets would produce. The United States needed fewer units of a given system to perform a mission, since each unit had more flexibility, quality, and performance ability than its Soviet counterpart. The United States needed only to have looked back to World War II for guidance—Sherman tanks were inferior to the German Tiger tanks in combat, but the United States deployed a lot of Shermans and overwhelmed the Tigers with numbers.

PROCESS

The functions of any system, obviously, are carried out by processes that will differ for different systems. That's true whether describing an organization, a weapons system, or an industrial system. Dissimilar organizations—for example, civil government, law

enforcement, military, and commercial organizations—have markedly different processes. Even similar types of organizations will have varied processes, especially in disparate cultures. The processes used by a terrorist organization such as Boko Haram in Nigeria are different from those used by Jemaah Islamiyah in Indonesia.

There are a correspondingly large number of analytic techniques for analyzing processes, many of which are industry, organization, or weapons systems specific. Analysts tend over time to develop process methodologies that are unique to their area of responsibility. Political, military, economic, and weapons systems analysts, for example, all use specialized process analysis techniques.

A process model describes a sequence of events or activities that produces results. Process models are frequently used in all types of intelligence analysis. One that finds wide use in weapons intelligence models is the process for developing a new weapons system. The customer's primary concern about systems under development usually centers on performance, as noted in the previous section. But sometimes the process and its associated schedule become critical factors, as they did during negotiations about Iran's nuclear weapons potential from 2006 to 2015.

BOX 18.6 THE P5+1 NEGOTIATIONS

In 2006, a group of six world powers referred to as P5+1 (the U.N. Security Council's five permanent members—the P5—plus Germany) joined together in diplomatic efforts to constrain Iran from producing nuclear weapons. The negotiations focused on maximizing Iran's time to "nuclear breakout," which is defined as the amount of time it would take Iran to produce sufficient weapons-grade uranium or plutonium for one nuclear weapon.

To produce weapons-grade material, uranium must be enriched (in the Iranian case, with centrifuges) to more than 90 percent of its U-235 isotope. The amount of enriched material required for one weapon is defined by the International Atomic Energy Agency as approximately 27 kilograms of uranium.⁶ The subsequent agreement limited the number of centrifuges that Iran could have, to lengthen the breakout time.

Anyone who is familiar with the target model framework will recognize a *seeming* flaw in the focus on breakout time. Producing bomb-grade material is just one step in creating a nuclear weapons system. The entire systems development process includes designing a bomb; configuring it to fit into a missile warhead; and developing a missile (including reentry vehicle and guidance system) with the range, accuracy, and throw weight to carry the warhead.

The Iranians pointed out this seeming flaw, emphasizing the need for all of these steps in arguing that the real time was measured in years, instead of in months, as estimated by the P5+1 negotiators. The Iranians argued that production of enough material for a bomb would realistically take them eighteen months: conversion

of the material to pure uranium metal, twelve months; molding into an explosive device, six months; developing a warhead around the device and mating it to a missile, an unknown time because Iran claims no experience in building nuclear warheads and fitting them to delivery systems.⁷

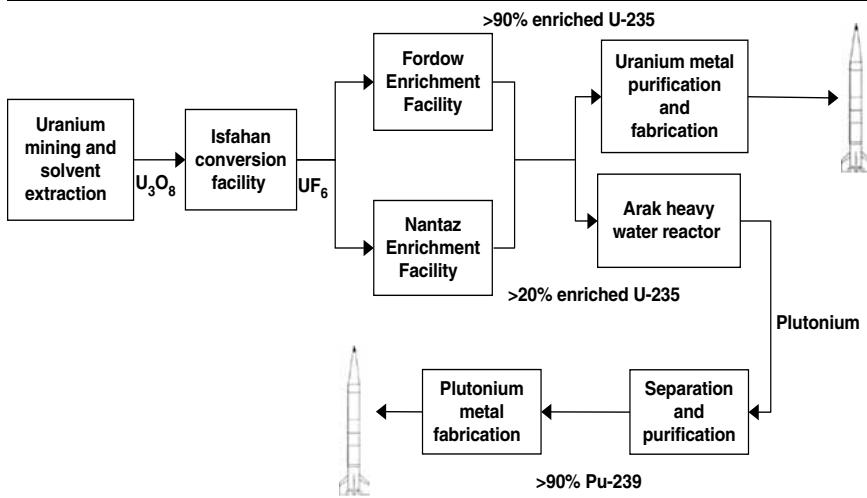
It's a specious argument. The remaining steps after the production of enough fissile material would be difficult for the P5+1 group to monitor, and even more difficult to stop. The P5+1 negotiators apparently recognized that their best bet was to control nuclear material production. The Iranian negotiations also are an excellent example of the importance, in intelligence, of understanding the customer's perspective: For the P5+1 negotiators, production of fissile material was the only step they could control.

The Iranian example reflects the importance of understanding schedule. In determining the schedule, the analyst examines the development process to identify the critical points in it. Let's look at an example of how a process model is used to do that, again using the Iranian nuclear agreement P5+1 negotiations.

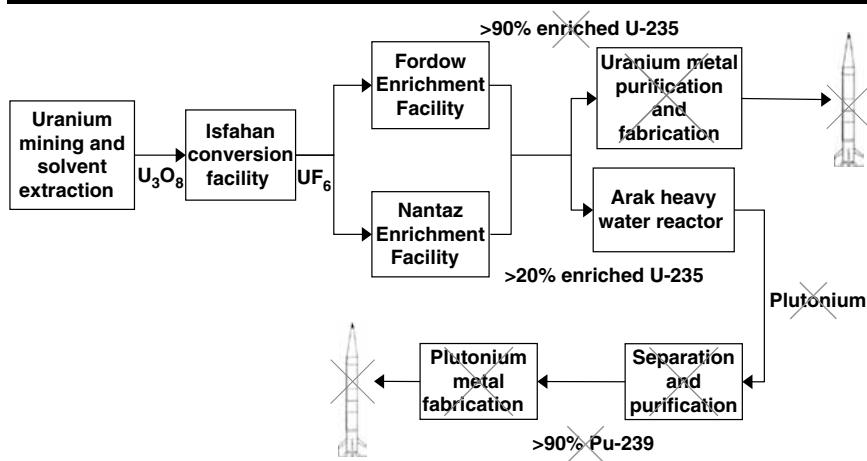
Two alternative process models for building a nuclear weapon exist. Figure 18.1 shows the two processes as they would be carried out by known Iranian facilities. One development results in a warhead with U-235 fuel. This alternative requires uranium enriched to greater than 90 percent U-235, as the figure indicates. Another approach is to use a combination of U-238 and at least 20 percent U-235, converting the U-238 to plutonium-239 in a heavy water reactor (in the figure, the reactor that Iran operates at Arak).

Chapter 12 introduced the iterative process of model improvement using new intelligence. Figure 18.2 shows how iterative modeling can be done using a development process model. In this example, the model shown in figure 18.1 envisions two alternative paths to a nuclear warhead. Suppose that in 2015 the analyst receives a report of the P5+1 accord under which Iran has agreed that the Arak plant will cease plutonium production and Fordow will cease producing highly enriched U-235. The analyst then revises the model, as shown in figure 18.2, to reflect the fact that Iran now has no obvious path to a nuclear warhead. Though much of the media attention centered on the accord's limit on U-235, the constraint on plutonium production was probably more important. Most nuclear weapons worldwide use plutonium, because it is easier and cheaper to produce, and is the preferred trigger for a thermonuclear weapon.⁸

After the United States withdrew from the accord in 2018, Iran resumed enrichment activities. Analysts in 2022 must reexamine the Figure 18.1 process model to determine which path Iran is taking, and what the timeline now is for warhead production.

FIGURE 18.1 ■ Process Model for an Iranian Nuclear Warhead

Source: Adapted from "The Ayatollah's Nuclear Gamble" (2012), Khosrow B. Semnani (nucleargamble.org). Used with permission.

FIGURE 18.2 ■ Analysis of a Revised Process Model

Program Cycle Model

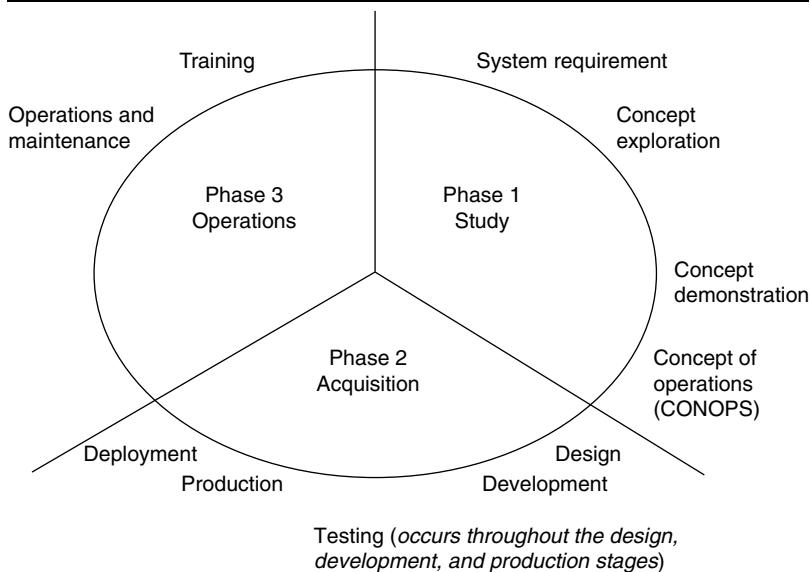
The process models shown in figures 18.1 and 18.2 are just one part—albeit an important part—of the larger systems process model known as the *program cycle*. A new system—whether a weapons system, a banking system, or computer software—develops and evolves through a process commonly known as the program cycle or the system life cycle. Beginning with system requirements and progressing to production,

deployment, and operations, each phase bears unique indicators and opportunities for collection and analysis. Intelligence customers often want to know where a major system is in this life cycle.

Each country, industry, or company has its own version of the program cycle. Figure 18.3 shows the major components of a generic program cycle. Different types of systems may evolve through different versions of the cycle, and product development differs somewhat from systems development. It is therefore important to first determine the specific names and functions of the cycle phases for the target country, industry, or company and then determine exactly where the target program is in that cycle. With that information, analytic techniques can be used to assess when the program might become operational or begin producing output.

Knowing where a program is in the cycle allows for accurate predictions. In assessing both Libya's and Iraq's WMD capabilities, analysts tended to equate procurement actions as indicating that a weapons capability existed—though the two occur at quite different phases in the program cycle. This tendency was partially a result of getting a large volume of procurement-related intelligence, possibly leading analysts to overestimate its importance.⁹ That tendency is an example of the Baader-Meinhof phenomenon discussed in chapter 11.

FIGURE 18.3 ■ The Generic Program Cycle



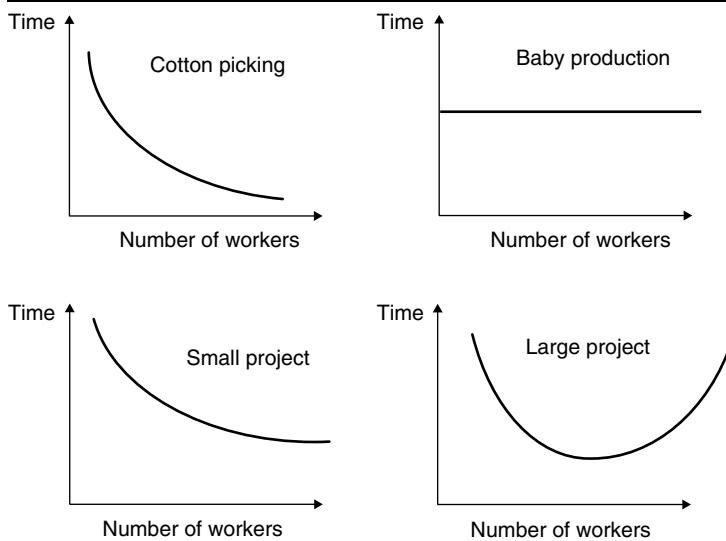
A general rule of thumb is that the more phases in the program cycle, the longer the process will take, all other things being equal. Countries and organizations with large, stable bureaucracies typically have many phases, and the process, whatever it may be, takes that much longer.

Program Staffing Model

The duration of any phase of the cycle shown in figure 18.3 is determined by the type of work involved and the number and expertise of workers assigned. Fred Brooks, one of the premier figures in computer systems development, defines four types of projects in his book *The Mythical Man-Month*.¹⁰ Each type has a unique relationship between the number of workers needed (the project loading) and the time it takes to complete the effort.

The graph at the upper left of figure 18.4 shows the time-labor profile for a perfectly partitionable task—that is, one that can be completed in half the time by doubling the number of workers. It is referred to as the “cotton-picking curve”: Twice as many workers can pick a cotton field in half the time. Few projects fit this mold, but it is a common misperception of management that people and time are interchangeable on any given project, such that a project that could be done in ten months by one person could be completed in one month by ten. It’s this dangerous and deceptive myth that provided Brooks with his book’s title.

FIGURE 18.4 ■ The Brooks Curves for Projects



The profile for a type of project that involves an unpartitionable task is shown in the upper right of figure 18.4. The profile is referred to here as the “baby production curve,” because no matter how many women are assigned to the task, it takes nine months to produce a baby.

Most small projects fit the curve shown in the lower left of the figure, which is a combination of the first two curves. In this case, a project can be partitioned into subtasks, but the time it takes for people working on different subtasks to communicate

with one another will eventually balance out the time saved by adding workers, and the curve levels off.

Large projects tend to be dominated by communication. At some point, shown as the bottom point of the lower right curve, additional workers begin to slow the project because all workers have to spend more time in communication. Failure to recognize this pattern, or to understand where a project is on the curve, has been the ruin of many large projects. As Brooks observes, adding workers to a late project makes it later.¹¹

These four curves can have wider applications in intelligence than those Brooks describes. That is, they can apply with parameters besides workers. In the Iranian nuclear breakout case, for example, U-235 production was defined by the cotton-picking curve, with number of centrifuges replacing number of workers. Doubling the number of centrifuges would halve the time required for nuclear breakout.

The Technology Factor

Technology is another important factor in any development process, and it is neither available nor applied in the same way everywhere. An analyst in a technologically advanced country may take for granted that certain equipment—test equipment, for example—will be readily available and of a certain quality. This can be a bad assumption with respect to the typical state-run economy.

It took some time for US analysts to recognize how low the productivity of Soviet engineers could be during the Cold War. In fairness to the engineers, the reasons had nothing to do with their competence. They often had to build their own oscilloscopes and voltmeters—items that were available in the United States at a nearby Radio Shack. Sometimes Soviet engineers would be idle for weeks waiting for a resistor so that they could finish the oscilloscope needed to test the microwave tube for the radar they were supposed to build, a phenomenon US analysts did not readily perceive.

As mentioned earlier, foreign weapons systems are often designed quite differently from those in the analyst's country. For example, the United States and the Soviet Union took strikingly different paths in ballistic missile development. US missiles had simple rocket engines operating at fixed thrust with very sophisticated guidance systems using onboard computers. The Soviets could build good rocket engines but did not have technology for building reliable guidance systems. To compensate, they used more sophisticated variable-thrust engines with simple guidance systems having very little onboard computation capability. The Soviet approach had the advantages of guidance simplicity and quick achievement of satisfactory reliability.¹²

There is a definite schedule advantage to not being the first to develop a system. A country or an organization that is not a leader in technology development has the advantage of learning from the pioneer's mistakes, allowing it to keep R&D costs low and avoid wrong paths. A basic rule of engineering is that you are halfway to a solution when you know there is a solution and are three-quarters there when you know how a competitor solved the problem. It took much less time for the Soviets to develop

atomic and hydrogen bombs than US intelligence had predicted. The Soviets had no principles of impotence or doubts to slow them down. They knew the bombs would work. The development time for nuclear weaponry has become even more compressed in the years since. And, as the Iranian nuclear negotiations illustrate, the time factor has become one of high intelligence significance.

RISK

Analysts often assume the opponent's programs and projects will be completed on time and the target system will work perfectly. They would seldom be so foolish in evaluating their own projects or the performance of their own organizations. Risk analysis needs to be done in any target program assessment. It is typically difficult to do and, once done, difficult to get the customer to accept. But it is important because intelligence customers, like many analysts, also tend to assume that an opponent's program will be executed perfectly. The Iranian nuclear breakout issue, discussed previously, might be an example of such a worst-case analysis.

One simple but often overlooked approach to evaluating the probability of success is to examine the success rate of similar ventures. In planning the 1980 Iranian hostage rescue attempt, the Carter administration could have looked at the Vietnam prisoner of war rescue attempts; only 21 percent succeeded. The Carter team did not study those cases, however, deeming them irrelevant, though the Iranian mission was more complex.¹³ Similar miscalculations are made every day in the world of information technology (though those do not typically include loss of life, as did the aborted hostage rescue). Most software projects fail. And predictably, the failure rate is higher for large projects, although the public typically doesn't hear about those.

Risk analysis is an iterative process in which an analyst identifies and prioritizes risks associated with the program, assesses the effects of the risks, and then identifies alternative actions to reduce them. Known risk areas can be readily identified from past experience and from discussions with technical experts who have been through similar projects. The risks generally fall into four major categories: programmatic, technical, production, and engineering. Analyzing potential problems requires identifying specific potential risks from each category. Some of these include the following:

- *Programmatic*: funding, schedule, contract relationships, political issues
- *Technical*: feasibility, survivability, system performance
- *Production*: manufacturability, lead times, packaging, equipment
- *Engineering*: reliability, maintainability, training, operations

Risk assessment quantitatively ranks risks to establish those of most concern. A typical ranking is based on the *risk factor*, a mathematical combination of the probabilities of failure and the consequences of failure. This assessment requires merging expertise with software tools in a structured and consistent approach to ensure that all risk categories are considered and ranked.

Risk management is the definition of alternative paths to minimize risk and set criteria on which to initiate or terminate the program being assessed. It includes identifying alternatives, options, and approaches to mitigation. Examples are initiation of parallel developments (for example, funding two manufacturers to build a satellite, where only one satellite is needed), extensive development testing, addition of simulations to check performance predictions, design reviews by consultants, or focused management attention on specific program elements. A number of decision analysis tools are useful for risk management. The most widely used is the program evaluation and review technique (PERT) chart, which shows on a timeline the interrelationships and dependencies among tasks in a program.

Risk management is of less concern to the intelligence analyst than is risk assessment. But one factor in evaluating the likelihood of a program failure is how well the target organization can assess and manage its program risks.

COST

Systems analysis in intelligence typically doesn't focus heavily on cost estimates. The usual assumption is that costs will not keep the system from being completed. Sometimes, though, the costs are important because of their effect on a country's overall economy.

Estimating the cost of a system usually begins with comparative modeling. What would it cost your country, organization, or industry to build something? Multiply that number by a factor that accounts for the difference in costs to the target organization, which will always be different. The result is a fairly straightforward cost estimate that is only as good as the analyst's understanding of the differences in the way the two organizations build a system. As noted in the earlier section on comparative modeling, there is much room for error in this understanding, especially when different countries and cultures are involved.

When several systems models are being considered, cost-utility analysis, an important part of decision prediction, may be necessary. Many decision-making processes, especially those that require resource allocation, make use of cost-utility analysis. For an analyst assessing a foreign military's decision whether to produce a new weapons system, it is a useful place to start with a caveat to be sure to take "rationality" into account. As noted earlier, what is "rational" is different across cultures and from one

leader to the next. It is important to understand the logic of the decision maker—that is, how the decision maker thinks about topics such as cost and utility. For example, Chinese leaders' decision to implement a manned space program and to soft-land the Chang'e 4 robotic probe on the far side of the moon in January 2019 can be subjected to cost-utility analysis, but a major pitfall would be to focus on typical elements. Hardware and launch costs can be estimated fairly well. Utility is measurable to some extent—by most standards, it is low. The benefits in prestige and advancements in Chinese space technology have to be quantified subjectively, but an analyst who does not capture these factors as dominant in the decision-making process would misstep.

SUMMARY

Any entity having the attributes of structure, function, and process can be described and analyzed as a system. Systems analysis is used in intelligence extensively for assessing foreign weapons systems performance. But it also is used to model political, economic, infrastructure, and social systems.

Modeling the structure of a system can rely on a deductive, inductive, or abductive approach. The deductive approach postulates an opponent's objectives and searches for evidence of systems development to meet those objectives. The inductive approach starts from intelligence reporting and identifies likely systems development that follows from the evidence. Where the reporting may be about more than one system, induction or abduction (using analyst instincts from long experience and sticking with problems) may work best.

Functional assessments typically require analysis of a system's performance. Comparative modeling is widely used in such assessments. Simulations, discussed in chapter 21, are used to prepare more sophisticated predictions of a system's performance.

Process analysis is important for assessing organizations and systems. Organizational processes vary by organization type and across cultures. Process analysis also is used to determine systems development schedules and in looking at the life cycle of a program. Program staffing and the technologies involved are other factors that shape development schedules.

Intelligence also is commonly interested in measuring programs' probabilities of success. Risk assessments are frequently used to measure these probabilities. Cost-utility analysis is often used to support predictions about an opponent's program decisions. Most leaders go through some form of cost-utility analysis in making major decisions; the trick is to apply the proper cultural and individual biases to both cost and utility. What appears to be a high cost in the analyst's culture can appear to be modest in the target's culture.

CRITICAL THINKING QUESTIONS

1. Select a country that has taken a different systems development path than your own country. This could be a system that falls into any of the PMESII categories: a welfare system, health care delivery, banking, law enforcement, education, or political representation, for example. Prepare a short systems analysis paper on the system you have selected. Consider function, structure, and process in your evaluation.
2. The section on “The Mirror-Imaging Challenge” describes three differences between US and USSR practices that led to miscalls in Soviet weapons systems analysis. Many such differences might be encountered when doing comparative systems analysis. In the analysis you did for question 1 above, there should be several such factors (they could be environmental, cultural, or both). Identify and discuss them.
3. For the system and country you selected in question 1, can you establish a basis for a comparative cost estimate? What are the major differences in cost between the two countries?

NOTES

1. George Crile, *Charlie Wilson's War* (New York, NY: Atlantic Monthly Press, 2003), 300–1.
2. Crile, *Charlie Wilson's War*, 303–5.
3. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 13, https://fas.org/irp/offdocs/wmd_report.pdf.
4. Ibid.
5. Herbert C. Rothenberg, “Identifying the Future Threat,” *Studies in Intelligence* 12, no. 4 (Fall 1968): 13–21.
6. Olli Heinonen, “Iran’s Nuclear Breakout Time: A Fact Sheet,” Belfer Center for Science and International Affairs, Harvard University, March 28, 2015, http://belfercenter.ksg.harvard.edu/publication/25174/irans_nuclear_breakout_time.html.
7. Kambiz Foroohar, “Iran’s Zarif Warns Nuclear Talks May Be Derailed on Centrifuges,” *BloombergBusiness*, June 11, 2014, <http://www.bloomberg.com/news/articles/2014-06-11/iran-s-zarif-warns-nuclear-talks-may-be-derailed-on-centrifuges>.
8. William J. Broad, “Plutonium Is Unsung Concession in Iran Nuclear Deal,” *New York Times*, September 7, 2015, <https://www.nytimes.com/2015/09/08/science/irans-unsung-plutonium-concession-in-nuclear-deal.html>.
9. *Report of the Commission on the Intelligence Capabilities of the United States*, 261.

10. Frederick P. Brooks Jr., *The Mythical Man-Month* (Reading, MA: Addison-Wesley, 1975), 16–25.
11. Ibid., 16–19.
12. David S. Brandwein, “Interaction in Weapons R&D,” *Studies in Intelligence* 12, no. 1 (Spring 1968): 13–20.
13. Hossein Askari, “It’s Time to Make Peace with Iran,” *Harvard Business Review* (September–October 1993), 13.

Relationships among entities—people, places, things, and events—are perhaps the most common subject of intelligence target modeling. Such models require a considerable amount of time to create, and maintaining them (known to those who do it as “feeding the beast”) demands much follow-on effort. But the models are highly effective in analyzing twenty-first-century problems, and the associated graphical displays are powerful in persuading customers to accept the results.

There are four levels of relationship models, each using increasingly sophisticated analytic approaches: hierarchy, matrix, link, and network models. They are closely related, each illustrating the same fundamental idea at different levels of complexity. This chapter focuses on network models, but it’s important to touch on the other three.

Hierarchy Models. The hierarchy model is a simple tree structure. Organizational modeling naturally lends itself to the creation of a hierarchy, as anyone who has ever drawn a corporate organizational chart is aware. A natural extension of such a hierarchy is the use of a weighting scheme to indicate the importance of individuals or sub-organizations in the hierarchy.

Matrix Models. The relationship matrix model is somewhat different from the matrix models introduced in chapter 9. Relationship matrices indicate the existence of a known or suspected association among individuals by cataloging communication connections such as emails, text messages, social media interactions, face-to-face meetings, and telephone conversations. An analyst can use the matrix to identify relationships that require more in-depth analysis.¹

Link Models. A link model allows the view of relationships in more complex tree structures. It physically resembles a hierarchy model (both are trees), but a link model differs in that it can show relationships among things as well as people, it is normally drawn horizontally, and it does not necessarily indicate subordination.

Network Models. A network model can be thought of as a more flexible version of a link model. It can deal with multiple hierarchies and with interactions on multiple levels. There are several types of network models, but two are widely used in intelligence:

- *Social network models* show patterns of human relationships. The nodes represent people, and the links show that some type of relationship exists between them.

- *Target network models* are, of course, most useful in intelligence. The nodes can represent any type of entity—people, places, things, events—and the links show that some type of relationship exists between them.

One of the most powerful tools in the analyst's toolkit is network modeling. It has been used for years in the US intelligence community against targets such as terrorist groups and narcotics traffickers. The netwar model of multidimensional conflict between opposing networks, described in chapter 3, is increasingly applicable to all intelligence, and network analysis is the best tool for examining opposing networks.

While this chapter centers on network modeling and analysis, such models are derived from the simpler link model form, and they share many of the same concepts. So let's start with a brief introduction to link models. First, a few definitions:

- *Network*: that group of elements forming a unified whole
- *Node*: an element of a network that represents a person, place, or physical thing
- *Cell*: a subordinate organization formed around a specific process, capability, or activity within a designated larger organization
- *Link*: a behavioral, physical, or functional relationship between nodes²

LINK MODELS

Link modeling has a long history. The Los Angeles Police Department reportedly used it first in the 1940s to assess organized crime networks. For decades thereafter, it was routinely used in national intelligence and law enforcement to identify espionage groups, narcotics trafficking groups, and terrorist organizations. Its primary purpose was to display relationships among people or between people and events. Link models have repeatedly demonstrated their value in discerning the complex and typically circuitous ties between entities. Their essence is the graphical representation of the connection patterns between nodes.

Most human minds simply cannot assimilate all the information collected on a topic over the course of several years. Yet a typical goal of intelligence analysis is to develop precise, reliable, and valid inferences from the available data over time. Link models directly support such inferences for use in strategic decision making or operational planning.

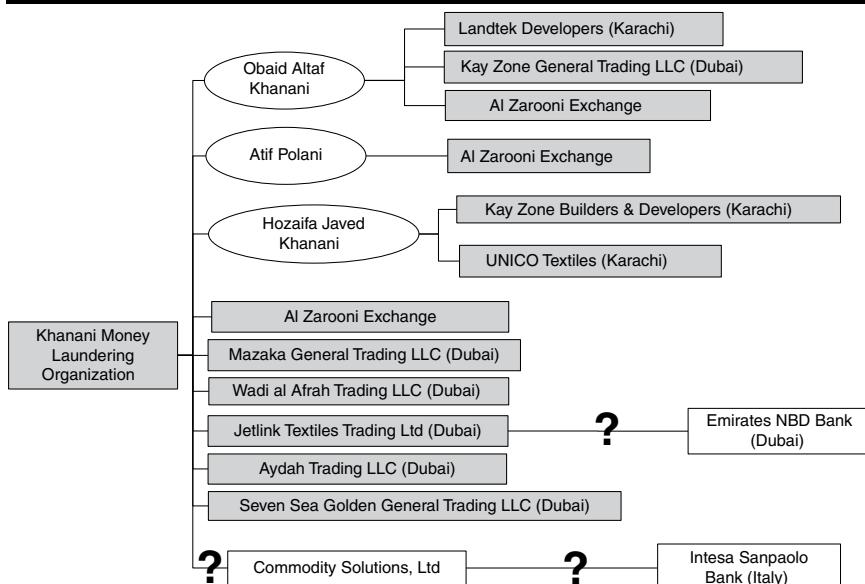
Before the 1970s, link modeling was an arduous and time-consuming endeavor because graphical trees had to be constructed on paper. Computer software contributed greatly to the expansion of link synthesis and analysis. Software tools simplify the process by allowing the relational storage of data as it comes in and graphically displaying different types of relationships among the entities. Once relationships have

been created in a database system, they can be displayed and analyzed from different perspectives in a link analysis program.

To understand the benefits of link modeling in practice, let's revisit the Khanani money laundering organization (MLO) from chapter 12.

Figure 19.1 is a link version of the Khanani MLO shown in figure 12.4 of that chapter. It illustrates the importance of being able to display second- and third-order links. Connections that are not apparent when each piece of evidence is examined separately become obvious when link displays are used.

FIGURE 19.1 ■ Khanani MLO Link Model



To be useful in intelligence, the links should not only identify relationships among entities but also show the nature of their ties. A subject-verb-object display has been used in the intelligence community for several decades to show the nature of such ties, and it is sometimes used in link displays. A typical subject-verb-object relationship from figure 19.1 might read: "Hozaifa Javed Khanani uses UNICO Textiles for funds integration."

Link diagrams also help identify areas for additional research. Looking at the chapter 12 figures again, refer to figure 12.3—the network at the time of Altaf Khanani's arrest. Comparing it to figure 12.4, for example, an analyst will note that organizations identified in the Altaf Khanani network have disappeared from the newly formed Khanani MLO. The analyst would highlight those for investigation as to whether they still are part of the network (the shaded boxes and "?" links in figure 19.1).

Most software today has filtering capabilities that show quantitative and temporal (date stamping) relationships. Filters allow the analyst to focus on connections of

interest and can simplify by several orders of magnitude the data shown in a link display. For example, the analyst could select “Jetlink Textiles Trading” in figure 19.1 as the root (that is, the start, or left side, of the link diagram) and display a link chart of all the group and personal associations of Jetlink Textiles Trading. Filters can then be chosen to display the Jetlink Textiles Trading network of associations for a specific date range (say, 1995–1998) and associations only with Swiss banks.

Understanding link modeling is important because the same principles undergird network modeling. However, link modeling has been replaced almost completely by network modeling, discussed next. Relationships within complex networks are more readily analyzed in a network model.

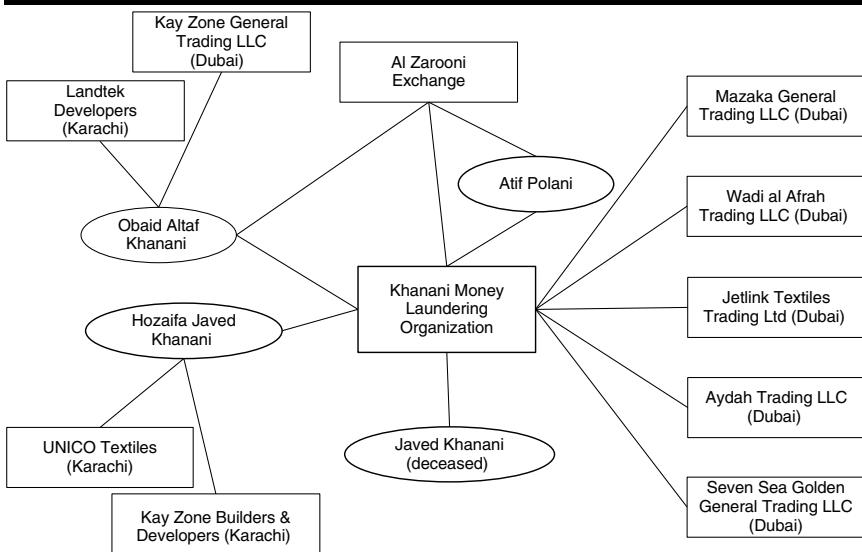
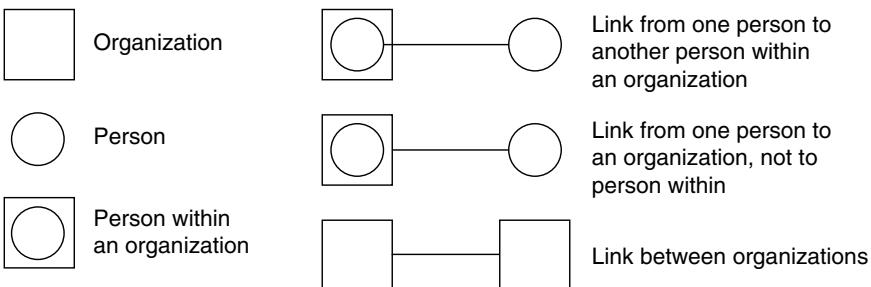
NETWORK MODELS

Most intelligence modeling today focuses on networks. Network models have been highly successful in helping to assess problems of terrorism, WMD proliferation, insurgencies, narcotics and human trafficking, as well as clandestine arms traffic and weapons systems development. They have become an indispensable tool in military intelligence for targeting and for planning combat strategies and tactics.

Staying with the Khanani MLO network example, let's examine a modified version of the financial relationships link model in figure 19.1, redrawn as a network model in figure 19.2. Both figures use ovals to indicate people and boxes to indicate organizations. Many network software packages incorporate additional features (not shown in the figure) to make both link and network diagrams convey more information. Color coding can indicate types of organizations—banks and customers, for example. Relationships can be shown as either positive (solid links) or negative (dashed links). Strength of relationship can be shown by the thickness of the linkage line. Additional techniques can convey more information—making the links dotted or colored to indicate a suspected relationship or making nodes larger or smaller to indicate relative importance in the model. With features such as these, network models can be a powerful tool to use in causal modeling (in chapter 15) and in creating influence nets (in chapter 16).

The two figures illustrate an advantage of network models over link models that becomes critical when the total number of entities displayed is large (on the order of a hundred or more): Each entity such as “Al Zarooni Exchange” appears only once in a network diagram, and multiple links to it are easy to see.

Intelligence units are concerned about relationships among people and organizations. But in dealing with organized crime, the law enforcement community has a requirement to highlight whether a relationship is to an organization, or just to a person within the organization. So, the law enforcement community developed a special notation in network models to make those relationships more apparent, as shown in figure 19.3.

FIGURE 19.2 ■ Khanani MLO Network Model**FIGURE 19.3 ■ Network Diagram Features Used in Law Enforcement Intelligence**

Network Model Types

There are numerous types of networks, but for this book's purposes they are all *target networks*, though that doesn't mean they are necessarily hostile. A target network can include friendly or neutral entities. Target network models can include neutrals that the customer wishes to influence—either to become an ally or to remain neutral. For example, during and immediately after World War I, British intelligence relied on the area knowledge and diplomatic skills of T. E. Lawrence (known as Lawrence of Arabia) and Gertrude Bell in assessing the tribal networks of Arabia and Iraq. Without the intelligence they furnished about neutral and friendly networks, the British probably would have had considerably less success militarily and diplomatically during and after

the war.³ Almost a century later, US intelligence created network models depicting friendly and neutral individuals in Afghanistan during its operations there, and likely did the same for Iraqi units (showing their Iranian connections) during joint operations against Daesh in Iraq.

Target networks can be a composite of several types. That is, they can have social, organizational, commercial, and financial elements, and they can show threat networks; those types are covered individually later. But target networks also can be characterized another way, taking into account the nature of the relationships among nodes. In creating a network model, analysts must understand which of the following relational forms they are dealing with:

- Functional networks. *These are formed for a specific purpose. Individuals and organizations come together to undertake activities based primarily on the skills, expertise, or particular capabilities they offer. Commercial networks, crime syndicates, and insurgent groups all fall under this label. The US Joint Forces Command calls these “specialized networks.” Most networks of intelligence interest are functional networks.*
- Family and cultural networks. *Some members or associates have familial bonds that may span generations. Or the network participants have bonds due to a shared culture, language, religion, ideology, country of origin, and/or sense of identity. Friendship networks fall into this category, as do proximity networks—where the network members have bonds due to geographic or proximity ties (such as time spent together in correctional institutions). Many gangs and terrorist groups fit into this category, and they also are functional networks.*
- Virtual networks. *Participants seldom (possibly never) physically meet but work together, usually via the Internet. Networks involved in online fraud, theft, or money laundering are virtual. Social media sites often are used to operate virtual networks.⁴*

A target network can be any combination of these, and it's not uncommon for the network to include more than one of these forms. It is possible, in fact, for a network to be functional, family, cultural, proximity, and have virtual elements. Again, analysts need to know which of these forms, or combinations of forms, they are primarily dealing with, because different network types reflect different strengths and vulnerabilities.

Before a network can be analyzed, it must be modeled. Target networks can be modeled manually or by using computer algorithms.

Manual Modeling

When network modeling was first developed as an analytic methodology, target network models were created manually, drawing circles and links on large sheets of

paper. Some network models created for intelligence purposes still are created manually (though not typically with pen and paper). Using open-source and classified HUMINT or COMINT, an analyst typically goes through the following steps in manually creating a network model:

1. *Understand the environment.* Understand the setting in which the network operates. This may require looking at all six of the PMESII factors that constitute the environment, but almost certainly at more than one of these factors. The PMESII approach applies to most networks of intelligence interest, again recognizing that “military” refers to that part of the network that exerts force (usually physical force) to serve network interests. Street gangs and narcotics traffickers, for example, typically have enforcement arms.
2. *Select or create a network template.* Use foundational analytic methods such as pattern analysis, link analysis, and social network analysis to develop the target network template. Are the networks centralized or decentralized? Are they regional or transnational? Are they functional, familial, or virtual? Are they a combination? This information provides a rough idea of their structure, adaptability, and resistance to disruption.
3. *Populate the network.* In the absence of a network template, a technique that is sometimes called “snowballing” can help. Begin with a few key members of the target network. Add nodes and linkages based on the information these key members provide about others. Over time, COMINT and other collection sources (OSINT, HUMINT) allow the network to be fleshed out. Identify the nodes, name them, and determine the linkages among them. Work to determine the nature of the link. For example, is it a familial link, a transactional link, or a hostile link?

Computer-Assisted and Automated Modeling

Although manual modeling is still used, commercially available software tools such as Analyst’s Notebook and Palantir are available to help. One option for using them is to enter the data manually but rely on the tool to create and manipulate the network model electronically.

The ideal would be to automate the process completely, that is, have network models created directly from raw data. Considerable progress has been made in doing just that. In the early 2000s, DARPA created the “evidence extraction and link discovery program,” intended to demonstrate the feasibility of extracting relationships from text. The program developed technologies and tools for automated discovery, extraction, and linking of sparse evidence contained in large amounts of classified and unclassified data sources such as telephone records, internet histories, or bank records. Because of privacy concerns, Congress suspended the program in 2003. But the technology for automating link discovery and network creation continues in the private sector and

in other parts of government. Automated creation of social network models now is prevalent using data- and text-mining techniques on open sources, e-mails, telephone conversations, and social network sites such as Facebook and Twitter.

Considerable effort has gone into developing systems that can learn from analysts and create network models from data. But take note: (1) A human analyst will always need to evaluate sources and validate results and (2) any system that purports to organize massive amounts of data also will generate massive false alarms.⁵

NETWORK ANALYSIS

Having created a network model, analysts are prepared to address the issues customers have posed about it. This involves answering the classic questions—*who, what, where, when, how, and why*—and placing the answers in a format the customer can understand and act on; that is, turning it into actionable intelligence. Analysis of the network pattern can help identify the *what, where, and when*. Social network analysis typically identifies *who*. And nodal analysis can tell *how* and *why*.

In network analysis, analysts are evaluating, among other things, the function and importance of individuals or organizations within the network and the assets available to them. Specifically, are they connected to a large number of other individuals or organizations? Who would provide them with access to resources such as financial, political, or equipment? What is their role in the network, for example, as brokers or intermediaries? How close are they on average to other actors in the networks? Do they have the power to easily share information in the network? The answer to such questions helps to identify the individuals to focus on and to determine the nature of the power they hold.⁶ Getting to the answers depends on one or more of the types of analysis discussed next.

Nodal Analysis

Nodes in a target network can include people, places, objects, and organizations (which also could be treated as separate networks). Where the node is an organization, it may be appropriate to assess the role of the organization within the larger network—that is, to simply treat it as a node.

Sometimes, nodal analysis involves assessing performance of an object—an aircraft, an improvised explosive device, a missile, or a radar, for example. A large military force is composed of many people, objects, and organizations. Some of the objects (military equipment) may be critical components to the success or failure of the military force. The HIND attack helicopter and the Oerlikon heavy machine gun discussed in chapter 18 are examples. The HIND was a critical node of the Soviet forces in Afghanistan; the Oerlikon alone was not the key to countering the HIND.

The key is to identify the most critical nodes in a target network. This requires analyzing the properties of individual nodes, and how they affect or are affected by other nodes in the network. The analyst must understand the behavior of many nodes and, where the nodes are organizations, the activities taking place within the nodes.

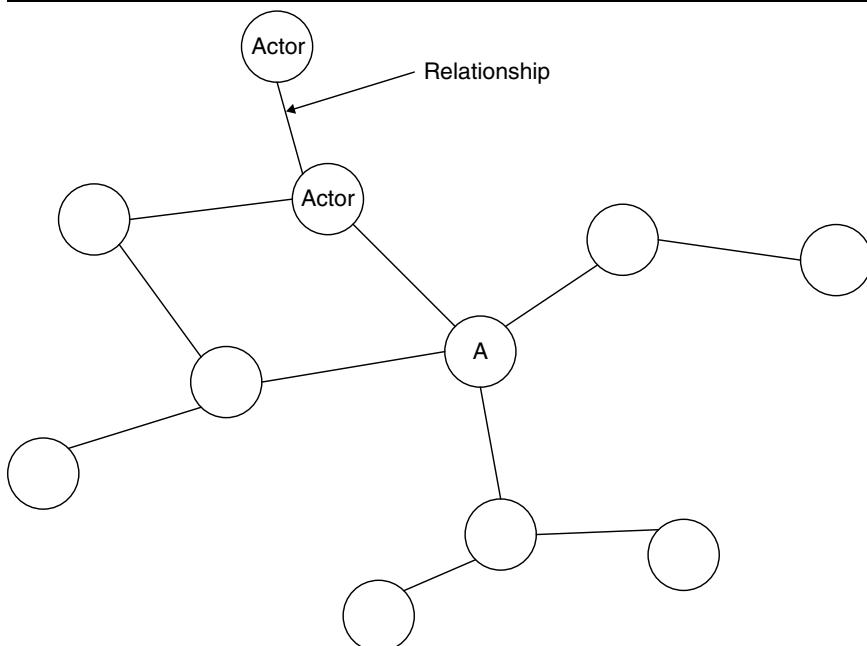
Social Network Analysis

When intelligence analysts talk about network analysis, they often are referring to social network analysis (SNA). SNA involves identifying and assessing the relationships among people and groups—the nodes of the network. The links show relationships or transactions between nodes. A social network model provides a visual display of relationships among people, and SNA provides a visual or mathematical analysis of the relationships.⁷ SNA is used to identify key people in an organization or social network and to model the flow of information within the network.⁸

Social network analysis, in which all of the network nodes are people or groups, is widely used in the social sciences, especially in studies of organizational behavior. Intelligence, as noted earlier, is more frequently concerned with *target network analysis*, in which almost anything can be a node. The Khanani MLO case illustrates the need to include entities such as banks, terrorist organizations, and companies as nodes. However, the basic techniques of SNA apply to target network analysis as well.

A social network is a set of individuals referred to as *actors* (shown graphically as nodes on figure 19.4) that are connected by some form of relationship (shown as lines in the figure). Such networks can comprise few or many actors with different bonds between actors. To understand a social network, analysts need a full description of the social relationships within it. Ideally, analysts would know about every relationship between each pair of actors in the network.

FIGURE 19.4 ■ Social Network Analysis Diagram



Graphics are fundamental as they suggest things to look for in the data—things that might not have surfaced if the network were described using only words. It is easy to see, in figure 19.4, that removing node *A* will have the most impact on the network. It might not be so obvious if all the relationships were described textually.

In summary, SNA is a tool for understanding the internal dynamics of a target network and how best to attack, exploit, or influence it. Instead of assuming that removing the leader will disrupt the network, for example, SNA helps identify the distribution of power and the influential nodes—those that can be removed or influenced to achieve a desired result.

It is rare, but the result of a well-executed SNA against military opponents occasionally appears in the headlines, as happened in the following case.

BOX 19.1 THE ABU SAYYAF RAID

On May 15–16, 2015, the US Army's Special Forces attempted to capture a Daesh commander during a raid at al-Omar in eastern Syria. He was killed while fighting capture. Abu Sayyaf was the key person directing the terrorist organization's illicit oil, gas, and financial operations, according to US Secretary of Defense Ashton Carter. Because of the importance of these operations in financing Daesh operations, Abu Sayyaf represented a critical—possibly irreplaceable—node in the Daesh network.⁹ The raw intelligence (computers, cell phones, and documents) seized in the raid were reported to be a bonus though probably one expected by the raid planners, given the importance of the node.

Over the next two years, US and allied military forces removed a number of other key Daesh leaders: In August 2016, a missile from a Reaper drone eliminated Abu Muhammad al-Adnani, Daesh's senior propaganda chief and strategist.¹⁰ In January 2017, a US Special Forces raid killed another Daesh leader in eastern Syria. While the US and its allies have several sources that could have provided targeting for these attacks, network analysis of the intelligence taken from the Abu Sayyaf raid was likely a prominent one.

Several analytic concepts are fundamental to SNA but two of the most useful are *centrality* and *equivalence*. They are present in all organizations—governmental, commercial, and private—but are especially important in the analysis of problems related to terrorism, arms trafficking, and organized criminal activity.

Centrality

Centrality refers to the sources and distribution of power in a social structure. The network perspective suggests the power of an individual actor arises from relationships with other actors. In fact, it is generally known that power comes from occupying an advantageous position in a social network. An actor's position in the network tells the analyst much about the extent to which that actor may be constrained by, or may be able to constrain, others. To understand networks and their participants, the analyst

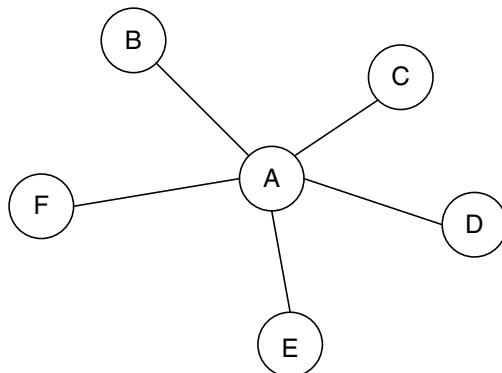
assesses the location of actors in the network, that is, their centrality. This measure provides insight into the various roles and groupings in the network—who the leaders or connectors are, where the clusters are and who is in them, who forms the core of the network, and who is on the periphery.¹¹

The extent to which an actor can reach others in the network is a major factor in determining the power that the actor wields. Three basic sources of this advantage are *high degree*, *high closeness*, and *high betweenness*.

The more ties an actor has to other actors, the more power (higher degree) that actor has. In the “star network” depicted in figure 19.5, actor *A* has degree five (ties to five other actors); all other actors have degree one (ties to just one other actor). Actor *A*’s high degree gives *A* more opportunities and alternatives than other actors in the network. If any actor chooses not to work with *A*, then that actor cannot effectively work within the network. But actor *A* still has the rest of the network available to work with. Actors who have many network ties have greater opportunities because they have choices. Their rich set of choices makes them less dependent than those who have fewer ties and, hence, more powerful.

The second reason why actor *A* is more powerful than others in figure 19.5 is that *A* is closer (high closeness) to more actors than anyone else. Power can be exerted by direct bargaining and exchange, but power also comes from being a center of attention and able to communicate directly with more actors. Actors who are able to reach others by shorter paths, or who are more reachable by other actors through shorter paths, have favored positions. Such a structural advantage translates into power.

FIGURE 19.5 ■ Social Network Analysis: A Star Network



A third reason (closely related to the second) that actor *A* is advantaged is *A*’s position between all other pairs of actors (high betweenness)—no other actors lie between *A* and other actors. If *A* wants to contact *F*, *A* may do so directly. If *F* wants to contact *B*, *F* must do so by way of *A*. This gives actor *A* the capacity to broker contacts among other actors—to extract “service charges” and to isolate actors or prevent contacts.

In the star network, all of these advantages are held by one actor. Look again at the original Altaf Khanani network from chapter 12 (figure 12.3) to see that it illustrates a star network. After Khanani's capture, the successor network looked more like figure 19.4.

The Japanese *Yakuza* (a term roughly equivalent to the American use of *Mafia*) are examples of star networks. Yakuza are probably the most centralized of organized crime networks. Beneath the head, or *oyabun*, are subordinate *kobun*, each of whom forms a lower-level star network in what is an elaborate hierarchy. The Yakuza organization contrasts with that of East Asian gangs such as the Chinese Triads, which comprise a loose conglomeration of criminals bonded together mostly by familial relations.

A terrorist network further illustrates the concept of centrality. In seeking to disrupt terrorists, one obvious approach is to identify the central players and target them for assessment, surveillance, or removal. The network centrality of the individuals will determine the extent to which the removal impedes continued operation of the terrorist activities. Thus centrality is an important ingredient (but by no means the only one) in considering the identification of network vulnerabilities.

Equivalence

Equivalence is another analytic concept central to SNA. The disruptive effectiveness of removing one individual or a set of individuals from a network (such as by making an arrest or hiring a key executive away from a business competitor) depends not only on the individuals' centrality but also on some notion of their uniqueness, that is, on whether or not they have *equivalents*. The notion of equivalence is useful for strategic targeting and is tied closely to the concept of centrality. If nodes in the social network have a unique role (no equivalents), they will be harder to replace. One of the strengths of Daesh that helped it survive for so long against repeated attacks is that it makes use of equivalence, in the form of substitutability or interchangeability of key players; as one counterterrorism expert put it, Daesh had “a deep bench.”¹²

When attacking an opponent's network, the most valuable targets will be both central and without equivalents. Continuing the example of a terrorist network, the network leader may have an equivalent, for example, a strong subordinate with a similar skill set who can take over. But an accountant who has unique expertise and knowledge may be an irreplaceable part of the network by virtue of centrality and lack of equivalents. Abu Sayyaf played such a role in the Daesh organization.

Organizational Network Analysis

Management consultants often use SNA methodology with their business clients, referring to it as *organizational network analysis*.¹³ It is a technique for appraising communication and social networks within a formal organization and, sometimes, between separate organizations as well. Organizational network modeling is used to create statistical and graphical models of the people, tasks, groups, knowledge, and resources of organizations.

Chapter 18 discussed systems modeling and analysis, with several examples focusing on weapons systems. The typical organization also is a system that can be viewed (and analyzed) from the same three systems perspectives discussed there: structure, function, and process. *Structure* here refers to the components of the organization, especially people and their relationships; this chapter deals with that. *Function* refers to the outcome or results produced by the organization and tends to focus on decision making, a topic of discussion in chapter 21. *Process* describes the sequences of activities and the expertise needed to produce the results or outcome. Liam Fahey, in his assessment of organizational infrastructure, describes four perspectives: structure, systems, people, and decision-making processes.¹⁴ Whatever their names, all three (or four, following Fahey's example) views must be considered.

For the analyst, an initial goal of organizational network analysis is to understand the strengths and weaknesses of the target organization. A higher-order goal would be predictive: to forewarn of changes in the target organization's structure, function, or process that may arise from changing forces. Policy-oriented customers can use the analysis in planning strategy; operations units can use it to adversely affect the target, for example, by possibly using information warfare. Depending on the goal, the analyst may need to assess the network's mission, power distribution, human resources, and decision-making processes. Questions to be answered would include these: Where is control exercised? Which elements provide support services? Are their roles changing? Network analysis tools are valuable for those types of answers.

Two of the most common applications in intelligence concern commercial and financial networks. Both are of special interest in law enforcement intelligence.

Commercial Networks

Organizational network analysis can do more than identify key people in an organization; it also can be a powerful tool for identifying suspicious activities that should be investigated in detail. Both capabilities have been demonstrated in the analysis conducted on the Enron network—after the fact, admittedly. But as the case demonstrates, analysts don't need the content of communications to identify either key people or nefarious activity; they can do it with just the network connections demonstrated in the communications.

BOX 19.2 THE ENRON NETWORK

Texas-based Enron Corporation in mid-2000 was an American success story. Its businesses included energy production, communications, and pulp and paper. The company had 20,000 staff and claimed revenues of over \$100 billion that year. *Fortune* magazine named it "America's Most Innovative Company" for six consecutive years (1996–2001).

By the end of 2001, Enron was undergoing the largest Chapter 11 bankruptcy in US history. Its stock was worth pennies. Investigators found that Enron's reported

financial condition was the result of accounting fraud. With the cooperation of Big Six accounting firm Arthur Andersen, Enron had used a creative set of deceptive, bewildering, and fraudulent accounting practices and tactics to conceal its true financial picture. In the aftermath of what became known as the Enron scandal, sixteen people pleaded guilty to crimes including fraud and insider trading, and five others were found guilty. Arthur Andersen was found guilty of criminal charges relating to the audits and subsequently folded.

After the investigation, the US Federal Energy Regulatory Commission (FERC) released more than 1.6 million emails senior Enron executives had sent and received between 2000 and 2002. The material was posted on the internet, and the FERC was criticized for releasing so much sensitive personal information about individuals—many of whom were guilty of no crime. The FERC subsequently cleaned up the dataset to remove much of the personal information, but the remaining set represents the largest email database available in the public domain. It has become the source material for many research studies on network modeling and analysis, and it has helped in the development of tools for counterterrorism analysis and fraud detection.¹⁵

Columbia University developed one of the early algorithms applied to the email dataset. The algorithm was used to recognize and rank key officers, groups, and individuals by email relationships, and to graphically draw an Enron organizational chart. The resulting network model highlighted relationships that revealed the “true social hierarchy” of the company over the course of time—which was significantly different from the official Enron hierarchy.¹⁶

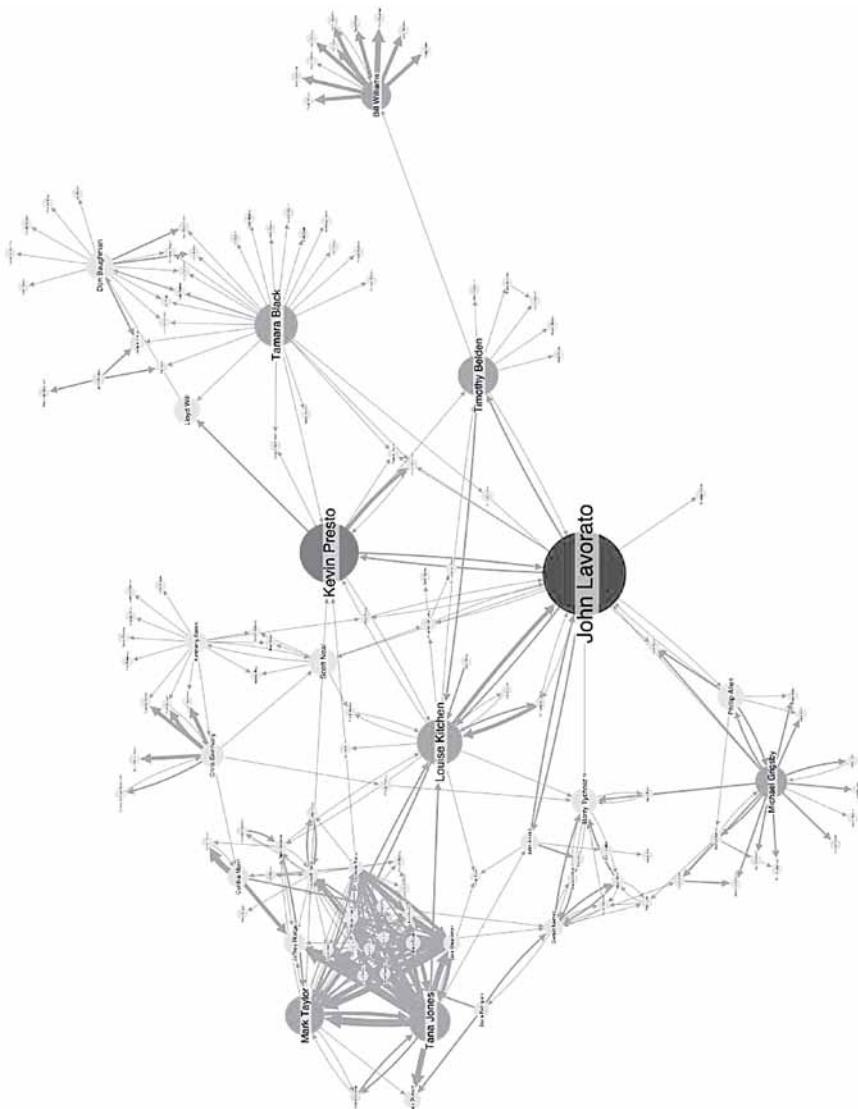
Figure 19.6 was created using Cambridge Intelligence’s KeyLines tool. It was used to identify features of Enron’s social network that illustrate points made in this chapter. Of all the nodes in the figure, John Lavorato is in the strongest position; he has the highest closeness and betweenness, indicating that he was a top executive in the organization. He was in fact the CEO of Enron America.

The figure also illustrates anomalies in the hierarchy that would likely attract the attention of an intelligence analyst—if it had been available prior to 2000. Timothy Belden is closely tied to CEO Lavorato but not to the Enron network generally. Bill Williams is connected to the network only through Belden; and his two administrative assistants were found to have similar social importance as their much higher ranking director, which is unusual. Belden was the head of trading for Enron Energy Services; he developed a scheme to manipulate the supply of electricity to California and drive up energy prices. His trading strategy resulted in the 2000–2001 energy crisis in California that led to large scale blackouts and the bankruptcy of Pacific Gas and Electric Company. Williams was a trader responsible for executing parts of Belden’s strategy. (Belden later pleaded guilty to one count of conspiracy to commit wire fraud as part of a plea bargain, in which he assisted in the prosecution of Enron’s top officers.)¹⁷

In identifying fraud or other illegal conduct in a network, the analyst’s job might be to identify anomalies suggesting suspicious relationships or activities, as in the Enron example. Against opposing networks, it might be to identify vulnerable points in the target organization so that intelligence customers—the decision makers—can select

the appropriate target to act on; that is, to identify where perception management or coercive techniques would be most effective. For example, the customers may want to know how to best convey to the organization's leadership that it can expect strong retaliatory actions if it behaves in a certain way.

FIGURE 19.6 ■ Partial Social Network of Enron Corporation



Source: Image from Cambridge Intelligence, creators of the KeyLines network visualization toolkit.

Commercial networks also are of interest to competitive intelligence professionals. Here, the focus is on networks where the nodes are organizations. As Fahey notes, competition in many industries is now as much competition between networked enterprises (companies such as Cisco and Walmart that have created collaborative business networks) as it is between individual stand-alone firms.¹⁸ Fahey describes several such networks and defines five principal types:

- *Vertical networks. Networks organized across the value chain; for example, 3M Corporation goes from mining raw materials to delivering finished products.*
- *Technology networks. Alliances with technology sources that allow a firm to maintain technological superiority, such as the Cisco Systems network.*
- *Development networks. Alliances focused on developing new products or processes, such as the multimedia entertainment venture DreamWorks SKG.*
- *Ownership networks. Networks in which a dominant firm owns part or all of its suppliers, as do the Japanese keiretsu.*
- *Political networks. Those focused on political or regulatory gains for their members, for example, the National Association of Manufacturers.¹⁹*

Hybrids of the five are possible, and in some cultures such as in the Middle East and Far East, families can be the basis for a type of hybrid business network.

Financial Networks

Financial networks also tend to feature links among organizations, though individuals can be important nodes, as in the Khanani MLO. Analysis focuses on topics such as credit relationships, financial exposures between banks, liquidity flows in the interbank payment system, and money laundering transactions. The relationships among financial institutions, and the relationships between financial institutions and other organizations and individuals, are best captured and analyzed with organizational network modeling.

Financial network modeling and analysis is used on a micro scale to identify white-collar crime such as fraud; illicit funds transfers to terrorist groups; and financial transfers connected to gray arms, stolen goods, human, and narcotics trafficking. It is useful on a macro scale in assessing high-volume financial risks and identifying potential financial crises. Global financial markets are interconnected and therefore amenable to large-scale modeling. Analysis of financial system networks helps economists to understand systemic risk and is key to preventing future financial crises. In 2014, Olivier Blanchard, the International Monetary Fund's chief economist at the time, identified breakdowns in supply chain networks as helping to explain the difficulties that East European transition economies encountered during the early 1990s.

Blanchard also identified financial network problems as contributing to the 2007–2009 economic recession in advanced economies.²⁰

Clandestine financial networks such as hawala are, by their nature, difficult to model. They usually require a combination of HUMINT and COMINT to penetrate. In contrast, some networks of intelligence interest are accessible on the internet and can be modeled using software tools. An example is the blockchain, the software tool that makes Bitcoin and other cryptocurrencies possible. It is a digital log file, publicly available but cryptographically protected, that secures online transactions. Its strength is that there is no central control; instead, transaction validation requires the agreement of blockchain participants. Financial institutions also appear to be adopting blockchain technology to secure interbank transfers.

Because they depend on peer-to-peer communication, blockchain financial networks can be modeled in detail. That has been done for the Bitcoin network, where “miners” use software to solve mathematical problems and thereby earn Bitcoin currency. The network modelers discovered that a few influential nodes of mining pools represent most of the mining power in the network and have disproportionate influence. Those nodes were characterized by their high centrality: 48 nodes in the Bitcoin network had remarkably high degrees of centrality, ranging from 90 to 708—compared to an average centrality of 8 to 12.²¹

Target Network Analysis

The preceding sections have discussed nodal, social network, and organizational network analysis. In intelligence work, we usually apply an extension of all three for target network analysis. The techniques described earlier for each of the three apply for almost all target networks. But whereas all the entities in SNA are people, and the entities in organizational network analysis are people and organizations, in target network analysis they can be anything. For example, an analyst who is charting a target network diagram for a terrorist organization will include associated organizations, weapons, physical locations, and means of conducting terrorist activities (for example, vehicles and types of explosives). The purpose of such target network models is usually to reveal things like the patterns of operations, likely future targets, and types of weaponry. Target network analysis thereby includes some aspects of functional analysis and process analysis.

Though target networks come in many forms, they typically fall into three types:

- They may be threat networks that must be countered, requiring analysis of strengths and vulnerable points in the network.
- They may be neutrals who must be influenced to join your side or at least maintain their neutrality.
- They may be friendlies or allies, whose goals and capability to support your network need to be assessed.

The job of analyzing all three target network types traditionally has been one for intelligence. But since threat networks are most commonly encountered, let's focus on them.

Threat Network Analysis

Military and law enforcement organizations define a specific type of target network they call a *threat network*. These are opponent networks, comprised of “people, processes, places, and material—components that are identifiable, targetable, and exploitable.”²²

Threat networks take many forms. Today they seldom are composed of states, though they may have state backing. They include insurgents, violent global jihadists, and international criminal organizations such as human and narcotics traffickers.

A premise of threat network modeling is that all such networks have vulnerabilities that can be exploited. Intelligence must provide an understanding of how the network operates so that customers can identify actions to exploit the vulnerabilities.

Some threat networks are territorially based. An example is the Japanese crime syndicate Yamaguchi-gumi, introduced in chapter 2. The Yamaguchi-gumi earn money primarily from drug trafficking, gambling, and extortion.²³

At the other extreme are transnational threat networks. Central and South American narcotics traffickers such as the Sinaloa drug cartel exemplify these networks. Some of the most powerful are the Russian Mafia groups (Solntsevskaya Bratva) that have roots in Russia but function across the globe—operating in Europe, southwestern Asia, and North and South America.²⁴ One of these groups, the Vory v Zakone (“thieves in law”), dates back nearly a century. The Vory now engage in narcotics trafficking, money laundering, and prostitution and have ties with the American Mafia and Colombian drug cartels.

Threat networks, no matter their type, can access political, military, economic, social, infrastructure, and information resources. They may connect to social structures in multiple ways (kinship, religion, former association, and history)—providing them with resources and support. They may make use of the global information networks, especially social media, to obtain recruits and funding and to conduct information operations to gain recognition and international support.

Analysts develop a detailed understanding of how a threat network functions by identifying its constituent elements, learning how its internal processes work to carry out operations, and examining how all of the network components interact. Assessing threat networks requires, among other things, looking at these six factors:

- *Command-and-control structure. Threat networks can be decentralized, or flat. They can be centralized, or hierarchical. The structures will vary, but they are all designed to facilitate the attainment of the network's goals and continued survival.*
- *Closeness. This is a measure of the members' shared objectives, kinship, ideology, religion, and personal relations that bond the network and facilitate recruiting new members.*

- *Expertise.* This includes the knowledge, skills, and abilities of group leaders and members.
- *Resources.* These include weapons, money, social connections, and public support.
- *Adaptability.* This is a measure of the network's ability to learn and adjust behaviors and modify operations in response to opposing actions.
- *Sanctuary.* These are locations where the network can safely conduct planning, training, and resupply.²⁵

Threat networks have several strengths, and the analyst must assess them. Many have the ability to adapt over time, specifically to blend into the local population and, as has been noted about Daesh, to quickly replace losses of key personnel and recruit new members. They can be difficult to penetrate because of their insular nature and the bonds that hold them together. They typically are organized into cells in a loose network where the loss of one cell does not seriously degrade the entire network.

They also have weaknesses. Threat networks tend to follow a standard operating pattern based on what has worked in the past. Once a pattern is pinpointed and thus becomes predictable, it is not hard to defeat. Some threat networks must compete with similar groups for resources, support, markets (narcotics traffickers), or territory (gangs). They must communicate between cells and with their leadership, exposing the network to discovery and mapping of links. To carry out the network's functions, the members must engage in activities that expose parts of the network to countermeasures.

Automating Network Analysis

Target network analysis has become one of the principal tools for dealing with complex systems, thanks to computer-based analytic methods. One tool that has been useful in assessing target networks is the Organization Risk Analyzer (called *ORA) developed by the Center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University. *ORA can group nodes and identify patterns of analytic significance. It has been used to identify key players, groups, and vulnerabilities, and to model network changes over space and time.²⁶ By 2021, the US Army had adapted *ORA into its “Attack the Network” strategy with the objective to “out-think, out-maneuver, out-partner, and out-innovate revisionist powers, rogue regimes, terrorists, and other threat actors.”²⁷

Intelligence analysis relies heavily on graphical techniques to represent the descriptions of target networks compactly. The underlying mathematical techniques allow analysts to use computers to store and manipulate the massive volumes of information quickly and more accurately than ever before. Suppose an analyst is examining the trade flows of fifty different commodities (such as corn, coal, tea, copper, and bauxite) among 150 nations in a given year. Here, the 150 nations can be thought of as nodes, and the amount of each commodity exported from each nation to each of the other

149 can be thought of as the strength of a direct tie from the exporting nation to the other. A customer might be interested in how the networks of trade in metal ores differ from networks of trade in grain. To answer this simple question requires a tremendous amount of data manipulation. That could take years to do by hand; a computer can do it in less than a minute.

SUMMARY

Relationship models allow analysts to investigate the relationships among elements of the target—people, organizations, places, physical objects, and events—over time. The four general types of relationship models are hierarchy, matrix, link, and network models. The most widely used of these, network models, are essential for describing complex intelligence targets.

One of the most powerful tools in the analyst's toolkit is network modeling. It is derived from link modeling, which organizes and presents raw intelligence in a visual form such that relationships among nodes (which can be people, places, things, organizations, or events) can be analyzed to extract finished intelligence.

Intelligence is concerned with many types of networks. Network modeling always is about the most general type, the target network—where “target” means a target of intelligence interest, not necessarily an opponent. Target networks can be

- *Social.* The nodes are all people or groups of people.
- *Organizational.* Models are used to assess the communication and social networks within a formal organization.
- *Commercial.* These can be structured as vertical, technology, development, ownership, political, or a hybrid.
- *Financial.* These are networks among financial organizations, typically banks and other financial institutions.
- *Threat.* These are opposing networks, comprising people, processes, places, and material components that can be targeted or exploited in conflicts. They can be social, organizational, commercial, or financial as well.

Target network models can be created manually, but the process of creating and updating them is tedious and time consuming. The goal is to have network models created and updated automatically from raw intelligence data by software algorithms. Although some software tools exist for doing that, human analysts must evaluate the sources and validate the results. False positives are also a caution to consider in automation.

Intelligence analysts examine network patterns and nodes. Their analysis can take several forms:

- Social network analysis is a tool for understanding the internal dynamics of a network and how to best use those to attack, exploit, or influence it. For the intelligence customer, relationship analysis is of the highest interest. Structural position generally confers power. A powerful individual has high centrality, meaning high degree (many ties to other members), high closeness (being close to many other members), and high betweenness (being the only connection between members). Another important measure of an individual in the organization is the individual's uniqueness, that is, whether the individual has equivalents.
- Organizational network analysis overlaps with the systems analysis covered in chapter 18. It is concerned with structure, function, and process, and it looks at power centers, decision making, and vulnerable points in the organization.
- Threat network analysis is quite similar to organizational network analysis. It includes identifying the network's constituent elements, understanding how its internal processes work to carry out operations, and understanding how all of the network components interact.
- Target network analysis, the most general type, can include all the analytic methods discussed throughout this book. Information technology shows promise in identifying patterns of significance to assist analysis.

CRITICAL THINKING QUESTIONS

1. The critical thinking questions in chapters 15 and 16 made use of the case studies in the 2013 RAND Corporation report *Paths to Victory*, accessible at https://www.rand.org/pubs/research_reports/RR291z2.html.²⁸ Consider again the case that you used there (your instructor may assign a different case). Using the bullet points in the section titled “Manual Modeling” as a guide, draw *target* network diagrams—one for each side—that show the key nodes and relationships for that side. Consider all the PMESII factors that might be represented by nodes in the network (financial supporting nodes, for example). Include nodes and links that must exist but that you cannot identify (labeled as such) from the material in the case or from research.
2. In 2016, Colombian police arrested Nidal Waked, a Panamanian who was accused of heading the Waked money laundering organization. This MLO is considered the world’s top money launderer for international drug traffickers. The US Treasury Department provided a list of the people and organizations associated with the MLO at <https://insightcrime.org/news/analysis/us-panama-nidal-waked/>. Based on it and other online sources, and using the bullet points in the section titled “Manual Modeling” as a guide, create a target network diagram—including people and organizations—of the Waked MLO. Identify the likely roles (placement, layering, or integration) of the *principal*

organizations associated with the MLO. (The principal organizations are listed on the first page of the US Treasury report.) Nidal Waked pleaded guilty to bank fraud before a Miami judge in 2017, was sentenced to twenty-seven months in prison with credit for time served, and is now free and back in Panama.

3. Extensive material has been published online about Iran's nuclear program. Drawing on it, create a *social* network diagram of the key people involved in the program. What advantages and disadvantages does the diagram have, in comparison to what a target network diagram would contain?
4. It has been observed that the traditional hierarchical description of an organizational structure does not sufficiently portray entities and their relationships. Give at least four reasons why this is so.

NOTES

1. US Joint Forces Command, *Commander's Handbook for Attack the Network* (Suffolk, VA: Joint Warfighting Center, 2011), IV-3, http://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/atn_hbk.pdf.
2. Ibid., appendix GL-1.
3. Janet Wallach, *Desert Queen* (New York, NY: Anchor Books, 2005).
4. US Joint Forces Command, *Commander's Handbook*, III-1.
5. See Defense Advanced Research Projects Agency, "DARPA Evidence Extraction and Link Discovery pamphlet," November 22, 2002, www.darpa.mil/iso2/EELD/BAA01-27PIP.htm.
6. Anasuya Raj and Jean-François Arvis, "How Social Connections and Business Ties Can Boost Trade: An Application of Social Network Analysis," The World Bank, April 28, 2014, <http://blogs.worldbank.org/trade/how-social-connections-and-business-ties-can-boost-trade-application-social-network-analysis>.
7. "Social Network Analysis: A Brief Introduction," [Orgnet.com](http://www.orgnet.com/sna.html), 2013, <http://www.orgnet.com/sna.html>.
8. Kristan J. Wheaton and Melonie K. Richey, "The Potential of Social Network Analysis in Intelligence," January 9, 2014, <http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/>.
9. Lizzie Dearden, "Senior Isis Commander Abu Sayyaf Killed by US Special Forces during Overnight Raid on House in Syria," *Independent*, May 16, 2015, <https://www.independent.co.uk/news/world/middle-east/isis-commander-killed-by-us-special-forces-during-overnight-raid-on-house-in-syria-10255130.html>.
10. Eric Schmitt, Rukmini Callimachi, and Anne Barnard, "Spokesman's Death Will Have Islamic State Turning to Its 'Deep Bench,'" *New York Times*, August 31, 2016, <https://www.nytimes.com/2016/09/01/world/middleeast/syria-isis-adnani.html>.
11. "Social Network Analysis: A Brief Introduction."

12. Schmitt, Callimachi, and Barnard, "Spokesman's Death Will Have Islamic State Turning to Its 'Deep Bench.'"
13. "Social Network Analysis: A Brief Introduction."
14. Liam Fahey, *Competitors* (New York: Wiley, 1999), 403.
15. Jessica Leber, "The Immortal Life of the Enron E-mails," *MIT Technology Review*, July 2, 2013, <https://www.technologyreview.com/s/515801/the-immortal-life-of-the-enron-e-mails/>.
16. German Creamer, Ryan Rowe, Shlomo Hershkop, and Salvatore J. Stolfo, "Segmentation and Automated Social Hierarchy Detection through Email Network Analysis," Columbia University, no date, <http://ids.cs.columbia.edu/sites/default/files/hierarchyv3.pdf>.
17. Reece Howard, "Using Social Network Analysis Measures," Cambridge Intelligence, July 21, 2015, <https://cambridge-intelligence.com/using-social-network-analysis-measures/>.
18. Liam Fahey, *Competitors*, 237.
19. Ibid., 238.
20. Carmelia Minoiu and Sanjay Sharma, "Financial Networks Key to Understanding Systemic Risk," *IMF Survey Magazine*, May 28, 2014, <http://www.imf.org/external/pubs/ft/survey/so/2014/RES052314A.htm>.
21. Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee, "Discovering Bitcoin's Public Topology and Influential Nodes," University of Maryland, 2015, <https://www.cs.umd.edu/projects/coinscope/coinscope.pdf>.
22. US Joint Forces Command, *Commander's Handbook*, III-1.
23. Chris Matthews, "Fortune 5: The Biggest Organized Crime Groups in the World," *Fortune*, September 14, 2014, <http://fortune.com/2014/09/14/biggest-organized-crime-groups-in-the-world/>.
24. Ibid.
25. US Joint Forces Command, *Commander's Handbook*.
26. Carnegie Mellon University, "*ORA," <http://www.casos.cs.cmu.edu/projects/ora/>.
27. US Army, "Advanced Network Analysis and Targeting (ANAT)," <https://oe.tradoc.army.mil/anat/>
28. Christopher Paul, Colin P. Clarke, Beth Grill, and Molly Dunigan, *Paths to Victory: Detailed Insurgency Case Studies* (Santa Monica, CA: RAND Corporation, 2013), https://www.rand.org/pubs/research_reports/RR291z2.html.

20

GEOSPATIAL MODELING AND ANALYSIS

Everything that happens on the Earth is spatially referenced. All activity happens at a place. It stands to reason that the geospatial model, which depicts locations and movement of objects and people, is one of the most widely used analytic tools today. It combines all sources of intelligence—OSINT, IMINT, HUMINT, COMINT, and other advanced technical collection methods—into a visual picture of a situation.

Consider geospatial modeling of a small area, such as a building. Layouts of buildings and floor plans are valuable in security analysis and in assessing production capacity, for example. Computer-aided design/computer-aided modeling, known as CAD/CAM, finds application in GEOINT. CAD/CAM models work well both in collection and in counterintelligence analysis of all sorts of facilities. Analysts can use them to create a physical security profile of a facility, allowing them to identify vulnerabilities by examining floor plans, construction details, and electronic and electrical connections—or to identify the purpose of the facility, as analysts did in looking at Rabta.

BOX 20.1 IDENTIFYING THE RABTA PLANT

Beginning in 1984, the Libyan government constructed a chemical agent production plant near the city of Rabta, forty miles southwest of Tripoli. According to the Libyans, the plant was to produce pharmaceuticals. Since the production facility was completely enclosed inside a warehouse-like structure, overhead photography revealed nothing about the process equipment inside, but the plant's oversized air-filtration system suggested an intention to produce toxic chemicals. This anomaly drew the attention of Western intelligence agencies.

The West German government was able to obtain construction blueprints of the Rabta plant from the engineering firm Salzgitter. These plans revealed other anomalous features that indicated not pharmaceuticals, but rather chemical warfare (CW) production. According to a German government report, "The joint planning of chemical plants and the metal processing plant as well as security facilities not usually found in a pharmaceutical facility (airtight windows and doors, gas-tight walls between the production and the control unit, burn-off unit, corrosion-proof lining on pipes, and escape routes) made it possible to draw the conclusion that 'Pharma 150' is a chemical weapon plant."¹

Under international pressure after the Rabta deception was exposed, the Libyan government eventually shut down the plant.

Covering a somewhat larger area than one facility, spatial models of local areas, such as city blocks, facilitate analytic inferences. For example, two buildings located within a common security fence can be presumed to have related functions, whereas no such presumption would follow if the two buildings were protected by separate security fences.

Intelligence analysts often need to discern a target's geographic location and observe what happens there over time in order to predict what may occur next. Although there are new terms for how we accomplish that, the analytic concept is very old. Sun Tzu in his *Art of War*, published about 500 B.C.E., advocated reliance on geospatial models in planning military movements. He observed that "we are not fit to lead an army on the march unless we are familiar with the face of the country—its mountains and forests, its pitfalls and precipices, its marshes and swamps."²

Spatial modeling and analysis have been practiced by military commanders, government leaders, and commercial entities for thousands of years. But there is something new today—the speed, accuracy, detail, and persistence with which they can be done. New and better collection sensors and communications systems have driven this change, making the intelligence product ever more useful to customers. Collection assets have shifted from relying on reconnaissance (periodic observations of a target) to surveillance (continuous observations of a target). Along with this success, the umbrella term *geospatial intelligence*, or *GEOINT*, arose. There are academic debates over what should or should not be included in the definition of GEOINT. Penn State University professor Todd Bacastow's definition covers the essential elements:

*Geospatial Intelligence is actionable knowledge, a process, and a profession. It is the ability to describe, understand, and interpret so as to anticipate the human impact of an event or action within a spatiotemporal environment. It is also the ability to identify, collect, store, and manipulate data to create geospatial knowledge through critical thinking, geospatial reasoning, and analytical techniques. Finally, it is the ability to ethically collect, develop, and present knowledge in a way that is appropriate to the decision-making environment.*³

He incorporates the key ideas of an intelligence mission: all-source analysis, not restricted to specific sources, and modeling *in both space and time*.

Other definitions of GEOINT are narrower and focus on imagery as the essential component. But it is possible to produce geospatial intelligence without reference to imagery at all. During World War II, although the Germans maintained censorship as effectively as anyone else, they did publish their freight tariffs on all goods, including petroleum products. Working from those tariffs, a young US Office of Strategic Services analyst, Walter Levy, conducted geospatial modeling based on the German railroad network to pinpoint the exact location of the refineries, which were subsequently targeted by allied bombers.⁴

More current examples illustrate the point:

- Every day, thousands of communications transmitters and radars are geolocated around the world using only the geolocation capabilities of SIGINT systems such as France's CERES satellite
- Every day, ships and submarines in the Atlantic and Pacific oceans are located, identified, and tracked using the Integrated Undersea Surveillance System (IUSS)—a MASINT sensor.
- Aircraft, ships, and satellites are continuously tracked by numerous radars—airborne, ship based, and land based—worldwide.
- Major seismic events are routinely geolocated and distinguished as to either underground explosions or earthquakes by a global network of event-monitoring stations—MASINT sensors.

The remainder of this chapter discusses where geospatial models and analysis are of most value in intelligence. The point to remember is that in all the examples, analysts are concerned with what is happening in selected locations over a period of time typically in relation to objects and human actors. Although customers sometimes are interested in a geospatial or temporal snapshot, the majority of intelligence now revolves around assessing activity in a location over time. We begin with static geospatial models and then focus on those that include temporal content.

STATIC GEOSPATIAL MODELS

Sometimes a customer may need only a snapshot in time. For that purpose, geospatial modeling typically uses electronically stored maps (of the world, of regions, of cities) to display geographically oriented data. The displays are valuable for visualizing complex spatial relationships. Networks often can be best understood by examining them in geospatial terms. Let's look at an example from the Korean War, followed by a completely different type of example still in process today.

BOX 20.2 THE INCHON LANDING

In July 1950, invading North Korean forces pushed South Korean and US forces into the southeastern corner of the Korean peninsula. General Douglas MacArthur, commanding the Allied forces, decided on a counterstrike that required UN naval forces to land at Inchon, a major port on Korea's Yellow Sea coast. From Inchon, MacArthur reasoned, the Allies could mount a major ground offensive to cut off North Korean forces in the south.

The North Koreans believed that the Inchon area was entirely unsuitable for a major amphibious operation. Tides rose and fell an average of 32 feet daily, producing strong currents in the narrow, winding waterways.⁵ The harbor approaches were easy to mine, lined by defensible islands, and marked by extensive mud flats, high seawalls, and dominating hills. The harbor facilities were rudimentary, with little room for logistics ships.

The Allied planning effort was an exemplar of both geospatial intelligence analysis and intelligence preparation of the battlespace. It made good use of overhead imagery from aircraft, debriefings of former inhabitants, and on-the-ground reconnaissance by naval special warfare teams. The intelligence allowed planners to select the best water approach, set the proper time for the amphibious assaults, and identify the North Korean Army line of communication as a critical vulnerability.

The amphibious landing on September 15 took the North Koreans completely by surprise. Two weeks later, the 1st Marine Division captured Seoul, and a large portion of the North Korean forces to the south were caught in a trap.⁶

Inchon, like the Desert Storm planning discussed in chapter 2, is an example of static geospatial modeling to support military operations. But static geospatial modeling also is applied widely in commercial enterprises, many of which have intelligence significance. The Trans-Afghanistan pipeline is an illustration.

BOX 20.3 THE NATURAL GAS PIPELINE

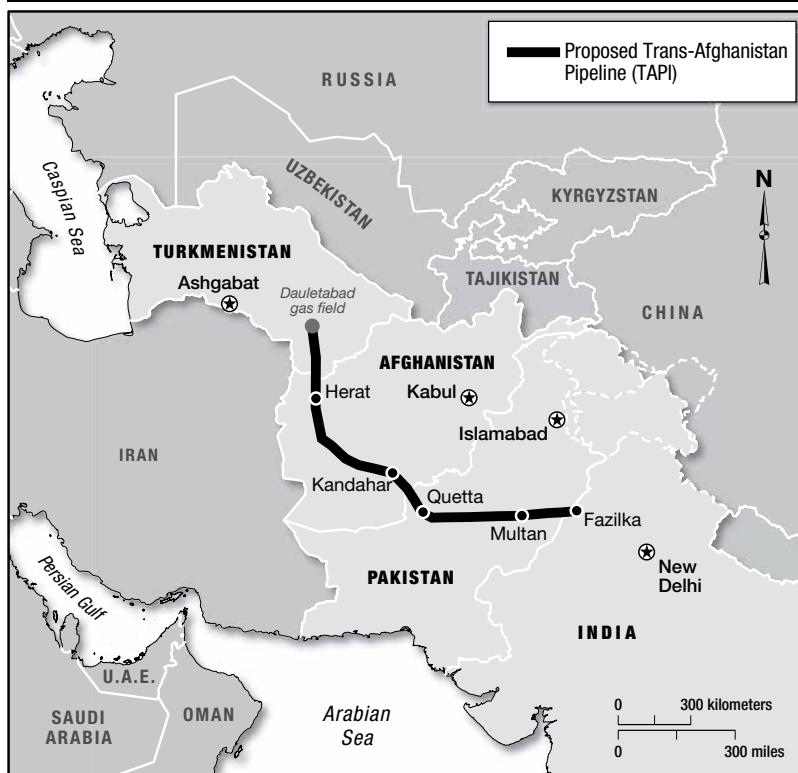
Geospatial models can be complex, with many associated submodels or collateral models. Figure 20.1 presents a geospatial model of a complex system—the Trans-Afghanistan pipeline (also known as the Turkmenistan-Afghanistan-Pakistan-India pipeline, or TAPI). TAPI is proposed to carry natural gas from fields in Turkmenistan to customers in Pakistan and India. Construction on the 1,700-kilometer, \$10 billion project started in Turkmenistan on December 13, 2015. The pipeline was still under construction in 2022, amid continuing uncertainty following the Taliban takeover of Afghanistan. The pipeline itself is a complicated system that includes a number of political issues (implementation agreements that have to be executed; the requirement for an unprecedented level of cooperation among traditionally hostile powers in the region); technical issues (specific route selection; design and construction of the pipeline); security issues (the pipeline is an obvious target for terrorists); and economic and commercial issues (pricing terms for gas; agreements regarding which companies and intermediaries get what benefits). When built and in operation, the pipeline will significantly change the economies in the region by providing investment and trading opportunities.

The effects of such a pipeline will reach far beyond South Asia. Commercial firms that stand to gain or lose from it are probably conducting their own

intelligence efforts. The pipeline will reshape the patterns of gas distribution worldwide—more gas will flow to customers in South Asia, and less to other regions. So governments (and their intelligence services) worldwide—not just in South Asia—are interested in the progress because of its political, economic, and military implications. The relevant system for analysis in this example is global and complex.⁷

Figure 20.1 shows a simple structural view of the system.⁸ A functional view would address the economic changes the pipeline would cause. A process model could show the patterns of gas extraction and delivery, the political processes to reach a pipeline agreement, and the security processes to protect it, among others. These topics involve political, military (for example, pipeline security), economic, social, and infrastructure models. As discussed in chapter 10, there are many possible submodels or collateral models of the system.

FIGURE 20.1 ■ Trans-Afghanistan Natural Gas Pipeline



Source: Public domain map produced by the US Government Energy Information Administration (2015), http://199.36.140.204/countries/analysisbriefs/India/images/natural_gas_infrastructure_map.png.

Another type of geospatial model is usually represented as static, primarily because it tends to change relatively slowly. It's called human terrain modeling.

Human Terrain Modeling

The US Army, in Iraq and Afghanistan in the decade from 2005 to 2015, piloted a program to refine a type of static geospatial model that had been used in the Vietnam War, though its use dates far back in history.⁹ In combating an insurgency, military forces need to develop a detailed model of the local situation, including political, economic, social, and infrastructure information, as well as military force information. In Iraq, that meant acquiring the following details about each village and town:

- The boundaries of each tribal area (with specific attention to where they adjoin or overlap)
- Location and contact information for each sheik or village mukhtar and for government officials
- Locations of mosques, schools, and markets
- Patterns of activity such as movement into and out of the area; waking, sleeping, and shopping habits
- Nearest locations and checkpoints of security forces
- Economic driving forces including occupation and livelihood of inhabitants; employment and unemployment levels
- Anti-coalition presence and activities
- Access to essential services such as fuel, water, emergency care, and fire response
- Local population concerns and issues¹⁰

Known as the Human Terrain System, the program originated as an experimental effort to embed academic social scientists with military units to improve local socio-cultural knowledge. It quickly expanded to a total of thirty-one teams in Iraq and Afghanistan. A team of five to nine people typically included a leader with military background, two social scientists drawn from academia, and data gatherers and classifiers.¹¹

The American Anthropological Association criticized the program primarily because of ethical concerns. First, the association's code of ethics requires that groups being studied must give "informed consent." Second, the association had concerns about the research's potential for use in targeting the enemy, an act that is antithetical to its ethical standards.¹²

Despite the criticism, the program reportedly had positive results both in military effectiveness and in reducing civilian casualties. Four studies based on interviews with military commanders concluded that it resulted in less use of destructive force and more effective use of counterinsurgency operations.¹³ One anthropological scholar who participated in the program reinforced those conclusions, commenting that “my job is to present what the population wants and expects, how it will react, and at all times promote nonlethal options.”¹⁴

The US Army officially terminated its Human Terrain System program in 2015, but it appears to have been re-formed and operates under the new name Global Cultural Knowledge Network. Military forces now generally consider human terrain modeling to be an essential part of planning and conducting operations in populated areas.

Human terrain modeling was a major feature of the “Great Game” in India in the nineteenth century. This was a competition for control of the balance of power and influence in the buffer states between the British and Russian empires. Beginning in 1878, the Intelligence Branch of the Quartermaster General’s Department in India developed human terrain models from various sources, including gazetteers, route books, personality reports, political assessments, and intelligence reports submitted by political and military officials in the field, travelers, and locally engaged clandestine agents.¹⁵ The intelligence reporting allowed the British to keep track of Russian activities in the region and to identify (and occasionally replace) local rulers who were working with the Russians. The term *great game* is attributed to a British intelligence officer in India, but it was popularized by Rudyard Kipling in his novel *Kim*. In Kipling’s book, an intelligence unit called the Ethnological Survey did the human terrain modeling. Human terrain modeling also has a history in supporting international deliberations. Following are two historical examples of its use to support negotiations.

BOX 20.4 THE 1919 PARIS PEACE CONFERENCE

In 1917, President Woodrow Wilson established a study group to prepare materials for peace negotiations that would conclude World War I. Human terrain maps such as the one in figure 20.2 would be important in determining the boundaries of the new nations that were to be established at the peace conference. He eventually tapped geographer Isaiah Bowman to head a group of 150 academics to prepare the report. It covered the languages, ethnicities, resources, and historical boundaries of Europe. With support from the American Geographical Society, Bowman directed the production of over three hundred maps per week during January 1919. The resulting product, which Bowman presented at the conference, was a major factor in shaping the boundaries in postwar Europe, for one reason: None of the other attendees had done anything comparable.

FIGURE 20.2 ■ The “Human Terrain” of Europe, 1914

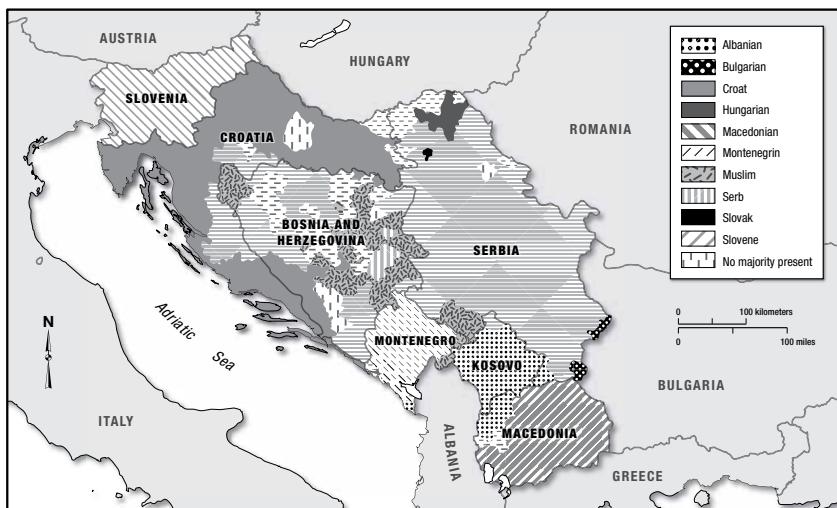
Source: Adapted from "Languages, Peoples and Political Divisions of Europe [1800 to 1914]," <http://www.srpska-mreza.com/MAPS/Ethnic-groups/map-Times-1978.html>.

BOX 20.5 THE DAYTON PEACE ACCORDS

During November 1995, representatives from the warring factions in Yugoslavia met in Dayton, Ohio, to negotiate what would become called the Dayton Peace Accords. The US participants were supported by a team from the Defense Mapping Agency and the US Army Topographic Engineering Center. The team provided, in near real time, the human terrain in the form of maps from the CIA and other sources of the disputed Balkans areas that included cultural and economic data. Three-dimensional imagery of the disputed areas permitted cartographers to guide negotiators on a virtual tour of the terrain. Figure 20.3 illustrates the sort of product provided in support of the negotiations.¹⁶

The Tools of Human Terrain Modeling

Today, human terrain modeling (or, in its most recent iteration, the Global Cultural Knowledge Network) is used extensively to support military operations in the Middle East. Many tools have been developed to create and analyze such models. The ability to do human terrain mapping and other types of geospatial modeling has been greatly expanded and popularized by commercial products such as Google Earth and Microsoft's Virtual Earth. Multiple layers of information are provided in the form of collateral models (as discussed in chapter 10) that include details about a

FIGURE 20.3 ■ The 1991 “Human Terrain” of Former Yugoslavia

Source: Public domain map produced by CIA in 1992. Accessed at <http://www.lib.utexas.edu/maps/europe/yugoslav.jpg>.

location such as building photographs, three-dimensional models of buildings, virtual tour videos that include interaction with locals, and textual material. It is an easy step to include detailed models of the building interiors, including blueprints or CAD/CAM models. This unclassified online material has several intelligence applications. For intelligence analysts, it permits planning for HUMINT and COMINT operations. For military forces, it supports precise targeting. For terrorists, it facilitates planning of attacks.

DYNAMIC GEOSPATIAL MODELS

Dynamic geospatial modeling and analysis are often described using terms that emphasize specific features of the basic concept. Three that are commonly used in intelligence are described in this section: movement intelligence, activity-based intelligence, and geographic profiling. Though they are related, each has a somewhat different meaning. Intelligence enigmas are also included in this discussion as dynamic modeling helps in understanding them as well.

Movement Intelligence

The term *movement intelligence* for a specialized intelligence product dates roughly to the wide use of two sensors for area surveillance during the 1990s. One was the moving target indicator (MTI) capability for synthetic aperture radars. The other was the

deployment of video cameras on intelligence collection platforms. Movement intelligence (usually referred to as MOVINT) can be defined as “an intelligence gathering method by which images (IMINT), non-imaging products (MASINT), and signals (SIGINT) produce a movement history of objects of interest.”¹⁷

MOVINT therefore relies heavily on the collection of what is called wide-area motion imagery, which can be obtained from certain types of electro-optical imagers or synthetic aperture radars. Wide-area motion imagery provides high-resolution images that allow, for example, tracking of vehicle and pedestrian movements across a large city. For smaller areas of coverage, full motion video (FMV) provides movement intelligence. But MOVINT depends on more than the detection of motion and change within an area. It also requires prior detailed knowledge of the terrain (to include urban areas) and the normal behavior of targets that move on that terrain. Sometimes it also requires knowledge of activity both on and *above* the terrain, drawn from a combination of imagery and other intelligence sources. Such was the case in understanding the events surrounding the tragedy of Malaysia Airlines Flight MH17.

BOX 20.6 MALAYSIA AIRLINES FLIGHT MH17

Figure 20.4 shows an example that fits into the MOVINT definition, relying as it does on search radar and communications as well as imagery. On July 17, 2014, Malaysia Airlines Flight MH17, en route from Amsterdam to Kuala Lumpur, was shot down over Eastern Ukraine, killing all 283 passengers and 15 crew on board. Based on the space-time model shown in the figure and on collateral intelligence, American and German intelligence sources concluded that the aircraft was shot down by pro-Russian insurgents in Ukraine. The collateral intelligence included sensors that traced the path of the missile, analysis of shrapnel patterns in the wreckage, voice print analysis of separatists’ conversations in which they claimed credit for the strike, and photos and other data from social media sites. Images released by the Office of the Director of National Intelligence showed the location of a surface-to-air missile launcher that fired the missile.¹⁸ The figure shows the flight profile of MH17.

A subsequent Dutch investigation concluded that Flight MH17 was shot down by a Buk-M1-2 surface-to-air missile (SAM) likely crewed by Russian military personnel. Photographic and video evidence, along with witness interviews, indicate that the SAM battery was brought across the border from Russia into Ukraine shortly before the incident.¹⁹

The term MOVINT is less commonly used today, having been absorbed into the concept of activity-based intelligence, described next.

FIGURE 20.4 ■ Flight Profile of Malaysia Airlines Flight MH17

Source: Adapted from "MH17 Flight Route (en)" © User: PM3 / Wikimedia Commons / CC BY 3.0. <http://creativecommons.org/licenses/by/3.0/>. Flight data from Flightradar24; restricted airspace zones as to NOTAMs A1383/14 and A1492/14.

Activity-Based Intelligence

Activity-based intelligence, or ABI, can be defined as “a discipline of intelligence where the analysis and subsequent collection is focused on the activity and transactions associated with an entity, population, or area of interest.”²⁰ ABI is a form of situational awareness that focuses on interactions over time. It has three characteristics:

- Raw intelligence information is constantly collected on activities in a given region and stored in a database for later metadata searches.
- Material is collected without advance knowledge of whether it will be useful for any intelligence purpose (the concept of “sequence neutrality”).
- Any source of intelligence may contribute and be of benefit, including open source (the concept of data neutrality).²¹

Recall from earlier chapters the difference between deductive and inductive logic in intelligence applications. ABI is an example of the inductive approach: developing a model based on the evidence.

The US director of national intelligence has defined ABI as “an inherently multi-INT approach to activity and transactional data analysis to resolve unknowns, develop object and network knowledge, and drive collection.”²² Patrick Biltgen, when a senior engineer in the intelligence and security sector at BAE Systems, described the development of ABI as a result of failure of the traditional intelligence cycle:

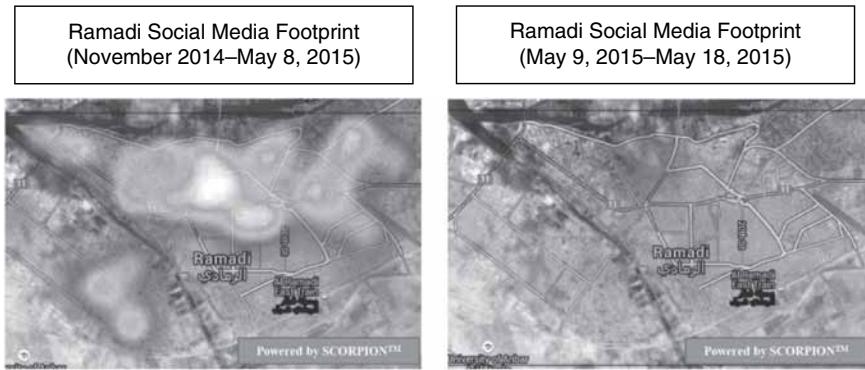
*ABI came out of the realization that the scheduled, targeted, one-thing-at-a-time, stove-piped analysis and collection paradigm was not relevant to non-nation-state and emergent threats. We are breaking this one-thing-after-another paradigm because information is flowing . . . all the time and we don't know what to do with it because if you've stopped to try and collect it, you've missed everything else that's coming.*²³

In this view, ABI is a variant of the target-centric approach, focused on the activity of a target (person, object, or group) within a specified target area—but without an upfront hypothesis. It includes both spatial and temporal dimensions. At a higher level of complexity, it can include network relationships. It differs from the analysis approach discussed in earlier chapters in one important respect: Specifically defining the intelligence issue does not come first. ABI involves discovery of targets of intelligence interest from observations, rather than identifying a specific target and then observing it.²⁴ Opponents are identified by their actions, that is, by temporal and visible activity patterns that indicate hostile or nefarious intent.²⁵ In that respect, ABI differs from pattern-of-life (POL) modeling discussed in chapter 9. While the two concepts are quite similar, POL analysis typically is targeted and collection is done to answer specific intelligence questions derived from a hypothesis. ABI is more akin to the law enforcement officer who walks a beat each day, more recently termed neighborhood policing. The officer, being familiar with the physical and human terrain, can easily spot a suspicious anomaly when it occurs.

Scott White, former associate deputy director of the CIA, has observed that “ABI is not a new concept. It’s been used in the past in the Intelligence Community.”²⁶ In fact, SIGINT, MASINT, and IMINT were used together for decades to monitor the normal activity patterns at Soviet missile test sites; deviations from the norm indicated possible missile test launch preparations. The intelligence enigmas (introduced in chapters 12 and 13 and discussed at the end of this chapter) undoubtedly were the targets of ABI modeling to identify their purpose. The difference is that today imagery surveillance of an area is possible, whereas in the past only reconnaissance was possible—and this still is the case in denied areas where UAVs cannot operate. Many targets of ABI—non-state actors such as criminal networks and insurgent groups—don’t have the protection of operating in areas denied to aerial surveillance.

Social media has provided a powerful tool for modeling behavior in space and time, especially for ABI. Such dynamic models can identify patterns of sentiment such as pro-Taliban or anti-Shiite attitudes in a region. ABI can also tip off major population shifts, such as the flight from Ramadi, Iraq, during fighting there, as illustrated in figure 20.5. In this case, the ABI product is based entirely on social media. While imagery is often used in ABI, it is not essential.

FIGURE 20.5 ■ Population Flees Ramadi, 2015



Source: These analytic insights are courtesy of SCORPION social media analytics software developed by Courage Services, Inc.

Though the term ABI is of recent origin and is tied to the development of surveillance methods for collecting intelligence, the concept of solving intelligence problems by monitoring activity over time has been applied for decades. It has been the primary tool for dealing with geographic profiling and intelligence enigmas, discussed next.

Geographic Profiling

Geographic profiling is a term used in law enforcement for a type of geospatial modeling, specifically to produce a dynamic space-time model that supports investigations of serial violent or sexual crime. Such crimes, when committed by strangers, are difficult to solve. Their investigation can produce thousands of tips and suspects, resulting in the problem of information overload. Geographic profiling—really, a form of ABI modeling—provides police with an effective method of prioritizing and managing the information they collect. The profiling process analyzes the locations connected to a series of crimes to determine the area where the offender potentially lives. The result helps focus an investigation and suggest new strategies to complement traditional methods. The case of the Leeds rapist indicates how profiling can work even with limited offender pattern information.

BOX 20.7 THE LEEDS RAPIST

Criminologist Kim Rossmo is a pioneer in geographic profiling and the developer of crime analysis software. He developed and applied the software to help solve murders and rapes as head of the geographic profiling unit at the Vancouver Police Department, beginning in 1995. Rossmo is currently director of the Center for Geospatial Intelligence and Investigation at Texas State University, where he applies techniques of geographic profiling to crime and counterterrorism.

In 1996, a UK police task force called on Rossmo to help in the search for a man who had abducted and raped five women over a fifteen-year period. A police task force from Leicestershire, West Yorkshire, and Nottinghamshire counties had been searching for the perpetrator for years. The police had DNA from a blood sample; they also had a partial fingerprint belonging to the rapist, but it was insufficient for use in an automated fingerprint search. And they had the locations of purchases that the rapist had made in the Leeds area with a credit card stolen from one of the victims. As Rossmo observed, they were all “routine purchases that you would normally make near where you live.”²⁷

Using the purchase locations in combination with the location of the abductions, Rossmo used his software to develop a geographic profile that zeroed in on two likely areas: the Killingbeck and Millgarth districts of Leeds. Local police accordingly began a manual search of the fingerprint records at the two police stations in those districts. In 1998, after a painstaking search of more than 7,000 records, police found a match to the partial fingerprint. The fingerprint belonged to Clive Barwell, a local lorry driver who had previously been imprisoned for armed robbery. The DNA also proved to be a match, and Barwell subsequently pleaded guilty and received eight life terms.²⁸

Rossmo’s software algorithm relies on known criminal patterns. For example, most crimes are committed near the offender’s home. However, criminals will avoid criminal activity very close to their home, to conceal their identity. So the probability display of a criminal’s activity on a map tends to look like a doughnut, with the offender located somewhere in the “hole.”²⁹

Intelligence Enigmas

Geospatial modeling and analysis frequently deals with unidentified facilities, objects, and activities—or enigmas. These present analysts with an initial difficulty: There is no existing target framework to start from, or at least it cannot be readily identified. For such targets, a static geospatial model—a snapshot in time—is, of course, insufficient. The key typically is to apply ABI techniques—to observe the facility, object, or activity over time and select or construct a target framework therefrom. Two examples, mentioned in earlier chapters, involve targets located in the Soviet Union/Russia: URDF-3 and Yamantau Mountain.

BOX 20.8 URDF-3

During the 1970s, US satellite reconnaissance images of the Soviet nuclear test site at Semipalatinsk showed the construction of an unusual facility. Several possible purposes for it were proposed and discussed within the intelligence community. The facility became a subject of heated debate when US Air Force major general George Kegan in 1977 claimed publicly that the Soviets had constructed a huge particle beam weapon at the site—called PNUTS (Possible Nuclear Underground Test Site) by the Defense Department and URDF-3 (Unidentified Research and Development Facility-3) by the CIA. During the 1970s and early 1980s, the United States expended considerable intelligence and scientific research effort exploring the suspicion that the Soviet Union was building a particle beam weapon capable of destroying ballistic missile warheads in flight.³⁰

After the fall of the Soviet Union in 1991, it was discovered that URDF-3 was in fact an attempt to develop a nuclear thermal rocket similar to the United States' Nuclear Engine for Rocket Vehicle Application (NERVA) project, with the objective of powering space exploration missions. The United States had ended the NERVA program in 1972, so a nuclear rocket development was not one of the alternative models considered by intelligence analysts. Had it been, that probably would have been selected as the most likely explanation, because it was consistent with observations of the facility. As it was, some analysts and scientists called in to consult about the facility force-fit the evidence into the particle beam weapon model—identifying the rocket test stands as beam weapons, the reactor assembly as a nuclear accelerator, and the liquid hydrogen tanks as nuclear pulse generators.³¹

In trying to discern the function of URDF-3, US intelligence committed extensive resources in monitoring activities at the site—to the extent possible. Soviet security services were very good at blocking HUMINT and COMINT targeting, and IMINT could be obtained only by periodic reconnaissance, not by surveillance.

One of the best-known current enigmas (referred to in chapters 12 and 13) has received much attention from the US government for over four decades. It concerns another Russian unidentified facility, Yamantau Mountain in the Ural Mountains.

BOX 20.9 YAMANTAU MOUNTAIN

Yamantau Mountain in the Urals was under construction prior to the end of the Cold War. According to one US official, the complex is “as big as the Washington area inside the Beltway,” or approximately 400 square miles, constructed inside the mountain. Because the facility appears to be hardened to withstand a nuclear attack, US officials reportedly have speculated that it is a survivable command-and-control center, a survivable weapons production center, or a weapons storage area. Because of its location relatively close to Russia’s main nuclear weapons laboratory called Chelyabinsk-70 and the extensive rail network serving the facility, some

observers suspect that the underground complex will be a nuclear warhead and missile storage site.³²

Russia appears to have engaged in a campaign to deliberately mislead the rest of the world about the purpose of the Yamantau Mountain project. Russian officials have made several conflicting claims about the purpose of the facility over the years. Some are far-fetched: that it is a mining and ore-processing complex or an underground warehouse for food and clothing. Others seem plausible: that Yamantau Mountain is to become a shelter for the Russian national leadership in case of nuclear war.³³

Enigmas, at least of the URDF-3 or Yamantau Mountain type, appear less common today, largely thanks to the availability of better geospatial intelligence, especially the application of ABI.

SUMMARY

One of the most widely used analytic models is the geospatial model, which combines all sources of intelligence to provide a geographically oriented picture of a situation. That picture is referred to as geospatial intelligence, or GEOINT. It is most properly defined as the professional practice of integrating and interpreting all forms of geospatial data to create historical and anticipatory intelligence products used for planning or for answering questions posed by decision makers.

Geospatial models are popular in military intelligence for weapons targeting and to assess the location and movement of opposing forces. The models can be static, that is, a snapshot in time—maps and imagery, for example. Static GEOINT products such as human terrain models are used by governments to support military operations and international negotiations. The commercial availability of tools such as Google Earth and Microsoft’s Virtual Earth allows human terrain modeling to support nongovernmental operations as well.

Many geospatial models are dynamic; they include temporal changes. This combination of geospatial and temporal models is perhaps the single most important trend in GEOINT. Dynamic geospatial models are used to observe how a situation develops over time and to extrapolate future developments. There are several terms for dynamic geospatial models that focus on specific features or uses of the basic concept:

- Movement intelligence, or MOVINT, is usually concerned with tracking the movement of an object—a vehicle or person, for example—over time. MOVINT is a less commonly used term today, having been absorbed by the concept of activity-based intelligence.
- Activity-based intelligence, or ABI, is a form of situational awareness that identifies and catalogs interactions of an entity, of a population, or in an area of

interest over time. It is a variant of the target-centric approach that is focused on discovery of targets of intelligence interest based on their activity patterns.

- Geographic profiling is a term used in law enforcement for a specific type of geospatial modeling, where pattern analysis focuses on the locations of criminal activity to identify perpetrators.

Geospatial modeling and analysis of unidentified facilities, objects, and activities, known as enigmas, requires something more than a snapshot in time. ABI, conducted by targeting the facility, object, or activity over an extended time frame, is an effective analytic tool against such targets.

CRITICAL THINKING QUESTIONS

1. Figure 20.5 shows the social media decline in Ramadi in 2015. The figure illustrates the hypothesis that the decline is the result of the population fleeing Ramadi. To some extent, that was the case. What other hypotheses might also explain the decline? Identify and discuss them. (This may require some research.)
2. This chapter cites a concise definition of geospatial intelligence offered by Penn State University professor Todd Bacastow. It differs from the United States' official definition contained in the US Code (10 U.S.C. § 467), which states that “the term ‘geospatial intelligence’ means the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.”
 - a. Select the definition that you believe more accurately describes GEOINT and justify your choice.
 - b. Now, take a devil’s advocate position. Justify why the other definition is preferable.
3. The 10 U.S.C. § 467 definition of geospatial intelligence contains an exclusion in its definition of “imagery,” stating that “such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations.” It does not, however, exclude other handheld photography—large amounts of which are available online, for example, in Facebook or Google Earth. Why the apparent inconsistency? In your opinion, should there be a distinction? Why or why not?
4. Having read this chapter, can you craft a definition for GEOINT that is better than the other two cited?

NOTES

1. Report Submitted by the Government of the Federal Republic of Germany to the German Bundestag on 15 February 1989 concerning the Possible Involvement of Germans in the Establishment of a Chemical Weapons Facility in Libya (English version provided by the Embassy of the Federal Republic of Germany to the United States, 1989), 9.
2. Sun Tzu, *The Art of War*, ed. James Clavell (New York, NY: Dell Publishing, 1983), 9.
3. Todd Bacastow, "What Is Intelligence and What Is Geospatial Intelligence," in *The Learner's Guide to Geospatial Intelligence*, Department of Geography, Penn State University, <https://www.e-education.psu.edu/sgam/node/91>.
4. Walter Laqueur, *The Uses and Limits of Intelligence* (Somerset, NJ: Transaction Publishers, 1993), 43.
5. Though one part of the model is dynamic (tides change level over the course of a day), the overall model is static.
6. US Navy, *Naval Doctrine Publication 2: Naval Intelligence*, no date, <https://apps.dtic.mil/sti/pdfs/ADA291749.pdf>.
7. Marc Grossman, "The Trans-Afghan Pipeline Initiative: No Pipe Dream," *YaleGlobal* 28 (August 2014), <http://yaleglobal.yale.edu/content/trans-afghan-pipeline-initiative>.
8. BBC News, "South Asia Gas Pipeline Talks End," July 13, 2005, http://news.bbc.co.uk/1/hi/world/south_asia/4674301.stm; Shamila N. Chaudhary, "Iran to India Natural Gas Pipeline," TED Case Studies, 11, no. 1 (January 2001).
9. US Department of Defense, Defense Science Board, "Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations," February 2011, 58, <https://dsb.cto.mil/reports/2010s/ADA543575.pdf>.
10. Jack Marr, John Cushing, Brandon Garner, and Richard Thompson, "Human Terrain Mapping: A Critical First Step to Winning the COIN Fight," *Military Review* (March-April 2008): 18–24.
11. Brian R. Price, "Human Terrain at the Crossroads," *National Defense University Joint Force Quarterly* 87, October 1, 2017, <http://ndupress.ndu.edu/Publications/Article/1325979/human-terrain-at-the-crossroads/>.
12. Scott Jaschik, "Embedded Conflicts," *Inside Higher Ed*, July 7, 2015, <https://www.insidehighered.com/news/2015/07/07/army-shuts-down-controversial-human-terrain-system-criticized-many-anthropologists>.
13. Price, "Human Terrain at the Crossroads."
14. Jaschik, "Embedded Conflicts."
15. Penelope Tuson, *British Intelligence on Russia in Central Asia, c. 1865–1949* (Leiden, Netherlands: Brill, 2005), <http://www.brill.com/british-intelligence-russia-central-asia-c-1865-1949>.
16. National Geospatial-Intelligence Agency, "Dayton Accords," in *The NGA in History*, no date, https://www.nga.mil/defining-moments/Dayton_Accords.html.

17. Erik P. Blasch, Stephen Russell, and Guna Seetharaman, "Joint Data Management for MOVINT Data-to-Decision Making," 14th International Conference on Information Fusion, Chicago, Illinois, July 5–8, 2011, 176, <https://apps.dtic.mil/sti/pdfs/ADA562579.pdf>.
18. Greg Miller, "U.S. Discloses Intelligence on Downing of Malaysian Jet," *Washington Post*, July 22, 2014, http://www.washingtonpost.com/world/national-security/us-discloses-intelligence-on-downing-of-malaysian-jet/2014/07/22/b178fe58-11e1-11e4-98ee-daea85133bc9_story.html.
19. Reuben F. Johnson, "Dutch Investigation Concludes MH17 Downed by Buk Missile from Russian Battery," *IHS Jane's 360*, March 19, 2015.
20. Gabriel Miller, "Activity-Based Intelligence Uses Metadata to Map Adversary Networks," *Defense News*, July 8, 2013.
21. Ibid.
22. Office of the Director of National Intelligence, "Proposed ODNI Activity-Based Intelligence [ABI] Lexicon," August 2013.
23. Miller, "Activity-Based Intelligence Uses Metadata."
24. Note, though, that you must still identify a general target; the definition of ABI requires identifying an "entity, population, or area of interest."
25. Edwin C. Tse, Chief Technologist, Ground Systems Business Unit, Office of Technology, Northrop Grumman Information Systems, "Activity Based Intelligence Challenges," PowerPoint presentation to the IMSC Spring Retreat, March 7, 2013.
26. Kristen Quinn, "A Better Toolbox," *Trajectory* (Winter 2012): 11–15.
27. João Medeiros, "How Geographic Profiling Helps Find Serial Criminals," *Wired*, November 10, 2014, <http://www.wired.co.uk/article/mapping-murder>.
28. Ibid.
29. Ibid.
30. John Pike, "The Death Beam Gap: Putting Keegan's Follies in Perspective," Federation of American Scientists, October 1992, <https://spp.fas.org/eprint/keegan.htm>.
31. Michael Dobbs, "Deconstructing the Death Ray," *Washington Post*, October 17, 1999, F01.
32. Michael R. Gordon, "Despite Cold War's End, Russia Keeps Building a Secret Complex," *New York Times*, April 16, 1996, <http://www.nytimes.com/1996/04/16/world/despite-cold-war-s-end-russia-keeps-building-a-secret-complex.html>.
33. Yamantau Mountain Complex: Beloretsk, Russia, http://thelivingmoon.com/45jack_files/03files/Yamantau_Mountain_Complex_Russia.htm.

Part III has established one point: anticipatory analysis is difficult to do. Fortunately, there is a powerful mechanism for dealing with difficult problems: simulation modeling. The preceding chapters described four powerful analytic approaches: scenarios, systems models, relationship models, and geospatial models. Increasingly, the analytic engine feeding them is some form of simulation model.

Simulation models are mathematical descriptions of the interrelationships believed to determine a system's behavior. They differ from other types of models in that the equations that constitute them cannot be solved simultaneously. Analysts usually turn to simulations when it is impossible or impractical to measure all the variables necessary to solve the set of simultaneous equations that would fully describe a system.

We often need to determine how something will behave without actually testing it in real life. Simulation models do that. They estimate the performance of real-world analogues under differing conditions to help decision makers choose among alternative actions. For example, outcomes and effects from events such as the detonation of nuclear devices, armed conflicts with insurgents, and environmental pollution contributing to climate change have all been the subjects of simulation models. They also are used to assess the performance of opposing weapons systems, the consequences of trade embargoes, and the success of insurgencies.

A typical example of a simulation model is EMBERS (Early Model Based Event Recognition using Surrogates), developed for the US intelligence community. EMBERS was designed to support anticipatory intelligence for national-level decision making. Using open-source searches, it has given advance warning of civil unrest events, disease outbreaks, and election outcomes.¹

In general, simulation models are most useful in making long-range forecasts where exact numerical estimates are not needed. They usually are most effective when used to compare the impact of alternative scenarios (resulting from policy decisions or natural phenomena, for example).

TYPES OF SIMULATIONS

Intelligence analysts have long used simulation models extensively to assess the performance of economies and military forces; more recently they have developed and applied them to social and political systems. These simulations comprise computer programs that solve individual equations or systems of equations and graphically

portray the results. They are interactive because the picture changes as new intelligence information is received and analyzed.

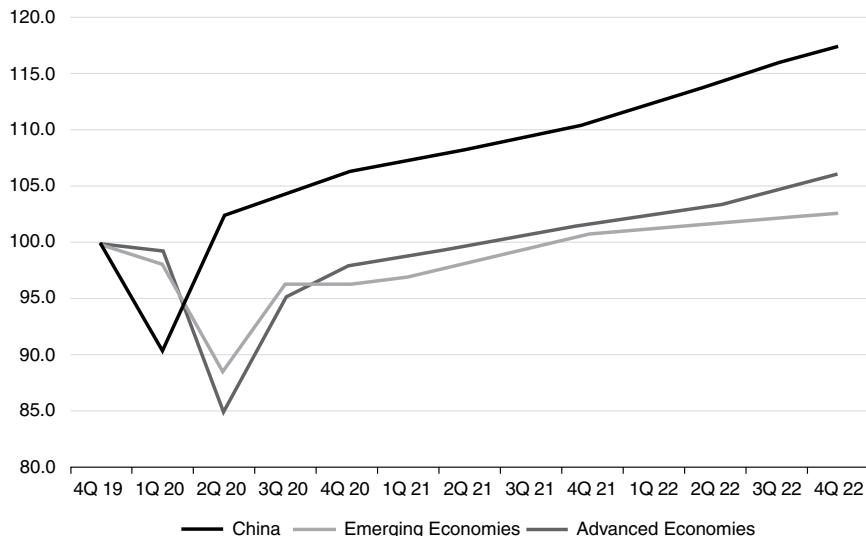
Economic Simulations

Economic, or more properly econometric, models are used to simulate the performance of an entire economy or any segment, for example, of any industry. An econometric model is a quantitative description of an economic system. It incorporates hypotheses on how the target systems function. The models are used widely in both the financial and intelligence communities for assessing trade, balance of payments, and worldwide energy production and distribution.

Figure 21.1 illustrates a typical forecast based on econometric modeling, drawn from International Monetary Fund data. It illustrates the dramatic effect the COVID-19 pandemic had on world economies generally. It also highlights both the rapid impact and rapid recovery experienced by China, compared to both emerging and developing economies and advanced economies.

Intelligence analysts often run econometric models to support trade negotiations. For example, analysts can create a simulation of another country's economy to show that their own government's trade proposals will benefit the other country's economy. A particularly effective technique is to obtain and run the other country's econometric model, since it should be more credible with the opposing negotiation team.

FIGURE 21.1 ■ Expected Growth in GDP for Some Major World Economies



Source: Drawn by the author from the International Monetary Fund's *World Economic Outlook*, January 2021, World Economic Outlook Update, January 2021: Policy Support and Vaccines Expected to Lift Activity (imf.org).

Military Simulations

Two types of military simulations are widely used: weapons systems simulations and wargaming simulations.

Weapons Systems

Weapons systems simulations range in complexity from assessing the performance of a single entity such as an aircraft to that of an elaborate interconnected system such as an air defense system. Even simulating the performance of a single weapon can be a complicated undertaking. For example, the design of a nuclear weapon requires complex modeling and simulation of the weapon detonation process. High-speed supercomputers and sophisticated simulation codes are necessary. The models used to support one's own nuclear weapons development can be used to assess the performance of another country's nuclear weaponry.

Many simulation models of weapons systems already exist. Commercial models also are available to simulate the performance of radars and communications systems and the orbits of satellites. Both the US and foreign intelligence services, for example, use commercial software to create satellite orbit simulations. These are used in turn to identify the occurrences of unfriendly satellite surveillance to conduct denial by concealing military equipment and formations until the satellite has passed. The US Department of Defense and its contractors also possess a large suite of performance models of missiles, ships, submarines, and air and missile defense systems, all used to evaluate their own systems. These models can be modified to simulate the performance of foreign systems, too. For example, the Backfire bomber case involved two competing simulation models, both derived from existing models of US aircraft.

BOX 21.1 THE BACKFIRE BOMBER SIMULATIONS

Throughout the 1960s, US Air Force intelligence consistently predicted that the Soviets would develop a new heavy bomber capable of striking US targets. In 1969, photos of a plant at Kazan revealed the existence of a new bomber, subsequently codenamed Backfire. Two alternative missions for Backfire became the center of an intelligence analysis controversy. Air Force analysts took the position that Backfire could be used for intercontinental attack. CIA analysts argued the aircraft's mission was peripheral attack—that is, attack of ground or naval targets near the Soviet mainland.

Over the next several years, national intelligence estimates shifted back and forth on the issue. The critical evaluation criterion was the aircraft's range. A range of 5,500 miles or more would allow Backfires to strike US targets from Soviet bases on one-way missions. A range of less than 5,000 miles would not allow such strikes, unless the Backfire received inflight refueling. (The 500-mile range difference in those numbers was a gray area, where the Backfire might or might not reach the

United States.) The answer was important for the US Department of Defense and particularly for the Air Force, because the longer range meant that Backfires were a threat to the United States that would have to be countered.

The Air Force and the Defense Intelligence Agency produced simulations from McDonnell Douglas aerospace engineers that showed the Backfire had a range of between 4,500 and 6,000 miles. The CIA produced estimates from a different set of McDonnell Douglas engineers that showed a range of between 3,500 and 5,000 miles. Each side accused the other of slanting the evidence.

The issue of the range of the Backfire bomber became even more important as it became enmeshed in Strategic Arms Limitation Talks (SALT). A Soviet intercontinental bomber would have to be counted in the Soviet array of strategic weaponry. The Russians eventually agreed as part of the SALT II process to produce no more than thirty Backfires a year and not to equip them for inflight refueling; the United States agreed not to count Backfires as intercontinental bombers. In later years, new evidence made it clear that the Backfire was in fact designed to be a peripheral attack bomber, never intended for intercontinental attack missions.

In weapons systems performance simulations, it can be easy to get lost in the details and lose sight of the main objective. It's a matter of professional pride for engineers to run simulations that compute the thrust of a rocket to within a pound, or to go to fractions of a decibel on radar performance analysis. The customers usually don't care. Sometimes, though, a relatively small performance difference can be critical. In the case of the Backfire bomber, it was.

The Backfire bomber case illustrates some of the analytic traps discussed in chapter 11: premature closure, in that analysts were trapped by previous predictions that the Soviets would develop a new intercontinental bomber, and “cherry picking”—preferring the evidence that supports your hypothesis. It also emphasizes the need for doing multidisciplinary analysis in systems analysis. A serious consideration of Soviet systems designs and requirements, and of what the Soviets foresaw as threats at the time, would likely have led analysts to zero in more quickly on the Backfire's mission of peripheral attack.

The case also highlights a common weapons systems analysis issue: presenting the worst-case estimate. National security plans often are made based on a systems estimate; out of fear that policymakers may become complacent, analysts are naturally inclined to make the worst case that is reasonably possible. In a later example, the WMD Commission noted that “the Intelligence Community made too much of an inferential leap, based on very little hard evidence, in judging that Iraq's unmanned aerial vehicles were being designed for use as biological warfare delivery vehicles and that they might be used against the United States”²—a case of moving to the most disturbing conclusion.

Wargaming Simulations

Wargaming simulations are closely related to weapons systems simulations and often incorporate them. They are used by defense organizations in planning systems

acquisition, for determining force mixes, and for troop training. Some examples are logistics models, vulnerability and weapons effects models, system reliability models, and force-on-force and campaign models that simulate combat between opposing forces. As with weapons systems simulations, the US Defense Department and its contractors rely on military simulations, and they can be adapted to assess foreign military systems as well. When models are designed to simulate combat, the intelligence and military operations communities work together, applying the target-centric approach: The military operations analysts understand their side, the intelligence analysts understand the opponent, and inputs from both are necessary to make the simulation run effectively.

North Korea has long been suspected of having a biological weapons capability that includes agents such as anthrax, smallpox, yellow fever, and hemorrhagic fever. In 2011, US and South Korean civilian and military officials participated in a wargame that simulated North Korean use of biological warfare in an attack on South Korea. The results indicated that an attack on South Korean cities, ports, and airfields would produce a death toll of about one million, mostly civilians, with a higher toll if the disease spread to neighboring countries (including North Korea itself). Based on the analysis, US and South Korean officials made changes designed to detect an attack and mitigate its effects. South Korea now has biological agent detection systems in place and an improved coordination of its military and public health networks. And South Korean soldiers and US troops are vaccinated against anthrax and smallpox.³ The 2011 wargame was military in nature, but it incorporated a social simulation, discussed in the next section.

Wargaming simulations may be moving to real time, and in the process becoming much more than simulations for planning. Suppose that feedback from both intelligence (what the military calls the "red" picture) and operations (the "blue" picture) can be consolidated and displayed for a force commander in real time. Then it is possible to do predictive analysis about an opponent's likely actions and allow the commander to counter them *before they happen*. That was the premise of a concept the Air Force explored in the early part of the twenty-first century, based loosely on the technology described in the 1985 science fiction novel *Ender's Game*.

The concept, called *predictive battlespace awareness*, has been described simply. It "involves those actions required to understand our adversaries to the extent of being able to accurately anticipate his actions before they make them" and even to "understand the enemy to such a level that he could anticipate the enemy's action before the enemy even decides to do it."⁴

This is, in a sense, the gold standard for anticipatory analysis. The concept was shelved by the Air Force, for several reasons having nothing to do with the merits of the idea.⁵ But the technology to do predictive battlespace awareness, not quite there twenty years ago, either is here today or will be soon. On May 1, 2011, President Obama was able, from the White House Situation Room, to observe in real time the operation to take down Osama bin Laden. It's not difficult to imagine taking the situation one step further: where a military commander, or even the president, goes beyond observation to controlling the

operation based on the combination of operational information and anticipatory intelligence. The concept was being tested by the US military in 2021, with the goal of applying artificial intelligence to predict an opponent's moves days in advance.⁶

Social Simulations

Simulations have been developed that search historical patterns, web activity, and social media to warn of possible disasters, disease activity, crimes, and geopolitical events. One such simulation predicted a 2012 cholera outbreak in Cuba a few weeks before the outbreak occurred, based on analyzing past weather and other factors that preceded earlier cholera outbreaks in Africa.⁷ Many law enforcement organizations in the United States and Canada use simulations to identify areas in their cities where crimes are likely to be committed each day.⁸

Social simulations often take the form of models discussed in the previous two chapters: network or geospatial models, or a combination of the two. Let's examine a few examples.

Social Networks

Simulation modeling is a powerful tool in analyzing networks. Carnegie Mellon's *ORA, described in chapter 19, has been used to demonstrate how money, information, disease, or technology can flow through a network.⁹ Simulations can be used to assess the impact on a network of removing one or more nodes, which nodes or links are most important to a network's functioning, and the estimated recovery time of the network after removal of a link or node.

Operation Dark Winter was a bioterrorism exercise conducted June 22–23, 2001, at Andrews Air Force Base in Maryland. It was a scenario exercise that dealt with the challenge of incorporating humans into an exercise by using real people. The basic scenario was this:

With tensions rising in the Taiwan Straits, and a major crisis developing in Southwest Asia, a smallpox outbreak was confirmed by the Centers for Disease Control and Prevention in Oklahoma City. During the thirteen days of the game, the disease spread to 25 states and 15 other countries. Fourteen participants and 60 observers witnessed terrorism/warfare in slow motion. Discussions, debates (some rather heated), and decisions focused on the public health response, lack of an adequate supply of smallpox vaccine, roles and missions of federal and state governments, civil liberties associated with quarantine and isolation, the role of the Department of Defense, and potential military responses to the anonymous attack.¹⁰

The scenario featured riots over vaccine and medical supplies and a collapsing national economy. The government was forced to take desperate measures, including the option to impose martial law.

While Dark Winter was a social network exercise, it did not rely heavily on simulations. If done with current technology, it likely would.

Geospatial

Geospatial simulations take a number of forms. They are used to produce flood models, using high-resolution terrain mapping from laser radar (LIDAR) or synthetic aperture radar (SAR) imagery. They produce trafficability models under different weather conditions. One such model was used to identify optimum locations to build Ebola treatment centers in Liberia during the 2014 outbreak.¹¹

One of the most powerful applications of geospatial simulations comes from combining them with network models such as *ORA. The key is to have geographic coordinates associated with each node in the network model. Then simulations can produce models such as the one of Syrian refugee population movement throughout Turkey shown in figure 21.2.

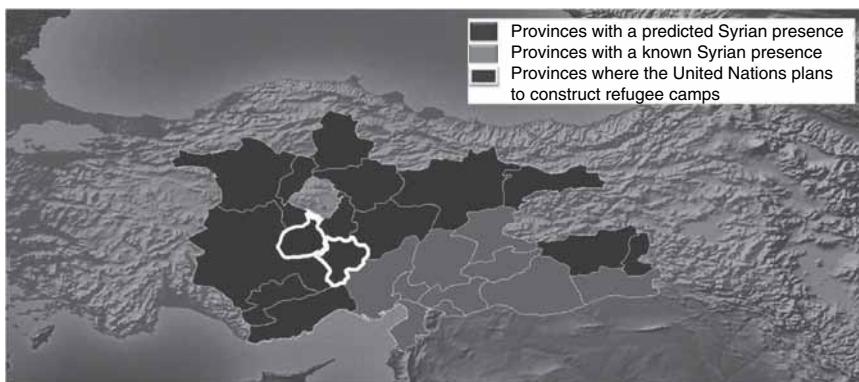
The combination of network and geospatial simulation can provide valuable analytic insights. Figure 21.3, developed in 2014, was remarkably accurate. Based on the results of the simulation, leaders could predict the areas that Syrian refugees were likely to move into during the following one to two years. By 2018, the refugees had moved into those regions and beyond, and the total refugee count in Turkey exceeded 3.5 million.

Compare this to the Ramadi social media footprints from chapter 20, shown in figure 20.5. That figure showed the flight of the Ramadi population, but with no indication of where the population might have gone. This Syrian migration simulation takes a step forward, analytically, in predicting population movement.

FIGURE 21.2 ■ Geospatial Network Simulation of Syrian Refugee Movement within Turkey



Source: Kristan J. Wheaton and Melonie K. Richey, "The Potential of Social Network Analysis in Intelligence," January 9, 2014, <http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/>.

FIGURE 21.3 ■ Estimate of Syrian Refugee Movement over a 12- to 24-Month Period

Source: Kristan J. Wheaton and Melonie K. Richey, "The Potential of Social Network Analysis in Intelligence," January 9, 2014, <http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/>.

Political Simulations

Simulations of political systems analyze such diverse issues as the interactions of political parties, diplomatic initiatives, and clashes of cultures. The CIA has used a simulation model of political processes, named Policon, to assess topics such as these:

- *What policy is Egypt likely to adopt toward Israel?*
- *What will the Philippines likely do about US bases?*
- *What stand will Pakistan take on the Soviet occupation of Afghanistan?*
- *To what extent is Mozambique likely to accommodate with the West?*
- *What policy will Beijing adopt toward Taiwan's role in the Asian Development Bank?*
- *How much support is South Yemen likely to give to the insurgency in North Yemen?*
- *What is the South Korean government likely to do about large-scale demonstrations?*
- *What will Japan's foreign trade policy look like?*
- *What stand will the Mexican government take on official corruption?¹²*

The answers to these questions depend on the decisions of a leader or of the dominant faction in a government. So political simulations typically take the form of decision modeling, as the Policon topics suggest. Intelligence customers want to know, "What decision is that government or organization likely to make?" They also usually

want to know, “How can we get them to make a decision that is more favorable for us?” That is the subject of chapter 22.

It is frequently important to assess the likely behavior of political and military leaders, specifically to determine what decisions they will make under given conditions. The purpose of behavioral analysis is always predictive: How will the target react to a given situation?

To do this sort of anticipatory analysis, simulation models of leadership decision making have been developed and tested over many years. Typically, analysts model the personality, problem-solving styles, values, goals, and environments of individual leaders. One example is Athena’s Prism, developed by the University of Pennsylvania. Athena’s Prism can be configured to identify likely decisions by real-world leaders in different conflict situations, relying on human behavior models from the social sciences.¹³

Decision modeling depends on the inclusion of many factors that are difficult to assess. In all behavioral analysis, but especially in decision prediction, four perspectives have to be considered individually and in combination: rational, administrative, cultural, and emotional.¹⁴ Let’s consider how the decision-making process plays out both for individuals and groups within those contexts.

Rational Models

Wharton business school professor Russell Ackoff, in his entertaining book *The Art of Problem Solving: Ackoff’s Fables*, tells the old story of an appliance manager who claimed that consumers are often irrational. The manager cited examples of new appliances, such as dishwashers (manufactured based on research showing that washing dishes was the most hated kitchen task), that were not selling. Yet recently introduced cooktops and ovens had been very successful, even though they offered no new features and were more expensive than the traditional all-in-one design. Ackoff and the manager agreed to an experiment—they would put the failed products on one side of the room, the successes on the other, and the two would tour the room together with a fresh eye. Almost immediately after entering the room, the manager retracted his assertion about consumer irrationality. He suddenly saw that consumers could use the successful appliances without bending or climbing; conversely, the dishwashers required squatting to load.¹⁵

Though opponents may sometimes be irrational, analysts are better served by assuming they are more often simply misunderstood. Rational decision making is broadly defined as a logical and normally quantitative procedure for thinking through difficult problems. Stated formally, rational decision making requires the systematic evaluation of costs and benefits accruing to potential courses of action. It entails identifying the choices involved, assigning values (costs and benefits) for possible outcomes, and expressing the probability of those outcomes being realized.

A rational model of decision making is based on two interrelated concepts:

- *Optimal choice.* Decision makers will make the choice that will have the best outcome for themselves or their organizations. This assumes that the decision maker is objective and well informed and will, therefore, select the most effective alternative.
- *Expected utility theory.* Decisions are made on an explicit or implicit cost-benefit analysis. The theory's origins are in the study of economic decision making and behavior, notably in the work of John von Neumann and Oskar Morgenstern.¹⁶ An individual faced with a decision will, consciously or subconsciously, identify the available options, the possible outcomes associated with each option, the utility of each option-outcome combination, and the probability that each combination will occur. The decision maker will then choose an option that is likely to yield the highest overall utility.

The following assumptions are embedded in expected utility theory:

- *The decision maker has a number of known alternative courses of action.*
- *Each alternative has consequences that are known and are quantified.*
- *The decision maker has a set of explicit or implicit cost-benefit parameters that will be used to assess the consequences and select an alternative.*¹⁷

Using these assumptions, rational decision simulations attempt to identify the most likely option that a decision maker will select in a given situation. A rational decision estimate, based on expected utility theory, is the place to start any decision simulation, but it is not the end point.

Administrative Models

The rational approach is useful in decision estimates but must be used with caution. We rarely if ever see a national leader, for example, who is truly rational. Leaders won't always make the effort to find the optimum action in a decision problem. The complexity of any realistic decision problem dissuades them. Instead, those in power tend to select possible outcomes that would be "good enough." They then choose a strategy or an action likely to achieve one of the good-enough outcomes.¹⁸

This tendency of leaders to adopt suboptimal choices leads to a variant of the rational decision-making simulation called the administrative model. It discards the three assumptions in expected utility theory and treats decision makers as people having incomplete and even false information, under time pressures, and perhaps beset with conflicting preferences. They consequently look for shortcuts to find acceptable solutions. Decision makers do not try to optimize; instead, they identify and accept a good-enough alternative. The optimal solution is the alternative with the highest

value; but what is called “satisficing” requires no more than finding the first alternative with an acceptable value.¹⁹

There are limits on how well we can simulate (and therefore predict) decisions based on either the rational or the administrative model. To improve decision estimates, we have to consider factors that can cause an opponent’s decision to be labeled as irrational. Cultural and emotional factors are always present and indeed are often dominant.

Cultural Models

Behavior cannot be predicted with any confidence without putting it in the decision maker’s social and cultural context. An analyst needs to understand elements of a culture such as how it trains its youth for adult roles and how it defines what is important in life. In behavioral analysis, culture defines the ethical norms of the collective to which a decision maker belongs. It dictates values and constrains decisions.²⁰ In general, culture is a constraining social or environmental force. Different cultures have different habits of thought, values, and motivations. Straight simulation modeling of a decision-making process without that understanding can lead an analyst into the “irrational behavior” trap, which is what happened to US and Japanese planners in 1941.

BOX 21.2 CULTURAL MIRROR IMAGING: PEARL HARBOR

Before Japan attacked Pearl Harbor, both the United States and Japan made exceptionally poor predictions about the other’s likely decisions. Both sides indulged in mirror imaging—that is, they acted as though the opponent would use a rational decision-making process as *they* defined *rational*.

US planners reasoned that the superior military, economic, and industrial strength of the United States would deter attack. Japan could not win a war against the United States, so a Japanese decision to attack would be irrational.²¹

The Japanese also knew that a long-term war with the United States was not winnable because of the countries’ disparities in industrial capacity. But Japan predicted that a knockout blow at Pearl Harbor would encourage the United States to seek a negotiated settlement in the Pacific and East Asia.²² To validate this assumption, the Japanese drew on their past experience—a similar surprise attack on the Russian fleet at Port Arthur in 1904 had eventually resulted in the Japanese obtaining a favorable negotiated settlement. The Japanese did not mirror image the United States with themselves, but with the Russians of 1904 and 1905. Japan believed that the US government would behave much as the tsarist government had.

Astonishing as it may seem to most Americans, Japanese leadership apparently thought that, with its Pacific fleet crippled or destroyed in a surprise attack, the US government could be persuaded to accept peace terms favorable to Japan.

Such errors in predicting an opponent's decision-making process are common when cultural differences are not taken into account. Cultural factors can cause competitors not to make the "obvious" decision. During the Cold War, US analysts of the Soviet leadership inside and outside the intelligence community—known as Kremlinologists—often encountered a cultural divide in assessing likely Soviet moves. Soviet leader Nikita Khrushchev reportedly disparaged US Kremlinologists, remarking, "They are from a highly educated nation and they look upon us as being highly educated. They don't know that we are dominated by an unimaginative and unattractive bunch of scoundrels."²³ Khrushchev proved his point in his missteps that led to the Cuban missile crisis, leading Sherman Kent to later observe,

No estimating process can be expected to divine exactly when the enemy is about to make a dramatically wrong decision.²⁴

Practitioners in the field of competitive intelligence encounter the same cultural divide when making estimates. US television manufacturers experienced such a surprise during the 1960s. At that time, all TV manufacturers could foresee a glut of TV sets on the market. US manufacturers responded by cutting back production, assuming that other manufacturers would follow suit. Japanese manufacturers, using different assumptions (giving priority to capturing market share instead of maintaining short-term profit), kept up production. As US manufacturers' market share dropped, they found their per-unit costs were rising, while the Japanese per-unit costs were dropping due to economies of scale. The US television set industry has never recovered.

Emotional Models

In the case of many leaders, the emotional factor may be the dominant one. People do many things because they are exciting or challenging. Ackoff told the story of a hand-tool manufacturer whose executive team was eager to get into the business of manufacturing the (then) newly discovered transistor—not because they knew what a transistor was, but because they were bored with their existing business and wanted a new challenge.²⁵ Pride or revenge are also examples of emotional motivators. Business leaders, generals, and even national leaders make some decisions simply because they want to pay back an opponent for past wrongs. The emotional aspect of behavioral prediction cannot be ignored. Personality profiling is one way to grasp it.

Competitive intelligence analysts have developed a methodology for personality profiling of competitors based on the lesson that personal idiosyncrasies and predisposition will have a greater bearing on an executive's decisions than will a calculated assessment of resources and capabilities.²⁶ As one practitioner of the art describes it, an executive who was a linebacker on a college football team will likely have a completely different decision-making style than an executive who was president of the chess club.²⁷

The resulting profile is a model that can be used to assess likely decisions.²⁸ Jerrold Post would likely agree with that approach. The keys that he used in personality profiling of national leaders are summarized in chapter 9.

The Operational Code Model

Alexander George proposed the operational code model for decision making in 1969.²⁹ It attempts to combine many of the different models just discussed, though not necessarily in simulation form. Its original form asked ten questions about a leader's decision-making propensities and core political beliefs. The model relies on identifying two sets of beliefs that drive a decision maker:

- *Philosophical beliefs about the world in which the decision maker operates, and the degree of control the decision maker has over it.*
- *Instrumental beliefs—the norms that shape the decision maker's choice of strategy or tactics and his or her approaches to weighing alternative courses of action.³⁰ Does the decision maker follow the rational, administrative, cultural, or emotional model, some combination, or something entirely different?*

The operational code model was applied in a 2018 assessment of Russian President Vladimir Putin. It concluded that he was fundamentally driven by a desire for order, and his greatest fear was a breakdown in that order that would lead to chaos and his loss of power. Therefore, his decisions, especially concerning terrorist groups and dissidents, would be shaped by that fear. It also noted that his attitude toward three western states and organizations—the United States, the European Union, and NATO—had moved in a steadily more hostile direction since 2014. His consequent actions regarding Ukraine, it concluded, would be more opportunistic than strategic.³¹

Group Decision-Making Models

Most major decisions of intelligence interest will be made by one person—typically a military leader or dictator. But key decisions are also made by groups, especially in democracies and oligarchies. Such cases require a collective decision-prediction approach. It is somewhat easier to estimate what a group will decide versus an individual—which is not to say that it is easy.

The collective decision-making model has been referred to simply as a political model. Its dominant assumptions are that

- Power is decentralized; therefore,
- In place of a single goal, value set, or set of interests of a single decision maker, there exist multiple and often competing goals, values, and interests among the decision makers; therefore,
- Decisions result from bargaining among individuals and coalitions.

Collective decision-making is a complex process of conflict resolution and consensus building; decisions are the products of compromises.³² Despite this complexity, simulations have been created to estimate the likely outcome of group decision making. One approach is based on the theories of social choice expounded by the Marquis de Condorcet, an eighteenth-century mathematician. He suggested the prevailing alternative should be the one that is preferred by a majority over each of the other choices in an exhaustive series of pairwise comparisons. Another technique is to start by drawing an influence diagram that shows the persons involved in the collective decision. Collective decisions tend to have more of the rational elements and less of the emotional. But unless the decision participants come from different cultures, the end decision will be no less cultural in nature.

Game Theory

Game theory is another powerful tool for decision modeling. It is a branch of the discipline operations research, covered in chapter 22. In brief, game theory is about analyzing the decision processes of two or more parties (referred to as the “players”) in conflict or cooperation.

It assumes the existence of two or more interdependent player strategies. The players must determine how the others likely will respond to their current or previous move. They next determine how they will respond to the predicted move of the other players, and the game cycle of action and response continues as a series. The idea is for the players to anticipate how their initial decisions will determine the end result of the game, much like a chess master does. Using this information, each player identifies an initial preferred decision.

The success of game theory depends on understanding the decision processes of the other players. It usually assumes that the other players will follow a rational decision process. When that is not the case, proponents of cultural and emotional models would assert that it becomes important to place yourself in the shoes of the other players, to understand their cultural perspective or emotional makeup. New York University professor Bruce Bueno de Mesquita, the most prominent figure in applying game theory to intelligence issues, argues otherwise. Over a thirty-year period, he has developed and refined a simulation model that applies game theory to produce political estimates. His method for assessing a leader’s decisions is straightforward but controversial among traditionalists. According to one interviewer:

When analyzing a problem in international relations, Bueno de Mesquita doesn’t give a whit about the local culture, history, economy, or any of the other considerations that more traditional political scientists weigh. In fact, rational choicers like Bueno de Mesquita tend to view such traditional approaches with a condescension bordering on disdain. . . . His only concern is with what the political actors want, what they say they want [often two very different things], and how each of their various options will affect their career advancement.³³

Bueno de Mesquita's estimates have an impressive success record:

- Five years before the death of Iran's Ayatollah Khomeini in 1989, he identified Khomeini's successor, Ali Khamenei.
- In February 2008, he predicted correctly that Pakistan's president, Pervez Musharraf, would be forced out of office by the end of summer.
- In May 2010, he predicted that Egypt's president, Hosni Mubarak, would be forced from power within a year. Mubarak left the country nine months later, amid massive street protests.³⁴

His forecasts are not always on target—no predictive simulations are. But he reportedly has produced many accurate political estimates as a consultant for the US Department of State, the Pentagon, the US intelligence community, and several foreign governments.³⁵

As the above examples illustrate, game theory can be used to assess political outcomes. Opponents can apply it as well, and intelligence has a role in identifying the opponent's game moves. Edieal J. Pinker, a Yale University professor of operations research, applied game theory to the P5+1-Iranian negotiations (see chapter 18) and developed a hypothesis about the Iranian strategy. According to Pinker,

Using game theory, we treat the situation as a leader/follower game, like chess, where opponents take turns moving. The first move goes to the West: to choose a threshold for action. The second move goes to Iran: to choose how to manage its weapons development program, taking into account the West's threshold for action.

What is Iran's best strategy, assuming that it wants to develop nuclear weapons? If you're Ayatollah Khamenei and you want to obtain a destructive nuclear military capability, the fastest way to achieve that goal is to do two things in parallel: enrich uranium and develop military delivery systems. But knowing your opponents, the US and Israel, you know that the fastest way is not the best way. You're aware that if you clearly demonstrate your military intentions, they will be forced to attack you. Another piece of intelligence: you know that there isn't very much political support for war in the US, especially in the wake of the recent conflicts in Afghanistan and Iraq. Your strategy, therefore, is to not cross the threshold that will compel the United States to act forcefully until the last moment possible.

Therefore your best choice is the slower choice: First, you declare that you are enriching uranium solely for peaceful purposes, like generating energy and providing nuclear materials for treating cancer patients. Second, you refrain from weaponizing the uranium until the very last moment possible. Since your enemies have already shown that they are reluctant to attack, if you don't step across their threshold, you can continue your nuclear program. Once you are ready, you will need to make a mad rush to complete the final steps toward a weapon before the US and Israel react.³⁶

The Pinker hypothesis illustrates the value of game theory in assessing the motivation behind an opponent's actions. Interestingly, Bueno de Mesquita in 2008 ran a

game theory simulation, using rational choice assumptions, that came to a different conclusion; it predicted Iran would reach the brink of developing a nuclear weapon and then stop as moderate elements came to power.³⁷ The part about moderates coming to power did occur when Hassan Rouhani assumed the presidency in 2013, subsequently losing to a conservative in 2021. So whether Pinker's hypothesis or Bueno de Mesquita's simulation more accurately describes the Iranian situation remains an open question.

USING SIMULATIONS

There are two basic types of simulations: deterministic and probabilistic. Analysts prefer to work with deterministic ones because of their ease of use. They function like a simple spreadsheet; the inputs are fixed. Only one solution appears, and the input numbers must be changed to get another answer. The Backfire bomber simulation could be described as a deterministic simulation: If an analyst knew the key input factors in determining the Backfire's range (such as aircraft weight, fuel load, and engine performance), the simulation would give an exact figure for the range.

Unfortunately, most intelligence questions aren't that simple, and require the second type of simulation. There are always information gaps and that means uncertainty. Analysts typically will not know the exact input numbers, and therefore must use a range of possible numbers. Introduced in chapter 16, one such model has been named the *Monte Carlo simulation*, after the gambling capital of Monaco. The computer "rolls the dice" to assign a value to each uncertain input and obtain an answer. Many repeated "dice rolls" then are made to obtain a range of answers. In the Backfire case, the result was a range of 3,500 to 5,000 miles or 4,500 to 6,000 miles, depending on which simulation was used.

Creating a Simulation

The process of developing and running a simulation is similar to the analysis process described in chapters 3 and 8:

1. Begin by looking at the issue definition discussed in chapter 8. Identify the parts of the overall issue that can best be answered by simulation.
2. Identify simulation packages that will provide the needed answers. Many are available commercially, in academia, or within the government, though they may need customization.
3. Provide the inputs needed for the simulation. In cases where there is not a high-confidence input number, use a probability range (so it's stochastic, not a deterministic simulation).
4. Confirm the simulation model's validity. It must accurately reflect what it is supposed to simulate. If possible, use a proven, validated model; that is, one that has had its simulations checked repeatedly against real-world results.

Running a Simulation

Analyzing the results of any modeling effort requires a “sanity check.” Examining the results to see if they seem reasonable may be the best possible confirmation available. If the results seem questionable, look again at the inputs. A valid model can give invalid results if the inputs are not chosen properly. Econometric models, for example, can give almost any desired simulation result simply by choosing different inputs. A smart customer of intelligence knows this and will want to know not only what model was used but also what the inputs were.

Red team analysis of the finished analytic product was discussed in chapter 14. It’s especially important to apply to decision modeling simulations. The idea of red team analysis in this case is similar: to put the team in the role of the decision-making individual or group (the target). The methodology can be used to guide a simulation or to check the results.

The process requires that a person or team with detailed knowledge of the situation and understanding of the target’s decision-making style put themselves in the target’s circumstances and react to foreign stimuli as the target would. For that reason, it is especially useful for checking the results of a game theory decision model. The CIA’s tradecraft manual recommends these steps for performing red team analysis of a decision estimate:

- Develop a set of “first-person” questions that the adversary would ask, such as: “How would I perceive incoming information; what would be my personal concerns; or to whom would I look for an opinion?”
- Draft a set of policy papers in which the leader or group makes specific decisions, proposes recommendations, or lays out courses of action. The more these papers reflect the cultural and personal norms of the target, the more they can offer a different perspective on the analytic problem.³⁸

SUMMARY

Simulations have long been a powerful tool to assess the capabilities of an opponent’s military hardware such as aircraft, tanks, and naval vessels. Today they are used to assess the performance of larger systems—air defense systems or entire economies, for example.

Most simulation models are systems of equations that must be solved for different input assumptions. There are several steps involved in simulation modeling, but the critical ones are to define the issue, validate the model (ensure that it approximates reality), select appropriate measures of effectiveness for the output, and properly choose the inputs.

Simulation modeling can range in complexity from a simple equation to a sophisticated econometric model. Many types of simulation models are used in intelligence, but the major ones are as follows:

- Econometric models, used to assess international economic activity, or the performance of a national economy or some sector of the economy
- Weapons systems models, used to assess the performance of major foreign weapons systems or specific subsystems
- Wargaming models, used to simulate military operations
- Network models, used to identify the results of likely actions against the network
- Geospatial models, used in a wide range of military, government, and commercial applications
- Political and social simulation models, used to identify likely leadership actions, unrest or instability, and election outcomes, among others

Simulation modeling is used to predict the decisions of government leaders and leadership groups. Such models must accurately capture the personality, problem-solving styles, values, goals, and environments of individual leaders or of collective leadership. To do that, they typically consider four aspects of the decision process: rational, administrative, cultural, and emotional factors. The cultural and emotional factors are difficult to take into account, yet they can dominate in the decision-making process.

Game theory is a powerful tool for decision modeling. It is used to analyze the decision processes of players in either conflict or cooperative efforts. It can be applied as a thought exercise. Because it makes use of mathematical models, it is frequently used in simulations.

Red team analysis is a technique for identifying likely decisions by a decision maker. It can be used to guide a decision-modeling process, to check simulation results, or as an independent technique for assessing an opponent's likely actions. It relies on having a person or team with detailed knowledge of the opponent's decision-making style act as a virtual surrogate in reacting to potential events or circumstances.

CRITICAL THINKING QUESTIONS

1. The 2014 estimate of Syrian refugee movement (see figure 21.3) actually took place, to some extent; though as with any estimate, there were some wrinkles. Many Syrians moved on from Turkey to Europe, creating an immigration crisis in the European Union. Identify and assess the forces that led many Syrians to attempt to enter Europe rather than remain in Turkey as the estimate in figure 21.3 indicated.

2. Select a national leader and discuss to what extent the leader's decision making reflects a rational, administrative, cultural, or emotional component—or a combination of these. Justify your choice based on more than one past decision or action taken by that leader.
3. The section on game theory presented the Pinker hypothesis on Iran's nuclear program and the result of Bueno de Mesquita's simulation.
 - a. Prior to doing research on the subject, do you view the Pinker hypothesis or the Bueno de Mesquita simulation as more likely?
 - b. Research the topic to identify current evidence that either hypothesis is more likely to be the case and provide your reasons.

NOTES

1. Heather M. Roff, *Uncomfortable Ground Truths: Predictive Analytics and National Security*, Brookings Institute, November 2020, <https://www.brookings.edu/research/uncomfortable-ground-truths/>.
2. *Report of the Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction*, March 31, 2005, 143, https://fas.org/irp/offdocs/wmd_report.pdf.
3. Yochi Dreazen, "Here's What War with North Korea Would Look Like," Vox, February 7, 2018, <https://www.vox.com/world/2018/2/7/16974772/north-korea-war-trump-kim-nuclear-weapon>.
4. Statement of James G. Roche, Secretary of the Air Force, and General John P. Jumper, Air Force Chief of Staff, to US Senate Appropriations Committee, May 15, 2002.
5. Michael W. Fowler, "The Air Force's Predictive Battlespace Awareness: The Siren Song of Ender's Game," *International Journal of Intelligence and CounterIntelligence* 29, no.1 (2016): 109.
6. Daphne Leprince-Ringuet, "The Pentagon Says Its New AI Can See Events 'Days in Advance,'" ZDNet, August 4, 2021, <https://www.msn.com/en-us/news/technology/the-pentagon-says-its-new-ai-can-see-events-days-in-advance/ar-AAMTuC8?ocid=msedgntp>.
7. Susan Karlin, "Kira Radinsky: Using Machine Intelligence and Data Mining, This Entrepreneur Predicts the Future," *IEEE Spectrum* (June 2015): 25.
8. Tim Mullaney, "Data-Toting Cops," *MIT Technology Review* 118, no. 1 (2015): 61.
9. Kristan J. Wheaton and Melonie K. Richey, "The Potential of Social Network Analysis in Intelligence," January 9, 2014, <http://www.e-ir.info/2014/01/09/the-potential-of-social-network-analysis-in-intelligence/>.
10. Johns Hopkins Center for Health Security, "Dark Winter," https://www.center-forhealthsecurity.org/our-work/events-archive/2001_dark-winter/about.html.
11. David Brown, "Computer Modelers vs. Ebola," *IEEE Spectrum* (June 2015): 62.

12. H. Bradford Westerfield, ed., *Inside CIA's Private World* (New Haven, CT: Yale University Press, 1995), 283.
13. Barry G. Silverman, Richard L. Rees, Jozsef A. Toth, Jason Cornwell, Kevin O'Brien, Michael Johns, and Marty Caplan, "Athena's Prism—A Diplomatic Strategy Role Playing Simulation for Generating Ideas and Exploring Alternatives," University of Pennsylvania, 2005, http://repository.upenn.edu/cgi/viewcontent.cgi?article=1321&context=ese_papers.
14. Jamshid Gharajedaghi, *Systems Thinking: Managing Chaos and Complexity* (Boston, MA: Butterworth-Heinemann, 1999), 34.
15. Russell Ackoff, *The Art of Problem Solving* (New York, NY: Wiley, 1978), 62.
16. Oskar Morgenstern and John von Neumann, *Theory of Games and Economic Behavior* (Princeton, NJ: Princeton University Press, 1980).
17. Col. Lionel R. Ingram, "Models of Organizational Decision-Making," University of New Hampshire, http://lionelingram.com/560_MODELS%20OF%20ORGANIZATION%20DECISION%20MAKING.pdf.
18. David W. Miller and Marin K. Starr, *Executive Decisions and Operations Research* (Englewood Cliffs, NJ: Prentice Hall, 1961), 45–47.
19. Ingram, "Models of Organizational Decision-Making."
20. Gharajedaghi, *Systems Thinking*, 35.
21. Harold P. Ford, *Estimative Intelligence* (Lanham, MD: University Press of America, 1993), 17.
22. Ibid., 29.
23. Dino Brugioni, *Eyeball to Eyeball: The Inside Story of the Cuban Missile Crisis* (New York, NY: Random House, 1990), 250.
24. Sherman Kent, "A Crucial Estimate Relived," CIA, *Studies in Intelligence* 36, no. 5 (Spring 1964): 111–19.
25. Ackoff, *The Art of Problem Solving*, 22.
26. Walter D. Barndt Jr., *User-Directed Competitive Intelligence* (Westport, CT: Quorum Books, 1984), 78.
27. Comment by Michael Pitcher, vice president of i2Go.com, in *Competitive Intelligence Magazine* 3 (July–September 2000): 9.
28. Ibid., 93.
29. Alexander L. George, "The Operational Code: A Neglected Approach to the Study of Political Leaders and Decision Making," *International Studies Quarterly* 13, no. 2 (1969): 190–222.
30. Stephen Benedict Dyson and Matthew J. Parent, "The Operational Code Approach to Profiling Political Leaders: Understanding Vladimir Putin," *Intelligence and National Security* 33, no. 1 (2018): 84–100.
31. Ibid.
32. Ingram, "Models of Organizational Decision-Making."

33. Michael A.M. Lerner and Ethan Hill, "The New Nostradamus," *Good Magazine*, October 4, 2007, <https://www.good.is/articles/the-new-nostradamus>.
34. Clive Thompson, "Can Game Theory Predict When Iran Will Get the Bomb?" *New York Times*, August 12, 2009.
35. "Game Theory in Practice," *Economist*, Technology Quarterly, September 3, 2011.
36. Edieal J. Pinker, "What Can Game Theory Tell Us about Iran's Nuclear Intentions," in *Yale Insight* (Yale School of Management), March 2015, <http://insights.som.yale.edu/i nsights/what-can-game-theory-tell-us-about-irans-nuclear-intentions>.
37. Thompson, "Can Game Theory Predict When Iran Will Get the Bomb?"
38. CIA Directorate of Intelligence, "A Compendium of Analytic Tradecraft Notes," February 1997, http://www.oss.net/dynamaster/file_archive/040319/cb27cc09c84d056b66616b4da5c02a4d/OSS2000-01-23.pdf.

Then-Secretary of State Colin Powell, in a 2004 address on intelligence reform, said that in over forty years of military and government service, he had one rule for his intelligence officers:

Tell me what you know. Tell me what you don't know. And then, based on what you really know and what you really don't know, tell me what you think is most likely to happen.¹

The last part of Powell's guidance was an invitation for the intelligence officer to provide anticipatory intelligence. There are no records of Powell asking the next logical question: "What should I do about it?" Military and government tradition, as indicated earlier in this book, has been to not ask that question of intelligence officers. It calls for an answer in the form of *prescriptive intelligence*, a controversial concept.

But Powell's instruction could have included a question that leaders could—perhaps should—ask of their intelligence officers: "*If I take this action, what is likely to happen?*" And that, if not actually prescriptive, elicits a similar result.

To illustrate the difference between prescriptive intelligence and descriptive and anticipatory intelligence, let's revisit the problem of developing economic sanctions, introduced in chapter 8. The issue decomposition appears in figure 8.4 where the second-level tier shows three boxes: weak areas and vulnerabilities, likely effects of sanctions, and cooperation required from allies. The "weak areas and vulnerabilities" box is descriptive intelligence; it would be used to identify possible sanctions. "Likely effects" is anticipatory and could be used to select a preferred set of sanctions, based on which ones are considered most effective. "Cooperation required" is prescriptive, because it pinpoints actions a policymaker must take in order to get cooperation from other countries and identifies unintended consequences.

Prescriptive intelligence was introduced in chapter 7 as a practice that intelligence professionals have historically, in the military and the national arenas, been warned against. Two reasons are often cited for the warning:

- When analysts provide prescriptive intelligence, they assume responsibility for the outcome if the customer follows the prescription.
- Analysts do not have the same knowledge of nonintelligence factors that decision makers must consider.

The first objection misses a key point: The customer *always* has the final say. The policymaker and the military commander are called decision makers for a reason. The intelligence officer is simply contributing the most complete picture, including unintended consequences, to focus attention on the best possible choice—*excluding* the factors that are uniquely within the decision maker’s purview. Furthermore, as noted in chapter 14, analysts already share responsibility when the customer fails to make use of the intelligence.

The second objection is valid but irrelevant in today’s environment. Customers, analysts, and collectors have become team players out of necessity. They have come to understand and appreciate what each brings to the table in approaching twenty-first-century intelligence issues. Each brings to bear specialized knowledge on the intelligence problem. While the assertion that analysts do not have the breadth of expertise in the policymaking arena remains valid, the opposite is also true: Policymakers do not have expertise or breadth of knowledge on the intelligence side. A shared target model brings together the skill sets from all participants to effectively tackle the problem. It enables synergy, which as chapter 15 observed, is a powerful problem-solver.

Decision makers obviously would like to know, in advance, the likely outcomes of their decisions. Especially the possibilities for unintended consequences. But they seldom have the time and expertise to do the research, modeling, and analysis needed to identify an optimum decision. In contrast, intelligence analysts increasingly have both the tools and the time to do what-if analysis, and to estimate the outcomes of different policies or actions. Bowman Miller, a veteran of the State Department’s Bureau of Intelligence and Research and a faculty member of the National Intelligence University, writes that trusted analysts may become a part of a policymaker’s kitchen cabinet. In his article on thinning the traditional wall between the two, he observes:

- *Policy makers wrestle with complexity, but given their need to come to decisions (and routinely to do so with less information than would be desirable), their urge is to ferret out facts, find simplicity, and, if possible, determine the one best answer.*
- *They hate surprise as much as they do roadblocks. Their desire is to be told how to achieve an objective, not why it appears unachievable.²*

A good illustration of Bowman’s points is presented in chapter 18. Recall the story of Michael Vickers’s success in providing prescriptive intelligence to the customer, Charlie Wilson, about how best to support the mujahedeen insurgency.

Because it can be an effective approach, prescriptive intelligence has been provided by analysts in law enforcement³ and commercial intelligence for years. At the national level, it may not be openly sanctioned or acknowledged for a while—but, as the Vickers case indicates, it has been in practice since as early as the 1980s.

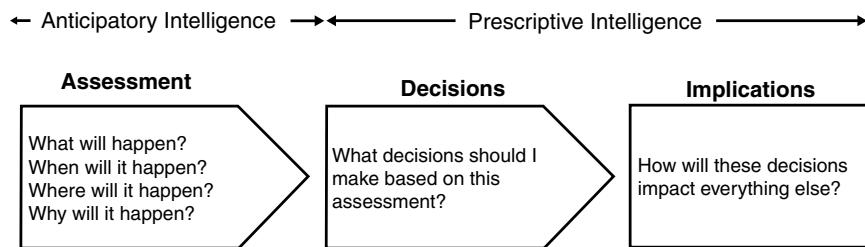
With that introduction, let’s look at the process of producing prescriptive intelligence.

THE PROCESS

Figure 22.1 illustrates the boundaries between anticipatory and prescriptive intelligence, in the form of questions to be answered.

A requisite part of prescriptive intelligence is the identification of unintended consequences. Attempts to assess them require answering the question in the implications block of figure 22.1. This is the feature where the target-centric approach is essential. The customer, receiving inputs on the consequences of a recommended decision, may choose a different one—but customers find it hard to see the unintended consequences associated with that alternative choice. *Unless* the analyst is aware of the alternative and has the opportunity to provide insights.

FIGURE 22.1 ■ Customer Questions in Anticipatory and Prescriptive Intelligence



A number of specialized methodologies are applied in the process for producing prescriptive intelligence. Many have been covered in the previous chapters and are revisited here. But the final product almost always takes the form of a scenario or a set of scenarios.

SCENARIOS

Randolph Pherson noted that every set of scenarios “should include at least one scenario that shows how decision-makers can fashion a future much more to their liking.”⁴ Therefore, the final step in scenario planning, indeed the rationale for it, is for the decision makers to formulate the actions they will take, based on the scenario.⁵ Any of the scenario types discussed in chapter 17 could be useful here. But two are especially relevant.

Normative Scenarios

Recall from chapter 9 that a normative model answers an optimization question—if the decision maker is trying to solve a problem, what is the optimal way to go about it? In intelligence, that means given the possible outcomes from anticipatory analysis,

what is the best (action) option for the decision maker to choose? And the product of a normative modeling effort is, logically enough, a *normative scenario*.

Policymakers often make use of normative scenarios, so analysts must understand their purpose. The normative scenario typically deals with the question of “What outcome do I want to see?” or “What outcome do I want to avoid?” The purpose then is to develop a preferred course of action or, alternatively, to avoid an unfavorable end state. Policymakers or decision makers help begin the process by identifying an outcome such as a stable international political environment, and the analyst works toward a normative scenario to describe the sequence of events by which that ideal could be achieved. Or the customer may identify an unfavorable outcome to avoid (for example, increasing international terrorism and governmental instability) and will want to know the sequence of events that lead to this end state along with points where they can intervene.

An unfavorable end typically takes the form of a *demonstration scenario*.

Demonstration Scenarios

Prescriptive analysis must take into account unlikely events that could have severe adverse effects. To do that, analysts make use of high-impact/low-probability analysis, discussed in chapter 16. It sensitizes customers to the consequences of unlikely developments. The analysis product—a demonstration scenario—describes how such a development might plausibly start and identifies its consequences. It provides indicators that can be monitored to warn that the improbable event is actually happening and show the points where a decision maker can act to avoid that outcome.

In creating this scenario, analysts identify the high-impact outcome and then the plausible paths that could lead to that result. Next, they identify triggering events along the path—events that represent points at which individual decisions or other occurrences shape the outcome. Any later occurrence of such an event indicates that a particular scenario is developing.

The main purpose of this scenario, then, is to focus attention on the *triggering events* rather than on the final outcome. Those are the points where the intelligence customer may be able to act to change the high-impact outcome.⁶ The analyst’s skill at identifying such events determines the value of the scenario.

Perhaps the classic high-impact/low-probability demonstration scenario is contained in Herman Kahn’s appropriately titled book *Thinking About the Unthinkable*, published in 1962. In it, Kahn addresses the likelihood of a global thermonuclear war, the probabilities of surviving it as individuals and as a nation, and the decisions that leaders need to make to keep it from happening. The book was widely read and controversial, and it is still relevant in 2022. The title character in Stanley Kubrick’s 1964 film *Dr. Strangelove* was modeled on Kahn.

OPERATIONS RESEARCH

Operations research (OR) is another discipline that has a long history of prescriptive analysis, with many applications in intelligence.

Operations research is a method of objectively comparing alternative means of achieving a goal or solving a problem and selecting the optimum choice. Its origins and first application were in fact for prescriptive intelligence. In World War II, the Allies had the problem of conducting antisubmarine warfare against German U-boats, which were taking a heavy toll on Allied convoys from the United States to Britain. Analysts examined the effectiveness of searching from aircraft and surface ships, the disposition of escorts around a convoy, and methods of attacking submarines. They subsequently formulated a model of U-boat operations in the North Atlantic and prescribed optimum approaches for conducting search-and-attack missions.⁷ The result was a marked increase in U-boat sinkings and a consequent decrease in convoy losses.

One OR application in prescriptive intelligence has been emphasized throughout this book: defining the problem.

Defining the Problem

Prescriptive intelligence begins in the problem definition stage. The customer frequently has defined the problem poorly and in some cases doesn't really understand it to begin with. But this is where operations research excels.

The discipline of operations research has a rigorous process for defining problems. As one specialist has noted, "It often occurs that the major contribution of the operations research worker is to decide what is the real problem."⁸ Understanding (and addressing) the problem requires examining the environment and/or system in which an issue is embedded, and operations researchers also do that well.

After defining the problem, operations researchers have specialized methods for solving it or, in this context, for providing prescriptive intelligence about it. Two techniques they use are linear programming, for allocating resources, and network analysis, for identifying target vulnerabilities.

Allocating Resources

Since its beginning in World War II, operations research has been applied repeatedly to predict bombing effectiveness, to compare weapons mixes, and to assess military strategies.⁹ In Afghanistan, where IEDs caused the most coalition casualties, operations research was a powerful tool for selecting the best method of countering them.¹⁰

The OR process requires representing the target in mathematical form. That is, the analyst builds a computational model of the target and then manipulates or solves the model to arrive at an answer that approximates how a real-world system should

function. Systems of interest in intelligence are characterized by uncertainty, so this application of operations research commonly relies on probability analysis.

The primary tool for allocating resources is called linear programming. It involves planning the efficient allocation of scarce resources, such as material, skilled workers, machines, money, and time.¹¹ Linear programs are simply systems of linear equations or inequalities that are solved in a manner that yields as its solution an optimum value—the best way to allocate limited resources, for example.

Linear programming is often used in intelligence for estimating foreign production rates, though it has applicability in a wide range of disciplines. During the Cold War, it was used to assess the ability of Warsaw Pact forces to sustain the predicted rates of advance in an attack on NATO forces. As an example, NATO intelligence needed to know the number of trucks that would have to be mobilized from the civil economy to provide necessary support, because the mobilization would be an indicator of an impending Warsaw Pact attack.

Targeting a Physical Network

Network analysis is another OR technique applicable for prescriptive intelligence. Network analysis in operations research is not the same as the process described in chapter 19, where the focus was on relationships among entities. Here, the networks are *physical*. They're typically interconnected paths over which things move. The things can be automobiles (along a network of roads), oil (through a pipeline system), electricity (with wiring diagrams or circuits), information signals (in communications systems), or people (in elevators or hallways).

Against such networks, analysts are frequently concerned with issues such as maximum throughput of the system, the shortest (or cheapest) route between two or more locations, or bottlenecks in the system. The role of prescriptive intelligence is to identify the most vulnerable points of a network for applying pressure, attack, or other countermeasures. Chapter 18 offered the straightforward example of the P5+1 negotiators using network analysis to identify the critical points in Iran's path to a nuclear weapon.

During World War II, Allied planners identified a likely bottleneck in German industries supporting the war effort. Ball bearings were essential in most of the country's weaponry, including their heavy machine guns. Analysis revealed that four plants at Schweinfurt produced most of Germany's supply of ball bearings. So Allied B-17s targeted Schweinfurt in two bombing raids, inflicting heavy damage.

The Schweinfurt raids also illustrate the importance of careful target definition: that is, in this case, looking at the entire target network. Though the Schweinfurt plants were severely damaged, Germany didn't encounter a ball bearing shortage. Allied planners apparently failed to ask their intelligence staff the obvious question: "Does Germany have alternative sources of ball bearings?" In fact, Germany had substantial reserves, along with alternative suppliers in Sweden, Italy, and Switzerland.

SIMULATIONS

Outcome scenarios increasingly are produced by simulations. And simulations have long been used for identifying preferred courses of action in many fields. Let's examine a few of them.

Economic Simulations

The expected impact of sanctions on a country's economy—and the costs to other countries—are complex issues best dealt with by simulation. A typical example is an independent simulation of the effects of the 2019 US decision to renew sanctions on Iranian trade. The simulation found that the international community would "at best partially comply with renewed US sanctions on Iranian crude oil and condensates."¹² Specifically, it found that countries such as Turkey, India, and China would ignore the sanctions, while others would reduce their trade and lobby to have the sanctions ended. The study found that even given that outcome, Iran would suffer financially.¹³ And the Iranian economy did indeed suffer severe contraction in 2019 and 2020 before starting to recover in 2021.

Recall the economic sanctions problem from chapter 8 in which the policymaker stated this problem: "Tell me what I need to know to develop economic sanctions against Iran." A good analyst, as discussed, would have created a decomposition of the issue to answer more specific questions such as "What impact would various types of sanctions have on Iran's economy?" That question clearly calls for a prescriptive response.

Military Simulations

In 2020, the US Air Force played out a simulation for a war scenario with China. It began with a Chinese biological weapon attack in the Indo-Pacific region. The resulting illness disabled US and Taiwanese bases and warship crews in the region. China then followed up with an air and amphibious attack on Taiwan while targeting US bases and warships with missile strikes. The result was the Chinese occupation of Taiwan amid a resounding US defeat.¹⁴ The simulation was prescriptive, in the sense of advocating a better US defense readiness posture.

The challenge of all military simulations, though, is that conflicts are filled with divergent phenomena. And all simulations require approximations. So, the question remains: Are these approximations realistic? Morale, the will to fight, a surprise, a commander's decisions or lack of them, and many other factors cannot be captured adequately in a simulation. In addition, the officers running the simulations often—intentionally or not—assume the opponent will execute its plan perfectly while unrealistically constraining the rules of engagement for their own side. The US response in the 2020 Air Force simulation may in fact have been unrealistically constrained.

Geospatial Simulations

Military simulations rely heavily on geospatial models—especially terrain modeling. But prescriptive geospatial simulations are most widely used in law enforcement and commerce.

GEOINT simulations—especially space-time models—are used for prescriptive policing—that is, using crime prediction analyses to focus law enforcement on crime prevention rather than control. It's well known that criminals tend to commit crimes within their "comfort zone." They repeat the locations, times, and modes of operation that have succeeded in previous experiences.

Law enforcement organizations in the United States and Canada use simulations to identify locations and times at which crimes are likely to be committed each day.¹⁵ These simulations rely on geographic indicators that, in certain combinations, point to an increased risk of crime in a specific area at a specific time. Those results in turn allow police forces to deploy effectively for prevention and control.¹⁶

In the commercial sector, prescriptive geospatial simulations are widely used. For some businesses, location *is* the business—ride-hailing companies, for example. Others, such as telecommunications and transportation companies, have long relied on geospatial intelligence as essential to their operations. Retail firms rely on what is called *location analytics* to understand their geographic markets, assess competitors, and find profitable locations for new stores.

Political and Social Simulations

Political simulations such as Policon, described in chapter 21, do more than predict likely decisions of government leaders. They also identify the factors or forces driving those decisions. Such simulations can be used to identify actions to take, and their timing, to shape an opponent's decisions more favorably.

Chapter 21 also discussed the use of social simulations to search historical patterns, web activity, and social media and provide warning of possible disasters, disease activity, crimes, and geopolitical events. It included an example of a simulation accurately predicting a 2012 cholera outbreak in Cuba that could have been used prescriptively.¹⁷

PREScriptive ANALYTICS

The tools and methodologies discussed in the previous sections fall within the broad category of *prescriptive analytics*. Routinely used in successful businesses, it has a promising future in intelligence because of its ability to deal with big data, introduced in chapter 11.

Prescriptive analytics is derived from the advances in predictive analytics—which only identifies likely outcomes. While predictive analytics can inform analysts of likelihoods and probabilities, prescriptive analytics goes one step further. It identifies

preferred outcomes and the actions that are likely to produce them. It guides or advises analysts and customers by using data from descriptive and predictive analytics to create scenarios that point to the most desirable outcomes. Then it relies on tools such as simulation and optimization to help answer the question, “What should be the next actions we take?

As a general example of how prescriptive analytics works, consider again the wargaming simulation in chapter 21. Predictive analytics indicated in detail the effects of a North Korean biological warfare attack on South Korea. The US and South Korean response, including vaccinating troops and emplacing biological agent detection sensors, was the result of a prescriptive analytics effort.

A major problem that prescriptive analytics must deal with is the amount of incoming raw data. Reports suggest the biggest problem facing the US military today is information overload.¹⁸ National-level policymakers would uniformly agree that the problem is not unique to the military. They deal with it every day. For example, the second action in the preceding paragraph—where to place biological sensors—is a “big data” problem. It could require considering the distribution and daily movement of the Korean population, along with typical weather patterns.

Because it uses big data, prescriptive analytics relies on artificial intelligence techniques, such as *machine learning*: the ability of a computer program to sift through the massive amounts of data it acquires and make judgments based on that data without additional human input. Machine learning finds patterns in large volumes of noisy data, and from those repeated patterns, builds models to apply to new situations.¹⁹ As it receives new data, the software program incorporates it and adapts, far faster than a human could.

In consequence, the computer algorithms improve automatically through experience. Machine learning algorithms build a model based on sample data, known as “training data,” to make predictions or decisions without being explicitly programmed to do so.

Prescriptive analytics also makes use of *natural language processing*, a subfield of linguistics, computer science, and artificial intelligence concerned with the interactions between computers and human language, especially how to program computers to process and analyze large amounts of natural language data.

Thanks to machine learning, software programs now can apply case-based reasoning, discussed in chapter 17. They learn from past patterns and outcomes and apply that knowledge to provide likely outcomes of current situations, including, of course, the preferred ones, along with the actions to take to likely effectuate them.

For example, machine learning has been used to examine trends in social media: applying tools such as probabilistic logic to make predictions about events such as “civil unrest, political elections, economic crises and disease outbreaks” and to “continually monitor data sources 24x7, mine them to yield emerging trends, and process these trends into forecasts.”²⁰

Prescriptive analytics has limits, of course. Machine learning cannot yet identify opportunities to apply synergy. As noted in chapter 15, actions in combination can be more effective than the sum of effects would indicate. An intelligence analyst sometimes must evaluate the likely effects of a given combination of actions and in some cases might even formulate likely combinations for a decision maker. Humans don't easily recognize possible synergy, but at present, we do it far better than machines can.

Also, prescriptive analytics is difficult to apply, not least because it requires a solid understanding of causes and effects.²¹ Causal models, discussed in chapter 15, contain many variables—one of the most important being human behavior. Machine learning, as noted previously, often depends on case-based reasoning, which means that it relies on the previous cases with which it has dealt.

A machine-human partnership, even in its infancy, allows the analyst to consider many factors and a level of complexity that a decision maker would be hard pressed to deal with. But prescriptive intelligence remains a decision-making aid, not a decision maker. It can suggest options and give the decision maker insights, rather than answers. It also can be an effective check on proposed decisions. It's easier to find holes in an argument than it is to construct the argument from scratch. In practice, that often puts the analyst in the position of being a devil's advocate.

SUMMARY

Prescriptive intelligence has long been off limits for military and national-level intelligence officers. But in the target-centric approach, prescriptive intelligence is possible, perhaps even desirable. The customer is part of the process, with the final say on what should be done; and intelligence has unique insights and expertise to bring to the table. The customers of intelligence always want to know the implications of their intended actions, and intelligence analysts are well positioned to identify likely unintended consequences.

The prescriptive intelligence product usually will be a scenario, more often a set of them. They typically include at least a normative one that identifies a preferred outcome or one to avoid. The one to avoid will likely be a demonstration scenario that describes a high-impact/low-probability outcome.

Prescriptive analysis also relies on operations research techniques. Operations research is useful in defining the customer's problem and in assessing vulnerable points in a target. Linear programming is used to examine an opponent's processes and identify critical points. Network analysis is used to define flows and vulnerable points within physical networks such as a communications or transportation network.

Simulations can provide prescriptive intelligence for complex problems where many extrinsic factors must be considered or large volumes of data manipulated. They have been used to address economic, military, geospatial, political, and social issues, among

others. But simulations remain, at best, only approximations of real-world outcomes. The inputs should be vetted carefully for accuracy, and the results for reasonableness.

Prescriptive analytics is the umbrella term for the tools of prescriptive analysis: scenarios, operations research, simulations, and machine learning. It requires the analyst to take a multidisciplinary perspective and consider the forces in play, such as inertia, feedback, and synergy. It therefore draws on the strengths of both information technology and human imagination and intuition.

CRITICAL THINKING QUESTIONS

1. The “Military Simulations” section describes the US Air Force 2020 China scenario. A summary of the scenario is available at <https://americanmilitarynews.com/2021/03/us-will-lose-fast-in-war-with-china-air-forces-simulation-shows-report/>. Can you identify specific areas in which the scenario might have unreasonably constrained either side, or overstated the advantages of the other? (It may be necessary to consult independent sources of information on the China-US balance of power.)
2. The US and international organizations have employed sanctions frequently over the past two decades against Iran, North Korea, China, and Russia, among others. Pick one example of a sanction that had unintended consequences.
 - a. Identify the unintended consequences.
 - b. Describe how those consequences might have been identified in advance.
 - c. Explain how they might have been mitigated in advance by more careful design.

NOTES

1. Colin L. Powell, “Intelligence Reform,” Opening Remarks before the Senate Governmental Affairs Committee, September 13, 2004.
2. Bowman H. Miller, “Intelligence and Policy: The Case for Thin Walls as Seen by a Veteran of INR,” *Studies in Intelligence* 62, no. 2 (2018).
3. US Department of Justice, “Reducing Crime Through Intelligence-Led Policing,” 2006, https://www.ncirc.gov/documents/public/Reducing_Crime_Through_ILP.pdf.
4. Randolph H. Pherson, “Leveraging the Future with Foresight Analysis,” *International Journal of Intelligence, Security, and Public Affairs* 20, no. 2 (2018): 102–31.
5. Avner Barnea and Avi Meshulach, “Forecasting for Intelligence Analysis: Scenarios to Abort Strategic Surprise,” *International Journal of Intelligence and Counterintelligence* 34, no. 1 (2021): 106–33.
6. Herman Kahn and Anthony Wiener, *The Year 2000* (New York, NY: Macmillan, 1967).

7. Brian McCue, *U-Boats in the Bay of Biscay* (Washington, DC: National Defense University Press, 1990).
8. Edward H. Kaplan, "Operations Research and Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, ed. Baruch Fischhoff and Cherie Chauvin (Washington, DC: National Academies Press, 2011), 39.
9. Theodore J. Gordon and M. J. Raffensperger, "The Relevance Tree Method for Planning Basic Research," in *A Practical Guide to Technological Forecasting*, ed. James R. Bright and Milton E. F. Schoeman (Englewood Cliffs, NJ: Prentice Hall, 1973), 129.
10. Ben Connable, Walter L. Perry, Abby Doll, Natasha Lander, and Dan Madden, "Modeling, Simulation, and Operations Analysis in Afghanistan and Iraq," (Santa Monica, CA: RAND Corporation, 2014).
11. Ibid.
12. Carlo Andrea Bollino, Brian Efird, Fakhri Hasanov, and Emre Hatipoglu, "Iran Sanctions: Implications for the Oil Market," May 2019, http://research.sabanciuniv.edu/37396/1/Iran_Sanctions__Implications_for_the_Oil_Market.pdf
13. Ibid.
14. Ryan Morgan, "US Will 'Lose Fast' in War with China, Air Force's Simulation Shows," *American Military News*, March 11, 2021, <https://americanmilitarynews.com/2021/03/us-will-lose-fast-in-war-with-china-air-forces-simulation-shows-report/>.
15. Tim Mullaney, "Data-Toting Cops," *MIT Technology Review* 118, no. 1 (2015): 61.
16. Epifanio Pecharromán, "Crime Predictive Analysis Based on Geointelligence," *International Journal of Intelligence, Security, and Public Affairs* 18, no. 3 (2016): 221–48.
17. Susan Karlin, "Kira Radinsky: Using Machine Intelligence and Data Mining, This Entrepreneur Predicts the Future," *IEEE Spectrum* (June 2015): 25.
18. Thom Shanker and Matt Richtel, "In New Military, Data Overload Can Be Deadly," *New York Times*, January 16, 2011, <https://www.nytimes.com/2011/01/17/technology/17brain.html>.
19. "The Rise of Machine Learning (ML): How to Use Artificial Intelligence in GIS," *GISGeography*, May 15, 2018, <https://gisgeography.com/deep-machine-learning-ml-artificial-intelligence-ai-gis/>.
20. Christopher Eldridge, Christopher Hobbs, and Matthew Moran, "Fusing Algorithms and Analysts: Open-Source Intelligence in the Age of 'Big Data,'" *Intelligence and National Security* 33, no. 3 (2018): 391–406.
21. Carlos Melendez, "Predictive and Prescriptive Analytics Represent the Future of AI—It's Up to Us to Use Them Wisely," *Forbes*, February 11, 2021, <https://www.forbes.com/sites/forbestechcouncil/2021/02/11/predictive-and-prescriptive-analytics-represent-the-future-of-aiits-up-to-us-to-use-them-wisely/?sh=33dc57a95a5d>.

A TALE OF TWO NIES

The two cases discussed in this chapter offer contrasting insights into the process of preparing intelligence estimates in the United States. They are presented here as the basis for a capstone set of critical thinking questions tied to the material discussed throughout this book.

In 1990, the National Intelligence Council produced an NIE—the most authoritative intelligence assessment produced by the intelligence community—on Yugoslavia. Twelve years later, the National Intelligence Council produced an NIE on Iraq's WMD program. The Yugoslavia NIE

- Used a sound estimative methodology
- Got it right
- Presented conclusions that were anathema to US policymakers
- Had zero effect on US policy

The Iraqi WMD NIE, in contrast,

- Used a flawed estimative methodology
- Got it wrong
- Presented conclusions that were exactly what US policymakers wanted to hear
- Provided support to a predetermined US policy

This chapter highlights the differences in analytic approaches used in the two NIEs. Both NIEs now are available online. The full text of the “Yugoslavia Transformed” NIE is available at <https://www.cia.gov/readingroom/docs/1990-10-01.pdf>. In 2014, the CIA released the most complete copy (with previously redacted material) of the original “Iraq’s Continuing Program for Weapons of Mass Destruction” NIE. See https://www.dni.gov/files/documents/Iraq_NIE_Excerpts_2003.pdf.

THE YUGOSLAVIA NIE

The opening statements of the 1990 Yugoslavia NIE contain four conclusions that were remarkably prescient:

- *Yugoslavia will cease to function as a federal state within one year, and will probably dissolve within two. Economic reform will not stave off the breakup.*
- *Serbia will block Slovene and Croat attempts to form an all-Yugoslav confederation.*
- *There will be a protracted armed uprising by Albanians in Kosovo. A full-scale, inter-republic war is unlikely, but serious intercommunal conflict will accompany the breakup and will continue afterward. The violence will be intractable and bitter.*
- *There is little the United States and its European allies can do to preserve Yugoslav unity. Yugoslavs will see such efforts as contradictory to advocacy of democracy and self-determination.¹*

The Yugoslavia NIE is important to examine because it illustrates anticipatory intelligence that uses force field analysis and the creation of alternative target models in the form of scenarios. It took a broad perspective of the issue, considering military, political, economic, and social forces. It also is an example of clear and unequivocal communication to that most difficult of intelligence customers, the policymaker; rarely does an NIE state its conclusions as concisely and powerfully as the four conclusions listed in the opening statement. Finally, the NIE reflected the story of a country torn apart by religious and ethnic divisions, where US policy was to try to keep it together, and where US troops might wind up in harm's way. It is a scenario that continues to have relevance. A similar scenario appeared in the 1980s' US involvement in Lebanon and more recently in Iraq and Syria. The potential for others in some countries exists today.

The Setting

Yugoslavia, a federation of six republics, has had a long history of instability. It was created in the aftermath of World War I, and for political reasons it incorporated three distinct ethnic groups—Serbs, Croats, and Slovenes. Yugoslavia's internal boundaries roughly reflected ethnic and historical divisions, but the population was so thoroughly mixed that it proved impossible to separate the various ethnic groups clearly. This was especially true of the dominant group, the Serbs, who were widely dispersed in the republics. Nationalistic tensions had long plagued the region. Religious divisions added to the problems: The Croats and Slovenes were primarily Roman Catholic, the Serbs were Eastern Orthodox, and Bosnia-Herzegovina and Kosovo had large Muslim populations. However, President Josip Broz Tito ruled Yugoslavia from 1945 until his

death in 1980, and he proved to be very effective at suppressing tensions and keeping the country united.

In 1990, though, Tito had been gone for a decade. The federal central government that was his legacy was not working well. Foreign debt, inflation, and unemployment had created a troubled situation. The economy was faltering, and nationalist pressures were causing increasing instability. In March and April of 1990, Slovenia and Croatia held their first multiparty elections in almost fifty years. In both elections the communists lost to parties favoring national sovereignty within Yugoslavia.

Marten van Heuven was the US national intelligence officer for Europe in 1990. In May of that year, he visited Yugoslavia to assess the situation. He concluded that pressures were building for a collapse of the federation. The ethnic problems alone, he thought, were fast becoming irresolvable. After returning from Belgrade, van Heuven directed the preparation of an NIE on Yugoslavia. It was prepared in two successive drafts. Both included force field analysis, but the two drafts had different target frameworks and consequently came to contrasting conclusions.

First Draft (the “Muddle-Through” NIE)

Van Heuven initially assigned the task of drafting the NIE to a State Department analyst who had extensive background on Yugoslavian and Eastern European affairs. In the first draft, completed during the summer of 1990, the author reviewed the evidence for and against the probability of Yugoslavia’s disintegration and concluded that there was more reason for the republics to stay together than to split apart. The first draft is sometimes referred to as the “muddle-through” NIE because, as van Heuven noted, it predicted that Yugoslavia would somehow muddle through. It identified a number of forces, which had existed for some time, that were working to hold Yugoslavia together. The analytic result was an *extrapolation* based on these forces:

- The threat of Soviet intervention had held Yugoslavia together during Tito’s life and for ten years after his death.
- The numerically dominant Serbs strongly preferred a united Yugoslavia. The officer corps of the Yugoslav National Army (the JNA) was overwhelmingly Serbian and therefore in a position to prevent the nation’s collapse.
- Economic incentives for remaining integrated were strong, since the republics’ economies by themselves were too small to be viable.
- Fear of the future, specifically fear of ethnic and religious conflict, would restrain potential breakaway republics.

Failures in objectivity may have included these factors:

- The US State Department had a vested interest in preserving Yugoslavia as a state (or at least in seeing a peaceful breakup if Yugoslavia could not hold together), an organizational bias that may have shaped the analysis. Wishful thinking may also have played its part.
- One of the forces cited for Yugoslavia staying together was “fear of the future.” But it appears that the fear was on the US side. When a National Security Council staff member told Slovene and Croat officials that a declaration of independence would start a war, they replied, “So what?”
- Finally, in Yugoslavia the United States encountered a different mindset, and ethnocentric biases may have been at work. Both the US culture and its legal system stress religious and ethnic tolerance. The republics of Yugoslavia had a long history of religious and ethnic strife and intolerance. The first NIE draft didn’t appear to take into account this critical force.

Van Heuven was skeptical of the conclusions; they didn’t fit with the situation he had observed in his visit to the region. He wanted to see an alternative model, and he got it in the form of a second draft NIE.

Second Draft (Alternative Projection)

Van Heuven assigned the task of producing a second NIE draft to other experienced observers of events in Yugoslavia, including CIA analyst Harry Yeide, who had served in the region and was intimately familiar with the issues involved. The second NIE draft presented an alternative model, or scenario, of the future. It concluded that the forces that had held Yugoslavia together in the past were now weak or nonexistent; changing forces were acting to tear Yugoslavia apart. Based on those changed forces, the analysis result was a *projection*:

- By 1990, the Soviet threat was gone.
- While the Serbs might prefer to continue the union, the JNA was not inclined to prevent a breakup unless Serbian interests were seriously threatened. It would not intervene in Croatia in any event, since Croatia had no Serbs.
- The breakup made no economic sense for Yugoslavia taken as a whole, as the first draft indicated. But Croatia and Slovenia would be better off economically as independent states.
- Fear of the future was not a factor. The United States may have had a fear of the future, but the breakaway states of Croatia and Slovenia did not.

The second draft incorporated two interrelated forces the first draft did not emphasize: one that had changed dramatically and one that had existed unchanged for a long time but suddenly became dominant:

- President Tito had been much more than just another dictator. The architect of postwar Yugoslavia and the first communist leader to defy Soviet hegemony over Eastern Europe, he had been almost revered by most Yugoslavs. His successors had none of those qualities, and no strong central leadership had replaced him.
- Yugoslavia from its beginning in 1918 had been composed of several distinct populations having ethnic and nationalistic differences, religious divisions, and a history of hostility and suspicion. Tito had handled potential conflicts among these groups with remarkable political skill, but in 1990 he was not a factor.

The final NIE, based on the second draft, took the changed forces into account. It was remarkable in several respects. All the major NIE contributors to the second draft agreed on the facts, and no one took footnotes to the conclusions. (Most NIEs contain footnotes indicating that a segment of the intelligence community disagrees with some of the conclusions.) The results of the second draft, the four predictions quoted at the beginning of this case study, were exceptionally accurate. Yet the NIE had almost no effect on US policy.

The Customer View

From a policymaker's point of view, the final NIE's conclusions were unwelcome. The NIE predicted what would happen, but it gave policymakers nothing to *do*. US policy preferences were, first, to keep Yugoslavia together. Failing that, policymakers wanted a peaceful breakup or, if all else failed, a managed disaster. They got none of the three. The disintegration began in 1991, and it was brutal and bloody. The fighting and "ethnic cleansing" that followed resulted in over 100,000 deaths and two million people displaced. US government attention at the time was rapidly becoming focused on events in the Middle East, where Iraq was about to invade Kuwait. So, as one analyst noted, the United States simply stopped caring until later, when the atrocities kept mounting.

Finally, the NIE apparently was leaked to the *New York Times*. Its subsequent publication in the *Times* may have hastened the dissolution of Yugoslavia by indicating to all the parties that the United States recognized the inevitable. The argument could be made that, because of its open publication, the NIE was a net disservice to the US government.

THE IRAQI WEAPONS OF MASS DESTRUCTION NIE

In October 2002, at the request of members of Congress, the National Intelligence Council produced an NIE entitled “Iraq’s Continuing Programs for Weapons of Mass Destruction.” That document concluded that Iraq

- *Was reconstituting its nuclear weapons program and was actively pursuing a nuclear device*
- *Possessed a biological weapons capability that was larger and more advanced than before the Gulf War and included mobile biological weapons production facilities*
- *Had renewed production of chemical weapons—including mustard, Sarin, GF (cyclo-sarin), and VX—and had accumulated chemical stockpiles of between 100 and 500 metric tons*
- *Possessed UAVs that were probably intended for the delivery of biological weapons²*

All of these conclusions were wrong. Concerning this NIE, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the WMD Commission) later found that

the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq’s weapons of mass destruction. This was a major intelligence failure. Its principal causes were the Intelligence Community’s inability to collect good information about Iraq’s WMD program, serious errors in analyzing what information it could gather, and a failure to make clear just how much of its analysis was based on assumptions, rather than good evidence.³

The Setting

In August 1990, Iraqi president Saddam Hussein invaded neighboring Kuwait, overthrowing the government and effectively seizing a quarter of the world’s oil resources and a large swath of coastline. President George H. W. Bush spearheaded a United Nations resolution authorizing the use of force (if Hussein had not exited Kuwait by January 15, 1991) and gained congressional approval at home by proposing a restrained plan of liberating Kuwait, but not getting mired in an ongoing Middle East war. On January 16, the coalition forces from over thirty nations overwhelmed Iraqi forces. Three months later, the legitimate government of Kuwait had been restored. Bush kept his promise; he chose not to pursue Hussein over the border, leaving his regime intact in Iraq. That decision later proved to be controversial.

Around the same time, another group in the Middle East was fast coming to prominence for its regime atrocities. Al Qaeda's original purpose was to support Muslims in fighting against the Soviet Union during the Afghan war, but when the Soviets withdrew, Al Qaeda set its sights on one primary target. It declared a "holy war" on the United States. Other radical Islamic terror groups were inspired: In 1993, a bomb was detonated in the garage of the World Trade Center in New York, injuring thousands and killing six.

In January 2001, George H. W. Bush's eldest son, George W. Bush, was inaugurated as the forty-third president of the United States. Eight months later, on September 11, Al Qaeda took credit for the worst attack on US soil in the country's history. Later that month, President Bush declared to Congress: "Our war on terror begins with Al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated."⁴ Also by this time, Saddam Hussein had become viewed as a sadistic, power-hungry dictator, seen as the top terror threat to America.

Key members of the Bush administration including Vice President Dick Cheney were convinced that Hussein was both developing WMD and providing support to Al Qaeda; they were determined to replace him. Achieving that goal required invading Iraq. But the administration needed both public and congressional support for a war.

Senator Bob Graham, chairman of the Senate Select Committee on Intelligence at the time, was concerned: Just what did the intelligence community know about the Iraqi WMD threat? In late summer 2002, Graham chaired a meeting of the committee with Director of Central Intelligence George Tenet at which Tenet reportedly presented the case for WMD in Iraq but acknowledged there was no existing NIE on the subject.⁵ Graham replied,

We want to have a national intelligence assessment. . . . This is the most important decision that we as members of Congress and that the people of America are likely to make in the foreseeable future. We want to have the best understanding of what it is we're about to get involved with.⁶

Graham got his estimate. The intelligence community had to produce it in three or four weeks—a remarkably short time for an NIE—to meet the congressional schedule for voting on a resolution authorizing the use of force in Iraq. The NIE was prepared in an environment that was succinctly described by Paul Pillar, NIO for the Middle East at the time:

A lot of intelligence analysts were caught up in several things: a previous consensus against which there just wasn't enough intelligence to challenge it; the consensus being that yes, there were [WMD] programs. The atmosphere in which they were working, in

which a policy decision clearly had already been made, in which intelligence was being looked to to support that decision rather [than] to inform decisions yet to be made, was a very important part of the atmosphere.⁷

The NIE

The result of this environment was a series of failures in both collection and analysis, and the WMD Commission report covers them exhaustively. We focus here on the analytic failures, beginning with one that the report touched on but did not emphasize.

Poor Issue Definition

Poor issue definition was perhaps the root cause of the analytic failures. The NIE began by failing to ask the right question, and consequently ran afoul of the framing effect. The drafters, constrained by the unreasonably short congressional deadline, accepted the problem as it was presented. An issue decomposition defined too narrowly, as this one was, limits the target framework and therefore the conclusions.

The issue definition centered solely on the question of whether Iraq had WMD programs and, if so, what those were. The focus on WMD programs made it too easy for analysts to fit the evidence into a WMD model. They assumed that Iraq had WMD programs, and analysis proceeded from that point.

A broader look at Iraq's overall military capability would have found more logical explanations for some of the evidence. In March 2001, intelligence reporting indicated that Iraq was acquiring high-strength aluminum alloy tubes.⁸ CIA and DIA analysts concluded that Iraq's purchase of aluminum tubes was intended to support a gas centrifuge uranium enrichment program. Focusing only on whether the tubes could be used for centrifuges, analysts ignored evidence that the tubes were better suited for use in rockets. The tubes in fact had precisely the same dimensions and were made of the same material as those used in Iraq's conventional rockets. In a classic example of premature closure, the CIA cited the existing judgment as a reason for rejecting the suggestion of one of its officers that they get the precise specifications of the rocket to evaluate the possibility that the tubes were in fact intended for rockets.⁹

The NIE also concluded that Iraq was developing small UAVs probably intended to deliver biological weapons agents. In reaching this conclusion, the intelligence community (except for the Air Force) failed to consider other possible uses for the UAVs and dismissed countervailing evidence. As one CIA analyst explained, the purpose of the NIE was to discuss Iraq's WMD programs, so the analysis did not explore other possible uses.¹⁰ A broader problem definition would likely have concluded, correctly, that the preponderance of evidence indicated that the UAVs were intended for battlefield reconnaissance.

A broader issue definition—one that required inputs from political, economic, and military analysts as well as weapons systems analysts—probably would have avoided some of the most serious analytic lapses in the NIE. As the WMD Commission noted, multidisciplinary issues were in fact key to the answer. In contrast to the broadly defined Yugoslavia issue, there was little serious analysis of the sociopolitical situation in Iraq or of the motives and intentions of the Iraqi leadership. Weapons systems analysts are not likely to ask questions such as, “Is Saddam Hussein bluffing?” or “Could Hussein have decided to suspend his weapons programs until sanctions are lifted?” An analyst of Iraq’s politics and culture would ask such questions.¹¹

Poor Evaluation of Sources and Evidence

The WMD Commission faulted analysts for making judgments based on insufficient evidence. It concluded that

- Analysts were too willing to find confirmations of their judgments in evidence that should have been recognized at the time to be of dubious reliability.
- They readily accepted any evidence supporting their theory that Iraq had stockpiles and was developing weapons programs.
- They explained away or disregarded evidence that pointed in other directions.

Two of the most egregious examples were the evaluation of a key HUMINT source on Iraq’s biological weapons program and of HUMINT and IMINT sources on Iraq’s chemical weapons program.

The conclusions about Iraqi biological weapons relied heavily on a single HUMINT source, an Iraqi chemical engineer nicknamed “Curveball.” He claimed that Iraq had several mobile units for producing biological weapons agents. The evidence presented by Curveball had a number of problems, the biggest of which was Curveball himself. He was variously described as a drinker, unstable, difficult to manage, “out of control,” and exhibiting behavior that is typical of fabricators.¹² There was no evidence of his *access* to biological weapons laboratories. Corroborating evidence only established that Curveball had been to a particular location, not that he had any knowledge of biological weapons activities being conducted there.¹³ He also had a motivation to provide interesting intelligence—resettlement assistance and permanent asylum.¹⁴ The reporting was through liaison with the German intelligence service, and US intelligence officials were not provided direct access to Curveball. The communications channel between Curveball and the WMD analysts therefore had many intermediate nodes, with consequent possibilities for the analysts to receive a distorted message.

Analysts evaluating Curveball's information were aware of some of these issues yet judged his reporting reliable and continued to make it the basis for the NIE assessment and subsequent judgments about Iraq's biological weapons program. They dismissed IMINT indications of flaws in Curveball's reporting as due to Iraqi denial and deception.¹⁵ That he was a fabricator was subsequently confirmed.

The NIE also erroneously concluded that Iraq had restarted chemical weapons production and increased its chemical weapons stockpiles, based on poor evaluation of both IMINT and HUMINT:

- Analysts relied heavily on imagery showing the presence of "Samarra-type" tanker trucks at suspect chemical weapons facilities. These distinctive trucks had been associated with chemical weapons shipments in the 1980s and during the Gulf War. Analysts also believed that they were seeing increased Samarra truck activity at suspect chemical weapons sites in imagery. They apparently did not consider an alternative hypothesis—that the trucks might be used for other purposes, as turned out to be the case. And they failed to recognize that the more frequent observed activity of the trucks was an artifact of increased imagery collection.¹⁶ The trucks were observed more often due to increased imagery reporting.
- One of the human sources, an Iraqi chemist, provided extensive reporting, about half of which was described in the WMD Commission report as implausible or absurd. Despite evidence that the source might not be credible, analysts used his reporting that Iraq had successfully stabilized the nerve agent VX because it fit their existing mindset.¹⁷ Another source reported that Iraq was producing mustard and binary chemical agents. But he also reported on Iraq's missile, nuclear, and biological programs. Given Iraq's known use of compartmentation to protect sensitive weapons programs, analysts should have recognized that the source was unlikely to have access to all of these programs.¹⁸

Failure to Consider Alternative Target Models

The Iraqi WMD NIE contained numerous examples of analysts' selecting a single hypothesis (or target model) and attempting to fit evidence into it. The failure to seriously consider alternative missions for Iraq's UAV program and alternative uses for the aluminum tubes were noted previously. In addition,

- Analysts failed to consider flaws in the target model they were using. If Iraqis had used all the aluminum tubes they were acquiring for centrifuges, the result would have been 100,000 to 150,000 machines, far more than any nuclear weapons proliferator would build.¹⁹ All target models should undergo a simple sanity check: Does the model intuitively make sense?

- They also failed to consider the Occam's razor alternative—the reason they could find no mobile biological weapons laboratories after an intensive search is that the labs didn't exist.²⁰ It is virtually impossible to prove a negative in the intelligence business, but the negative at least deserves to be considered.

The most compelling such failure, though, was the one that Martin van Heuven avoided. As the national intelligence officer in charge of the Yugoslavia NIE, he forced the consideration of an alternative target model, which ultimately was used in the NIE. The Iraqi WMD drafters, facing a short congressional deadline, gravitated to a single model and apparently failed to consider a logical top-level alternative hypothesis or model: that Iraq had temporarily abandoned its WMD programs.

Poor Analytic Methodology

The raw intelligence available to analysts was mostly historical, due in large part to Iraq's denial and deception programs. Intelligence about developments from the late 1990s to 2003 depended heavily on IMINT and questionable HUMINT. Other technical collection, COMINT, and open source contributed very little.²¹ As a result, analysts had to, in effect, "predict" the present state of the WMD programs based on knowledge of where the programs were in 1991.

They did so by extrapolation based on past history. Specifically, the Iraqis had

- The same leadership, presumably with the same objectives concerning WMD
- Expertise in biological weapons, chemical weapons, and nuclear weapons development
- A history of effectively concealing these activities

As one example, the UAV estimate mentioned earlier was based heavily on a straight-line extrapolation. Before the Gulf War, Iraq had been in the early stages of a project to convert MiG-21 jet aircraft into UAVs for biological weapons delivery. In addition, Iraq had experimented in 1990 on a biological weapons spray system, designed to be used with the MiG-21 UAV. In the mid-1990s, Iraq also began testing another modified jet aircraft, the L-29, as a UAV. Analysts concluded that the L-29 was a follow-on to the MiG-21 program. When these new and smaller UAVs made their appearance, NIE drafters extrapolated that they were simply a continuation of the biological weapons delivery program, despite Air Force objections that the UAVs appeared intended for other uses.²²

The resulting straight-line extrapolation was much like the extrapolation that resulted in the "muddle-through" Yugoslavia NIE draft. Analysts assumed that the forces that were present in 1991 Iraq were still present, making no allowance for new forces in the intervening decade. But there were new forces:

- Since the Gulf War, Iraq had been under constant international scrutiny, so there was a high risk that any continuing WMD program would be discovered and be a catalyst for additional sanctions or military action.
- The threat Iraq faced from Iran had intensified throughout the 1990s, marked by low-level conflicts. Saddam Hussein had a powerful incentive to conceal his *lack* of WMD because of its deterrent effect on Iran.²³

Neither force was taken into account.

Poor Interaction with Collectors and Customers

A shared target model—shared with both collectors and customers of intelligence—is critical for good analytic outcomes. The Iraqi WMD NIE effort failed on both counts.

Analysts did not share with collectors how much they relied on intelligence from sources that the collectors knew to be unreliable—Curveball and the Iraqi chemist who reported on Iraq's purported chemical weapons program being two examples.

In dealing with the customers, analysts left the impression that their sources were much more credible than was the case. It is true that the analysts were ill served in this effort by pressures from the White House to provide a rationale for the planned invasion of Iraq. But, ultimately, analysts must assume responsibility for their product. As the WMD report noted, the NIE did not communicate the weakness of the underlying intelligence. Analysts did not adequately communicate their uncertainties to policymakers. The NIE also obscured how much their conclusions rested on inferences and assumptions.²⁴

The Customer View

The NIE was created at the direction of the Senate Select Committee on Intelligence, so Congress was the customer. For members of Congress, the report provided welcome cover in their vote on the resolution to invade Iraq. Those who read the report (less than half reportedly read the full ninety-two pages) generally appeared to have accepted it as accurate. The administration presented no objections; the NIE supported the administration's position.

Congress accepted the NIE's conclusions. On October 26, 2002, a joint resolution of Congress, known as the Authorization for Use of Military Force against Iraq Resolution of 2002, was adopted; it did exactly what its name implies. A total of 77 senators and 297 representatives voted for the resolution, with 23 senators and 133 representatives voting against it. Many of the key participants within and outside Congress question whether the NIE had a significant effect on that vote.²⁵

The NIE started out on the wrong foot with a poor issue definition. It ended badly, as the WMD Commission noted, in a failure to communicate.²⁶

CAPSTONE CRITICAL THINKING QUESTIONS

1. The Yugoslavia NIE does not expressly show the issue definition. Develop a statement of the issue and provide an issue decomposition (suggestion: a PMESII decomposition may work best). (See chapter 8.)
2. Create a parallel list (perhaps using table 10.1 as a model), comparing the Yugoslavia model perspectives presented in the NIE second draft with the views held by the US State Department policymakers. (This will require independent research.) (See chapter 10.)
3. The Yugoslavia NIE had no effect on policy, as noted at the beginning of this case study.
 - a. Identify at least two conclusions or recommendations that the NIE drafters might have included to make the NIE useful to, and accepted by, policymakers (in this case, the State Department). (See chapter 14.)
 - b. Draft the conclusions or recommendations in a form that might have constructively engaged the policymakers. (See chapter 7.)
4. The Yugoslavia NIE contains a section titled “An Unlikely Outcome” that describes the “muddle-through” option (see page 9) and a brief summary of the situation faced by Serbian president Slobodan Milošević (see page 2). A profile of Milošević that was available to the NIE drafters is available at <https://www.rferl.org/a/1091492.html>. Based on these sources, prepare an influence net model showing the factors that would drive Milošević toward or away from a compromise to preserve Yugoslavia. (See chapter 16.)
5. The two Yugoslavia NIE drafts discuss a number of forces that were present in Yugoslavia that year. Inertia, opposition, contamination, feedback, and synergy forces were not specifically identified. Which one or more of these types appear to have been dominant in each NIE draft? Explain your reasoning, citing specific provisions. (See chapter 15.)
6. The final Yugoslavia NIE was anticipatory and used a projection. The Iraqi WMD NIE relied on extrapolation. Could a projection have been used in the Iraqi WMD NIE? If so, how? (See chapter 16.)
7. The Iraqi WMD NIE ran into trouble from the beginning because of a poor issue definition. Provide an issue definition statement that would likely have resulted in a better product, and an issue decomposition (again, PMESII may work best). (See chapter 8.)

8. Jerrold Post prepared a personality profile on Saddam Hussein in 2003. It is available online at <https://www.airuniversity.af.edu/Portals/10/CSDS/Books/knowthyenemy3.pdf>. Identify features in Saddam's profile that would support an assessment that he was concealing his WMD programs. Identify features that would indicate that he was concealing his lack of WMD. (See chapter 9.)
9. Create a target framework for the *issue definition that was used* in preparing the Iraqi WMD NIE. (You may have to infer the issue definition from the NIE and the WMD Commission report.) Carry the framework down to two subordinate levels of detail. (See chapter 10.)
10. Create a target framework for the *issue definition that should have been used* in preparing the Iraqi WMD NIE. Carry the framework down to two subordinate levels of detail. (See chapter 10.)
11. One of the key HUMINT sources in the Iraqi WMD estimate had the foreshadowing nickname "Curveball." The WMD Commission report criticized the dependence on Curveball as a source. Additionally, a detailed news article about Curveball is available in the *Los Angeles Times* at <http://www.latimes.com/world/middleeast/la-na-curveball20nov20-story.html>. Using the criteria outlined in chapter 11 for evaluating the source and the communications channel, provide a point-by-point assessment of the credibility of Curveball's reporting. (See chapter 11.)
12. Chapter 11 lists three credentials of evidence. Give specific examples where each of the three credentials was ignored in the Iraqi WMD NIE. Try *not* to use Curveball in the examples. (See chapter 11.)
13. Chapter 11 lists seven pitfalls to avoid in evaluating evidence. Give a specific example of failure to avoid each pitfall that was present in the Iraqi WMD NIE. (See chapter 11.)
14. Identify gaps in knowledge present in the Iraqi WMD NIE. This may require independent research. (See chapter 12.)
15. Iraq's history of denial and deception had a prominent effect in shaping the erroneous assessments that were reached in the NIE. Those effects are summarized in the WMD Commission report. Chapter 13 identifies situations that call for special awareness of the possibility of deception. Which ones were present in the Iraq situation? What analytic methodologies could have been applied to avert the erroneous judgments based on analyst concern about possible deception? (See chapter 13.)

NOTES

1. CIA, NIE 15-90, "Yugoslavia Transformed," October 18, 1990, iii, <https://www.cia.gov/library/readingroom/docs/1990-10-01.pdf>.
2. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 31, 2005, 8–9, https://fas.org/irp/offdocs/wmd_report.pdf.
3. Ibid., cover letter.
4. President George W. Bush, "Address to a Joint Session of Congress and the American People," September 20, 2001, <https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html>.
5. "The October '02 National Intelligence Estimate (NIE)," *Frontline*, June 20, 2006, <http://www.pbs.org/wgbh/pages/frontline/darkside/themes/nie.html>.
6. Ibid.
7. Ibid.
8. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 55.
9. Ibid., 57, 68.
10. Ibid., 145.
11. Ibid., 13.
12. Ibid., 91, 97.
13. Ibid., 113.
14. Ibid., 96.
15. Ibid., 92.
16. Ibid., 122, 125.
17. Ibid., 127.
18. Ibid., 128.
19. Ibid., 85.
20. Ibid., 93.
21. Ibid., 165.
22. US Government Printing Office, "United States Congressional Serial Set, Serial No. 14876, Senate Report No. 301, U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq, Report of Select Committee on Intelligence," January 20–December 7, 2004, 231.
23. Ibid., 168–169.
24. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 12.
25. "The October '02 National Intelligence Estimate (NIE)."

26. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 3.

LIST OF COMMONLY USED ACRONYMS.

ABI	activity-based intelligence
ACH	analysis of competing hypotheses
BMD	ballistic missile defense
BMP	Boyevaya Mashina Pekhoty (infantry fighting vehicle)
BW	biological warfare
C4ISR	command, control, communications, computer, intelligence, surveillance, and reconnaissance
CAD/CAM	computer-aided design/computer-aided modeling
CASOS	computational analysis of social and organizational systems
CCS	collaborative collection strategies
CIA	Central Intelligence Agency
COMINT	communications intelligence
CPI	corruption perceptions index
CSB	collection support brief
CW	chemical warfare
D&D	denial and deception
DARPA	Defense Advanced Research Projects Agency
DCI	director of central intelligence
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIME	diplomatic, information, military, and economic
DNA	deoxyribonucleic acid
DNI	director of national intelligence
DoD	Department of Defense
DRI	Digital Research Intergalactic
DST	Direction de la Surveillance du Territoire (France)

EEI	essential elements of information
ELINT	electronic intelligence
EMCON	emissions control
ESM	electronic support measures
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FMV	full motion video
GCHQ	Government Communications Headquarters (United Kingdom)
GDP	gross domestic product
GEOINT	geospatial intelligence
GPS	Global Positioning System
GRU	Main Intelligence Directorate of the General Staff (Russia)
HIDTA	high intensity drug trafficking area
HUMINT	human intelligence
I&W	indications and warning
ICBM	intercontinental ballistic missile
IDF	Israeli Defense Forces
IED	improvised explosive device
IFF	identification friend or foe
IMINT	imagery intelligence
INT	intelligence
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria
IT	information technology
IUSS	Integrated Undersea Surveillance System
JCS	Joint Chiefs of Staff
JNA	Yugoslav National Army
KGB	Komitet Gosudarstvennoy Bezopasnosti (Russia)
KIQ	key intelligence question
KIT	key intelligence topic
LIDAR	laser radar
LPI	low probability of intercept
MASINT	measurement and signature intelligence

MLO	money laundering organization
MOE	measure of effectiveness
MOVINT	movement intelligence
MTI	moving target indicator
NATO	North Atlantic Treaty Organization
NERVA	nuclear engine for rocket vehicle application
NGA	National Geospatial-Intelligence Agency
NGO	nongovernmental organization
NIE	national intelligence estimate
NIH	not invented here
NIO	national intelligence officer
NIPF	National Intelligence Priorities Framework
NSA	National Security Agency
NSC	National Security Council
NYPD	New York Police Department
OBP	object-based production
OSINT	open-source intelligence
OSS	Office of Strategic Services
PDB	President's Daily Brief
PLA	People's Liberation Army (China)
POL	pattern-of-life
PMESII	political, military, economic, social, infrastructure, and information
S&T	scientific and technical
SAC	Strategic Air Command
SALT	Strategic Arms Limitation Talks
SAM	surface-to-air missile
SAR	synthetic aperture radar
SAT	structured analytic techniques
SCI	sensitive compartmented information
SDI	Strategic Defense Initiative
SIGINT	signals intelligence
SNA	social network analysis
SVR	Foreign Intelligence Service (Russia)

SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWOT	strengths, weaknesses, opportunities, and threats
TAPI	Turkmenistan-Afghanistan-Pakistan-India pipeline
TCPED	tasking, collection, processing, exploitation, and dissemination
UAV	unmanned aerial vehicle
UGF	underground facility
UN	United Nations
URDF-3	Unidentified Research and Development Facility-3
USSR	Union of Soviet Socialist Republics
WMD	weapons of mass destruction

INDEX

- Abduction, 77, 346
AC-130 Spectre gunship, 46
ACH. See Analysis of competing hypotheses (ACH)
Ackoff, R., 415, 418
Actionable intelligence, 24
Active deception technique, 240
Activity-based intelligence (ABI), 397, 398–399, 399 (figure), 402
Ad hoc teams, 91–92
Administrative model, 416–417
Advanced Air Defense (AAD), 156
Air Force, 26, 115, 249, 409–410 (box), 411, 435
Al-Assad, B., 15
Al-Assad, H., 129 (box)
Alert fatigue, 105
Aliyev, I., 128, 166
Al-Kasaesbeh, M., 197
Allen, C., 104
All-source vs. single-source intelligence, 110–111
Almanac Trial, 189 (box)
Al Qaeda, 114, 299, 300, 447
Al-Shabaab ideology, 163–165
Al-Shabaab insurgency, 308, 331
influence tree for, 310 (figure), 312–314, 312 (figure)
smuggling, sensitivity analysis, 316, 317 (figure)
Alternative frameworks, 176–178
American Anthropological Association, 392
Amin, H., 5
Analysis of competing hypotheses (ACH), 205–207, 209, 210
Analyst-collector interaction, 227–229
Analyst-policymaker relationship, 63
Analysts
as advocate, 268–270
critical and logical thinking, 73–75
D&D, 248
defense, 114–115
good instincts, 77
historical perspective, 77
long-term perspective, 76–77
objectivity, 75–76
role, 78
Analytic managers, 106
Analytic methodology, 9, 63, 205, 281, 368, 451–452
Analytic network
collaboration and sharing, 95–97
homeland security and law enforcement, 92–94
military services, 94
NGOs, 94–95
US national intelligence network, 89–92
Analytic product
business leaders, 67
Congress, 63
Devil's advocate, 267
management review, 266
peer review, 265–266
red teams, 266–267
Analytic teams
benefits, 79
changing, analytic method, 83
collectors, 81
costs, 79
customers, 80–81
economy, 82
external sources, 81
interpersonal skills, 82
issue definition, 82–83
leadership, 84
project definition/research plan, 83–84
project review conferences, 84
standardizing terms, 83
Andropov, Y., 5, 7
Anglo-American judicial system, 188
Anticipatory intelligence, 277–279, 294
forces, 281–295
methodology, 297–324
prescriptive and, 431 (figure)

- Arquilla, J., 15
 Arthur Andersen, 376 (box)
The Art of Problem Solving: Ackoff's Fables (Ackoff), 415
 Asymmetric warfare, 14, 20
 Athena's Prism, 415
 Automated network modeling, 369–370, 381–382
 Automobile production cycle, 39–40 (box)
 Azerbaijan government, 165
 economic model, 168, 168 (figure)
 ethnic model, 170, 171 (figure)
 information model, 172–173
 infrastructure model, 170–172
 Internet users, percentage of, 173 (figure)
 military model, 167–168, 167 (figure)
 oil and natural gas structure, 172 (figure)
 petroleum production and consumption, 168 (figure)
 political model, 166, 166 (figure)
 social model, 168–170
 Azerbaijan, issue decomposition
 design of economic sanctions, 135–136, 136 (figure)
 economy, 135, 136 (figure)
 political situation, 134, 134 (figure)
- Baader-Meinhof phenomenon, 191
 Baby production curve, 356
 Bacastow, T., 388
 Backfire bomber simulations, 409–410 (box), 410, 422
 Baldwin, D., 165, 169
 Ballistic Missile Defense (BMD) program, 156, 156 (figure)
 Barwell, C., 400 (box)
 Battle damage assessment, 30, 32
 Battlespace awareness, 29, 30
 Bayesian analysis, 205
 Bayes, T., 205
 Belden, T., 376 (box)
 Bell, G., 367
 Benchmarking, 148
 Bessemer, H., 284 (box)
 Bessemer steelmaking process, 284, 284 (box)
 Big data, 208, 436–437
 Biltgen, P., 398
 Bin Laden, O., 5, 51, 116, 146
 Bioterrorism, 412
 Bitcoin, 21, 22 (box), 379
 Blanchard, O., 378–379
 Blockchain financial networks, 379
 Bowman, I., 393 (box)
 Boyevaya Mashina Pekhoty (BMP), 46–47, 161, 221
 Brainstorming, 138–139
 Breivik, A., 17
 Brezhnev, L., 5
 Brooks curves, 356–357, 356 (figure)
 Brooks, F., 356–357
 Brunson, A., 23 (box), 313–314
 Bueno de Mesquita, B., 76, 304, 420–422
 Bush, G. H. W., 91 (box), 446, 447
 Bush, G. W., 5, 447
 Business leaders, 67–68
- Carter, J., 115
 Case-based models, 336–337
 Caspian Sea Monster, 349, 349–350 (box)
 Causal modeling, 298–299, 300
 features of, 292
 global warming, 292
 Iraqi political reconciliation, 293–294, 293 (figure)
 Cell, 364
 Central Intelligence Agency (CIA), 8, 61–62, 97, 108, 202, 302
 Clandestine Service, 114
 Congress, 63–64
 politicization problem, 113
 Soviet economy, 272
 Tradecraft Primer, 130, 144, 187, 188, 281, 304, 328, 338
 Centrality, 372–374
 Chernobyl disaster, 290
 Churchill, W., 196, 260, 271
 CIA. See Central Intelligence Agency (CIA)
 Cisco Systems, 51
 Clandestine network target framework, 163
 deconstruction, 164 (figure), 165 (figure)
 top level, 164 (figure)
 Clapper, J., 42, 90
 Clarke, B., 106
 Clark, R., 185, 251
The Clash of Civilizations and the Remaking of World Order (Huntington), 143
 Cocaine network, 47–48, 48 (figure), 49, 50 (figure)

- Cohen, D., 97
- Cold War, 19, 241, 250, 322, 351, 418, 434
- Collaborative collection strategies (CCS), 226
- Collection performance, measures of, 229
- Collection strategy development, 222, 232
- assets, 222–223
 - cost-benefit analysis, 225–226
 - examples of, 224–225
 - innovative approaches, 223
 - Khanani MLO network, 223–224
 - military intelligence, 223
 - political intelligence, 223
 - requirements, 230–232
- Collection support briefs (CSBs), 227
- Collective decision-making model, 419
- Collectors, 81, 249–250
- Combat damage assessment, 30
- COMINT. *See* Communications intelligence (COMINT)
- Commander's Handbook for Attack the Network*, 163
- Commercialization of intelligence, 3
- Commercial network, 375–378, 382
- Communications channel
- entropy, 191–193, 192 (figure)
 - hearsay rule, 193
 - noise, 191
 - organizational or personal biases, 192
 - primary and secondary sources, 192
- Communications intelligence (COMINT),
- 36, 59, 185–187, 228, 270
 - corroborative and cumulative redundancy, 204
 - ELINT data, 194
 - financial transactions, 219
 - hearsay, 198
 - HUMINT and, 223–224, 233, 260, 395
 - Kiang Kwan*, 203
 - radio communications, 143, 197
 - "Secret" level, 67
 - single-source analysts, 110
 - types of, 243
- Comparative models
- Caspian Sea Monster, 349, 349–350 (box)
 - German engine killer, 350, 350 (box)
 - ICBMs, 347
 - keiretsu, 150
 - Knickebein, 348, 348–349 (box)
 - lists, 148
 - matrices, 148, 149 (table)
 - mirror imaging, 150
- Würzburg radar, 347–348 (box)
- Competitive frameworks, 178, 179 (table)
- Competitive intelligence analysts, 347, 378, 418
- Complex issue decomposition, 136–138
- Complex projection, 305
- Complex systems, target as, 47–48
- Computational Analysis of Social and Organizational Systems (CASOS), 381
- Computer-aided design/computer-aided modeling (CAD/CAM), 387
- Computer-assisted network modeling, 369–370
- Conceptual models, 8, 119
- deterministic/stochastic, 146
 - dynamic, 147
 - linear/nonlinear, 146
 - mathematical models, 145
 - solvable/simulation, 147
 - static, 147
- Condorcet, M. de, 420
- Conflict tools
- diplomatic, 19
 - economic, 21–22
 - information, 19–20
 - military, 20–21
- Congress, 63–64
- Constraints, intelligence product, 107
- boundaries, 109–112
 - limits, 108–109
 - pressures, 112–116
- Contamination, 286, 293
- economic, 286
 - indications, 287
 - phenomena, 287
 - social, 287–288, 293
- Convergent evidence, 204
- Convergent phenomena, 298–301
- Corroborative redundancy, 204
- Corruption
- correlation, 307, 307 (figure)
 - forms of, 286, 288
 - political, 75
- Corruption Perceptions Index (CPI), 307
- Cost-benefit analysis, 225–226
- Cost-utility analysis, 359–360
- Cotton-picking curve, 356
- Counterintuitiveness, 322
- Countervailing (opposition) forces, 286, 293
- COVID-19 outbreak, 95, 104, 127, 286, 337, 408

- Criminal/offender profiling, 152
- Critical thinking, 73–74, 84–85
- Cross-impact analysis, 337
- Cry wolf syndrome, 105
- Cuban missile crisis, 202–203, 202 (box), 246–247 (box)
- Cultural models, 417–418
- Cumulative redundancy, 204–205
- Curators, 78
- Current intelligence, 102–103, 106–107
- Customers
 - analysts and, 80–81
 - business leaders, 67–68
 - competitive intelligence, 59
 - Congress, 63–64
 - homeland security, 65–66
 - interaction, 267–268
 - law enforcement, 66–67
 - military leadership and operations, 64–65
 - money laundering, issues, 217
 - opportunities and threats, 58
 - prospect theory, 68
 - reduce uncertainty, 58
 - single-source analysts, 59
 - uncertainty effect, 68
 - See also* Policymakers
- Cyber collection, 229
- Cyber operations, 20
- Cyberspace, 14, 52

- Darknets, 20, 21
- Dark web, 20, 21
- Davis, J., 80, 81, 113, 114
- Dayton Peace Accords, 394 (box)
- D&D. *See* Denial and deception (D&D)
- Deception: Counterdeception and Counterintelligence* (Clark and Mitchell), 251
- Deception techniques
 - active, 240
 - aircraft, illicit activities, 241
 - information instrument, 241–242
 - The Man Who Never Was* (Montagu), 240 (box)
 - media disinformation, 241
 - passive, 239–240
 - traditional and social media, 242
- Decision-making process, 319, 330, 375, 416–417, 431
 - beliefs in, 419
- collective, 419
- costs, 359–360
- cultural models, 417–418
- EMBERS, 407
- group models, 419–420
- operational code model, 419
- rational, 415, 416
- red teams, 266
- U-2 program, 226
- Deductive approach, 74, 345, 360
- Deep web, 20, 21
- Defense Advanced Research Projects Agency (DARPA), 209, 369
- Defense analysts, 114–115
- Defense Intelligence Agency (DIA), 111, 202 (box), 410 (box)
- Delphi method, 201
- Demonstration scenario, prescriptive intelligence, 305, 432
- Denial and deception (D&D), 237
 - analyst, 248–249
 - collectors, 249–250
 - compartmentation, 243, 244
 - countering, 247–254
 - customers, 250–252
 - fundamental factors, 238
 - perception management, 245
 - signaling, 252–254
 - sources and methods, 242–247
- Denial types, 239
- Department of Defense (DoD), 38, 39
 - (figure), 50, 64, 250 (box), 409, 410 (box)
- Department of Homeland Security (DHS), 59
 - fusion centers, 92–93
 - law enforcement organizations, 93–94
 - responsibilities, 92
 - risks and threats, 65
- Deregulation benefits, 290
- Descriptive intelligence, 101
- Desert Shield/Desert Storm, 27, 27 (box)
- Deterministic model, 146
- Deutsche Bank, 51
- Devil's advocate, 267
- DHS. *See* Department of Homeland Security (DHS)
- The Dictator's Handbook* (Bueno de Mesquita and Smith), 76
- Diplomatic, information, military, and economic (DIME) instrument, 19, 31, 46, 125, 126, 165, 168

- Diplomatic (political) tool, 19
 Disk Operating System (DOS), 300 (box)
 Divergent evidence, 203
 Divergent phenomena, 298–301
 DoD. See Department of Defense (DoD)
 Dodging missiles, 43–44 (box)
 Domestic vs. foreign intelligence, 111
 Driving-force scenarios, 330–331, 339
 Drones, 21
 Dupont, A., 13
 Dynamic geospatial models, 395, 402
 ABI, 397, 397–399, 399 (figure)
 geographic profiling, 399–400
 intelligence enigmas, 400–402
 movement intelligence, 395–396
 Dynamic model, 146, 179
- Early Model Based Event Recognition using Surrogates (EMBERS), 407
 Econometric model, 408, 423–424
 Economic conditions, 309–310, 311
 Economic contamination, 286–288
 Economic instruments, 21–22
 Economic simulations, 408, 408 (figure), 435
 Edison, T., 79
 Einstein, A., 77, 79
 Electronic intelligence (ELINT), 111, 185, 187, 194, 227, 244
 Electronic support measures (ESM), 112
 Emissions control (EMCON), 249
 Emotional models, 418–419
 Empathy, 75–76, 263
 Enigmas, 395, 400–402
 Ennis, R., 73
 Enron Corporation network, 375, 375–376 (box), 377 (figure)
 Equivalence, social network, 374
 Erdoğan, R. T., 17
 vs. Gülen, 18 (box), 22, 23 (box), 313
 Ermarth, F., 109
 Essential elements of information (EEI), 134
 Estimative analysis, 278, 298
Estimative Intelligence (Ford), 103
 Ethnocentric bias, 6–7
 Evidence-based reasoning, 74
 Evidence evaluation
 access, 189
 bona fides, 188
 Cold War, 195
 communications channel, 191–193, 192 (figure)
 competence, 188–189
 data and, 196
 expert opinions, 199–201
 fact, direct and indirect information, 194
 favouring/disfavoring, 198
 hearsay, 198–199
 HUMINT, COMINT and OSINT data, 194, 197
 multiple pathologies, 196
 Occam's razor, 188
 premature closure and philosophical predisposition, 201–203
 quality of information check, 187–188
 vested interest and bias, 189–191
 vividness weighting, 196–197
 Expected future scenario, 327
 Expected utility theory, 416
 Exponential/disaster curves, 153, 154 (figure)
 External pressures, 113–114
 Extrapolation mechanism, 301, 305–308, 306 (figure), 323
- Fahey, L., 305, 375, 378
 Failures, intelligence
 Afghanistan (1979–1989), 5
 customers, 7–8
 Falkland Islands (1982), 4
 information sharing, 5–6
 mindsets, 6–7
 Operation Barbarossa (1941), 3–4
 Singapore (1942), 4
 Yom Kippur (1973), 4
 False positive feedback, 290
 Family and cultural networks, 368
 Farewell Dossier, 69, 250–251 (box), 288
 Faurer, L., 115
 Federal Bureau of Investigation (FBI), 93, 94, 110, 111, 152, 250 (box)
 Federal Energy Regulatory Commission (FERC), 376 (box)
 Feedback loop, 230, 313
 Feedback mechanism, 288
 false positive, 290
 nuclear power industry, 290
 positive/negative, 289–290
 strengths of, 289
 Ferdinand, A. F., 299, 300
 Fermi, E., 133

- Field intelligence groups, 93
- Filling gaps, 215–216
- Financial networks, 378–379, 382
- Fingar, T., 95, 96, 109, 121, 293
- Finished intelligence, 111, 183–184
- The Five Disciplines of Intelligence Collection* (Lowenthal and Clark), 185
- Flawed channel, 193 (box)
- Flynn, M., 23 (box)
- Foley, J., 197
- Force analysis, 308
- Force field analysis, 302–303, 442
- Forces, anticipatory analysis
 - causal models, 291–294
 - contamination, 286–288
 - feedback mechanism, 288–290
 - inertia, 283–285
 - methodology, 297, 298 (figure)
 - opposing forces, 285–286
 - PMESII factors, 282–283
 - synergy, 290–291
- Ford, H., 39–40, 39 (box)
- Ford Motor Company, 288
- Forecasting mechanism, 302, 316–317, 323
 - complex projection, 305
 - criteria on, 320
 - evaluating, 320–321
 - force field analysis, 303
 - nonlinear approach, 318–319
 - techniques and analytic tools, 319–320
- Foreign instrumentation signals
 - intelligence (FISINT), 185, 244
- Foresight analysis, 327
- Framing effect, 64, 122
- Franklin, B., 148
- Full motion video (FMV), 396
- Functional networks, 368
- Fusion centers, 92–93
- Futures Group, 337

- Game theory, 420–422, 424
- Gap analysis
 - filling, 215–216
 - identifying, 220–222
- Gates, B., 300 (box)
- Gates, R., 65, 108, 112, 113
- Gaussian/normal curve, 153, 154 (figure)
- GDP. See Gross domestic product (GDP)
- Generic program cycle, 355, 355 (figure)

- Generic target framework, 162
 - customers' issue connections, 217, 218 (figure)
 - money laundering, 217, 217 (figure)
- Genetic engineering, 290, 317
- Geographic profiling, 399–400, 402
- George, A., 419
- Geospatial intelligence (GEOINT), 59, 110, 185, 201, 388, 402, 436
- Geospatial models, 343, 387–389, 424
 - dynamic, 395–402
 - static, 389–395
- Geospatial simulations, 413, 413 (figure), 436
- German engine killer, 350, 350 (box)
- Globalization of intelligence, 3
- Global Positioning System (GPS), 20, 337
- Glycerin refinery, 287
- Gneezy, U., 68
- Gorbachev, M., 108
- Goto, K., 197
- Government Communications Headquarters (GCHQ), 110
- Graham, B., 447
- Great Game, 393
- Gresham's law, 286
- Gross domestic product (GDP), 17, 152, 168, 170, 408 (figure)
- Group decision-making models, 419–420
- Guerrilla warfare, 14
- Gülen, F., 17
 - vs. Erdoğan, 18 (box), 22, 23 (box), 313

- Hall, K., 38
- Hawala system, 21, 224, 379
- Headrick, J., 265
- Hearsay evidence, 198
- Henry VIII, King, 321–322
- Herman, M., 38, 58, 114–115, 186, 197, 232, 264
- Heuer, R. J., 177, 198, 205, 206
- Hierarchy model, 145 (figure), 363
- High-impact/low-probability analysis, 304–305
- High Intensity Drug Trafficking Area (HIDTA), 92, 93
- Hitler, A., 260, 271
- Hizmet, 18 (box)
- Horizon scanning, 335
- Hull, C., 253–254

- Human intelligence (HUMINT), 28 (box), 35, 36, 81, 97, 184–187, 228, 230
bona fides, 188
 COMINT and, 194, 223–224, 233, 260, 395
 CSBs, 227
 evaluation, 449, 450
 expert opinion, 199
 financial networks, 379
 hearsay, 198
 I&W, 103
Kiang Kwan, 203, 204
 network model, manual, 368–369
 nuclear tests, 245 (box)
 targeting analysts, 110
 vested interest, 189
 Human Terrain System program, 392–395, 394 (figure), 395 (figure)
 HUMINT. *See* Human intelligence (HUMINT)
 Huntington, S. P., 143, 144, 169, 286
 Hussein, S., 114, 178, 199, 252, 254, 271, 446–447
 Hybrid wars, 13
- IBM, 300 (box)
 Il-sung, K., 319
 Imagery intelligence (IMINT), 67, 185, 226, 229, 451
 COMINT and, 194, 223
 D&D, 239, 243, 248
 evaluation, 450
 Iraq's chemical weapons program, 449
 Soviet missiles, 398
 Improvised explosive devices (IEDs), 20–21, 163, 370, 433
 Inchon landing (Korean War), 389–390 (box)
 Indian nuclear test (1998), 244–245 (box)
 Indications and warning (I&W) intelligence
 competitive intelligence, 105
 conventional military attacks, 104, 105
 Japanese plans and intentions, 103
 military conflicts, 104
 Pearl Harbor attack, 104, 105
 purpose, 103
 tradeoff problem, 105
 unconventional/extraordinary event, 105
 Indiscriminate weapons, 20–21
 Inductive/synthesis approach, 74, 346
 Inertia, 283–285, 293
 Influence links, 313
 Influence net modeling, 313–314, 314 (figure)
 Influence net topology, 313
 Influence nodes, 313
 Influence trees and diagrams
 al-Shabaab insurgency, 310 (figure), 311, 312 (figure), 313–314
 economic conditions, 309–310
 probabilistic reasoning, 311
 Information instrument, 19–20
 Information sharing, 97–98
 Information technology (IT), 19–20, 38, 208–209, 358
 Instrumental beliefs, 419
 Instruments of national power, 19
 Insurgents, 17, 18, 126, 344 (box)
 Integrated Undersea Surveillance System (IUSS), 389
Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform (Pillar), 113, 144
Intelligence Collection (Clark), 185
 Intelligence cycle. *See* Traditional intelligence cycle
 Intelligence-led policing, 28, 93
 Intelligence-policy divide, 110
 Intelligence preparation of the battlefield (or battlespace), 26, 31
 Intelligence research, 102, 106
 Intellipedia, 96
 Intercontinental ballistic missiles (ICBMs), 226, 347
 Intergalactic Digital Research (DRI), 300 (box)
 Internal pressures, 112–113
 International Charter 'Space and Major Disasters', 66
 Internet service provider (ISP), 221
 Investigative Support Center (ISC), 92, 93
 Iraqi WMD Commission, 5, 176, 193, 202, 269
 Iraqi WMD NIE, 441, 446
 alternative target models, 450–451
 analytic methodology, 451–452
 collectors/customers, interaction with, 452
 customer view, 452–453
 issue definition, 448–449
 setting, 446–448
 sources/evidence, evaluation, 449–450

- Israeli Defense Forces (IDF), 4, 28 (box)
- Issue decomposition
 - Azerbaijan, 134–135, 134 (figure), 136 (figure)
 - classic method, problem solving, 134
 - complex, 136–138
 - economic sanctions, 135, 136 (figure)
 - SAT, 138–139
 - strategies-to-task, 133
 - target framework and, 216–220
 - taxonomy, 133
- Issue definition
 - assumptions, 129–131
 - categories, 125
 - Fingar’s statements, 121
 - focusing question, 131–133
 - framing effect, 122
 - PMESII factors, 125–128
 - preliminary questions, 122–124
 - question clarification, 124, 129
- I&W intelligence. *See* Indications and warning (I&W) intelligence

- Johnson, L., 62
- Joint Chiefs of Staff (JCS), 14, 62, 64, 271
 - The Joint Force in a Contested and Disordered World*, 14
- Joint Terrorism Analysis Centre, 93
- Jones, R. V., 89, 200, 200 (box), 348, 348–349 (box)

- Kahn, H., 432
- Kegan, G., 401 (box)
- Keiretsu, 150
- Kelly, J., 254
- Kelly, W., 284 (box)
- Kennan, G., 299
- Kennedy, J., 61–62
- Kent, G., 133
- Kent, S., 10, 38, 57, 80, 259
- Kerr, D., 59
- Kerr, R., 107
- Key intelligence questions (KIQs), 68, 133–134
- Key intelligence topics (KITs), 68
- Khanani, A., 217–219
 - Khanani money laundering organization (MLO), 221, 222 (figure), 365, 371 associations, 220 (table)
- link model, 365 (figure)
- network model, 218 (box), 217–219, 219 (figure), 367 (figure)
- Khashoggi, J., 313–314
- Khomeini, A., 62, 80, 421
- Khrushchev, N., 418
- Kiang Kwan, 203, 204
- Kildall, G., 300 (box)
- Kipling, R., 393
- Kissinger, H., 196, 269
- Knickebein, 348, 348–349 (box)
- Knorr, K., 203
- Komatsu Corporation, 286
- Kremlinologists, 418
- Kurzweil, R., 305

- Landes, D. S., 137, 270
- Langmuir, I., 287, 299
- Laqueur, W., 77
- Lau, J. Y. F., 74
- Lavorato, J., 376 (box)
- Law enforcement, 14, 37, 59, 90, 152
 - cultural challenge, 66
 - difficulties, 67
 - homeland security and, 92–94
 - network models, 366, 367 (figure)
 - operational intelligence, 26, 28
 - organizations, 217, 436
 - policymakers and military operations, 66
 - strategic intelligence, 25
 - transportation and distribution infrastructure, 49
- Lawrence, T. E., 367
- Lebanon debacle, 129 (box), 178, 179 (table)
- Lebanon war (2006), 27, 28 (box)
- Leeds rapist, 400 (box)
- Libyan government, 387 (box)
- Lincoln, A., 189 (box)
- Lindemann, F., 349 (box)
- Linear models, 146
- Linear programming, 434, 438
- Link model, 363–366
- List, J., 68
- Location analytics, 436
- Logical thinking, 74–75, 84
- Lone-wolf terrorists, 17
- Long, L., 41
- Lowenthal, M., 46, 185, 278

- Low probability of intercept (LPI) techniques, 239
- Lucas, G., 35
- MacArthur, D., 389 (box)
- Machiavelli, N., 14, 75, 77
- Machine learning, 437–438
- Malaysia Airlines Flight MH17, 396 (box), 397 (figure)
- Management review, 266
- Manosevitz, J., 165
- Manual network modeling, 368–369
- The Man Who Never Was* (Montagu), 240 (box)
- Marić, M., 79
- Marrin, S., 63
- MASINT. See Measurements and signatures intelligence (MASINT)
- Mathematical models, 145, 158
- curves, 153
 - exponential/disaster curves, 153, 154 (figure)
 - Gaussian/normal curve, 153, 154 (figure)
 - S curves, 153, 154 (figure)
 - single equations, 152
 - spreadsheets and simulations, 153
- Matrix model, 148–149, 149 (table), 363
- McChrystal, S., 49, 51
- McCone, J., 80, 202 (box)
- McConnell, M., 38, 177
- McDonnell Douglas, 410 (box)
- McKenzie, F., 44
- McNamara, R., 60, 62
- Measurements and signatures intelligence (MASINT), 110, 185, 229, 233, 389, 398
- Message presentation
- acronyms, 264
 - challenge in, written message, 264
 - communication skills, 263
 - graphics, 265
 - impression, 263
 - main points, 263
 - read/listen, easy making, 263–264
 - visual, 265
 - written reports and verbal briefings, 262
- Methodology, anticipatory intelligence, 297–298, 298 (figure)
- alternative scenarios, 308–309
- convergent/divergent phenomena, 298–301
- estimative approach, 301–304
- extrapolation, 305–308
- forecasting, 316–321
- high-impact/low-probability analysis, 304–305
- influence net modeling, 313–314, 314 (figure)
- influence trees/diagrams, 309–313
- iterative approach, 301–302, 303 (figure)
- probabilistic projection methods, 315
- projection, 308
- sensitivity analysis, 315–316
- unintended consequences, 321–322
- Microsoft, 300 (box)
- Military leadership and operations, 64–65
- Military services, 94
- Military simulation models, 409–412, 435
- Military tool, 20
- Miller, B., 430
- Milton, J., 68
- Mindsets, 6
- ethnocentric bias, 6–7
 - parochial interests, 7
 - policymakers, 61–62
 - premature closure, 7
 - status quo biases, 7
 - wishful thinking, 7
- Mirror-imaging, 150
- challenge, 348 (box), 350–351
 - cultural, 417–418 (box)
- Mission managers, 90
- Mitchell, W., 251
- Modal personality profiles, 150–152
- Momentum scenarios, 332–333
- Money laundering, 286
- Monopolitania BW development organization, 173
- collateral models, 174–176, 175 (figure), 176 (figure)
 - submodels, 173, 174 (figure)
- Montagu, E., 240 (box)
- Monte Carlo simulation method, 315
- Moore's law, 305, 306 (figure)
- Morris, J., 191
- Movement intelligence (MOVINT), 395, 396, 402
- Moving target indicator (MTI), 395
- Mubarak, H., 421
- Muddle-through NIE, 443–444

- Mueller, R., 23 (box)
- Mujahedeen insurgency, 344–345 (box)
- Multidisciplinary analysis, 318
- Musharraf, P., 421
- The Mythical Man-Month* (Brooks), 356
- National character, 150
- National Intelligence Council (NIC), 95, 122, 328, 441, 446
- National intelligence estimate (NIE), 8, 81, 96, 264, 315
- ad hoc teams, 91, 91 (box)
 - Iraqi WMD, 446–453
 - policymakers, 59–60
 - SIGINT representatives, 81
 - Yugoslavia, 441–445
- National intelligence managers (NIMs), 90
- National intelligence officer (NIO), 271
- National Intelligence Priorities Framework (NIPF), 62
- National Security Act of 1947, 62
- National Security Council (NSC), 40, 59, 96, 121, 293
- NATO. See North Atlantic Treaty Organization (NATO)
- Natural gas pipeline, 390–391 (box)
- Natural language processing, 437
- Nature of intelligence, 24–25
- Naval gunnery, 190, 285 (box)
- Negative feedback systems, 289–290
- Negus, G., 77, 115
- Netwar, 15–16, 364
- cocaine network, 49, 50 (figure)
 - competition, 49, 50 (figure)
 - Erdoğan-Gülen, 18 (box), 22, 23 (box), 313
- Network(s), 364
- air defense, 49
 - commercial, 375–378
 - communications, 48
 - companies, 50–51
 - development, 378
 - family and cultural, 368
 - financial, 378–379
 - functional, 368
 - national intelligence efforts, 51
 - vs. network, 48–49, 50 (figure)
 - nodes, 48
 - nonstate actors, 48
- ownership, 378
 - political, 378
 - social, 412–413
 - targeting physical, 434
 - technology, 378
 - vertical, 378
 - virtual, 368
- Network analysis, 370
- automating, 381–382
 - organizational, 374–375
 - SNA, 371–372
 - target, 379–380
 - threat, 380–381
- Network-centric conflict, 15, 50–51
- Network-centric warfare, 50
- Network model, 363–364, 366, 424
- automated, 369–370
 - computer-assisted, 369–370
 - diagram features, 367 (figure)
 - manual, 368–369
 - nodal analysis, 370
 - template, 369
 - types, 367–368
- Newton's first law of motion, 283
- New York Police Department (NYPD), 94
- NGOs. See Nongovernmental organizations (NGOs)
- NIE. See National intelligence estimate (NIE)
- 9/11 attacks, 6, 93, 97, 104, 108, 286, 300
- Nodal analysis, 364, 370
- Nongovernmental organizations (NGOs), 15, 22, 28 (box), 51, 94–95
- Nonlinear models, 146
- Nonstate actors, 16–18
- individuals, 17
 - insurgents, 17
 - political tools, 19
 - terror weapons, 18
 - transnational criminal enterprises, 17
- Normative model, 145
- Normative scenario, 431–432
- North Atlantic Treaty Organization (NATO), 91, 97, 167, 419, 434
- Nuclear Engine for Rocket Vehicle Application (NERVA), 401 (box)
- Nuclear power industry, 290
- Nuclear test, 244–245 (box)
- NYPD Intelligence Bureau, 94

- Obama, B., 292, 411
- Object-based production (OBP), 42
- Obscurity, 109
- Occam's razor, 188
- Oerlikon heavy machine gun, 344–345 (box)
- Ogilvy, J., 337
- Open-source intelligence (OSINT), 110, 184–187, 194, 219, 228, 233, 243, 260
- Operating system, 300 (box)
- Operational code model, 419
- Operational ELINT (OPELINT), 111
- Operational intelligence
- capabilities and intentions, 26
 - Desert Shield/Desert Storm, 27, 27 (box)
 - vs. information, 111–112
 - intelligence-led policing, 28
 - law enforcement, 26, 28
 - Lebanon war (2006), 27, 28 (box)
 - planning scenarios, 26
 - predictive, 27
 - SWOT method, 26
 - targeting process, 27
- Operation Barbarossa, 3–4
- Operation Dark Winter, 412–413
- Operation Iraqi Freedom, 45
- Operations research (OR), 433
- problem definition, 433
 - resource allocation, 433–434
 - targeting physical network, 434
- Opium poppy processing, 162
- Opium production, Afghanistan, 157, 157 (figure)
- Opportunity costs, 226
- Opportunity-driven process, 96
- Organizational network analysis, 374–375, 383
- commercial, 375–378
 - financial, 378–379
 - function, 375
 - process, 375
 - structure, 375
- Organization Risk Analyzer (*ORA), 381
- OSINT. See Open-source intelligence (OSINT)
- P5+1-Iranian negotiations, 352–353 (box)
- Panetta, L., 65
- Paris Peace Conference (1919), 393 (box)
- Parochial interests, 7
- Passive deception technique, 239
- Pasteur, L., 6
- Pattern models
- histograms, 157, 157 (figure)
 - POL, 155, 158
 - recognition, 155
 - statistical analysis, 155
 - temporal, 155
 - timelines, 156, 156 (figure)
- Pattern-of-life (POL) modeling, 155, 158
- Pearl, D., 197
- Pearl Harbor attack, 103, 105, 417 (box)
- Pearl Harbor: Warning and Decision* (Wohlstetter), 104
- Peer review, 265–266
- People's Liberation Army (PLA), 13, 111, 318
- Perception management, 245, 255
- Performance analyses, 346
- comparative modeling, 347–350
 - mirror-imaging challenge, 350–351
- Petersen, M., 269
- Pherson, R. H., 177, 327, 333
- Philip II, 61
- Philosophical beliefs, 419
- Philosophical predisposition, 203
- Physical model, 145
- Pillar, P., 113, 144
- Pinker, E. J., 421–422
- Plausible future scenarios, 328
- PMESII factors. See Political, military, economic, social, infrastructure, and information (PMESII) factors
- Point/interval estimation method, 315
- Policon, 414–415, 436
- Policymakers, 126, 270, 281, 286, 319, 432
- analyst interactions, 62–63
 - business customers, 67
 - competitive framework, 178, 179 (table)
 - environment, 60–61
 - Lebanon case, 129 (box), 130
 - mindset, 61–62
 - NIEs, 59–60
 - pressures, 113, 114
 - priorities, 62
 - problems, complexity, 60
 - scientific experts, 270
- Political corruption, 75

- Political, military, economic, social, infrastructure, and information (PMESII) factors, 127 (figure), 139, 166–173, 282–283, 369
- Azerbaijan's plans, 128
- description, 126–127
- DIME actions, 125, 126
- government's plans, 128
- law enforcement, 127
- system-change scenarios, 331
- Political stability, 138
- Political systems simulation, 414–415, 424, 436
- Positive feedback systems, 289–290
- Possible future scenarios, 328
- Possible Nuclear Underground Test Site (PNUTS), 401 (box)
- Post, J., 151, 289, 419
- Poverty relief program, 309, 313
- Powell, C., 429
- Precision weapons, 20
- Predictive battlespace awareness, 411–412
- Predictive mechanisms, 301
- Preferred future scenarios, 328
- Premature closure, 7, 201–202
- Prescriptive analytics, 436–438
- Prescriptive intelligence, 101, 110, 429–430
- analytics, 436–438
 - anticipatory and, 431 (figure)
 - operations research, 433–434
 - process, 431
 - scenarios, 431–432
 - simulations, 435–436
- President's Daily Brief (PDB), 59, 107
- Pressures, 112
- defense analysis, 114–115
 - external, 113–114
 - internal, 112–113
 - temporal, 115–116
- The Prince* (Machiavelli), 14
- Probabilistic graphical model, 292, 294
- Probabilistic projection methods, 315
- Probabilistic reasoning, 308, 311
- Probable future scenarios, 327
- Process models, 351–352
- Iranian nuclear warhead, 353, 354 (figure)
 - prescriptive intelligence, 431
 - program cycle/staffing model, 354–357, 355 (figure)
 - revised analysis, 353, 354 (figure)
 - technological factor, 357–358
- Profile models, 150–152, 158
- Program cycle model, 354–355, 355 (figure)
- Program evaluation and review technique (PERT) chart, 359
- Program for Monitoring Emerging Diseases (ProMED), 95
- Program staffing model, 356–357
- Projection mechanism, 301, 308
- Prospect theory, 68
- Psychology of Intelligence Analysis* (Heuer), 205
- Putin, V., 108, 299–300, 419
- Qiao Liang, 13, 14, 19
- Quality of information check, 187–188
- Quantum physics, 299
- Rabta plant, 387 (box)
- Ransomware, 30 (box)
- Rational models, decision making, 415–416
- Raw intelligence, 3, 90, 111, 115
- analysts and customers, 186–187
 - data handling, automation, 187
 - information, 397
 - literal and nonliteral, 186–187, 186 (figure)
- US collection taxonomy, 184–185, 185 (figure)
- Reagan, R., 129 (box), 250 (box)
- Red teams, 266–267, 423
- Reducing uncertainty, 24, 31
- Regional information sharing system (RISS) centers, 93
- Relationship models, 343, 363
- hierarchy model, 363
 - link model, 363–366
 - matrix model, 363
 - network analysis, 370–382
 - network model, 363–370
- Resource allocation, 433–434
- Revolution in military affairs, 65
- Risk analysis, 358–359
- assessment, 359, 360
 - management, 359
- Rockwell, N., 189 (box)
- Rommel, E., 197
- Ronfeldt, D., 15
- Roosevelt, F., 196
- Roosevelt, T., 285 (box)
- Rossmo, K., 400 (box)
- Royal Dutch Shell, 50–51
- Rusk, D., 61

- Sales intelligence, 269
 Sanders, B., 292
 SATs. *See Structured analytic techniques (SATs)*
 Sayyaf, A., 372 (box), 374
 Scenarios, anticipatory intelligence, 327
 Alternative Scenarios for 2040, 328–329
 demonstration, 432
 driving-force, 330–331, 339
 dynamic, 334
 forms of, 327–328
 intelligence steps, 339
 logics, 334, 336
 military, 334
 momentum, 332–333
 normative, 431–432
 perspectives, 332
 planning, 332, 335
 prescriptive intelligence, 431–432
 SARS outbreak, 337
 Shell energy, 333–338, 334 (figure)
 straight-line extrapolation, 332
 strategies, 330
 system-change, 331
 tools for, 343
 Schlesinger, J., 114
 Schum, D., 177, 191
 Schwartz, P., 332, 337. *See also Shell energy scenario*
 Scientific and technical (S&T) analysis, 9, 60, 149, 185, 223, 264
 S curves, 153, 154 (figure)
 Sensitive compartmented information (SCI) system, 243
 Sensitivity analysis, 315–316, 324
 September 11 attacks. *See 9/11 attacks*
 Shannon, C., 191, 193
 Shell energy scenario, 333–335, 334 (figure)
 case-based models, 336–337
 cross-impact analysis, 337
 driving forces/factors, 335
 implications in, 337–338
 issue definition, 335
 logics selecting, 336
 monitoring, 338
 target framework, 335
 Signaling, D&D
 analyzing, 252
 cultural differences, 253, 253 (figure)
 declaration of war, 253
 failure to understand, 254
 Iraq/Kuwait example, 254
 massing troops, 252
 verbal and nonverbal, 252
 Signals intelligence (SIGINT), 3, 44, 185, 191, 396, 398
 CCS operations, 226
 D&D, 238, 248
 France's CERESsatellite, 389
 Lebanon war, 28 (box)
 NIE process, 81
 Operation Desert Shield/Desert Storm, 27 (box)
 Silk Road, 21, 22 (box)
 Simple projection, 305
 Sims, W., 284, 285 (box)
 Simulation models, 146, 153, 343, 438–439
 administrative models, 416–417
 Backfire bomber, 409–410 (box), 422
 creating, 422
 cultural models, 417–418
 economic, 408, 408 (figure), 435
 emotional models, 418–419
 game theory, 420–422
 geospatial, 413, 436
 group decision-making models, 419–420
 military, 409–412, 435
 operational code model, 419
 political systems, 414–415, 436
 prescriptive intelligence, 435–436
 rational models, 415–416
 running, 423
 social, 412–413, 436
 types of, 407–408
 wargaming, 410–412
 weapons systems, 409–410
 Single-source analysis, 110–111
 Smith, A., 76
 SNA. *See Social network analysis (SNA)*
 Snowballing technique, 369
 Snowden, E., 97
 Social contamination, 287, 293
 Social network analysis (SNA), 369, 379, 383
 actors, 371
 centrality, 372–374
 diagram, 371 (figure)
 equivalence, 374
 graphics, 372
 star network, 373–374, 373 (figure)
 Social network models, 363
 Social simulations, 412, 436
 geospatial, 413
 social networks, 412–413

- Society for Worldwide Interbank Financial Telecommunication (SWIFT), 224
- Soleimani, Q., 43–44 (box)
- Solntsevskaya Bratva, 17, 380
- Solvable model, 147
- Spatial and temporal attributes, target, 51–52
- Spreadsheets, 153
- Stalin, J., 3–4, 7, 271
- Starbursting, 138–139
- Star network, 373–374, 373 (figure)
- Static geospatial models, 389–395, 402
- Static model, 147
- Status quo biases, 7
- Statute of Uses, 321
- Stochastic model, 146
- Straight-line extrapolation, 305, 332, 451
- Strange attractors, 299
- Strategic Arms Limitation Talks (SALT), 410 (box)
- Strategic Defense Initiative (SDI), 302
- Strategic intelligence, 25, 102
- Structured analytic techniques (SATs), 9–10, 63, 138–139
- Structured Analytic Techniques for Intelligence Analysis* (Heuer and Pherson), 177
- Structured argumentation, 205
- ACH, 205–207
- Bayesian analysis, 207–208
- Structuring message
- communication skills, 259
 - conclusions, 261
 - customers, 260–261
 - facts, 261–262
 - presentation, analysts, 259–260
- Sun Tzu, 302, 388
- Surface-to-air missile (SAM), 17, 20, 245 (box), 291, 344 (box), 346, 396 (box)
- Swarm approach, 291
- SWOT (strengths, weaknesses, opportunities, and threats) method, 25, 58, 65
- Symantec's tactical intelligence, 30 (box)
- Synergy, 290–291, 294
- of tools, 22
- Synthesis approach, 346
- Synthetic aperture radar (SAR), 185, 395, 396, 413
- Syrian refugee movement, 413, 413 (figure), 414 (figure)
- System-change scenarios, 331, 339
- System dynamics, 302
- System life cycle, 354
- Systems modeling and analysis, 343–345
- aspects of, 346
 - cost, 359–360
 - function, 344
 - methodology, 345–346
 - performance, 346–351
 - process, 344, 351–358
 - risk, 358–359
 - structure, 344
- Tactical intelligence, 25, 102–103
- battle damage assessment, 30
 - battlespace awareness, 29
 - geospatial analysis, 29
 - symantec, 30 (box)
 - weapons technology, 29
- Target-centric approach/process, 8, 41 (figure), 297, 314
- Al Asad case, 45
- all-source and single-source analysts, 42
- characteristics of intelligence, 42–43
- collaborative team concept, 45–46
- customer satisfaction, 45
- Iranian air defense system, 44
- knowledge gaps/information requirements, 43
- network process, 40
- OBP, 42
- sequence neutrality, 41
- SIGINT and HUMINT, 44
- stakeholders, 40
- team-generated view, 45
- Target framework
- al-Shabaab ideology, 163–165
 - alternative, 176–178
 - Azerbaijan, 165–173
 - competitive, 178–179
 - complex, 161
 - dynamic, 179
 - generic, 162
 - Monopolitania BW development organization, 173–176
 - system, 161, 162
- Targeting analyst, 110, 227
- Target models
- assumption, 144
 - COMINT analysts, 143
 - comparative models, 148–150

- conceptual models, 145–147
- economic analysts, 143
- fact, 144
- hierarchy of, 145, 145 (figure)
- hypothesis, 144
- imagery analysts, 143
- mathematical models, 152–153
- operations research and systems analysis, 144
- pattern models, 155–157
- physical model, 145
- profiles, 150–152
- thinking and creativity, 144
- Target network analysis, 364, 367, 371, 379–380, 382–383
- Tasking, collection, processing, exploitation, and dissemination (TCPED), 41
- Technological factor, process model, 357–358
- Technophiles, 305
- Temporal pressures, 115–116
- Tenet, G., 447
- Thalidomide, 290
- Thinking About the Unthinkable* (Kahn), 432
- Threat network analysis, 380–383
- Tito, J. B., 443
- Tradecraft Primer*, 130, 144, 187, 188, 281, 304, 328, 338
- Traditional intelligence cycle, 35, 36 (figure)
 - analysis, 36, 38
 - antisocial, 37
 - collection, 36, 37
 - dissemination, 37, 268
 - DoD, 38, 39 (figure)
 - Ford production cycle, 39–40 (box), 40
 - intelligence officers and policymakers, 37
 - planning/direction, 36
 - problem solving, 38
 - processing, 36
 - requirements, 36
- Trans-Afghanistan natural gas pipeline, 390–391 (box), 391 (figure)
- Transnational criminal enterprises, 17
- Trend impact analysis, 337
- Triggering events, 432
- Trump, D., 22, 260, 313
- Tsarnaev, D., 152
- Tuchman, B., 299
- Turkmenistan-Afghanistan-Pakistan-India pipeline (TAPI), 390 (box)
- Turner, S., 62, 80
- Tutwiler, M., 254
- Twenty-first-century conflicts
 - networks, 15–16
 - nonstate actors, 16–18
- Ulbricht, R., 22 (box)
- Unidentified Research and Development Facility-3 (URDF-3), 115, 401 (box)
- Unintended consequences, law of, 321–323
- Union of Soviet Socialist Republics (USSR), 7, 169, 288, 336
- Unmanned aerial vehicle (UAV), 21, 46, 167, 337, 446, 448, 450, 451
- Unrestricted Warfare* (Qiao Liang and Wang Xiangsui), 13
- USA PATRIOT Act, 111
- US containment policy, 19, 299
- US intelligence community, 278, 338, 364
- US national intelligence network
 - ad hoc teams, 91–92
 - all-source analysis groups, 89–90
 - matrix structure, 90
 - NIMs, 90
 - structural issues, 90
 - virtual teams, 92
- V-2 rocket, 200 (box)
- Van Heuven, M., 443–444, 451
- Vested interest, 189–190
- Vickers, M., 365 (box), 344
- Virtual networks, 368
- Virtual teams, 92
- Vividness weighting, 196–197
- Walmart, 51
- Walsingham, F., 215, 216, 230
- Wang Xiangsui, 13, 14, 19
- WannaCry, 30 (box)
- Wargaming simulations, 410–412, 424
- Warning of war, 271
- Warsaw Pact, 434
- Weapons of mass destruction (WMD), 78, 90, 115, 178, 199, 229, 355, 410.
 - See also* Iraqi WMD Commission; Iraqi WMD NIE
- Weapons systems simulations, 409–410, 424
- Western powers, 22

- White, S., 398
Wide-area motion imagery, 396
Williams, B., 376 (box)
Wilson, C., 344 (box)
Wilson, W., 393 (box)
Wishful thinking, 7
WMD. See Weapons of mass destruction (WMD)
Wohlstetter, R., 104
World War I, 299, 300
World War II, 104, 197, 200, 240 (box), 248, 347 (box), 350 (box), 388, 433–434
Wright, P., 199
Wu, G., 68
Würzburg radar, 347–348 (box)
- Yakuza organization, 374
Yamaguchi-gumi, 17
Yamantau Mountain, 401 (box)
Yom Kippur War, 4, 7, 108, 318
Yugoslavia NIE, 441
 alternative projection, 444–445
 customer view, 445
 muddle-through NIE, 443–444
 setting, 442–443
- Zapatista netwar, 15, 16

ABOUT THE AUTHOR

Robert M. Clark has over five decades of US intelligence community experience. A USAF lieutenant colonel (retired), Dr. Clark served as an electronics warfare officer and intelligence officer. At the CIA, he was a senior analyst and group chief responsible for developing analytic methodologies. He was cofounder and CEO of the Scientific and Technical Analysis Corporation, a privately held company serving the US intelligence community. Clark holds an SB from MIT, a PhD in electrical engineering from the University of Illinois, and a JD from George Washington University. Beyond analyzing wicked intelligence issues, his passion is writing on the topic of intelligence. In addition to *Intelligence Analysis: A Target-Centric Approach*, his books include *The Technical Collection of Intelligence* (2010), *Intelligence Collection* (2014), and *Geospatial Intelligence* (2020). He is coauthor, with Dr. William Mitchell, of *Target-Centric Network Modeling* (2015) and *Deception: Counterdeception and Counterintelligence* (2019); and coeditor, with Dr. Mark Lowenthal, of *The Five Disciplines of Intelligence Collection* (2015). Dr. Clark also develops and teaches courses for audiences in academia, national intelligence, and the military. He currently serves as a lecturer at the Johns Hopkins University, teaching graduate courses.