INTTELLIGENCE
ANALYSIS

FOURTH EDITION
Contents

Tables, Figures, and Boxes xii

Preface xvi

Introduction xix
   Why We Fail xix
   Failure to Share Information xx
   Failure to Analyze Collected Material Objectively xxi
   Failure of the Customer to Act on Intelligence xxii
What the Book Is About xxiii
Summary xxiv

Part 1 Introduction to Target-Centric Analysis 1

1 The Intelligence Process 1
   The Nature of Intelligence: Reducing Uncertainty in Conflict 3
   The Traditional Intelligence Cycle 4
   Intelligence as a Target-Centric Process 7
   The Target 11
      The Target as a Complex System 12
      The Complex Target as a Network 13
Summary 17

2 Defining the Intelligence Problem 19
   Statement of the Problem 20
   The Problem Definition Product 22
   Detailed Problem Definition: Strategies-to-Task 23
   Strategies-to-Task and Complex Problems 25
   Example: Defining the Counterintelligence Problem 28
Summary 29

3 An Analysis Approach to the Target 31
   The Concept of a Model 32
   Using Target Models for Analysis 35
   Counterintelligence Analysis 37
      Targets 37
      Operations 37
      Linkages 38
   Target Model Combinations 38
      Submodels 39
      Collateral Models 40
Summary 42
4 The Analytic Spectrum 44
   The Conflict Spectrum 44
      Strategic Intelligence 46
      Operational Intelligence 46
      Tactical Intelligence 50
   The Temporal Analysis Spectrum 52
      Long-Term Research Versus Current Intelligence 53
   The Tyranny of Current Intelligence 54
   Fusion Centers 55
      Capabilities, Plans, and Intentions 55
   Indications and Warning 56
   Summary 59

Part 2 Synthesis: Creating the Model 61

5 Overview of Models in Intelligence 62
   Creating a Conceptual Model 62
   Generic Models 63
      Lists 63
      Curves 63
      Comparative Modeling (Benchmarking) 65
   Pattern Models 66
   Relationship Models 70
   Profiles 77
   Process Models 79
   Simulation Models 80
   Combination Models 82
   Geospatial Models 82
   Human Terrain Models 84
   Space-Time Models 85
   Geographic Profiling 86
   Summary 87

6 Sources of Intelligence Information 89
   Existing Reports 89
   A Taxonomy of Intelligence Sources 90
   Literal Intelligence Sources 93
      Open Source 93
      Human Intelligence 96
      Communications Intelligence 101
      Cyber Collection 106
   Nonliteral Intelligence 112
      Remote and In Situ Sensing 112
      Imaging and Spectral Sensing 114
Passive Radiofrequency Intelligence 117
Radar Intelligence 119
Geophysical and Nuclear Intelligence 119
Materiel and Materials Collection 121
Biometrics 123
Summary 123

7 Evaluating and Collating Data 127
Evaluating Evidence 127
  Evaluating the Source 128
  Evaluating the Communications Channel 131
  Evaluating the Credentials of Evidence 133
  Pitfalls in Evaluating Evidence 136
Combining Evidence 143
  Convergent and Divergent Evidence 143
  Redundant Evidence 143
  Formal Methods for Combining Evidence 144
Summary 145

8 Collection Strategies 147
The U.S. Collection Management Problem 148
The Problem Breakdown and
  Target Model Relationship 151
Identifying Gaps 154
Developing the Collection Strategy 156
  Using Existing Collection Assets 156
  Dealing with Enigmas 162
Planning for Future Collection: Filling
  the Long-Term Gaps 163
  Executing Collection Strategies 164
Summary 165

9 Denial, Deception, and Signaling 167
Denial and Deception 167
Defense Against D&D: Protecting Intelligence
  Sources and Methods 169
Higher Level Denial and Deception 171
  The Man Who Never Was 171
  The Cuban Missile Crisis 172
  The Farewell Dossier 173
  The Indian Nuclear Test 174
Countering Denial and Deception 175
Signaling 178
Analytic Tradecraft in a World of D&D 180
Summary 181
Part 3  Predictive Analysis  183

10  Analytic Methodologies  184
    Structured Argumentation  184
       Wigmore’s Charting Method  185
       Bayesian Techniques for Combining Evidence  186
    Competitive and Alternative Target Models  188
       Competitive Analysis  188
       Alternative Analysis  189
    The Role of Information Technology  191
    Summary  192

11  Prediction  195
    Introduction to Prediction  195
    Convergent and Divergent Phenomena  196
    The Predictive Approach  198
       Introduction to Force Synthesis/Analysis  202
       Qualitative Force Synthesis/Analysis  203
    Scenarios  203
       Why Use Scenarios?  204
       Types of Scenarios  205
       Scenario Perspectives  207
       How to Construct Scenarios  207
       Indicators and the Role of Intelligence  212
       A Scenario Exercise: The Global Information
          Environment in 2020  213
    Summary  216

12  Predictive Techniques  218
    Extrapolation  219
       Extrapolation Techniques  219
       Correlation and Regression  221
       Limitations of Extrapolation  222
    Projection  223
       Generating Alternatives  223
       Influence Trees or Diagrams  224
       Influence Nets  228
       Making Probability Estimates  229
       Sensitivity Analysis  230
    Forecasting  231
       The Nonlinear Approach to Forecasting  232
       Techniques and Analytic Tools of Forecasting  234
       Evaluating Forecasts  234
    Summary  235
13 Shaping Forces 237
   Inertia 237
   Countervailing Forces 239
   Contamination 240
   Synergy 242
   Feedback 244
      Strength 246
      Time Delay 246
   Regulation 247
   Summary 250

14 Organizational Analysis 252
   Structure 253
      Organizational Size and Capabilities 253
      Type of Structure 254
      Network Analysis 254
   Function 260
      Rational Aspect 260
      Cultural Aspect 262
      Emotional Aspect 266
      Collective Decision Making 267
   Process 267
      Operations Research 268
      Schedule 270
      Cost 274
   Summary 276

15 Technology and Systems Analysis 279
   Technology Assessment 279
      Future Performance 280
      Innovation 282
      Technology Use, Transfer, and Diffusion 286
   Systems Analysis 290
      Future Systems 291
      Performance Analyses 293
   Systems Simulation 299
      Simulations Used in Intelligence Analysis 300
      Creating and Running a Simulation 301
   Summary 303

16 The Intelligence Customer 306
   Introduction 306
      Policymakers 307
      Congress 311
Business Leaders 312
Military Leadership 312
Military Operations 313
Homeland Security 313
Law Enforcement 314
What All Customers Want 315
Analyst-Customer Interaction 316
Analyst as Communicator: Getting the Customer to Understand the Message 317
Analyst as Advocate: Getting Buy-In 318
The Defense Analysis Challenge 321
Presenting Analysis Results 322
Support Every Analytic Conclusion 322
Write or Brief with a Purpose 323
Separate Facts from Analysis 323
Get to the Point 324
Write or Brief to Inform, Not to Impress 324
Make It Easy and Enjoyable to Read or Listen To 325
Write as You Would Talk 325
Avoid Acronyms 326
Use Graphics 326
Summary 326

17 Managing Analysis 329
Introduction 329
Who Are the Customers, and What Do They Need? 330
What Should the Unit Produce? 331
Structure 332
Topical or Regional Structure? 332
Fusion Centers 333
To Firewall or Not to Firewall 334
Process 335
The Analyst 335
Recruiting and Developing Analysts 338
Planning the Analysis Project 340
Managing Team Efforts 341
Peer and Management Review 346
Collaborative Tools 347
Sharing Versus Protection of Sources and Methods 347
Limits and Boundaries 348
Limits 349
Boundaries 350
Function 353
Pressures 353
Tables, Figures, and Boxes

Part 1  Introduction to Target-Centric Analysis  1

1  The Intelligence Process  2
   Figure 1–1: Traditional Intelligence Cycle  5
   Figure 1–2: A Target-Centered View of the Intelligence Process  8
   Figure 1–3: Example Target: Cocaine Network  12
   Figure 1–4: Netwar Competition: Network Versus Network  14
   Figure 1–5: Netwar Example Against a Cocaine Network  15

2  Defining the Intelligence Problem  19
   Figure 2–1: Political Situation Strategies-to-Task Problem Breakdown  24
   Figure 2–2: Country X Economic Problem Breakdown  25
   Figure 2–3: Economic Sanctions Problem Breakdown  26
   Figure 2–4: Counterintelligence Problem Breakdown  29

3  An Analysis Approach to the Target  31
   Box 3–1: Analysis Principle 3–1: The Essence of Intelligence  32
   Figure 3–1: The Model Hierarchy  33
   Figure 3–2: Generic Biological Weapons System Process Model  39
   Figure 3–3: Biological Weapons System Test Process Submodel  40
   Figure 3–4: Biological Weapons Development Organization Model  40
   Figure 3–5: Collateral Model of Biological Weapons Facilities  41
   Figure 3–6: Chronological Model of Biological Weapons Development  42

4  The Analytic Spectrum  44
   Figure 4–1: The Conflict Spectrum  45
   Figure 4–2: The Temporal Synthesis/Analysis Spectrum  53

Part 2  Synthesis: Creating the Model  61

5  Overview of Models in Intelligence  62
   Figure 5–1: The Exponential (or Disaster) Curve  64
   Figure 5–2: The “S” Curve  65
   Figure 5–3: The Normal Curve  65
   Figure 5–4: Histogram of Opium Production, 2000 to 2008  68
   Figure 5–5: Chronological Model of Firm’s Expected External Actions  68
   Figure 5–6: Satellite Visibility and Set Over Bermuda, Day
6 Sources of Intelligence Information 89

7 Evaluating and Collating Data 127

8 Collection Strategies 147

9 Denial, Deception, and Signaling 167

Part 3 Predictive Analysis 183

Analytic Methodologies 184
11 Prediction 195
Figure 11–1: The Prediction Methodology 200
Figure 11–2: Applying an Iterative Approach to the Prediction Methodology 201
Box 11–1: Analysis Principle 11–1: Force Analysis According to Sun Tzu 202
Figure 11–3: Predictive Model of the 2010 Global Information Environment 215
Figure 11–4: Extrapolated Model of the 2010 Global Information Environment 215

12 Predictive Techniques 218
Figure 12–1: Trend Extrapolation for Productivity of Civil and Military Transport Aircraft 220
Figure 12–2: Trend Extrapolation for Repeating Phenomena: The Sunspot Cycle 221
Figure 12–3: Correlation of Number of Telephones with Gross National Product (GNP), 1998 222
Figure 12–4: An Influence Tree for Insurgency 226
Figure 12–5: Influence Tree with Probabilities 228
Figure 12–6: An Example Influence Net Model 230
Figure 12–7: Sensitivity Analysis for Biological Warfare Virus Prediction 231

13 Shaping Forces 237
Box 13–1: Analysis Principle 13–1: Inertia 237
Box 13–2: Analysis Principle 13–2: Newton's Third Law (the Dialectic) 239
Figure 13–1: The Feedback Process 245
Box 13–4: Analysis Principle 13–4: The Law of Unintended Consequence 248

14 Organizational Analysis 252
Figure 14–1: The Laffer Curve for Tax Rates 254
Figure 14–2: Social Network Analysis Diagram 256
Figure 14–3: Social Network Analysis: A Star Network 257
Figure 14–4: Linear Programming Solution for Tank Production 270
Figure 14–5: The Generic Program Cycle 271
Figure 14–6: The Brooks Curves for Projects 272
Figure 14–7: A Cost/Utility Plot 275
15 Technology and Systems Analysis 279
   Figure 15–1: The S Curve for Technology Development 282
   Table 15–1: Effectiveness of Technology Transfer Mechanisms 289

Appendix I: A Tale of Two NIEs 365
   Figure AI-1: Influence Net Model: Yugoslavia NIE First Draft 367
   Figure AI-2: Influence Net Model: Yugoslavia NIE Second Draft 369

Appendix II: Example Project Plan 376
   Figure AII-1: Example Problem Breakdown of Major Drug Threats 377
Preface

T
he first edition of this book was published in 2003, soon after the terrorist attack on U. S. soil of September 11, 2001, and the U. S. led invasion into Iraq, more commonly called the Iraq War, on March 20, 2003. Those two events focused the world’s attention on apparent failures of the U. S. intelligence community.

But as Professor Stephen Marrin has pointed out, in the case of the 9/11 attack, more important are the strategic policy failures that preceded the intelligence failures.\(^1\) And as former National Intelligence Officer Paul Pillar has pointed out, the 9/11 Commission report (published in September of 2004) appears to have been shaped to fit political purposes rather than to conduct an objective inquiry.\(^2\) I submit that both the 9/11 attack and the Weapons of Mass Destruction (WMD) debacle resulted primarily from failures in U.S. strategic policy, abetted by intelligence failures. The intelligence failures in both cases were collaborative rather than causative.

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

If an intelligence community is interested in real improvement, it should begin with a focus on process, not on structure and function. An effective intelligence process then will engender effective structure and function. A major contribution of both the 9/11 and the Iraqi WMD Commissions was their focus on a failed process, specifically on that part of the process where intelligence analysts interact with their policy customers.

Thus, this book has two objectives:

- The first objective is to redefine the intelligence process to help make all parts of what is commonly referred to as the “intelligence cycle” run smoothly and effectively, with special emphasis on both the analyst-collector and the analyst-customer relationships.
- The second goal is to describe some methodologies that make for better predictive analysis.

The book therefore defines a better intelligence analysis process, one that appears to be emerging within the U.S. and other intelligence communities.
and puts specific analysis techniques in context, showing how they interrelate within that process.

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

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

The second goal is to clarify and refine the analysis process by drawing on existing prediction methodologies. These include the analytic tools used in organizational planning and problem solving, science and engineering, law, and economics. In many cases, these are tools and techniques that have endured despite dramatic changes in information technology over the past 50 years. All can be useful in making intelligence predictions, even in seemingly unrelated fields. In fact, a number of unifying concepts can be drawn from these disciplines and applied when creating scenarios of the future, assessing forces, and monitoring indicators. The book highlights these concepts in boxes called analysis principles and treats them as fundamental principles of intelligence analysis. These boxes should make the book a valuable reference even as the world continues to change.

This book was written originally for the practicing intelligence analyst, though it intended to be of interest to all intelligence professionals, students, and customers of intelligence. Intelligence professionals can spend their entire careers on specialized topics such as behavioral analysis, 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 in-depth studies and reports on specific techniques. The book offers insights that intelligence customers and
analysts alike need to become more proactive in the changing world of intelligence and to extract more useful intelligence.

Many examples of intelligence failures are discussed in the book, possibly leading a reader to get the impression that we experience more failures than successes. Quite the opposite is true. Most major intelligence services probably have more analytical successes than failures. But the failures, real and perceived, are more visible, and the book concentrates on failures for two reasons. First, sharing our intelligence failures openly ensures that there will be fewer of them in the future. Second, we probably learn more from our failures than from our successes.

This fourth edition has been prepared primarily in response to suggestions made by readers. The previous editions’ wide use in academia and by government agencies and contractors has resulted in a number of excellent recommendations, and I have attempted to incorporate those ideas throughout. New chapters on analytic methodologies and on managing the analytic unit have been added to increase the value of the book to managers in the intelligence community. The remainder of the book has been extensively revised and updated.

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

Note

Acknowledgments
Many people throughout the U.S. and British intelligence communities, academia, and the business intelligence world have provided wisdom that I have incorporated; I cannot name them all, but I appreciate their help. I am especially grateful to reviewers within and outside the U.S. intelligence community who have contributed their time to improving the text. I also want to thank Elise Frasier at CQ Press for her support and encouragement in shaping this book.

Robert M. Clark
Wilmington, North Carolina
Introduction

_The greatest derangement of the mind is to believe in something because one wishes it to be so._

*Louis Pasteur*

We learn more from our failures than from our successes. As noted in the preface to this book, there is much to be learned from what have been called the two major U.S. intelligence failures of this century—the attacks of September 11, 2001, and the miscall on Iraqi WMD. So this book begins with an overview of why we fail.

Why We Fail

As a reminder that intelligence failures are not uniquely a U.S. problem, it is worth recalling some failures of other intelligence services in the last century:

- **Operation Barbarossa, 1941.** Josef Stalin acted as his own intelligence analyst, and he proved to be a very poor one. He was unprepared for a war with Nazi Germany, so he ignored the mounting body of incoming intelligence indicating that the Germans were preparing a surprise attack. German deserters who told the Russians about the impending attack were considered provocateurs and shot on Stalin’s orders. When the attack, named Operation Barbarossa, came on June 22, 1941, Stalin’s generals were surprised, their forward divisions trapped and destroyed.¹

- **Singapore, 1942.** In one of the greatest military defeats that Britain ever suffered, 130,000 well-equipped British, Australian, and Indian troops surrendered to 35,000 weary and ill-equipped Japanese soldiers. On the way to the debacle, British intelligence failed in a series of poor analyses of their Japanese opponent, such as underestimating the capabilities of the Japanese Zero fighter and concluding that the Japanese would not use tanks in the jungle. The Japanese tanks proved highly effective in driving the British out of Malaya and back to Singapore.²

- **Yom Kippur, 1973.** Israel is regarded as having one of the world’s best intelligence services. But in 1973 the intelligence leadership was closely tied to the Israeli cabinet and often served both as policy advocate and information assessor. Furthermore, Israel’s past military successes had led to a certain amount of hubris and belief in inherent Israeli superiority. Israel’s leaders considered their overwhelming military

¹
²
advantage a deterrent to attack. They assumed that Egypt needed to rebuild its air force and forge an alliance with Syria before attacking. In this atmosphere, Israeli intelligence was vulnerable to what became a successful Egyptian deception operation. The Israeli intelligence officer who correctly predicted the impending attack had his report suppressed by his superior, the chief intelligence officer of the Israeli Southern Command. The Israeli Defense Force was caught by surprise when, without a rebuilt air force and having kept their agreement with Syria secret, the Egyptians launched an attack on Yom Kippur, the most important of the Jewish holidays, on October 6, 1973. The attack was ultimately repulsed but only at a high cost in Israeli casualties.3

- **Falkland Islands, 1982.** Argentina wanted Great Britain to hand over the Falkland Islands that Britain had occupied and colonized in 1837. Britain’s tactic was to conduct prolonged diplomatic negotiations without giving up the islands. There was abundant evidence of Argentine intent to invade, including a report of an Argentine naval task force headed for the Falklands with a marine amphibious force. But the British Foreign and Commonwealth Office did not want to face the possibility of an Argentine attack because it would be costly to deter or repulse. Britain’s Latin America Current Intelligence Group (dominated at the time by the Foreign and Commonwealth Office) accordingly concluded, on March 30, 1982, that an invasion was not imminent. On April 2 Argentine marines landed and occupied the Falklands, provoking the British to assemble a naval task force and retake the islands.4

The common theme of these and many other intelligence failures discussed in this book is not the failure to collect intelligence. In each of these cases, the intelligence had been collected. Three themes are common in intelligence failures.

**Failure to Share Information**

From Pearl Harbor to 9/11 and the miscall on Iraq’s possession of WMD, the inability or unwillingness of collectors and analysts to share intelligence has been a recurring cause of failure.

Intelligence should be a team sport. 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 complex problems of today—will quickly fall apart.5

Nevertheless, the Iraqi WMD Commission (the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, which issued its formal report to President George W. Bush in March 2005) found that collectors and analysts failed to work as a team.6 They
did not effectively share information. And the root causes for the failure to share remain, in the U.S. intelligence community as well as 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. Most governmental intelligence organizations, including the U.S. intelligence community, place more emphasis on secrecy than on effectiveness. The penalty for producing poor intelligence usually is modest. The penalty for improperly handling classified information can be career ending. There are legitimate reasons not to share; the U.S. intelligence community has lost many collection assets because details about them were too widely shared. So it comes down to a balancing act between protecting assets and acting effectively in the world. Commercial organizations are more effective at intelligence sharing because they tend to place more emphasis on effectiveness than on secrecy; they also have less risk of losing critical sources from compromises.

Experts on any subject have an information advantage, and they tend to use that advantage to serve their own agendas. Collectors and analysts are no different. At lower levels in the organization, hoarding information may have job security benefits. At senior levels, unique knowledge may help protect the organizational budget. So the natural tendency is to share the minimum necessary to avoid criticism and to protect the really valuable material. Any bureaucracy has a wealth of tools for hoarding information, and this book discusses the most common of them.

Finally, both collectors of intelligence and analysts find it easy to be insular. They are disinclined to draw on resources outside their own organizations. Communication takes time and effort. It has long-term payoffs in access to intelligence from other sources but few short-term benefits.

In summary, collectors, analysts, and intelligence organizations have a number of incentives to conceal information and see few benefits in sharing it. The problem is likely to persist until the incentives to share outweigh the benefits of concealment.

**Failure to Analyze Collected Material Objectively**

In each of the cases cited at the beginning of this introduction, intelligence analysts or national leaders were locked into a mindset—the consistent thread in analytical failures. Falling into the trap that Louis Pasteur warned about in the observation that I quoted earlier, they believed because, consciously or unconsciously, they wished 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 on 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.

- **Wishful thinking** involves excessive optimism or avoiding unpleasant choices in analysis. The British Foreign Office did not predict an Argentine invasion of the Falklands because, in spite of intelligence evidence that an invasion was imminent, they did not want to deal with it. Josef Stalin made an identical mistake for the same reason prior to Operation Barbarossa.

- **Parochial interests** cause organizational loyalties or personal agendas to affect the analysis process.

- **Status quo biases** cause analysts to assume that events will proceed along a straight line. The safest weather prediction, after all, is that tomorrow’s weather will be like today’s. An extreme case is the story of the British intelligence officer who, on retiring in 1950 after 47 years of 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.”

  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 solution to a problem 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 solution and to reject (or dismiss as unimportant) evidence that conflicts with it.

All of these mindsets can lead to poor assumptions and bad intelligence if not challenged. And as the Iraqi WMD Commission report notes, analysts often allow unchallenged assumptions to drive their analysis.

**Failure of the Customer to Act on Intelligence**

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

A senior state department official once remarked, half in jest, “There are no policy failures; there are only policy successes and intelligence failures.”

The remark rankles intelligence officers, but it should be read as a call to action. Intelligence analysts should accept partial responsibility when their customer fails to make use of the intelligence provided and also accept the challenges to engage the customer during the analysis process to ensure that the resulting intelligence is taken into account when the customer must act.

In this book I devote considerable discussion to the vital importance of analysts being able to objectively assess and understand their customers and
their customers’ business or field. The first part of the book describes a collaborative, target-centric approach to intelligence analysis that 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. The last chapter of the book discusses ways to ensure that the customer takes the best available intelligence into account 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 policymaking intelligence customers to avoid losing objectivity in the national intelligence estimates process. The disadvantages of that separation became apparent, as analysis was not addressing the customer’s current interests, and intelligence 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. But in many cases analysts have been able to work closely with policymakers and to make intelligence analyses relevant without losing objectivity.

What the Book Is About

This book is for intelligence analysts, and it develops a process for successful analysis—including avoiding those three themes of failure.

Studies have found that no baseline standard analytic method exists in the U.S. intelligence community. Any large intelligence community is made up of a variety of disciplines, each with its own analytic methodology. Furthermore, intelligence analysts routinely generate ad hoc methods to solve specific analytic problems. This individualistic approach to analysis has resulted in a great variety of analytic methods, more than 160 of which have been identified as available to U.S. intelligence analysts.

There are good reasons for this 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.

But all intelligence analysis methods derive from a fundamental process. This book is about that process. It develops the idea of creating a model of the intelligence target and extracting useful information from that model. These two steps—the first called synthesis and the second called analysis—make up what is known as intelligence analysis. All analysts naturally do this. The key
to avoiding failures is to share the model with collectors of information and customers of intelligence. While there are no universal methods that work for all problems, a basic process does in fact exist.

There also are standard widely used techniques. An analyst must have a repertoire of them to apply in solving intelligence problems. They might include pattern analysis, trend prediction, literature assessment, and statistical analysis. A number of these techniques are presented throughout the book in the form of analysis principles. These analysis techniques together form a problem-solving process that can help to avoid the intelligence blunders discussed earlier.

Sherman Kent noted that an analyst has three wishes: “To know everything. To be believed. And to exercise a positive influence on policy.”

This book will not result in an analyst’s being able to know everything—that is why we will continue to have estimates. But chapters 1–15 should help an analyst to learn the tradecraft of analysis, and chapter 16 is intended to help an analyst toward the second and third wishes.

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, but most of the incentives in large intelligence organizations promote concealment rather than sharing of information.

• Analysts’ failure to analyze the material collected objectively. The consistent thread in these failures is a mindset, primarily biases and preconceptions that hamper objectivity.

• Failure of customers to 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 fully understand it.

This book is about an intelligence process that can reduce such failures. A large intelligence community develops many analytic methods to deal with the variety of issues that it confronts. But the methods all work within a fundamental process: creating a model of the intelligence target (synthesis) and extracting useful information from that model (analysis). Success comes from sharing the target model with collectors and customers.

Notes

2. Ibid., 102.
3. Ibid., 218.
4. Ibid., 260.
7. Johnson, Analytic Culture, xvi.
8. Ibid., 11.
9. There exists some justification for the harsh penalty placed on improper use of classified information; it can compromise and end a billion-dollar collection program or get people killed.
17. Ibid., 72.
19. Ibid., 12.
Part 1

Introduction to Target-Centric Analysis
The Intelligence Process

Future conflicts will be fought more by networks than by hierarchies, and whoever masters the network form will gain major advantages.

John Arquilla and David Ronfeldt, RAND Corp.

George Lucas’s original Star Wars movie describes the final stages of a human intelligence operation. The heroine, Princess Leia, obtains the plans for the evil Galactic Empire’s ultimate battle machine, the Death Star, from the robot R2-D2, which is functioning as a mobile dead drop.\textsuperscript{1} Leia gives 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 intelligence 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, most of the major failures in intelligence are due to inadequate or nonexistent analysis and most of the rest are due to failure to act on the analysis, as noted in the introduction. The information is usually there, at least in hindsight. So, unfortunately, is a large volume of irrelevant material that has to be examined and discarded. All intelligence organizations today are saturated with incoming information. Furthermore, in large intelligence communities critical information about an intelligence matter may not be effectively shared because the intelligence activity is organized around the flawed concept of an “intelligence cycle.” Before we explore this flawed concept we should define the term intelligence.
The Nature of Intelligence: Reducing Uncertainty in Conflict

Intelligence is about reducing uncertainty in conflict. Because conflict can consist of any competitive or opposing action resulting from the divergence of two or more parties’ ideas or interests, conflict is not necessarily physical combat. If competition or negotiation exists, then two or more groups are in conflict. There can be many different levels of conflict, ranging from friendly competition to armed combat. Context determines whether another party is an opponent or an ally. As a rule, friends and allies do not conduct intelligence operations on one another. However, parties can be allies in one conflict, opponents in another. For example, France and the United States are usually military allies, but they are opponents in commercial affairs.

Reducing uncertainty requires that intelligence obtain information that the opponent in a conflict prefers to conceal. This definition does not exclude the use of openly available sources, such as newspapers or the Internet, because competent analysis of such open sources frequently reveals information that an opponent 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, those types of research are also intended to reduce uncertainty. The answer is that most of the methods of intelligence research 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, then a wide range of specialized techniques and methods unique to the intelligence field are called into play. Academics are unlikely to have intercepted telephone communications at their disposal as a means for collection and analysis. Nor must academics deal routinely with concealment, denial, or deception.

Because intelligence is about conflict, it supports operations such as military planning and combat, diplomatic negotiations, trade negotiations and commerce policy, and law enforcement. The primary customer of intelligence is the person who will act on the information—the executive, the decision maker, the combat commander, or the law enforcement officer. Writers therefore describe intelligence as being actionable information. Not all actionable information is intelligence, however. A weather report is actionable, but it is not intelligence.
What distinguishes intelligence from plain news is support for operations. The operations customer does (or should do) something in response to intelligence, whereas TV viewers normally do not do anything in response to the news—though they may do something about the weather report. The same information can be both intelligence and news, of course: Food riots in Somalia can be both if the customer takes action on the information.

Finally, intelligence is always concerned with a target—the focus of the problem about which the customers want answers. In the Star Wars example the target was the Death Star. The rebel intelligence effort supported operations by locating its weak point.

Logic dictates that the intelligence 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 an intelligence problem, using a target-centric approach. This process is different from that depicted in most introductory texts and courses, but it is the new direction that intelligence is taking in practice. A brief review of the traditional intelligence cycle will illustrate why.

**The Traditional Intelligence Cycle**

Intelligence has traditionally been described as following a series of steps called the **intelligence cycle**. Figure 1-1 illustrates the cycle in elementary form.

The cycle typically begins with a **requirements** or **needs** step, which amounts to a definition of the intelligence problem. Usually it takes the form of a rather general question from an intelligence 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 have to be tasked to gather missing bits of information. Analysts have to be assigned to do research and write a report on Ethiopian government stability.

The cycle then proceeds to **collection** or gathering information. Ethiopian newspapers have to be acquired. Communications intelligence (COMINT) has to be focused on Ethiopian government communications. Human intelligence (HUMINT) operatives have to 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. Film or digital signals must be translated into visible imagery. Responses from HUMINT sources must be validated and organized into a report format.

The newly collected and processed material must be brought together with relevant historical material to create intelligence in an **analysis** phase. An analyst must create outcome scenarios based on the current Ethiopian situation, generate profiles of Ethiopian leaders, and assess their likely responses to possible events. The analysis 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 4) is done.
The finished intelligence must be *disseminated* to the customer in a written report (usually sent electronically) or a briefing. Then comes a transition to new requirements or needs, and a new cycle begins.

Over the years, the intelligence cycle has become almost a theological concept: No one questions its validity. Yet when pressed, many intelligence officers admit that the intelligence process “really doesn’t work like that.” In other words, effective intelligence efforts are not cycles. Here are some reasons why.

The cycle defines an *antisocial* series of steps that constrains the flow of information. It separates collectors from processors from analysts and too often results in “throwing information over the wall” to become the next person’s responsibility. 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 feedback loop inherent in a true cycle is absent; 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 often are almost totally ignorant of one another’s business. In the military the gap may be less severe—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 usually have not had

---

**Figure 1-1  Traditional Intelligence Cycle**

![Diagram of the traditional intelligence cycle](image-url)

*Note: The dotted line represents the transition from one cycle to the next, during which the customer reviews the analysis product and formulates new requirements and needs.*
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 U.S. government, the collection element (see Figure 1-1) 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 almost completely unfunded and requires extensive feedback from intelligence consumers. The system depends on the customers voicing their needs. Military organizations have a formal system for that to occur. Policymakers, with one important exception that is discussed in chapter 16, do not. The policymaker's input is largely informal, dependent on feedback to the analyst, and often passes through several intermediaries. And for the newest class of customers of U.S. intelligence—law enforcement—the feedback is rudimentary. No entity has the clear responsibility to close the loop. Analysts and their managers, who normally have the closest ties to intelligence customers, usually determine customer needs. But it is 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 also prevails because it fits a conventional paradigm for problem solving. It flows logically from the precept that the best way to work on an intelligence 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. Analysis techniques are then applied to answer the question. This pattern of thinking is taught in the simplest problem-solving texts, and we use it almost instinctively. 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 process: 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.

Despite its irrelevance to the real world of intelligence, the concept of an intelligence cycle persists. Some of the foremost experts in U.S. and British intelligence, such as Mike McConnell, former U.S. director of national intelligence, and noted British author Michael Herman, have questioned its relevance. Both McConnell and Herman noted that the so-called cycle is actually a collection of feedback loops. But old habits tend to fade very slowly, and so the intelligence cycle continues to be taught in introductory intelligence courses.
U.S. 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. As Keith Hall, former director of the National Reconnaissance Office, 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.”

In summary, the traditional cycle may adequately describe the structure and function of an intelligence community, but it does not describe the intelligence process. In the evolving world of information technology, the traditional cycle may be even less relevant. Informal networks (communities of interest) increasingly are forming to address the problems that Kent identified and enable a nonlinear intelligence process using secure Web technology.

The cycle is still with us, however, because it embodies a convenient way to organize and manage intelligence communities like those in large governments and large military organizations. And it is in some respects a defensive measure; it makes it difficult to pinpoint responsibility for intelligence failures.

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. No one had responsibility for the final result. Today automobile production is a team effort—with marketing, sales, design, and production 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 faster production of higher quality, more market-oriented products. Although producing intelligence is a more complex undertaking than automobile manufacturing, the interactive approach works for both. This book defines an alternative approach, one that is gaining currency in intelligence communities, for a world where intelligence problems are becoming increasingly complex.

**Intelligence as a Target-Centric Process**

An alternative to the traditional intelligence cycle is to make all stakeholders (including customers) part of the intelligence process. Stakeholders in the intelligence community include collectors, processors, analysts, and the people who plan for and build systems to support them. U.S. customers on a given issue could include, for example, the president, the National Security Council staff, military command headquarters, diplomats, the Department of Homeland Security, local law enforcement, and the commanders of U.S. naval vessels. To include them in the intelligence process, the cycle must be redefined,
not for convenience of implementation in a traditional organizational hierarchy but so that the process can take full advantage of evolving information technology and handle complex problems.

Figure 1-2 defines this target-centric, or objective-oriented, view of the intelligence process. Here the goal is to construct a shared picture of the target, from which all participants can extract the elements they need to do their jobs and to which all can contribute from their resources or knowledge, so as to create a more accurate target picture. It is not a linear process, 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 U.S. intelligence community as a “network-centric collaboration process.”

In the process depicted in Figure 1-2, customers who have operational problems look at 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 picture, 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 picture. From this picture, analysts extract actionable intelligence, which they provide to the customers, who may in turn add their own insights to the shared target picture. They may also add new information needs.

Let us bring some meaning to the process shown in Figure 1-2: The date is December 2, 1993. Colombian police lieutenant Hugo Martinez watches the signal display on his computer screen and listens to his headphones as his police surveillance van moves through the streets of Medellin, Colombia. Electronic intelligence has traced the cell telephone calls of drug kingpin Pablo Escobar to this neighborhood. Martinez is trying to find the exact house where a desperate Escobar is talking to his son about getting the family out of Colombia.

The signal on the computer screen and in the headphones strengthens and peaks. The van stops next to a house, and Martinez looks up to see a fat

---

**Figure 1-2** A Target-Centered View of the Intelligence Process
man standing at a window holding a cell phone. The man turns away, and the cell phone conversation abruptly ends. Martinez reports to his commander: “I’ve got him located. He’s in this house.” The commander snaps out orders for all units to converge and surround the building. Five police officers force their way in the front door and exchange gunshots with the occupants. Ten minutes later, the gunfire stops. On the building rooftop, Pablo Escobar lies dead.⁹

This example, a true story, was the end of an intense cooperative effort between U.S. and Colombian intelligence officers that had endured for more than a year. In this case, the intelligence effort had several customers—an operations team comprising the Colombian police, the U.S. Army support team in Colombia, and the Colombian and U.S. governments, each with different intelligence needs. The information sources included COMINT focused on Escobar’s cell phones and those of his associates, HUMINT from Escobar’s associates, and financial information from other sources. The operations team focused on finding Escobar; the intelligence analysts who supported them had a more extensive target that included Escobar’s family, his business associates, his bankers, and his agents in the Colombian government. Escobar would not have been caught if the intelligence search had focused solely on him and had ignored his network.

In the Escobar case, as in other less time-critical operations, intelligence analysis is implicit and pervasive. But it 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 providers possess valuable insights about the target, and both want their insights included in the final analytical product. However, someone must make the process work: create and maintain the picture of the target, elicit customer needs and change them into requirements for new information, accept new information and incorporate it into the target picture, and then extract actionable intelligence and ensure that it gets to the customer. All of these are functions that analysts have always performed. In the target-centric process, analysts still perform these functions, but collectors and customers can see into the process and have more opportunity to contribute to it. The analyst’s job becomes more like that of a process manager and a conduit of information to the other participants.

The team-generated picture of the target is intended to facilitate and encourage interaction among collectors, analysts, and customers, who may be geographically remote from one another, via an electronic web. Because the team view 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 the target. The team-generated view brings the full resources of the team to bear on the target. During U.S. operations in Afghanistan in 2002, intelligence officers used screens similar to Internet chat rooms to share data in an interactive process that in no way resembled the traditional intelligence cycle,¹⁰ and they continued that successful pattern during Operation Iraqi Freedom. It now is an established method of
producing tactical intelligence that is likely to be used in all future U.S. and coalition operations. But the method that has worked at the tactical level remains a work in progress at the national intelligence level. As the WMD Commission report noted in referring to national intelligence, “Information sharing still depends too much on physical co-location and personal relationships as opposed to integrated, community-wide information networks.”

The process shown in Figure 1-2 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.

The 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 different 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 unique needs.

The target-centric approach has more promise for complex problems and issues than the traditional cycle view. Though depicted as a cycle, the traditional process is in practice linear and sequential, whereas the target-centric approach is collaborative by design. Its nonlinear analytic process allows for participation by all stakeholders, so real insights into a problem can come from any knowledgeable source. Involving customers increases the likelihood that the resulting intelligence will be used. It also reminds the customers of (or introduces them to) the value of an analytical approach to complex problems. It has been asserted that in the United States, government has detached itself from the analytical process and relied too much on the intelligence community to do its analytical thinking. Increasing policymakers’ exposure to the analytical process could help reverse that trend.

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

- **The information glut.** Analysts are overloaded with incoming material from collectors. The team 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. Unfortunately, large intelligence communities, such as that in the U.S. government, have not succeeded in applying this remedy to the information glut. The barriers among collectors, processors, analysts, and customers still hold firm, and compartmentalization constrains collaboration.

- **The customer demand for more detail.** All intelligence customers are demanding increasingly greater detail about intelligence targets.
This should not be surprising given that targets are more complex and the range of the customer’s options to deal with opponents has become richer. If the operations target is a building (such as an embassy or a command and control center), for example, target 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 have to provide incentives to share that outweigh the disincentives discussed in the introduction. Team members have to have a wealth of mutual trust and understanding; both require team building and extended social interaction. Some companies have been highly successful at collaboration; the U.S. government still is working at it, and most government intelligence services worldwide haven’t even started.

It is important to note also what the collaborative process is not. As Mark Lowenthal has stated, it is not a substitute for competitive analysis—the process by which different analysts present alternative views of the target.\textsuperscript{13} Collaboration, properly handled, is intended to augment competitive analysis by ensuring that the competing views share as much information about the target as possible.

The Target

In Norfolk, Virginia, a young intelligence officer controls a Predator Unmanned Aeronautical 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 Spectre 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, 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 picture of potential Taliban targets, and the BMP fit the picture in its location and characteristics. The BMP in Afghanistan was a specific operations target; the intelligence view of the target was much larger. It included details of the road network in Afghanistan that could support the BMP and maps delineating areas of Taliban control. A good 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 starts by thinking about the target as a system. A system comprises structure, function, and process, and the analyst has to deal with each of the three in systems thinking. The *structure* of a system is defined by its components and the relationships among them. *Function* involves the effects or results that the system produces, that is, the system outputs. *Process* refers to the sequence of events or activities that produce results.

The Escobar drug cartel is (or was) an example of a system. Figure 1-3 is a macro-level picture of a cocaine cartel’s structure, showing the 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 component, for example, has subcomponents such as the farmers, land, seed, and farm equipment. A cocaine cartel also has several major functions, such as survival in the face of state opposition, making a profit, and providing cocaine to its customers. Each component also has additional functions that it performs. 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. As this example illustrates, most intelligence targets are systems that have subordinate systems, also called *subsystems*. The Escobar leadership comprised a subsystem whose structure included components such as security and finance; it had a function (managing the cocaine network) and a process for carrying it out.

As a counterexample, a geographical 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 geographical entity could not be considered an intelligence target. The government of a region is a system—it has structure, function, and process.

---

**Figure 1-3  Example Target: Cocaine Network**
All intelligence targets are systems. Furthermore, most are complex systems because

- they are dynamic and evolving, and
- they are nonlinear, in that they are not adequately described by a simple structure such as a tree diagram or the linear structure that I used in Figure 1-1 to illustrate the traditional intelligence cycle.

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, however, usually be described as a network. Most complex systems of intelligence interest are, in fact, networks.

**The Complex Target as a Network**

Although intelligence has always targeted opposing systems, it has often tended to see them as individual, rather than connected, entities. Such a narrow focus downplays the connections among organizations and individuals—connections that can be the real strength or weakness of an opposing system taken as a whole. That is the reason why we focus on networks.

Networks, by definition, comprise nodes with links between them. Several types of networks 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 cocktail party or in an investment club.

In this book, unless otherwise specified, network means a generalized network, in which the nodes can be almost any kind of entity—people, places, things, or concepts. A cocaine supply system is a generalized 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 generalized network is the preferred concept for intelligence analysis and is widely used.

In intelligence, the opposing generalized network typically is some combination of governments; individuals; nongovernmental organizations (NGOs), such as environmental, human rights, and religious groups; commercial firms; or illicit organizations—all tied together by some purpose, as suggested by the diagram in Figure 1-4. In conflicts, the goal of intelligence is to develop an understanding of the opposing network, so as to 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 competing commercial firm or alliance, or a narcotics production and distribution network must take a network view. As an example, intelligence organizations concerned with the balance of power in the Middle East sometimes look at Syria, Saudi Arabia, Iraq, and Iran 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 bound by ties of mutual mistrust and suspicion.

It is also important to look at both sides as networks. 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 assets form a network and fully exploit its strengths. The collaborative, collector-analyst-customer target-centric approach creates an effective network to deal with the opposing network. Figure 1-5 shows the example of a cocaine supply target network and some components of the opposing (that is, U.S. and Colombian) intelligence customer network. As the figure indicates, it makes sense that U.S. law enforcement would target the transportation and distribution infrastructure, because much of that infrastructure is located within U.S. borders. U.S. law enforcement would not normally be able to target the cartel leadership in Colombia. Colombian law enforcement, on the other hand, could target both the cartel leadership and its transportation and distribution infrastructure, but 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.

John Arquilla and David Ronfeldt of RAND Corporation described the network target in their discussion of the impact of new communications and information technologies on military structures, doctrines, and strategies. They coined the term netwar and defined it as a form of information-related conflict, in which opponents form networks. Specifically, Arquilla and Ronfeldt use the term to describe the “societal struggles” that make use of new technologies.15
The technologies they discuss are available and usable anywhere, as demonstrated by the Zapatista netwar: In January 1994, a guerrilla-like insurgency in Chiapas, Mexico, by the Zapatista National Liberation Army and the Mexican government’s repressive response caused a collection of activists associated with human-rights, indigenous-rights, and other types of nongovernmental organizations elsewhere to link electronically with similar groups in Mexico to press for nonviolent change. What began as a violent insurgency in an isolated region mutated into a nonviolent but disruptive social netwar that engaged the attention of activists around the world and had both nationwide and foreign repercussions for Mexico. The Zapatista insurgents skillfully used a global media campaign to create a supporting network of NGOs and embarrass the Mexican government in a form of asymmetric attack (a form of conflict that exploits dissimilarities in capability between two opponents).16

Netwar is not the same as information warfare, though the two may overlap in some problems. Information warfare, also called information operations, encompasses the use of information systems, including computers, communications networks, and databases, for competitive advantage against an opponent. Thus information warfare can be one of the “levers” that are pulled in netwar; computer networks may be a part of the target. But one can engage in netwar without attacking the opponent’s information systems.
Within the U.S. Department of Defense, netwar is currently referred to as *network-centric warfare*. Defense planners have identified three themes:

- A shift in focus 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
- The importance of making strategic choices to adapt—or merely to survive—in the changing system

Network-centric warfare is not a new concept in the business world. Companies such as Royal Dutch Shell were creating networks of this kind, including allied outsiders, two decades ago. Participants in that network found it a powerful mechanism for bringing a wide range of expertise to bear on problems. The World Wide Web 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 Wal-Mart have made the collaborative network a key part of their business strategy. In Wal-Mart’s network-centric 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 Wal-Mart products. Another example is the network-centric securities trading system Autobahn, created by Deutsche Morgan Grenfell. 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 Wal-Mart and Deutsche Morgan Grenfell forces their competitors to adopt similar approaches or lose out in competition.

Business intelligence might be ahead of government intelligence in applying the netwar strategy. Even military organizations, with their traditions of hierarchical structure, are considering the advantages of the network structure. 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 must understand 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.

Any discussion of the network target should touch on the intelligence target of the last decade: Osama bin Laden. In person, he was a hard target to miss, being 6’ 5” 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 to find, almost impossible if considered alone. However, like Pablo Escobar, he had to run a large network. He had to have some form of communication with the network. Despite bin Laden’s very good security system, intelligence analysts and collectors focused on the network as a target were able to
pinpoint his location in Abbottabad, Pakistan, in 2010 through 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. Even so, that it took nearly ten years for the allied intelligence services to track bin Laden down illustrates the importance of making the intelligence network as inclusive as possible. The opposing network, unfortunately, included significant elements of the Pakistani government who supported bin Laden, making allied intelligence operations in Pakistan more difficult.

Summary

Intelligence is about reducing uncertainty in conflict. It supports operations, and it is always concerned with a target. Traditionally, intelligence has been described as a cycle: from requirements to planning or direction, collection, processing, analysis and production, dissemination, then back to requirements. That traditional 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 is useful for describing structure and function and serves as a convenient rationale for organizing and managing a large intelligence community. But it does not describe how the process works or should work.

Intelligence as a process is becoming a nonlinear and target-centric network—that is, a collaborative team of analysts, collectors, and consumers collectively focused on the intelligence target. The rapid advances in information technology are aiding this transition.

All significant intelligence targets of this target-centric network 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. Conflict with such networks has been called netwar or network-centric conflict. In dealing with opposing networks, the intelligence network must be highly collaborative. Historically, however, large intelligence organizations, such as those in the United States, provide disincentives to collaboration. If those disincentives can be removed, U.S. intelligence will increasingly resemble the most advanced business intelligence organizations in being both target-centric and network-centric.

Having defined the target, the first question to address is, What do we need to learn about the target that our customers do not already know? This is the intelligence problem, and for complex targets, the associated intelligence problems are also complex. The next chapter discusses how to define the intelligence problem.

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.
Analytic Methodologies

There is nothing more deceptive than an obvious fact.

Sherlock Holmes, “The Boscombe Valley Mystery”

The target-centric approach, discussed in the preceding chapters, depends on constructing a shared model of the target (the synthesis step), and then extracting intelligence judgments from that model to meet customer needs (the analysis step). Both synthesis and analysis depend on the application of analytic methodologies. A very large number of analytic methodologies exist—as noted in the introduction, one study identified more than 160.

A subset of these analytic methodologies is referred to as structured analytic methodologies or techniques, and these are the subject of a companion CQ Press book by Richards Heuer and Randolph Pherson called Structured Analytic Techniques for Intelligence Analysis. This book does not attempt to cover the many techniques that are discussed in the Heuer/Pherson book. Instead, we’ll introduce two of the long-standing approaches to structured argumentation in this chapter. The following chapters, 11 through 15, discuss some specific methodologies that are primarily focused on prediction.

Structured Argumentation

Chapter 7 discussed some qualitative and intuitive approaches for combining evidence. It often is important to combine the evidence and demonstrate the logical process of reaching a conclusion based on that evidence by careful argument. The formal process of making such an argument is called structured argumentation. Such formal structured argumentation approaches have been around at least since the 17th century.

Structured argumentation is an analytical process that relies on a framework to make assumptions, reasoning, rationale, and evidence explicit and transparent. The process begins with breaking down and organizing a problem into parts so that each one can be examined systematically, as discussed in the earlier chapters. As analysts work through each part, they identify the data requirements, state their assumptions, define any terms or
Analytic Methodologies

concepts, and collect and evaluate relevant information. Potential explanations or hypotheses are formulated and evaluated with empirical evidence, and information gaps are identified.

Formal graphical or numerical processes for combining evidence are time-consuming to apply and are not widely used in intelligence analysis. They are usually reserved for cases in which the customer demands them, whether because the issue is critically important, because the customer wants to examine the reasoning process, or because the exact probabilities associated with each alternative are important to the customer. Two such formal processes of structured argumentation are Wigmore’s charting method and Bayesian analysis.

Wigmore’s Charting Method

John Henry Wigmore (1863–1943) was the dean of the Northwestern University Law School and author of a 10-volume treatise commonly known as *Wigmore on Evidence*. In that treatise he defined some principles for rational inquiry into disputed facts and methods for rigorously analyzing and ordering possible inferences from those facts.\(^2\)

Wigmore argued that structured argumentation brings into the open and makes explicit the important steps in an argument and thereby makes it easier to judge both their soundness and their probative value.\(^3\) One of the best ways to recognize any inherent tendencies one may have to make biased or illogical arguments is to go through a body of evidence using Wigmore’s method.

The method is complex and is not detailed here. It is, however, a very powerful tool for comparing alternative models or hypotheses. It requires the construction of elaborate diagrams that incorporate all important evidence and that have the following main features (a few of which are illustrated in Figure 10-1):

- Different symbols are used to show different kinds of evidence—explanatory, testimonial, circumstantial, corroborative, undisputed fact, and combinations.
- Relationships between symbols (that is, between individual pieces of evidence) are indicated by their relative positions (e.g., evidence tending to prove a fact is placed below the fact symbol).
- The connections between symbols indicate the probative effect of their relationship and the degree of uncertainty about the relationship. For example, a double arrowhead on the connector indicates that strong credit is given to the relationship; a question mark next to the connector signifies doubt about the probative effect of the connection; a zero on the connector indicates a negating effect.\(^4\)

Wigmore intended his approach to be used by trial lawyers. But the trial lawyers basically ignored him because his diagrams were too hard to prepare.\(^5\) The approach has fared no better with intelligence analysts, as even proponents
admit that it is too time-consuming for most practical uses, especially in intelligence analysis, where the analyst typically cannot afford the luxury of such a formal approach.

Recognizing this shortcoming, Wigmore proposed a narrative form, listing rather than charting the evidence, to simplify the process and make it more readily usable by a novice. But even the narrative approach runs into trouble when one is dealing with the large mass of data that is typical of complex problems. Efforts have been made in recent years to incorporate a structured argumentation process into software to aid intelligence analysts. Making Wigmore's approach, or something like it, widely usable in intelligence analysis would be a major contribution. His method brings into the open and makes explicit the important steps in an argument and thereby makes it easier to evaluate the soundness of any conclusion.

**Bayesian Techniques for Combining Evidence**

By the early part of the eighteenth century, mathematicians had solved what is called the “forward probability” problem: What is the probability of a given event happening when all the facts about a situation are known? For example, if you know the numbers of black and white balls in a bag, it is easy to determine the probability of drawing a black ball from the bag. In the middle of the eighteenth century, Thomas Bayes, a British mathematician and Presbyterian minister, dealt with the “inverse problem”: Given that an event has occurred, what can be determined about the situation that caused the event? Continuing our bag of balls example, if you draw three black balls and one white ball from 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? Intelligence analysts find this problem 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’s rule.

Bayesian analysis is the best known of the formal numerical processes. Based on Bayes’s rule, it is a formal method for using incoming data to modify previously estimated probabilities. It therefore can be used to narrow the error bounds on both estimates and predictions. Each new piece of information can be 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 likely or less 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.

To explain Bayes’s rule, let us assume that we know how often a given event normally occurs. We can assign that event a probability: $P(event)$. Assume also that we have previously made an intelligence conclusion and given it a likelihood, or probability, of $P(conclusion)$. Finally, we are fairly sure that if our conclusion is true, it changes the probability $P(event)$. We call this changed probability $P(event | conclusion)$, which is read as “probability that the event will occur, given that the conclusion is true.”

Now, suppose that the event does occur. Its occurrence changes the probability of our conclusion to a new probability $P(conclusion | event)$, which is read as “probability that our conclusion is true, given that the event has occurred.” The new probability is given by Bayes’s rule, which is expressed by the formula,

$$P(conclusion | event) = \frac{P(event | conclusion) P(conclusion)}{P(event)}$$

A simple illustration will help make Bayes’s rule clear. Suppose an analyst has previously made an estimate based on existing evidence that a particular bank is laundering narcotics funds and has given the estimate a probability $P(conclusion) = 0.4$. The analyst knows that the probability of similar banks making profits in excess of 12 percent is 0.2 if the bank operates legally. The bank in question, however, recently made a profit of 20 percent, which certainly looks suspicious. The analyst concludes that there is a 30 percent (.3) chance of the bank making this much profit if it is in the fund-laundering business. The probability that the bank is laundering funds has increased:

$$P(conclusion | event) = \frac{(.3)(.4)}{.2} = .6$$

One problem with Bayesian analysis is that it does not deal well with ignorance. That is, if the analyst assigns probabilities to either conclusions or
events based on very little knowledge, contradictions can result. The solution to this problem in Bayes's rule is to use a more formal methodology called the Dempster-Shafer approach to combining evidence. The Dempster-Shafer approach is mathematically complex and is not described in detail here.7

Both Bayes's rule and Dempster-Shafer rely on placing a numerical weight on bits of evidence. There are three approaches to numerical weighting: ordinal scale, interval scale, and ratio scale weighting. Ordinal scales simply indicate rank or order, but no mathematical operations are possible. Interval scales have equal intervals between numbers, but the lack of an absolute zero reference does not allow multiplication or division. The Fahrenheit and Celsius scales are interval scales for measuring temperature because both scales have a somewhat arbitrary zero reference. Only ratio scaling, which has an absolute zero reference, allows the multiplication and division required for Bayesian or Dempster-Shafer analysis. The Kelvin temperature scale is an example of a ratio scale; it has an absolute zero reference—the temperature where all motion of atomic particles stops.

**Competitive and Alternative Target Models**

Competitive analysis and alternative analysis are somewhat different things, though they are frequently confused with each other. Let's look at them in turn, starting with the simpler of the two.

**Competitive Analysis**

It is well established in intelligence that, if you can afford the resources, you should have independent groups provide competing analyses. This is because we're dealing with uncertainty. Different analysts, given the same set of facts, are likely to come to different conclusions. The U.S. intelligence community, as a result of its size and the presence of analysis groups in most of its 16 members, has done competitive analysis for years.

The problem has at times been so serious that the U.S. intelligence community has been directed to empower independent groups to provide alternative target models. In 1976, the President's Foreign Intelligence Advisory Board and Director of Central Intelligence (DCI) George H. W. Bush created an independent analysis team, known as Team B, to provide an alternative National Intelligence Estimate on Soviet strategic objectives and capabilities.8 What became known as the A team—B team exercise is perhaps the best known example of competitive analysis. The effort engendered considerable resentment among the intelligence community analysts who had prepared the Team A estimate. This effort was unusual in that the B team was comprised mostly of experts from outside the intelligence community. Most competitive analysis in the United States involves competing analyses from different intelligence community agencies.

Unfortunately, competitive analysis engenders some bad practices. We always want to beat our competition, and some techniques that are used in the
intelligence community to “win” are counterproductive. For example, hoarding information is an easy way to gain a competitive advantage, and some analysts will do just that.

Alternative Analysis

In contrast to competitive analysis, alternative analysis is usually done by a single analyst or analytic team, not by competing teams. A number of formal alternative analysis methodologies have been defined and given names such as Analysis of Competing Hypotheses, Argument Mapping, Signpost Analysis, and Challenge Analysis. Again, these are discussed in detail in the Heuer and Pherson book, *Structured Analytic Techniques for Intelligence Analysis*.

Alternative analysis applies structured techniques that challenge underlying assumptions and broaden the range of possible outcomes considered. Its purpose is to deal with the natural tendencies of analysts to perceive information selectively through the lens of preconceptions, to search for facts that would confirm rather than discredit existing hypotheses, and to be unduly influenced by premature consensus within a group dynamic. Alternative analysis involves a fairly intensive and usually time limited effort to challenge assumptions or to identify alternative outcomes.9

Alternative analysis is a good idea that typically is poorly executed. In practice, it seems to become pro forma. Many intelligence assessments now conclude with a skimpy and inadequately supported “alternative outcome” that obviously was put in at the direction of management rather than as a hypothesis that was seriously considered and examined by the analyst from the beginning. To deal with this tendency, some analysis organizations have set up separate teams to do “alternative analysis”—though technically, this is simply competitive analysis done within the same organization.

Alternative models are an essential part of the synthesis process. In studies describing the analytic pitfalls that hampered past assessments, one of the most prevalent is failure to consider alternative scenarios, hypotheses, or models.10 Analysts seem to be addicted to single-outcome scenarios. One national intelligence officer has observed that “analysts . . . rarely engage in systematic testing of alternative hypotheses.”11 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.”12 There are a number of reasons why analysts do not make use of alternative models, either initially or as new evidence comes in to suggest that a different target model is more appropriate:

- Analysts are usually facing tight deadlines. The temptation is to go with the model that best fits the evidence without considering alternatives.
- Presented with two or more target models, customers always pick the one that they like best, but that may or may not be the most likely model. Analysts know this.
Maintaining a corporate judgment is a pervasive and often an unstated norm in the intelligence community. Customers tend to view a change in judgment as indicating that the original judgment was wrong, not that new evidence forced the change.

It has been noted that it serves the interest of any intelligence agency to be perceived as decisive rather than academic and contradictory, and that message quickly becomes embedded in any analysis culture. A similar motivation long ago led judicial systems to adopt the principle of stare decisis: Let previous decisions stand, wherever possible. Both analysts and judges face the same tension: Do you want to be consistent, or do you want to come up with the answer that best fits with the facts?

Building alternative models takes time. Analysts, always rushed, don’t want to do it. Also, as former director of national intelligence (DNI) Mike McConnell has observed, analysts inherently dislike alternative, dissenting, or competitive views. But it is important to keep more than one possible target model in mind, especially as conflicting or contradictory intelligence information is collected.

Sometimes the policymakers provide an alternative target model. For example, in 1982 the United States committed U.S. Marines to Lebanon in an ambitious attempt to end a civil war, force occupying Israeli and Syrian armies out of Lebanon, and establish a stable government. The U.S. administration withdrew from Lebanon 18 months later, its policy discredited and its reputation damaged, with more than 250 Americans dead, most of them marines killed in a terrorist bombing. The U.S. intelligence community had one assessment of the Lebanon situation; the Washington policymaking community had a strikingly different assessment that envisioned Lebanon as a role model for future Middle East governments. Table 10-1 shows a parallel list comparing these two alternative models of the Lebanon situation.

Note that this is far from a complete picture of Lebanon, which today, as in 1982, has all the elements of a complex problem as defined in chapter 2. The table also is more than a target model; it contains a number of analytical judgments or hypotheses that were drawn from two competing target models.

It is best to be inclusive when defining alternative models, especially when dealing with intelligence enigmas—a subject discussed in chapter 8. During the 1970s and early 1980s, the United States expended considerable intelligence and scientific research effort in the suspicion that the Soviet Union was building a particle beam weapon capable of destroying ballistic missile warheads in flight. The source of this suspicion was one of several competing models of an unidentified facility in the Soviet Union located near the Semipalatinsk nuclear testing area. The U.S. Air Force called it PNUT—possible nuclear underground test facility, and the CIA called it URDF-3—unidentified research and development facility three. Some Air Force officials
argued that the facility was a test site for a particle beam weapon. The Air Force position was supported by U.S. researchers who had a vested interest in funding for particle beam weapons research.\(^{17}\)

While a number of alternative hypotheses were proposed for PNUT/URDF-3, the real explanation apparently was not seriously considered: It was a nuclear rocket testing program. The major reason for this oversight appears to have been that the United States, which had previously dropped its own nuclear rocket program, simply did not include the nuclear rocket hypothesis in considering the facility.\(^ {18}\) If analysts had included the nuclear rocket model hypothesis, an application of Occam’s razor to the available evidence would have made it the leading contender to explain the facility’s purpose.

### The Role of Information Technology

It is difficult for new analysts today to appreciate the markedly different work environment that their counterparts faced 30 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 often kept on 5” x 7” cards in card catalog boxes. Less tidy analysts filed their most interesting raw intelligence on their desktops and cabinet tops, sometimes in stacks over two feet high.

Information technology (IT) has dramatically altered that work environment for at least the major government intelligence services.

---

**Table 10-1 Alternative Models of the Lebanon Situation in 1982**

<table>
<thead>
<tr>
<th>Policymakers</th>
<th>Analysts</th>
</tr>
</thead>
<tbody>
<tr>
<td>We can negotiate speedy Israeli and Syrian withdrawals from Lebanon.</td>
<td>President Assad won’t pull Syrian troops out unless convinced that he will be attacked militarily.</td>
</tr>
<tr>
<td>Lebanon can be unified under a stable government.</td>
<td>Lebanon in effect has no borders, and you can’t say what a citizen is.</td>
</tr>
<tr>
<td>President Gamayel can influence events in Lebanon.</td>
<td>President Gamayel doesn’t control most of Beirut, and even the Christians aren’t all behind him.</td>
</tr>
<tr>
<td>We have five military factions to deal with: the Christian Phalange, Moslem militia, Syrian forces, the PLO, and Israeli forces.</td>
<td>There are 40 militias operating in West Beirut alone.</td>
</tr>
<tr>
<td>The marines are peacekeepers.</td>
<td>The marines are targets.</td>
</tr>
</tbody>
</table>
IT systems allow analysts to acquire raw intelligence material of interest (incoming classified cable traffic and open source); and to search, organize, and store it electronically. Such IT capabilities have been eagerly accepted and used by analysts because of their advantages in dealing with the information explosion.

Most analysts also have been willing to make use of IT tools for extracting meaning from the data. A wide range of such tools exist to do this, including ones for visualizing the data and identifying patterns that are of intelligence interest; statistical analysis tools; and simulation models. Analyst acceptance of these tools varies, depending in part on their areas of responsibility and the type of analysis that they do. Analysts with responsibility for counterterrorism, organized crime, counternarcotics, counterproliferation, or financial fraud can choose from commercially available tools such as Palantir, CrimeLink, Analyst's Notebook, Netmap, Orion, or VisuaLink to produce matrix and link diagrams, timeline charts, telephone toll charts, and similar pattern displays.\(^{19}\) Tactical intelligence units, military, and law enforcement find geospatial analysis tools to be essential.

Some 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 data base structures are generally not compatible with each other. The result is that these tools are less effectively used than they might be, and the absence of a single standard tool 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 SEAS\(^{20}\) 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 US intelligence community. An open-source version of ACH called Analysis of Competing Hypotheses is available online.\(^{21}\) Use of ACH tools may be increasing, at least in the U.S. intelligence community; it is too early to tell. Like Wigmore's charting method, they may ultimately be too difficult for the average analyst to use.

**Summary**

A large number of analytical methodologies are available to the analyst. Some of the most useful fall into the two broad categories of structured argumentation and alternative or competitive analysis. A third category, predictive methodologies, is discussed in the following chapters.

Structured argumentation is a formal process of combining evidence graphically or numerically. 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. But it is time consuming to apply, and therefore is often ignored in favor of informal evidence combination methods. Two of the most enduring formal methods are Wigmore’s evidence charting method and Bayesian analysis.

Alternative target models are an essential part of the process. Properly used, they help the analyst deal with denial and deception and avoid being trapped by analytic biases. But they take time to create; analysts are reluctant to change or challenge existing judgments; and alternative models can play into the hands of policymakers who want support only for preconceived notions. Because analysts generally don’t like alternatives, too often the result of alternative analysis is proforma, not a serious attempt.

Information technology has provided a major boost to analyst productivity and to the quality of analysis. Tools to acquire, organize, search, store, and retrieve raw intelligence are widely available and enthusiastically accepted by analysts. Tools to extract meaning from data, for example, by relationship, pattern, and geospatial analysis, are used by analysts 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, but whether they will find serious use in intelligence analysis is still an open question.

Notes
3. Ibid., 119.
4. Ibid., 112.
12. Ibid., 170.
18. Ibid.
20. See the description of SEAS, the Structured Evidential Argumentation System, at http://www.ai.sri.com/project/GENOA.