Introduction to Intelligence Analysis: A Hands-On Approach with TIACRITIS

Gheorghe Tecuci, David Schum, Mihai Boicu, Dorin Marcu
Learning Agents Center, George Mason University
ACKNOWLEDGEMENTS

The development of the TIACRITIS system and the writing of this book were partially supported by the Department of Defense and by George Mason University.

The TIACRITIS system and textbook are based on the research performed under the project *A Computational Theory of Intelligence Analysis*, supported by the National Geospatial-Intelligence Agency’s NURI program (PM: Phillip Hwang), on the Virtual Experts project (PMs: Susan Durham and Joan McIntyre), and on the Disciple learning agent theory and technology developed for many years in the Learning Agents Center.

This research, development, and application effort was guided by the following Advisory Board: Donald Kerr (chair), Kelcy Allwein, Keith Anthony, Cindy Ayers, Sharon Hamilton, Jim Homer, Joan McIntyre, William Nolte, George Stemler, and Benjamin Wible.

Cristina Boicu contributed to the development of TIACRITIS. Gary Roemmich and Benjamin Wible contributed to Section 13 Analysis of Military Intelligence. Katherine Russell, Miruna Tecuci, and Emilia Butu provided editorial comments.

The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and opinions expressed in this book are those of the authors and do not necessarily reflect the official policy or position of any agency of the U.S. Government.
# TABLE OF CONTENTS

## PREFACE 

## 1 INTELLIGENCE ANALYSIS: “CONNECTING THE DOTS”

1.1 How Easy Is It to Connect the Dots? ................................................................. 5
   1.1.1 Problem 1: There Is More Than One Kind of Dot to Be Connected ......................... 5
   1.1.2 Problem 2: Which Evidential Dots Should Be Connected? .......................................... 6
   1.1.3 Problem 3: Which Evidential Dots Can Be Believed? .................................................. 8
   1.1.4 Problem 4: What Are the Connections between Evidential Dots and Hypotheses? .......... 10
   1.1.5 Problem 5: What Do Our Arguments Mean? .............................................................. 11
   1.1.6 Problem 6: Whose Dots Should Be Connected? ....................................................... 13
1.2 Connecting the Dots through the Discovery of Evidence, Hypotheses, and Arguments ........... 14
1.3 Analysis of Competing Hypotheses ............................................................................. 16
1.4 Case Study: Defining a Personalized Course in Intelligence Analysis ............................... 17
   1.4.1 Objective ....................................................................................................................... 17
   1.4.2 Summary ....................................................................................................................... 17
   1.4.3 Instructions ................................................................................................................... 17
1.5 Case Study: Introduction to the Use of TIACRITIS ......................................................... 21
   1.5.1 Objective ....................................................................................................................... 21
   1.5.2 Summary ....................................................................................................................... 21
   1.5.3 Instructions ................................................................................................................... 21

## 2 DIVIDE AND CONQUER: A NECESSARY APPROACH TO COMPLEX ANALYSES

2.1 Holistic Approach to Analysis ..................................................................................... 25
2.2 Divide and Conquer ..................................................................................................... 26
2.3 Problem Decomposition as a Guide for Evidence Collection ........................................ 27
2.4 Problem Reduction and Solution Synthesis .................................................................. 30
2.5 Divide and Conquer through Problem Reduction and Solution Synthesis ..................... 31
2.6 Case Study: Analyzing Hypotheses through Problem Reduction and Solution Synthesis .... 34
   2.6.1 Objective ....................................................................................................................... 34
   2.6.2 Summary ....................................................................................................................... 34
   2.6.3 Instructions ................................................................................................................... 34

## 3 EVIDENCE 

3.1 What Is Evidence? ...................................................................................................... 39
3.2 The Credentials of All Evidence ................................................................................... 42
   3.2.1 Relevance ..................................................................................................................... 43
   3.2.2 Believability ................................................................................................................ 44
   3.2.3 Force or Weight of Evidence ..................................................................................... 46
3.3 Arguments Linking Evidence to Hypothesis ............................................................... 47
3.4 Case Study: Making Assessments and Assumptions in Arguments ................................. 49
   3.4.1 Objective ..................................................................................................................... 49
   3.4.2 Summary ..................................................................................................................... 49
   3.4.3 Instructions .................................................................................................................. 49
4 ESTABLISHING THE RELEVANCE OF EVIDENCE BY ARGUMENTS

4.1 Relevance and the Question: So What? ......................................................... 56
4.2 Case Study: Evidence-based Hypothesis Analysis ........................................ 62
  4.2.1 Objective ............................................................................................... 62
  4.2.2 Summary ............................................................................................... 62
  4.2.3 Instructions ............................................................................................ 62

5 ASSESSING THE BELIEVABILITY OF EVIDENCE ........................................... 71

5.1 Believability: The Foundation of All Arguments from Evidence .................... 71
5.2 Classification of Evidence Based on Believability ......................................... 71
5.3 Tangible Evidence ....................................................................................... 72
  5.3.1 Real Tangible Evidence: Authenticity .................................................... 73
  5.3.2 Demonstrative Tangible Evidence: Authenticity, Accuracy, and Reliability 73
  5.3.3 Examples of Tangible Evidence ............................................................. 75
5.4 Testimonial Evidence .................................................................................. 75
  5.4.1 Competence: Access and Understandability .......................................... 75
  5.4.2 Credibility: Veracity, Objectivity, and Observational Sensitivity .............. 76
    5.4.2.1 Veracity or Truthfulness .................................................................. 76
    5.4.2.2 Objectivity ...................................................................................... 76
    5.4.2.3 Observational Sensitivity ............................................................... 76
  5.4.3 Types of Testimonial Evidence .............................................................. 77
  5.4.4 Examples of Testimonial Evidence ........................................................ 78
5.5 Missing Evidence ....................................................................................... 79
  5.5.1 Uncertainties Associated with Missing Evidence ..................................... 79
  5.5.2 Examples of Missing Evidence ............................................................. 80
5.6 Accepted Facts .......................................................................................... 80
5.7 Mixed Evidence ....................................................................................... 81
  5.7.1 Analysis of Mixed Evidence .................................................................. 81
  5.7.2 Examples of Mixed Evidence ............................................................... 81
5.8 Case Study: Believability Analysis .............................................................. 83
  5.8.1 Objective ............................................................................................... 83
  5.8.2 Summary ............................................................................................... 83
  5.8.3 Instructions ............................................................................................ 83
5.9 Case Study: Self-testing on Believability Analysis .......................................... 89
  5.9.1 Objective ............................................................................................... 89
  5.9.2 Summary ............................................................................................... 89
  5.9.3 Instructions ............................................................................................ 90

6 CHAINS OF CUSTODY .................................................................................. 97

6.1 What Is a Chain of Custody? ....................................................................... 97
6.2 A Chain of Custody for Testimonial Evidence ............................................. 101
6.3 A Chain of Custody for Demonstrative Tangible Evidence ......................... 103
  6.3.1 Chain of Custody for a Photo Given Directly to the Analyst ...................... 103
  6.3.2 Chain of Custody for a Written Description of a Photo Given to the Analyst 106
6.4 Case Study: Analyzing a Chain of Custody ................................................ 106
6.5 Drill-Down Analysis of Chains of Custody ................................................ 110
7 RECURRENT SUBSTANCE-BLIND COMBINATIONS OF EVIDENCE .......................................................... 113
  7.1 Introduction .............................................................................................................................................. 113
  7.2 Case Study: Hypothesis Analysis Review .............................................................................................. 115
    7.2.1 Objective ........................................................................................................................................... 115
    7.2.2 Summary .......................................................................................................................................... 115
    7.2.3 Instructions ....................................................................................................................................... 115
  7.3 Harmonious Evidence ................................................................................................................................. 116
    7.3.1 Basic Forms of Harmonious Evidence ............................................................................................ 116
    7.3.2 Patterns of Evidential Harmony ...................................................................................................... 117
  7.4 Dissonant Evidence .................................................................................................................................. 118
    7.4.1 Basic Forms of Dissonant Evidence .................................................................................................. 118
    7.4.2 Patterns of Evidential Dissonance .................................................................................................... 119
  7.5 Evidential Redundance ................................................................................................................................ 120
    7.5.1 Basic Forms of Redundant Evidence ................................................................................................ 120
    7.5.2 Patterns of Evidential Redundance .................................................................................................... 121

8 THE MAJOR SOURCES OF UNCERTAINTY IN MASSES OF EVIDENCE ............................................... 123
  8.1 Introduction .............................................................................................................................................. 123
  8.2 Case Study: Evidence Collection and Hypothesis Analysis ...................................................................... 127
    8.2.1 Objective ........................................................................................................................................... 127
    8.2.2 Summary .......................................................................................................................................... 127
    8.2.3 Instructions ....................................................................................................................................... 127
  8.3 Incompleteness ....................................................................................................................................... 129
    8.3.1 What Is Incompleteness of Evidence? ............................................................................................. 129
    8.3.2 Examples and Questions ..................................................................................................................... 130
  8.4 Inconclusiveness ..................................................................................................................................... 132
    8.4.1 What Is Inconclusiveness of Evidence? ........................................................................................... 132
    8.4.2 Examples and Questions ..................................................................................................................... 132
  8.5 Ambiguity ............................................................................................................................................... 133
    8.5.1 What Is Ambiguity of Evidence? ....................................................................................................... 133
    8.5.2 Examples and Questions ..................................................................................................................... 133
  8.6 Dissonance .............................................................................................................................................. 133
    8.6.1 What Is the Dissonance of Evidence? ............................................................................................. 133
  8.7 Imperfect Believability ............................................................................................................................... 134

9 ASSESSING AND REPORTING UNCERTAINTY: SOME ALTERNATIVE METHODS .............................. 137
  9.1 Introduction .............................................................................................................................................. 137
  9.2 Case Study: Hypothesis Analysis .............................................................................................................. 140
    9.2.1 Objective ........................................................................................................................................... 140
    9.2.2 Summary .......................................................................................................................................... 141
    9.2.3 Instructions ....................................................................................................................................... 141
  9.3 General Classes of Probability and Uncertainty ...................................................................................... 141
  9.4 Enumerative Probabilities: Obtained by Counting .................................................................................. 142
  9.5 Non-enumerative Probabilities: Nothing to Count ................................................................................. 144
    9.5.1 Epistemic Probability (1): The Subjective Bayesian View ................................................................. 145
    9.5.2 Epistemic Probability (2): Belief Functions ....................................................................................... 146
One of our most important protections against terrorists and other enemies is the imaginative and critical reasoning abilities of our intelligence analysts who face the highly complex task of drawing defensible and persuasive conclusions from masses of evidence of all kinds from a variety of different sources (e.g. Schum, 1987). These conclusions are necessarily probabilistic in nature because our evidence is always incomplete (we can look for more, if we have time), usually inconclusive (it is consistent with the truth of more than one hypothesis or possible explanation), frequently ambiguous (we cannot always determine exactly what the evidence is telling us), commonly dissonant (some of it favors one hypothesis or possible explanation but other evidence favors other hypotheses), and with various degrees of believability (Schum, 2001). Arguments, often stunningly complex, requiring both imaginative and critical reasoning, are necessary in order to establish and defend the three major credentials of evidence: its relevance, believability, and inferential force or weight.

These assorted evidential characteristics are not the only elements of the complexity of intelligence analysis tasks. A major objective of intelligence analysis is to help insure that the policies and decisions reached by our government and military leaders, at all levels, are well informed. Analysts face different requirements in their efforts to serve these policy and decision-making “customers.” In some cases, they are required to answer questions that are of immediate interest and that do not allow time for extensive research and deliberation on available evidence. In other cases, teams of analysts participate in more lengthy finished intelligence that combines evidence from every available source. Sometimes finished intelligence can refer to long-term assessments on matters of current and abiding interest.

Based on our years of experience in training intelligence analysts, law students, and high ranking military officers, we have arrived at several conclusions. The first is that training in the evidential reasoning tasks required in these and other important contexts cannot be learned effectively just by listening to someone discuss his/her own analyses or just by giving students lectures and assigned readings on the topics. What is absolutely necessary is regular practice involving analyses of evidence using either hypothetical situations or examples drawn from actual situations. In short, evidential analysis is mastered best by performing analyses contrived to illustrate the wide variety of subtleties or complexities so often encountered in actual evidential analyses.

The second conclusion is based on our inspection of the materials offered in several courses for training intelligence analysts. It appears that analysts are so often trained in the production of intelligence analyses rather than on the actual process of analysis itself. Very little training is offered regarding the properties, uses, discovery, and marshaling of the evidence upon which all analyses rest. As Douglas MacEachin (1999), former DDI, CIA, remarked, “Information and expertise are a necessary but not sufficient means of making intelligence analysis the special product that it needs to be. A comparable effort has to be devoted to the science of analysis.”

The third conclusion is based on the strong emphasis currently placed in the Intelligence Community on the development of computer-based tools to assist analysts. Indeed, analysts need all the help they
can get in the face of a tsunami of information and the requirement to answer questions of immediate interest that do not allow time for extensive research on and deliberation of available evidence. Therefore, analysis tools based on solid theoretical foundations should be integrated into intelligence analysis courses to teach the process of analysis (including the properties, uses, discovery, and marshaling of the evidence) through a learning-by-doing approach.

The present book and the TIACRITIS (Teaching Intelligence Analysts Critical Thinking Skills) system have been developed in response to the above conclusions, to be used in intelligence analysis courses that are necessary, or frequently advisable, for persons throughout the Intelligence Community and those it serves. This includes collectors of intelligence information, evaluators of incoming intelligence information at various levels and in different offices, and even the policy-making “customers” of intelligence analysts. Everyone in the business of evaluating and acting upon intelligence information should be knowledgeable of the many subtleties and complexities of reasoning based on evidence. This learning venture is one important element of a task we all hear about by means of the metaphor “connecting the dots.” The matters discussed in this tutorial venture are applicable regardless of the subject of an intelligence analysis and the kinds of intelligence information required, such as HUMINT, IMINT, SIGINT, MASINT, and Open Source information.

This textbook is written in a style congenial to the interests of student analysts regardless of their prior background and training. It will teach you basic knowledge about the properties, uses, and marshaling of evidence to show you what is involved in assessing the relevance, believability, and inferential force credentials of evidence. It includes a wide array of examples of the use of the TIACRITIS system and hands on exercises involving both real and hypothetical cases chosen to help you recognize and evaluate many of the complex elements of the analyses you are learning to perform.

TIACRITIS is a web-based system with case studies and knowledge bases incorporating a significant amount of knowledge about evidence, its properties, uses, and discovery. It is a personalizable agent that will help you acquire the knowledge, skills, and abilities involved in discovering and processing of evidence and in drawing defensible and persuasive conclusions from it, by employing an effective learning-by-doing approach. You will practice and learn how to link evidence to hypotheses through abductive, deductive, and inductive reasoning that establish the basic credentials of evidence: its relevance, believability, and inferential force or weight. You will experiment with “what-if” scenarios and study the influence of various assumptions on the final result of analysis.

So, your learning experience will be a joint venture involving this book together with your interaction with TIACRITIS.

You will have access to the TIACRITIS system as you begin to read this book. As you will see in the following sections of this book, a variety of vital information about evidential reasoning in intelligence analysis is presented. As we present this information, you will be asked to use TIACRITIS at various points to study and construct specific examples of matters and procedures described in the book. Here we encounter the reasoning and tutoring capabilities of TIACRITIS. This system is truly a “smart” system since it has itself already been taught on many of the evidential and inferential elements required in
complex intelligence analysis. This allows TIACRITIS to be a valuable tutor since it knows what questions to ask you, and that you should answer, as you confront the various problems you and TIACRITIS will address. Therefore, TIACRITIS can be a most valuable guide along the route to your “hands on” learning experience concerning some truly complex matters encountered in intelligence analysis.

Here is a route or map we will follow in the learning venture you will have with the assistance of TIACRITIS. Section 1 is introductory in nature and includes discussion of the problems we all face in forming defensible and persuasive conclusions about events in a non-stationary world that keeps changing all the while we are trying to understand events we have observed. In the process, we will also provide an account of the process of “connecting the dots” and what this process actually entails. As you well know, critics of our intelligence services abound in the media. A very frequent charge made by these critics is that intelligence analysts are deficient in the task of connecting the dots. A major trouble is that these critics have almost no awareness themselves of what is actually involved in doing this. When examined carefully, the task of connecting dots is astonishingly difficult even under the best of conditions. Careful study of the topics included in this joint learning venture involving TIACRITIS should, among other things, assist intelligence analysts to respond more effectively to their critics.

At the beginning of each of the following sections we will present basic information about some important matters. Then we will ask you to make use of TIACRITIS to observe how this system can incorporate these matters by way of examples. In some cases you will be asked to provide TIACRITIS with information required to solve an analytic problem. TIACRITIS will assist you in this process since it will know generally the kinds of information that is required. This is the “hands on” capability of the approach we are taking to help you learn more about the complexities of complex evidential reasoning.

Section 0 first contains discussion of an approach that seems necessary in complex intelligence analysis; this approach can be termed “divide and conquer,” or “task decomposition,” in which we break some complex situation into simpler elements and then reassemble these elements in forming a final conclusion. It is here that we first introduce you to the TIACRITIS system. We will use TIACRITIS to illustrate how we can decompose a complex analysis problem into more detailed elements that involve judgments that are more specific and usually easier to make.

Sections 3 through 7 contain basic information about evidence, its three basic properties or credentials, the various uses of evidence, and the recurrent forms and combinations of evidence regardless of its content or substance. The basic credentials of evidence are: relevance, believability, and inferential force or weight. These credentials are not inherent properties of evidence, but analysts must establish them through defensible and persuasive arguments. We consider carefully the process of generating these arguments for items and masses of evidence. This process calls for both imaginative and critical reasoning. Constructing multiple defensible and persuasive arguments from masses of evidence involves what are currently called inference networks. The basis for these complex argument structures has been work that is nearly one hundred years old, though until recently, no one has paid much attention to this valuable work. In each of these sections you will use TIACRITIS to see examples of the concepts involved and to provide responses to problem situations that are posed for you to test your ability to provide appropriate responses.
In Sections 8 and 9 we discuss the important task of drawing defensible and persuasive conclusions from masses of evidence. Any conclusions based on evidence must be hedged or stated probabilistically. We discuss five major reasons why all conclusions based on evidence are necessarily probabilistic in nature. We also discuss four uncertainty methods that are used to assess and report the uncertainty. This is necessary because each such method captures some important elements of probabilistic reasoning, but no single view captures all of them.

Section 10 overviews several problems with argument construction and includes case studies using TIACRITIS to compare the analyses of competing hypotheses, as well as the analyses of the same hypothesis performed by different analysts.

In Section 11 we discuss how the intelligence analysis concepts and methods embedded into TIACRITIS, which are based on the Science of Evidence and Artificial Intelligence, may help the analysts perform better analyses, no matter what analysis methods they use. They include the systematic approach to the development of argumentation structures, the substance-blind classification of evidence, and the associated procedure for assessing the believability of evidence, the drill-down analysis and assumptions-based reasoning. In particular, we review what is probably the most popular structured analytic method, Richards J. Heuer’s Analysis of Competing Hypothesis (ACH) (Heuer, 1999; 2008), showing how it can be improved by employing the concepts and methods embedded in TIACRITIS.

The last two sections, 12 and 13, present the application of the developed computational theory of intelligence analysis and of TIACRITIS to geospatial intelligence and to military intelligence.

Naturally, we hope that your learning venture with the assistance of TIACRITIS will be a most valuable experience in which you have discovered many very important elements of intelligence analysis, some of which you might not have heard anything about before. We also hope that this venture has been directly relevant to tasks you face, or will face, every day in your analytic careers. Finally, we hope that it will be as enjoyable as it is informative. So, as you begin this learning venture, we wish you Bon Voyage!
1 INTELLIGENCE ANALYSIS: “CONNECTING THE DOTS”

1.1 How Easy Is It to Connect the Dots?

One way to describe the process of intelligence analysis is to employ a metaphor that is so often used, and misused, in discussions of intelligence analyses. How many times have you seen accounts in printed sources or heard “talking heads” on television say that our intelligence analysts have failed to “connect the dots” in some important matter concerning our national security? A fair question is: how well would these news writers or talking heads connect the dots themselves if they were faced with the complex judgments and other matters involved in modern intelligence analysis? In some accounts, it is made to sound as if the process of connecting intelligence-related dots is as simple as the tasks most of us faced as children when we were asked to use a pencil to connect some collection of numbered dots on a printed page. If the dots were connected in an appropriate order, a representation of some familiar object or person, such as Santa Claus, a witch, or a puppy, would be revealed. Our belief is that critics employing this metaphor in criticizing intelligence analysts have very little awareness of how astonishingly difficult the process of connecting the dots can be in so many contexts, especially in intelligence analysis. The following represents an account of a variety of problems that may so easily be overlooked in discussions of the task of connecting the dots in situations as complex as intelligence analysis.

1.1.1 Problem 1: There Is More Than One Kind of Dot to Be Connected

It is so easy to assume that the only kind of dot to be connected concerns details in the observable information or data we collect that may eventually be considered as evidence in some analysis. We might refer to these dots as being evidential dots. Sherlock Holmes had another term for the details in observations he made, calling them trifles. As he told Dr. Watson: “You know my method, it is based on the observance of trifles.” A related problem here is that most items of intelligence evidence may contain many details, dots, or trifles, some of which are interesting and others not. What this means is that incoming intelligence information must be carefully parsed in order to observe its significant evidential dots. In Sections 3 and 4 we give special attention to the problem of what qualifies as an evidential dot. Not all data or items of information we have will ever become evidence in an analysis task. Arguments necessary to justify an item of information being evidence are discussed in Section 6. But the details in our evidence form only one form of dot or trifle we need to connect.

The second type of dot concerns ideas we have about how some evidential dot, or a collection of evidential dots, is connected to matters we are trying to prove or disprove. We commonly refer to the matters to be proved/disproved as hypotheses. Hypotheses commonly refer to possible alternative conclusions we could entertain about matters of interest in an analysis. These other dots, that we call idea dots, come in the form of links in chains of reasoning or arguments we construct to link evidential dots to hypotheses. Each of these idea dots refer to sources of uncertainty or doubt we believe to be interposed between our evidence and our hypotheses. This is precisely where imaginative
reasoning is involved. The essential task for the analyst is to imagine what evidential dots mean as far as hypotheses or possible conclusions are concerned. Careful critical reasoning is then required to check on the logical coherence of sequences of idea dots in our arguments or chains of reasoning. In other words, does the meaning we have attached to sequences of idea dots make logical sense?

Figure 1 below shows an abstract example of the distinction between an evidential dot and what we have termed idea dots. Suppose we have a situation in which we have observed a potential evidential dot X and we contemplate its bearing on some hypothesis H. It could have happened that evidential dot X has caused us to generate hypothesis H and someone has asked us to say why H explains our observation of evidential dot X. We note that H is also an idea dot since it is also a source of doubt or uncertainty.

![Diagram of Types of Dots](image)

Figure 1. Types of dots to be connected: evidence, ideas, and hypotheses.

As you will observe in Section 6, the TIACRITIS system knows about the two forms of dots: evidential and idea dots. It will assist you in forming chains of reasoning or sequences of idea dots that allow you to form defensible and persuasive arguments from a mass of evidential dots. But, so far, we have only mentioned the first of several problems that arise in connecting the dots.

### 1.1.2 Problem 2: Which Evidential Dots Should Be Connected?

Here is where the astonishing complexity of intelligence analysis begins to arise, even in the simplest of cases, in any form of analysis based on evidence. Considering just the evidential dots or details we have mentioned, any connections among them require us to consider possible combinations of these individual details. It would be rare indeed for any analytic conclusion to be based on just a single evidential dot. Right off the bat we encounter an exponential explosion. Suppose we consider having some number N of evidential dots. We ask the question: How many combinations C of two or more evidential dots are there when we have N evidential dots? The answer is given by the following expression: $C = 2^N - (N + 1)$. In the part of this expression $(N + 1)$, $N$ refers to the number of ways in which we could examine the N dots one at a time. The number 1 means the number of cases in which we examine none of these dots. What is left after subtracting $(N + 1)$ from $2^N$ is the number of cases in which we examine combinations of two or more evidential dots.

The expression $C = 2^N - (N + 1)$ by itself does not reveal how quickly this combinatorial explosion takes place. Here are a few examples showing how quickly C mounts up with increases in N:
For $N = 10$, $C = 1013$
For $N = 25$, $C = 33,554,406$
For $N = 50$, $C = 1.13 \times 10^{15}$
For $N = 100$, $C = 1.27 \times 10^{30}$

There are several important messages in this combinatorial analysis for intelligence analysis. The first concerns the size of $N$, the number of potential evidential dots that might be connected. Given the array of sensing devices and human observers available to our intelligence services, the number $N$ of potential evidential dots is as large as you wish to make it. In most analyses $N$ would certainly be greater than 100 and would increase as time passes. Remember that we live in a non-stationary world in which things change and we find out about new things all the time. So, in most cases, even if we had access to the world’s fastest computer, we could not possibly examine all possible evidential dot combinations even when $N$ is quite small.

Second, trying to examine all possible evidential dot combinations would be the act of looking through everything with the hope of finding something. This would be a silly thing to do, even if it were possible. The reason of course is that most of the dot combinations would tell us nothing at all. What we are looking for are combinations of evidential dots that interact or are dependent in ways that suggest new hypotheses or possible conclusions. If we examined these dots separately or independently we would not perceive these new possibilities. Figure 2 is an abstract example; real life examples follow later.

In Figure 2 there are four numbered evidential dots. The numbers might indicate the order in which we obtained them. In part (a) of the figure we show an instance where these four dots have been examined separately or independently in which case they tell us nothing interesting. Then someone notices that, taken together, these four dots combine to suggest a new hypothesis $H_k$ that no one has thought about before, as shown in part (b) of the figure. What we have here is a case of evidential synergism in which two or more evidence items mean something quite different when they are examined jointly than they would mean if examined separately or independently. Here we come to one of the most interesting and crucial evidence subtleties or complexities that have, quite frankly, led to intelligence failures in the past: failure to identify and exploit evidential synergisms. We will address this matter in other problems we mention concerning connecting the dots.
It might be said that the act of looking through everything in the hope of finding something is the equivalent of giving yourself a prefrontal lobotomy, meaning that you are ignoring any imaginative capability you naturally have concerning which evidential dot combinations to look for in your analytic problem area. Later in this book will discuss the process of discovery or investigation that forms the basis for all intelligence analyses. This is an ongoing seamless activity in which we have evidence in search of hypotheses, hypotheses in search of evidence, and the testing of hypotheses all going on at the same time. Later we discuss how TIACRITIS can assist you in the imaginative task of deciding which combinations of evidential dots to examine. Hypotheses you entertain, questions you ask, particular evidence items, and your accumulated experience, all allow you to examine which evidential dot combinations are inferentially significant. TIACRITIS has been designed to help you identify evidential dot combinations in which there could possibly be synergisms.

1.1.3 Problem 3: Which Evidential Dots Can Be Believed?

The next problem we discuss is one of the most important, challenging, and interesting problems raised in any area of intelligence analysis. From some source, a sensor of some sort, or from a person, we obtain an evidential dot saying that a certain event has occurred. Just because this source says that this event occurred does not entail that it did occur. So what is vitally necessary is to distinguish between evidence of an event and the event itself. We adopt the following notational device to make this distinction:

- $E$ represents the actual occurrence of event $E$.
- $E_{*i}$ represents the reported occurrence of event $E$ from source $I$.

So, a basic inference we encounter is whether or not $E$ did occur based on our evidence $E_{*i}$. Clearly, this inference rests upon what we know about the believability of source $I$. There are some real challenges here in discussing the believability of source $I$. Section 5 of this book is devoted to the task of assessing the believability of our sources of intelligence evidence. As we will see, the TIACRITIS system already knows much about this crucial task.

We might easily have said in Problem 1 above that there are even distinctions to be made in what we have called evidential dots. Some of these dots arise from objects we obtain or from sensors that supply us with records or images of various sorts. So one major kind of evidential dot involves what we can call tangible evidence that we can observe for ourselves to see what events it may reveal. In many other cases we have no such tangible evidence but must rely upon the reports of human sources who allegedly have made observations of events of interest to us. Their reports to us come in the form of testimonial evidence or assertions about what they have observed. Therefore, an evidential dot $E_{*i}$ can be one of the following types:

- **Tangible evidence** such as objects of various kinds, or sensor records like those obtained by SIGINT, IMINT, MASINT, and other possible sources.
- **Testimonial evidence** obtained from human sources (HUMINT).

We have much more to say about the forms and combinations of evidence in Section 7 of this book.
The origin of one of the greatest challenges in assessing the believability of evidence is that we must ask different questions about the sources of tangible evidence than those we ask about the sources of testimonial evidence. Stated another way, the believability attributes of tangible evidence are different from the believability attributes of testimonial evidence. But there is another difficulty that is not always recognized that can cause endless trouble. While, in the case of tangible evidence, believability and credibility may be considered as equivalent terms, human sources of evidence have another characteristic apart from credibility; this characteristic involves their competence. As we discuss in Section 5.4, the credibility and competence characteristics of human sources must not be confused; to do so invites inferential catastrophes, as we will illustrate. The questions required to assess human source competence are different from those required to assess human source credibility. The TIACRITIS system knows what credibility-related questions to ask of tangible evidence and the competence and credibility-related questions to ask of HUMINT sources.

There is no better way of illustrating the importance of evidence believability assessments than to show how such assessments form the very foundation for all arguments we make from evidence to possible conclusions. In many situations people will mistakenly base inferences on the assumption that an event E has occurred just because we have evidence $E^*_I$ from source I. This amounts to the suppression of any uncertainty we have about the believability of source I (whatever this source might be). In Figure 3 is a simple example illustrating this believability foundation; it will also allow us to introduce the next problem in connecting the dots.

![Figure 3. The believability foundation for an argument.](image)

What this figure shows is an argument from evidence $E^*_I$ to whether or not hypothesis H is true. As shown, the very first stage in this argument concerns an inference about whether or not event E actually occurred. This is precisely where we consider whatever evidence we may have about the believability of source I. We may have considerable uncertainty about whether or not event E occurred. All subsequent links in this argument concern the relevance of event E on hypothesis H. As we noted in Figure 1, these relevance links are the idea dots we discussed. As the figure shows, each idea dot is a source of uncertainty associated with the logical connection between whether or not event E did occur and whether or not H is true. Consideration of these relevance links is our next problem in connecting the dots.
1.1.4 Problem 4: What Are the Connections between Evidential Dots and Hypotheses?

As discussed in Section 3, all evidence has three major credentials or properties: relevance, believability, and inferential force or weight. No evidence ever comes to us with these three credentials already attached; they must be established by defensible and persuasive arguments linking the evidence to the hypotheses we are considering. As we will see, relevance answers the question: So what? How is this datum or information item linked to something we are trying to prove or disprove? If such relevance linkage cannot be established, this datum is irrelevant or useless. As discussed above, believability answers the question: Can we believe what this evidence is telling us? The force or weight credential asks: How strong is this evidence in favoring or disfavoring the hypothesis? This is where probability enters our picture since, for very good reasons, the force or weight of evidence is always graded in probabilistic terms.

A relevance argument is precisely where the idea dots become so important. Considering an item of information, an analyst must imagine how this item could be linked to some hypothesis being considered before it could become an item of evidence. These idea dots forming this linkage come in the form of propositions or statements indicating possible sources of doubt or uncertainty in the imagined linkage between the item of information and hypotheses being considered. For a simple example, look again at Figure 3 above where we show a connection between evidence E* and hypothesis H. An analyst has an item of information from source I concerning the occurrence of event E that sounds very interesting. This analyst attempts to show how event E, if it did occur, would be relevant in an inference about whether hypothesis H is true or not. So the analyst forms the following chain of reasoning involving idea dots. The analyst says: “If event E were true, this would allow us to infer that event F might be true, and if F were true, this would allow us to infer that event G might be true. Finally, if event G were true, this would make hypothesis H more probable.” If this chain of reasoning is defensible, the analyst has established the direct relevance of evidence E* on hypothesis H. There is another form of relevance, called indirect relevance, which we discuss in Section 4.

In forming this argument the analyst wisely begins with the believability foundation for this whole argument: Did event E really occur just because source I says it did? Also notice in Figure 3 that we have indicated the uncertainty associated with each idea dot in this argument. For example, the analyst only infers from E that F might have occurred and so we note that we must consider F and not F as possibilities. The same is true for the other idea dots G and H.

There are several important things to note about relevance arguments; the first concerns their defense. Suppose the argument in Figure 3 was constructed by analyst A. A shows this argument to analyst B who can have an assortment of quibbles about this argument. Suppose B says: “You cannot infer F directly from E; you need another step here involving event K. From E you can infer that K occurred, and then if K occurred, then you can infer F.” Now comes analyst C who also listens to A’s argument. C says: “I think your whole argument is wrong. I see a different reasoning route from E to hypothesis H. From E we can infer event R, and from R, we can infer event S, and from S we can infer T, which will show that hypothesis H is less probable.” Whether or not there is any final agreement about
the relevance of evidence $E^*_i$, analyst $A$ has performed a real service by making the argument openly and available for discourse and criticism by colleagues. There are several important messages here.

First, there is no such thing as a uniquely correct argument from evidence to hypotheses. What we all try to avoid are disconnects or non sequiturs in the arguments we construct. But even when we have an argument that has no disconnects, someone may be able to come up with a better argument. Second, we have only considered the simplest possible situation in which we used just a single item of potential evidence. But intelligence analyses are based on masses of evidence of many different kinds and that come from an array of different sources. In this case we are obliged to consider multiple lines of argument that can be connected in different ways. It is customary to call these complex arguments inference networks.

From years of experience teaching law students to construct defensible and persuasive arguments from evidence, we have found that most of them often experience difficulty in constructing arguments from single items of evidence; they quickly become overwhelmed when they are confronted with argument construction involving masses of evidence. But they gain much assistance in such tasks by learning about argument construction methods devised nearly a hundred years ago by a world-class evidence scholar named John H. Wigmore (1937). Wigmore was the very first person to carefully study what today we call inference networks. We will encounter Wigmore’s work in several places in our discussions and you will see that the TIACRITIS system employs elements of Wigmore’s methods of argument construction.

There is also a message here for critics such as news writers and the taking heads on television. These critics always have an advantage never available to practicing intelligence analysts. Namely, they know how things turned out or what actually happened in some matter affecting our nation’s security. In the absence of clairvoyance, analysts studying a problem will never know for sure, or be able to predict with absolute certainty, what will happen in the future. A natural question to ask these critics is: “What arguments would you have constructed if all you knew was what the analysts had when they made their assessments?” This would be a very difficult question for them to answer fairly, even if they were given access to the classified evidence our analysts may have known at the time.

1.1.5 Problem 5: What Do Our Arguments Mean?

Here we consider the direction and force of our arguments based on the combined evidence we have considered. Direction refers to the hypothesis we believe our evidence favors most. Force means how strongly we believe the evidence favors this hypothesis over alternative hypotheses we have considered. There are two uncontroversial statements we can make about the force or weight of evidence. The first is that the force or weight of evidence has vector-like properties. What this means is that evidence points us in the direction of certain hypotheses or possible conclusions with varying degrees of strength. The second is that the force or weight of evidence is always graded in probabilistic terms indicating our uncertainties or doubts about what the evidence means in terms of its inferential direction and force. But beyond these two statements, controversies begin to arise.
Before we consider assorted controversies, it is advisable to consider where our uncertainties or doubts come from in the conclusions we reach from evidence. Have a look once again at Figure 3 involving a simple example based on a single item of evidence. Our evidence here was $E^*$, from source $I$, saying that event $E$ occurred. We ask the question: How strongly does this evidence $E^*$ favor hypothesis $H$ over not-$H$? As we discussed, this argument was indicated by what we termed idea dots, each one indicating what the analyst constructing this argument believed to be sources of doubt or uncertainty associated with the argument from the evidence to the hypothesis. As you see, there are two major origins of uncertainty: those associated with the believability of source $I$, and those associated with links in the analyst’s relevance argument. So, the force of evidence $E^*$ on hypotheses $H$ and not-$H$ depends on how much uncertainty exists in this entire argument involving each one of its believability and relevance links. The interesting message here is that the evidence force or weight credential depends on its other two credentials: believability and relevance.

In the simple example just discussed there are four major origins of uncertainty, one associated with believability and three associated with relevance. But this is the easiest possible situation since it involves only one item of evidence. Think of how many sources of uncertainty there might be when we have a mass of evidence together with multiple complex and possibly interrelated arguments. The mind boggles at the enormity of the task of assessing the force or weight of a mass of evidence commonly encountered in intelligence analysis when we have some untold numbers of sources of believability and relevance uncertainties to assess and combine. We are certain that critics of intelligence analysts have never considered how many evidential and idea dots there would be to connect.

So, the question remains: How do we assess and combine the assorted uncertainties in complex arguments in intelligence analysis, and in any other context in which we have the task of trying to make sense out of masses of evidence? Here is where controversies arise. The problem is that there are several quite different views among probabilists about what the force or weight of evidence means and how it should be assessed and combined across evidence in either simple or complex arguments. Each of these views has something interesting to say, but no one view says it all. Later in this book we will discuss how the TIACRITIS system allows you to assess and combine probabilistic judgments in situations in which many such judgments are required. There is further difficulty as far as judgments of the weight or force of evidence is concerned. Analysts, or teams of analysts, may agree about the construction of an argument but disagree, often vigorously, about the extent and direction of the force or weight this argument reveals. There may be strong disagreements about the believability of sources of evidence or about the strength of relevance linkages. These disagreements can only be resolved when arguments are made carefully and are openly revealed so that they can be tested by colleagues. A major mission of the TIACRITIS system is to allow you to construct arguments carefully and critically, and encourage you to share them with colleagues so that they can be critically examined.

There is one final matter of interest in making sense out of masses of evidence and complex arguments. Careful and detailed argument construction might seem a very laborious task, no matter how necessary it is. This is one major objective of the entire TIACRITIS project. Now consider the task of revealing the conclusions resulting from an analysis to some policy-making “customer” who has decisions to make that rest in no small part on the results of an intelligence analysis. What this
“customer” will probably not wish to see is a detailed inference network analysis that displays all of the dots that have been connected and the uncertainties that have been assessed and combined in the process. A fair guess is that this “customer” will wish to have a narrative account or a story about what the analysis predicts or explains. In some cases, “customers” will require only short and not extensive narratives. This person may say: “Just tell me the conclusions you have reached and briefly why you have reached them.” So the question may be asked: Why go to all the trouble to construct defensible and persuasive arguments when our “customers” may not wish to see their details?

There is a very good answer to the question just raised. Your narrative account of an analysis must be appropriately anchored on the evidence you have. What you wish to be able to tell is a story that you believe contains some truth; i.e. it is not just a good story. The virtue of careful and critical argument construction is that it will allow you to anchor your narrative not only on your imagination, but also on the care you have taken to subject your analysis to critical examination. There is no telling what questions you might be asked about your analysis. Rigor in constructing your arguments from your evidence is the best protection you have in dealing with “customers” and other critics who might have entirely different views regarding the conclusions you have reached. The TIACRITIS system is designed to allow you and others to critically evaluate the arguments you have constructed.

1.1.6 Problem 6: Whose Dots Should Be Connected?

There are several very easy answers to this question. Unfortunately, TIACRITIS does not allow us to provide all of these answers. One obvious answer is that all the potential evidential dots collected by any intelligence service that bear upon a problem involving our nation’s security should be shared or brought together. Since September 11, 2001, so many examples of potential relevant evidence, gathered by different intelligence services, were never shared across agencies and offices. The basic problem this creates is that the extremely important evidential synergisms we discussed in Problem 2 (Section 1.1.2) can never be detected and exploited in reaching analytic conclusions. In some cases, this has resulted in our failure to reach any conclusion at all in some important matter. This forms the basis for one of the major criticisms of our intelligence services in their failure to “connect the dots.” In some instances in the past, potential evidence may have been viewed as a “proprietary” commodity to be shared only at the discretion of the agency that collected it. In other cases, there have been various statutory rules preventing sharing of evidence across intelligence-related services. Whatever the causes for this lack of sharing of intelligence information, this problem has been of great concern in the past few years.

But there is one way that the TIACRITIS process can assist in the detection and inferential exploitation of possible evidential synergisms and it is something that rests on analysts, and analyst teams, at work on an intelligence problem. Careful argument construction will help reveal the incompleteness of available evidence. The analysts might easily observe that not all questions that should be asked about the problem at hand have in fact been answered. So, this forms the basis for asking questions such as:

- Have any other agencies or offices attempted to answer these questions that we believe
have gone unanswered?

- If these other agencies have gathered such evidence, how can we best justify or be able to have ready access to it?
- What collection efforts should be mounted to gather evidence necessary in order to provide more complete assessments of evidence necessary to form more productive conclusions?

In many cases such evidence may have never been collected. In these cases, analysts can play very important roles in directing effective and productive evidence collection efforts. In so many instances it seems that we try to collect everything with the hope of finding something. This is one reason why we often correctly believe that we are drowning in information. More imaginative efforts are required in order to collect potential evidential dots of actual relevance in inference problems faced by intelligence analysts. This is another area in which the imagination of analysts becomes so important.

1.2 Connecting the Dots through the Discovery of Evidence, Hypotheses, and Arguments

Coping with the astonishing complexity of intelligence analysis requires a systematic approach, grounded in the Science of Evidence, which integrates imaginative and critical reasoning to connect the dots, in a continuously changing world, through ceaseless discovery and testing of evidence, hypotheses, and arguments. Figure 4 illustrates such a systematic approach which involves evidence in search of hypotheses (through abductive or imaginative reasoning), hypotheses in search of evidence (through deductive reasoning), and evidential tests of hypotheses (through inductive reasoning), all going on at the same time.

Imagine that you, a counterterrorist analyst, read in today’s *Washington Post* an article where a person named Willard reports that a canister of cesium-137 has gone missing from a company XYZ in Maryland (see Table 1). This item of evidence (E*i*) leads you to abductively leap to the hypothesis H_k that a dirty bomb will be set off in the Washington, DC area. Asked to justify it, you may provide the following abductive reasoning shown in the left hand side of Figure 5 and in Table 2. In this case, we have evidence in search of hypotheses where an item of evidence “searches” for hypotheses that explain it. Notice here the connections between the various types of dots discussed in Section 1.1.1: evidence dot (E*i*), idea dots (H_a, H_c, H_e), and hypothesis dot (H_k).

The diagram in the middle of Figure 4 illustrates the process of hypotheses in search of evidence. Once the new hypothesis H_k has been generated, the analyst has to assess it, through deductive reasoning. The reasoning might start as follows: “If H_k were true, there are sub-hypotheses, listed as H_d and H_e, that would be necessary and sufficient to make H_k true. If H_d were true then one would need to observe evidence that supports it.” Similarly, H_e and its sub-hypotheses allow the analyst to deduce potential items of evidence (shown as shaded circles) that bear upon them. Here we have hypotheses in search of evidence that guides the process of collecting new evidence. Notice that this helps answer the questions:

- Which evidential dots should be connected? (see Section 1.1.2)
• Whose dots should be connected? (see Section 1.1.6)

![Diagram showing the process of connecting dots through evidence, hypotheses, and arguments.]

Figure 4. Connecting the dots through the discovery of evidence, hypotheses, and arguments.

Table 1. Surprising information

| INFO-001-Willard: The XYZ company in Baltimore, MD, manufactures devices for sterilizing medical equipment. A person named Willard reported in a *Washington Post* article that a canister containing powder, including approximately 3000 curies of cesium-137, had gone missing from the company’s warehouse in Baltimore. |

Table 2. Abductive reasoning justifying a hypothesis.

<table>
<thead>
<tr>
<th>Evidence</th>
<th>Hypotheses</th>
<th>Evidentiary tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>E_i</td>
<td>H_k</td>
<td>H_e</td>
</tr>
</tbody>
</table>

There is evidence $E_i^*$ that the cesium-137 canister is missing.

$\Rightarrow$ It is possible that the cesium-137 canister is indeed missing.

$\Rightarrow$ It is possible that the cesium-137 canister was stolen.

$\Rightarrow$ It is possible that it was stolen by someone associated with a terrorist organization.

$\Rightarrow$ It is possible that the terrorist organization will use it to construct a dirty bomb.

$\Rightarrow$ It is possible that the dirty bomb will be set off in the Washington, DC area.

Now, some of the newly discovered items of evidence may trigger new hypotheses (or the refinement of the current hypothesis). So, as indicated at the bottom left of Figure 4, the processes of
evidence in search of hypotheses and hypotheses in search of evidence take place at the same time, and in response to one another.

The combination of evidence in search of hypotheses and hypotheses in search of evidence results in hypotheses which have to be tested, through inductive reasoning, based on the discovered items of evidence, as illustrated in the right-hand side of Figure 4. This is a probabilistic inference network that shows how the evidence at the leaves of the network (shown as black circles) is linked to hypotheses (e.g., $H_a$, $H_c$, $H_e$, $H_d$, $H_k$) through arguments that establish the relevance, believability and inferential force of evidence with respect to those hypotheses. The result of the testing process is the likelihood of the considered hypothesis (e.g., $H_k$: It is likely that a dirty bomb will be set off in the Washington, DC area). Building such a probabilistic inference network helps answer the following questions:

- Which evidential dots should be connected? (see Section 1.1.2)
- Which evidential dots can be believed? (see Section 1.1.3)
- What are the connections between evidential dots and hypotheses? (see Section 1.1.4)
- What does our argument mean? (see Section 1.1.5)

### 1.3 Analysis of Competing Hypotheses

For each abducted hypothesis from the left hand side of Figure 4 (such as “the cesium-137 canister was stolen”), one would need to consider competing hypotheses (e.g., “the cesium-137 canister was misplaced” or “the cesium-137 canister was used in a project without being checked-out”), as illustrated in Figure 5. Moreover, for each such competing hypothesis one has to search for relevant evidence and use the evidence to test it, as discussed above and illustrated in Figure 5.

![Figure 5. Analysis of competing hypotheses.](image-url)
We have now discussed six problems involved in the task of connecting the dots. Our belief is that most critics of intelligence analysts, using this metaphor, have little awareness of what these natural problems are. In discussing these problems we have given an account of what we believe to be many of the major problems analysts confront when they attempt to make defensible and persuasive conclusions from masses of evidence. One of our major objectives has been to provide intelligence analysts with means to effectively counter these critics. But in doing so we also acknowledge that there are special problems associated with these tasks that are germane to the business of modern intelligence analysis.

We will use this example in the following sections both to introduce important intelligence analysis concepts and the use of TIACRITIS.

### 1.4 Case Study: Defining a Personalized Course in Intelligence Analysis

#### 1.4.1 Objective

If you are an instructor, run TIACRITIS while following this case study to learn how to define various intelligence analysis courses for your students.

#### 1.4.2 Summary

You will start the system and see that there are several courses already defined. Each of them consists of a subset of all the chapters and case studies represented in TIACRITIS. Then you will use the Preferences menu to define a new course for your students, titled *Geospatial Intelligence*, by selectively hiding chapters and case studies from the complete version of the Intelligence Analysis course represented in TIACRITIS. Proceed as indicated in the following instructions.

#### 1.4.3 Instructions

1. Start TIACRITIS and you will see the introductory screen in Figure 6.

![Welcome to TIACRITIS](image)
2. Click-on [CONTINUE]. As a result, TIACRITIS will display the screen in Figure 7 showing several available courses. Select one of them (e.g. “Intelligence Analysis (short version)”) by clicking on its name. Then click on [START].

![Figure 7. Selecting the course available in TIACRITIS.](image)

3. Click-on the Preferences menu and you will see three types of preferences in the left panel (Course version, User type, and User model).

4. Select User type and notice that the current type is [INSTRUCTOR], as also indicated at the top of the screen. As an instructor, you may also choose the [STUDENT] type, to experience the use of the system as a student. However, you will not be able to define courses as a student.

5. Select Course version and notice in the right panel the four course versions currently defined. Since “Intelligence Analysis (short version)” is selected, its topics are shown at the bottom of the right panel. We will define a new course version.

6. In the right panel, after “Select the current course version,” click-on [NEW]. As a result, TIACRITIS defines a new version of the course (temporarily called “version-0”) which initially contains all the chapters and case studies available with the TIACRITIS system, as shown in Figure 8. We will define a course titled Geospatial Intelligence by renaming the course and hiding some of the chapters and case studies.
7. In the right panel, after “version-0,” click on [RENAME]. Then, in the displayed pane, type the course name: Geospatial Intelligence. Then click on [SAVE].

8. Skip chapters and case studies from the complete course by clicking on [HIDE] following their names in the course’s table of contents. Notice in Figure 9 that their titles are grayed-out. You may add them back by clicking on the corresponding [SHOW] command.

9. Notice the [SAVE] command at the top of the right panel, after “Remember to save the modifications performed.” You need to click on [SAVE] if you wish to save the new course or any modifications done to the existing courses. In this case we will not save the course.
This concludes the current case study.

Figure 9. Defining the Geospatial Intelligence course.
1.5 Case Study: Introduction to the Use of TIACRITIS

1.5.1 Objective

This case study will help you learn how to operate the TIACRITIS system.

1.5.2 Summary

You will start the system, select a course to follow, and learn to perform some basic operations, such as initializing the user model, ending a case study, and starting another one (either explicitly or automatically). Proceed as indicated in the following instructions.

1.5.3 Instructions

1. Start TIACRITIS. You will see the introductory screen in Figure 6 (pg.17).
2. Click on [CONTINUE]. As a result, TIACRITIS will ask you to select one of the course versions the instructor has defined for you, as shown in the left panel of Figure 7 (pg. 18).
3. Click on one of the courses and then click on [START]. The right panel shows the contents of the selected course.
4. In the right panel, click on [START CASE STUDY] and TIACRITIS will display a more detailed description of the case study, including a summary and the instructions that you will need to follow to complete it (see Figure 10). From now on we will follow these instructions.

5. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 11 will be displayed. It contains several hypotheses to
6. Select the hypothesis analysis problem: “Assess whether the cesium-137 canister is missing from XYZ warehouse.” The Reasoner is automatically invoked to analyze the hypothesis, as shown in the top part of Figure 12. Notice also that all the menu items at the top of the window are now selectable. Each case study will direct you to select some of them and perform various analysis tasks.

7. Select the Preferences menu. Notice in Figure 13 that the User model is selected. This model keeps track of your progress with the case studies so that, when you start the system again you will continue from the point where you were when you closed the system. You may reset the student model by clicking on [RESET USER MODEL]. As a result, next time you will use the system you will start from the very beginning, as if you were using the system for the first time. Therefore, any analysis that you may have done will be deleted.
8. Select the Case Study menu. As shown in Figure 10, you have several continuation options:

- Clicking on [SAVE & FINISH] at the bottom of the left panel or in the right panel will end the current case study and will automatically introduce the next case study.
- Clicking on [CANCEL] will cancel the case study as if you have not started it yet.
- Clicking on [FINISH WITHOUT SAVING] will end the case study without saving any analysis you may have done. You will then be automatically directed to the next case study.
- Clicking on [SAVE] will save your current analysis without ending the case study (you may continue with the current case study).
- Clicking on [DISCARD YOUR ANALYSIS AND RESTART] will discard any analysis you may have done and will restart the case study from the beginning.

9. Click on [SAVE & FINISH] to end this case study. You may now continue with the next case study or quit the system.
2 DIVIDE AND CONQUER: A NECESSARY APPROACH TO COMPLEX ANALYSES

2.1 Holistic Approach to Analysis

In our work, and in our personal affairs, we can address inference and decision problems at various levels of detail. As an introductory example, we describe a situation in which we do not decompose a problem at all and consider some of the consequences of failure to do any decomposition. Faced with the task of drawing a conclusion about some matter of interest, we may gather some information that seems relevant and credible, we think about it for a while, and eventually we draw at least a tentative conclusion. We do this all in our own heads without recording of any of the stages and details in our analysis. Furthermore, there is usually no orderly structure to our trains of thought in this analysis. This approach has a name, it is called a holistic approach to emphasize the fact that we deal with some problem in its perceived entirety all at once and without any kind of outside assistance or interference. In simple problems involving our own personal affairs, we may do this very frequently. But there are some natural hazards involved in a completely holistic approach to inference and decision problems. The following is a very simple example of what can happen as a result of an entirely holistic approach.

Suppose, in discussing with your spouse an upcoming political election, you say that you have reached the conclusion that person X will be the best candidate. Here are just a few of the questions your spouse might raise while listening to your conclusion:

Your spouse first says, “Tell me what evidence you used to reach the conclusion that X would be the best candidate?” Suppose you say, “Well, I believe I considered evidence A, B, C, and D, that I thought on balance favored X.” Your spouse listens to your account and has further questions.

Your spouse says, “Why did you believe that evidence B was relevant at all; and why did you believe that the source of evidence D deserved to be believed?” You search for answers to these questions and have difficulty deciding what you had previously thought about these matters, if you thought about them at all.

Your spouse asks a related question saying, “I would have thought that evidence E, F, and G should also be taken into consideration. Why did you not consider these items?” You say, “Well I might have considered E but I don’t believe I considered F and G.”

Then your spouse asks, “You say that this evidence ‘on balance’ favors candidate X. This means that you considered some other candidates; which ones did you consider?” You say, “Well, I did consider another candidate, Y,” to which your spouse replies, “Two weeks ago Z announced her candidacy, why did you not consider her as well?” Here you draw a complete blank since you did not consider Z.

Finally, your spouse asks, “As far as the evidence items you did consider, which ones were the strongest in favoring candidate X?” Here, unfortunately, you say that you considered evidence items B
and D to be the strongest in favoring candidate X. But they are the two items your spouse challenged as far as their relevance and believability are concerned. One trouble you have is your inability to say why you believed these two items to be relevant and credible.

Let’s leave aside any consideration of the extent to which your spouse’s penetrating analysis of your holistic conclusion affects your subsequent marital harmony. You could have several possible defenses to your inability to answer your spouse’s questions. First, you could say that it is all a matter of memory; who can remember all of the details in one’s trains of thought? You say you did not tape record all the ideas you considered while thinking about this election candidate problem and note that almost no one would ever do so. But there is another problem you may or may not have recognized; it concerns your likely failure to consider the structure of your inferential problem and to consider all the factors or elements it requires. Your only defense here is to say that you are not a logician, a probabilist, or an attorney, but only an ordinary person who draws conclusions every day without being an expert in evidence and inference.

2.2 Divide and Conquer

Reading about the problems with holistic assessments in the example discussed in the previous section, you might believe that they have very little relevance to intelligence analysis. You might say that complex intelligence analysis requires teams of analysts working together to address some problem; it rarely involves just a single analyst thinking alone in some secluded office. You might easily give an example involving counterterrorism. In this situation we would have weapons experts, existing terrorist group experts, geopolitical experts, cultural affairs experts, and a whole host of other experts at work trying to predict the next occurrence of a terrorist incident. But this is actually the very first stage of a problem we now address concerning the structure of an intelligence problem and its specific ingredients. All we have done so far is to note the obvious multidimensional nature of so many intelligence problems. We have just begun the process called divide and conquer.

Within any of the areas of expertise just noted, there are questions raised that require answers, there are masses of evidence to be considered, and there are many dots to be connected. And there are further dots to be connected when conclusions from the experts in each area are brought together in order to draw any conclusion. Now consider any of the experts such as in the counterterrorism example just mentioned. Each one of these experts faces the problems just discussed in Section 1 concerning the task of connecting the dots. We have no way of knowing about the extent to which intelligence experts employ holistic approaches to some degree such as that described in the example above. But we strongly suspect that most analysts take great care to be able to defend their conclusions more extensively than in the example involving the dialogue with your spouse. One well-established key to being more easily able to defend the conclusions in some inferential or decision problem you face is to decompose this problem into smaller elements; this is the basic strategy of divide and conquer.

It has been recognized for many years that decomposing a problem into smaller elements seems an obvious way of simplifying difficult problems. The study of task decomposition has been an object of study by psychologists and others for a long time. As obvious as the benefits of divide and conquer
approaches are, there are some difficulties that are not always recognized. First, it is not always recognized how many pieces or smaller elements there are in some problem being decomposed. This is of course related to the issue: How deep do we wish to decompose a problem? There could be any number of levels or gradations of any problem decomposition. If we do not make our decomposition fine enough, or detailed enough, we may fail to make important distinctions that should be made and that will affect the accuracy of our conclusions. On the other hand, when we decompose a problem into too many smaller elements, we may easily be overcome by their number and never reach any conclusion at all. We have all heard the expression “paralysis by analysis.” Too detailed an analysis is one reason for this paralysis. So, an abiding issue is: How detailed should task decomposition be and how many of the complexities of an evidential reasoning problem should we try to capture and analyze? Another way of stating this problem is to ask: How many sources of doubt should we try to expose in our intelligence analysis?

But there is a second problem often associated with task decomposition. It is often alleged that the smaller elements into which a complex problem is decomposed are easier to deal with. Unfortunately, this is not always the case. In making holistic, or even partially decomposed, judgments we may so often fail to recognize how many and how difficult these judgments actually are.

TIACRITIS helps in alleviating these difficulties by allowing the analyst to decompose a problem at various levels of detail (depending on the available time and evidence), and to evaluate the problems at those levels, as discussed in the following sections.

### 2.3 Problem Decomposition as a Guide for Evidence Collection

Let us consider again the scenario described in Sections 1.2 and 1.3 which involves evidence $E^*_i$ (Willard’s report on the missing of the cesium-137 canister from the company XYZ), shown at the bottom left of Figure 4. Just because an analyst has evidence of an event does not mean that the event actually occurred. Thus, as indicated at the bottom of Figure 5, two hypotheses need to be tested: $E_i$ (The cesium-137 canister is missing from the XYZ warehouse) and not-$E_i$ (The cesium-137 canister is NOT missing from the XYZ warehouse).

As indicated by the blue tree from the middle of Figure 4, one needs to put the hypothesis of interest at work to guide in the collection of additional items of evidence that will be relevant to proving or disproving the hypothesis. Then the collected evidence will be used in assessing the likelihood of the hypothesis, as indicated in the right hand side of Figure 4.

Figure 14 shows the decomposition of the problem “Assess whether the cesium-137 canister is missing from XYZ warehouse” into three simpler assessment problems. This suggests that one should perform the collection tasks shown at the bottom of Figure 14 and in Table 3.
Figure 14. Hypothesis in search of evidence.

Table 3. Evidence collection tasks obtained from the analysis in Figure 14.

<table>
<thead>
<tr>
<th>Collection Task1</th>
<th>Look for evidence that the cesium-137 canister was in the XYZ warehouse before being reported as missing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Task2</td>
<td>Look for corroborative evidence that the cesium-137 canister is no longer in the XYZ warehouse.</td>
</tr>
<tr>
<td>Collection Task3</td>
<td>Look for evidence that the cesium-137 canister was not moved to another location.</td>
</tr>
</tbody>
</table>

Guided by the evidence collection tasks in Table 3 you contact Ralph, the supervisor of the XYZ warehouse, who provides you the information from Table 4.

Table 4. Information obtained through the collection tasks in Table 3.

| INFO-002-Ralph | Ralph, the supervisor of the warehouse, reports that the cesium-137 canister is registered as being in the warehouse, that no one at the XYZ company had checked it out, but it is not located anywhere in the hazardous materials locker. He also indicates that the lock on the hazardous materials locker appears to have been forced. |

When we are given testimonial information, or descriptions of tangible items, the information might contain very many details, dots, or trifles. Some of the details might be interesting and relevant evidence, and others not. What we always have to do is to parse the information to extract the information that we believe is relevant in the inference task at hand. Consider, for example, the information from Table 1, provided by Willard. We parse it to extract the relevant information represented as EVD-001-Willard in Table 5. Similarly, Ralph’s testimony from Table 4 provides us with
several dots or items of evidence that are relevant to solving the hypothesis assessment problems from the middle of Figure 14. These items of evidence are represented in Table 5.

Table 5. Dots or items of evidence obtained from Willard and Ralph.

<table>
<thead>
<tr>
<th>Evidence ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVD-001-Willard</td>
<td>Willard’s report in the <em>Washington Post</em> that a canister containing cesium-137 was missing from the XYZ warehouse in Baltimore, MD.</td>
</tr>
<tr>
<td>EVD-002-Ralph</td>
<td>Ralph’s testimony that the cesium-137 canister is registered as being in the XYZ warehouse.</td>
</tr>
<tr>
<td>EVD-003-Ralph</td>
<td>Ralph’s testimony that no one at the XYZ Company had checked the cesium-137 canister out.</td>
</tr>
<tr>
<td>EVD-004-Ralph</td>
<td>Ralph’s testimony that the canister is not located anywhere in the hazardous materials locker.</td>
</tr>
<tr>
<td>EVD-005-Ralph</td>
<td>Ralph’s testimony that the lock on the hazardous materials locker appears to have been forced.</td>
</tr>
</tbody>
</table>

Figure 15 shows the association of the evidence from Table 5 with the hypothesis assessment problems to which they are relevant.
2.4 Problem Reduction and Solution Synthesis

Having identified evidence relevant to the sub-problems in Figure 15, the next step is using it in order to determine the solutions of these problems. Let us assume that based on this evidence, you conclude that these problems have the solutions from the middle of Figure 16.

![Figure 16. Problem reduction and solution synthesis.](image)

In these solutions, “almost certain” and “likely” are names for probability intervals, as indicated in Figure 17. They are similar to the names used in the U.S. National Intelligence Council’s standard estimative language.

![Figure 17. Symbolic probabilities and their corresponding probability intervals.](image)

As shown in Figure 17, indicating that a hypothesis is “likely” is equivalent to saying that its probability of being true is between 0.55 and 0.75. Thus you believe that, based on Ralph’s report that

EVD-002-Ralph: Ralph’s testimony that the cesium-137 canister was in the XYZ warehouse before being reported as missing.

EVD-001-Willard: Willard’s report about the missing of the cesium-137 canister.

EVD-004-Ralph: Ralph’s testimony that the canister is not located anywhere in the hazardous materials locker.

EVD-003-Ralph: Ralph’s testimony that no one at the XYZ Company had checked out the cesium-137 canister.
no one at the XYZ Company had checked out the cesium-137 canister (i.e., EVD-003-Ralph), the likelihood that the cesium-137 canister was not moved to another location is between 0.55 and 0.75. Of course, the actual symbolic probabilities and the associated intervals from Figure 17 are just examples. You may decide that you want to use other names for symbolic probabilities, as well as other associated intervals, as discussed by Kent (1994) and Weiss (2008).

Figure 16 represents a simple example of problem reduction and solution synthesis. The top level problem from Figure 16 was decomposed or reduced to three simpler problems. Solutions of these simpler problems have been found (see middle of Figure 16), and these solutions have been combined into the solution of the top problem. It is this type of reasoning paradigm that is used by TIACRITIS to solve hypothesis analysis problems, as will be discussed in more details in the next section.

2.5 Divide and Conquer through Problem Reduction and Solution Synthesis

TIACRITIS assesses hypotheses by employing the general problem reduction / solution synthesis reasoning paradigm introduced in the previous section. This general divide-and-conquer approach to problem solving has a grounding in the problem reduction representations developed in Artificial Intelligence (Nilsson, 1971; Tecuci, 1988; Tecuci, 1998), and in the argument construction methods provided by the noted jurist John H. Wigmore (1937), the philosopher of science Stephen Toulmin (1963), and the evidence professor David Schum (1987; 2001).

Consider the problem “Assess hypothesis H₁” from the top of Figure 18. We want to solve it by employing various strategies that reduce it to simpler problems.

We ask the question: Which is a relevant item of evidence?

If E₁ is such an item of evidence, then we reduce the top level assessment to two simpler assessments: “Assess H₁ assuming that E₁ is believable” and “Assess the believability of E₁.”

![Figure 18. Reduction of a hypothesis analysis problem to simpler problems](image)
If E₂ is another relevant item of evidence, then we reduce the top level assessment to two other simpler assessments: “Assess H₁ assuming that E₂ is believable” and “Assess the believability of E₂.”

Now let us assume that we have obtained the solutions of the leaf problems, as shown at the bottom of Figure 18:

“Assuming that E₁ is believable, H₁ is very likely” and “The believability of E₁ is likely.”

“Assuming that E₁ is believable, H₁ is certain” and “The believability of E₁ is almost certain.”

We now need to combine all these solutions to obtain the solution of the top level problem, as illustrated in Figure 19. First we need to combine the conditional relevance of E₁ (very likely) with its believability (likely) to obtain the inferential force of E₁ on H₁, which is the solution associated with the question/answer pair “Which is a relevant item of evidence? E₁.” We may use various combination functions (e.g., min, max, average, weighted sum) but in the case of these problems it makes sense to use min since only evidence that is both relevant and believable will convince us that a hypothesis is true. We thus obtain “Based on E₁, hypothesis H₁ is likely.” Similarly we obtain the inferential force of E₂ on H₁, “Based on E₂, hypothesis H₁ is almost certain.” This is the solution associated with the question/answer pair “Which is a relevant item of evidence? E₂.”

Next we have to combine the solutions associated with these two question/answer pairs to obtain the inferential force of both items of evidence on H₁, which is the evidence-based assessment of H₁. While various combination functions may again be used, in this case it makes sense to use max. Thus the obtained solution is: “Based on all the available evidence, hypothesis H₁ is almost certain.”

![Figure 19. Wigmorean inference network for hypothesis analysis.](image)

The tree in Figure 20 is a generalization of the tree in Figure 19, where there are two strategies to solve Problem 1. One strategy is to solve Problem 2 and Problem 3, if the answer to the Question 1 is Answer a. The other strategy is to solve Problem 4 and Problem 5, if the answer to the Question 2 is Answer b.
We again need to obtain the solutions of these subproblems and combine them, from bottom-up, to obtain the solution of Problem 1. We combine “Solution of Problem 2” with “Solution of Problem 3” to obtain “Solution a of Problem 1.” Similarly, we obtain “Solution b of Problem 1” by combining “Solution of Problem 4” with “Solution of Problem 5.” Finally, we combine “Solution a of Problem 1” with “Solution b of Problem 1” to obtain “Solution of Problem.”

This type of problem reduction and solution synthesis logic is used in all the problems solved with TIACRITIS. To summarize it:

1) We solve a complex hypothesis analysis problem by successively reducing it to simpler and simpler problems, guided by questions and answers, down to the level of elementary problems.

2) We assess the solutions of the elementary problems.

3) We combine these solutions, from bottom-up, by selecting a combination function for each node in the reasoning tree (both the question/answer nodes and the problem nodes).
2.6 Case Study: Analyzing Hypotheses through Problem Reduction and Solution Synthesis

2.6.1 Objective

This case study has two complementary objectives:

- Learning how to browse an analysis tree.
- Better understanding the process of hypothesis analysis through problem reduction and solution synthesis.

2.6.2 Summary

This case study concerns the analysis of the problem “Assess whether the cesium-137 canister is missing from XYZ warehouse” which is part of the analysis example discussed in Section 1.2. You will select this hypothesis and then you will browse its analysis tree to see how it is decomposed into simpler hypotheses and how the solutions of these simpler hypotheses are composed. You will visualize both detailed descriptions of these decomposition and synthesis operations, as well as abstract ones, including an abstract view of the entire tree. You will visualize the descriptions of the concepts and instances that are referred in the analysis tree. Proceed as indicated in the following instructions.

2.6.3 Instructions

1. Start this case study in TIACRITIS and select the Hypothesis menu on the top of the window. This will display the hypothesis selection module and the interface in Figure 21. It contains one or several hypotheses to select from.

![Figure 21. Hypothesis selection.](image-url)
2. Select the hypothesis analysis problem: “Assess whether the cesium-137 canister is missing from XYZ warehouse.” Notice that the bottom pane provides guidance on how to perform the case study. This guidance will no longer be shown in the following figures used to describe the case study.

Once a hypothesis is selected, the Reasoner is automatically invoked to analyze the hypothesis, as shown in the top part of Figure 22. The right panel shows the decomposition of the top level problem into three simpler problems, including the corresponding question/answer pair that determined it. Notice the solutions of the three sub-problems. How these solutions have been obtained will be discussed below. Here just notice that these solutions are combined, from bottom-up, to obtain the solution associated with the question/answer pair (very likely), and then the solution of the top level problem (very likely). The solution associated with the question/answer pair is computed with a weighted sum function (with a weight of high for the left sub-problem, very high for the middle one, and medium for the right one). This solution is then transmitted upward, as the solution of the top-level problem (since the maximum of a single value is the value itself).

The left panel shows an abstraction of this problem reduction and solution synthesis step where the problems were abstracted to shorter sentences.

![Figure 22. Problem reduction and solutions synthesis.](image)
3. Right-click on the top problem in the left panel and select **Expand**. As a result, the left panel shows the entire abstract reasoning tree (see Figure 23).

The solutions with yellow background are assessments made by the analyst (as discussed in Case Study 3.4).

Notice how the solutions of the leaf problems are automatically combined, from bottom-up, into the solutions of the upper-level problems.

![Abstract reasoning tree](image)

**Figure 23. Abstract reasoning tree.**

6. Under **cesium-137 canister is not in XYZ warehouse: very likely,** click on “favoring evidence: very likely.” The right panel shows the details of the corresponding reasoning step (see Figure 24).

The phrases in dark blue, such as **EVD-001-Willard,** represent specific objects from the application domain. The phrases in lighter blue, such as **evidence,** represent concepts.
7. Click on the word “evidence” from the description of the top problem in the right panel. The Description module is automatically invoked to display the description of this concept (if it exists in the knowledge base of TIACRITIS), as shown in Figure 25.

Clicking on Show All in the upper left side will result in displaying all the elements with descriptions in the left panel. Clicking on one of them will display the corresponding description.

9. Click on the Reasoner menu to continue the browsing of the hypothesis analysis tree.

10. Click on other abstract problems in the left panel and see the details in the right panel.

11. Select Case Study.

12. Click on [SAVE & FINISH] to end the case study.
Evidence

Here is a term that resists easy definition. If you look up this term in the Oxford English Dictionary you will be led in a circle and are eventually brought back to the word evidence. One major trouble is that, in terms of its substance or content, evidence has a near infinite variety. We know of three disciplines in which persons drawing conclusions must be prepared to evaluate evidence of nearly every conceivable substance or content. The disciplines are: intelligence analysis, law, and history [it is possible that we have overlooked some others]. But we can recognize quite a small number of recurrent and distinguishable forms of evidence regardless of its substance or content. We will mention these various forms of evidence as we proceed.

There are some very interesting problems associated with the term evidence in intelligence analysis. Some persons in intelligence analysis and elsewhere believe that the term evidence only applies in the field of law and refers to whatever is produced at trial by the parties in contention. Evidence scholars in the field of law have noticed this themselves and have scoffed at the idea that evidence is only encountered in law. They agree that evidence is encountered in any context in which conclusions are being reached. Many analysts prefer the use of the terms data or items of information instead of the term evidence, but this can be very misleading. Any datum or item of information only becomes evidence when its relevance to hypotheses being considered can be established by a defensible argument. For example, your car license plate number is a datum on record by your state’s department of motor vehicles. But you would have a very difficult time showing how this datum is relevant to any hypothesis you are considering concerning events in Iraq. Here we have a datum or item of information that will never become evidence in this inference concerning Iraq. Someone would say, "Your car license number is totally irrelevant to our present inferences". What is true of course is that a datum or item of information may be totally irrelevant in one context but relevant in another. If you were suspected of committing a crime, your car license number might be quite relevant.

On occasion the term fact is used instead of the term evidence; this can also be very misleading. We often hear someone say, "I want the facts before I draw any conclusion". The problem is: What fact is this person talking about? What we must do is to distinguish between evidence for an event and the event itself. We obtain evidence of some sort and can regard this evidence as factual since we are observing it with one of our own senses. But what the evidence tells us we will have some uncertainty about; we cannot always regard what the evidence says as being factual. For example, we all hear Mary telling us that it was John who ran into her car last night. We regard Mary’s report as a fact since we all just heard what she said. But whether John was the person who ran into Mary’s car last night we cannot regard as factual without assaying Mary’s credibility. Perhaps she was mistaken or being untruthful. In most cases in intelligence analysis we will have some uncertainty about what is reported in the evidence that was obtained.

There are five basic kinds of evidence (Schum, 2001) and we have listed four of them: tangible evidence, two kinds of testimonial evidence, and authoritative record [also called accepted facts]. But we can also say that missing evidence can be evidence itself when we explore various reasons why we cannot obtain evidence we expect to obtain. In some cases there may be innocent explanations for our failure to find evidence; we are looking in the wrong places; the evidence never existed, or it was lost or destroyed. But another possibility is not so innocent; someone or some group is keeping the evidence from us. This would entitle us to infer that the person or group denying us access to this evidence was engaged in denial or deception efforts against us.

Story 1

Here is an analyst who reads in the Washington Post about some cesium-137 that has gone missing from a company in Baltimore, MD. This company makes devices for sterilizing medical equipment of various sorts and uses radioactive materials such as cesium-137. The analyst also knows that cesium-137 could also be an ingredient in a...
3 EVIDENCE

3.1 What Is Evidence?

You might think that a section with this title is silly or unnecessary since everyone knows what evidence is. However, matters are not quite that simple since the term evidence is not so easy to define and its use often arouses controversy, especially in the field of intelligence analysis. One problem with definition of evidence is that several other terms are often used synonymously with it when, in fact, there are distinctions to be made among these terms that are not always apparent. Quite unnecessary controversy occurs since some believe that the term evidence only arises and has meaning in the field of law. It will benefit us to discuss these matters early on, since evidence is the foundation of all intelligence analyses.

We are actually not assisted very much in defining evidence by consulting a dictionary. For example, look at the *Oxford English Dictionary* (OED) under the term evidence and you will be led in a circle; evidence is ultimately defined as being evidence.

A variety of terms are so often used as synonyms for the term evidence: data, items of information, facts, and knowledge. When examined carefully, there are some valid and important distinctions to be made among these terms. First, consider the terms data and items of information. There are untold trillions of data or items of information in existence that will almost certainly never become evidence in any intelligence analysis or in most other inferences either. Here’s a datum or item of information for you: Professor Schum has a long and steep driveway in front of his house that makes shoveling snow off of it very difficult in the winter. Can you think of any intelligence analysis problem in which this datum could become evidence? About the only matter in which this datum could become interesting evidence involves the question: Why did Schum and his wife, Anne, ever purchase this house in the first place? As we will discuss, data or items of information only become evidence when their relevance is established regarding some matter to be proved or disproved.

Now consider the term fact; there are some real troubles here as far as its relation to the term evidence is concerned. How many times have you heard someone say, “I want all the facts before I draw a conclusion or make a decision?” Or, “I want to know the facts in this matter?” The first question is easily answered; we will never have all the facts in any matter of inferential interest. Answers to the second question require a bit of careful thought. Here is an example of what is involved: Suppose we are case officers interviewing a HUMINT asset or informant having the code name “Mouse.” Mouse tells us that a person of interest, Amad M., attended an al Qaeda weapons training class near Madyan in Northwest Pakistan in October, 2009. Now we regard it as fact that Mouse gave us this information; we all just heard him give it to us. But, whether Amad M., actually did attend an al Qaeda weapons training class near Madyan in Northwest Pakistan in October, 2009, is only an inference and is not a fact. This is precisely why, in Section 2, we carefully distinguished between an event and evidence for this event.
Here is what we have:

Mouse has given us evidence $E^*$, saying that event $E$ occurred, where $E$ is the event that Amad M., attended an al Qaeda weapons training class near Madyan in Northwest Pakistan in October, 2009.

Whether this event $E$ did occur or not is open to question and depends on Mouse’s competence and credibility.

If we take it as fact that event $E$ did occur, just because Mouse said it did, we would be overlooking the credibility foundation for any inference we might make from his report $E^*$. Unfortunately, it so often happens that people regard the events reported in evidence as being facts when they are not. Doing this suppresses all uncertainties we may have about the source’s credibility and competence if the evidence is testimonial in nature. We have exactly the same concerns about the credibility of tangible evidence. For example, we have been given a tangible object or an image as evidence $E^*$ that we believe reveals the occurrence of event $E$. But we must consider whether this object or image is authentic and it is what we believe it to be. In any case, the events recorded in evidence can only be regarded as facts if provided by perfectly credible sources, something we never have.

The term knowledge is as perplexing as it is interesting, particularly when we try to relate it to evidence from our sources, whatever they are. As you know, the field of epistemology is the study of knowledge and what we believe it may be. We have heard intelligence analysis described as being “applied epistemology.” Here is an example of why this makes a great deal of sense. Two questions we would normally ask regarding what our source Mouse just told us are as follows:

- Does Mouse really know what he just told us regarding Amad M., attending an al Qaeda weapons training class near Madyan in Northwest Pakistan in October, 2009?
- Do we ourselves then also know, based on Mouse’s report, that Amad M., actually attended this al Qaeda weapons training class near Madyan in Northwest Pakistan in October, 2009?

Let’s consider the first question regarding our source Mouse. For over two millennia, some very learned people have troubled over the question: What do we mean when we say that person \( A \) knows that event $B$ occurred? To apply this question to our source Mouse, let’s make an assumption that will simplify our answering this question. Let’s assume that Mouse is a competent observer in this matter. Suppose we have evidence that Mouse was actually himself at the al Qaeda weapons training center near Madyan in Northwest Pakistan in October, 2009; and suppose Mouse knows Amad M. by sight. What we can then focus on is Mouse’s credibility.

Here is what a standard or conventional account says about whether Mouse knows that Amad M. was at the al Qaeda weapons training center near Madyan in Northwest Pakistan in October, 2009:

- Amad M. was in fact at the al Qaeda weapons training center near Madyan in Northwest Pakistan in October, 2009.
- Mouse got nondefective evidence that Amad M. was at the al Qaeda weapons training center near Madyan in Northwest Pakistan in October, 2009.
• Mouse believed this evidence.

If all of these three things are true, we can state on this standard analysis that Mouse knows that Amad M. was at the al Qaeda weapons training center near Madyan in Northwest Pakistan in October, 2009.

But now we have several matters to consider in answering the second question: Do we ourselves also know, based on Mouse’s report, that Amad M. actually attended this al Qaeda weapons training class near Madyan in Northwest Pakistan in October, 2009? The first and most obvious fact is that we do not know the extent to which any of the three events just described in the standard analysis are true. Starting at the bottom, we do not know for sure that Mouse believes what he just told us about Ahmad M. being at the al Qaeda training center. This is a matter of Mouse’s veracity or truthfulness. We would not say that Mouse is being truthful if he told us something he did not believe.

Second, we do not know what sensory evidence Mouse obtained, on which to base his belief, and whether he based his belief at all on this evidence. Mouse might have believed that Ahmad M. was at the al Qaeda weapons training center either because he expected or desired Ahmad M. to be there. This involves Mouse’s objectivity as an observer. We would not say that Mouse was objective in this observation if he did not base his belief on the sensory evidence he obtained in his observation.

Finally, even if we believe that Mouse was an objective observer who based his belief about Ahmad M. on sensory evidence, we do not know how good this evidence was. Here we are obliged to consider Mouse’s sensory sensitivities or accuracy in the conditions under which Mouse made his observations. Here we consider such obvious things as Mouse’s visual acuity. But there are many other considerations such as, “Did Mouse only get a fleeting look at the person he identified as Ahmad M.?”, “Did he make this observation during a sand storm?”, and “What time of day did he make this observation?” For a variety of such reasons, Mouse might simply have been mistaken in his observation; it was not Ahmad M. who Mouse observed.

So, what it comes down to is that the extent of our knowledge about whether Ahmad M. was at the al Qaeda weapons training center, based on Mouse’s evidence, depends on these three attributes of Mouse’s credibility. We will have much more to say about assessing the credibility of sources of evidence, and how TIACRITIS can assist you in this difficult process, in Section 7 of this book. But there is yet another matter concerning the relation between evidence and knowledge; this matter arises when we consider various hypotheses we may entertain concerning which of Mouse’s evidence might be relevant. As far as the linkage between Mouse’s evidence and these hypotheses, the extent of our knowledge about the relative likeliness of these hypotheses depends on the defensibility and strength of our relevance arguments and these credibility considerations. The whole point here is that the relation between evidence and knowledge is not a simple one at all.

Finally, we must consider the controversy over the use of the term evidence instead of the other terms we just examined. We have read several accounts by intelligence officials saying that intelligence analysis does not involve evidence since intelligence services are not courts of law. The idea expressed here is that evidence only concerns objects, testimony, or other items introduced in a court trial.
same argument often occurs in other areas in addition to intelligence analysis. But this controversy and confusion has been recognized by eminent evidence scholars in the field of law. For example, in his marvelous book Evidence, Proof, and Facts: A Book of Sources, Professor Peter Murphy (2003, p.1) notes the curious fact that the term evidence is so commonly associated only with the field of law.

*The word ‘evidence’ is associated more often with lawyers and judicial trials than with any other cross-section of society or form of activity. ... In its simplest sense, evidence may be defined as any factual datum which in some manner assists in drawing conclusions, either favorable or unfavorable, to some hypothesis whose proof or refutation is being attempted.*

He notes that this term is appropriate in any field in which conclusions are reached from any relevant datum. Thus, physicians, scientists of any ilk, historians, and persons of any other conceivable discipline, as well as ordinary persons, use evidence every day in order to draw conclusions about matters of interest to them.

We believe there is a very good reason why many persons are so often tempted to associate evidence only with the field of law. It happens that our Anglo-American system of laws has provided us with by far the richest legacy of experience and scholarship on evidence of any field known to us. This legacy has arisen as a result of the development of our adversarial system for settling disputes and the gradual emergence of our jury system whose members deliberate on evidence provided by external witnesses. This legacy has now been accumulating over at least the past six hundred years. Some of us have tried repeatedly to make persons in a variety of disciplines, including intelligence analysis, aware of this rich legacy, but we have not always been successful. In Section 7 we provide an account of how many recurrent and generic forms and combinations of evidence there are. Development of this account was initially stimulated by the rich legacy concerning evidence that our system of laws has provided.

The TIACRITIS system already knows about many of the distinctions we have just discussed. You will have practice in entering various kinds of evidence and observe that TIACRITIS will be able to ask you necessary questions about this evidence.

### 3.2 The Credentials of All Evidence

As we have noted on several occasions in the preceding sections of our work, evidence has three major properties or credentials: relevance, believability, and inferential force or weight. It is useful to make sure we understand what these credentials mean. To introduce discussion of these matters, let’s return briefly to the dialogue in Section 2.1 that you had with your spouse concerning your rather casual holistic assessment of the suitability of candidates in a forthcoming election. You said you believed that candidate $X$ was the most suitable candidate. Your spouse first asked you a natural question regarding what evidence you considered in arriving at this judgment. You mentioned several items, whereupon your spouse challenged the relevance and believability of some of the evidence items you mentioned. Then, your spouse asked you a question regarding which evidence items were the strongest in supporting your judgment regarding candidate $X$. In this example, for various reasons associated with holistic judgments, you did not give very satisfactory answers to these very appropriate questions raised
by your spouse. But these are exactly the kinds of questions that would or should be asked of the evidential basis for any conclusions reached in an intelligence analysis. Let’s now make sure that we understand what these three evidence credentials mean and why they are so important.

3.2.1 Relevance

We know of no better definition of the term relevance, applied to evidence, than the one provided in our Federal Rules of Evidence for United States Courts (Mueller et al., 1988). These Federal Rules of Evidence (FREs) govern the offering and admissibility of evidence introduced in our courts, and they are the result of centuries of experience in our Anglo-American system of common law. But these rules are not set in stone and can be revised in light of new experience and insight. One of these numbered rules, FRE-401, defines relevant evidence; here is what FRE-401 says (Federal Rules of Evidence, 2009-2010 Edition):

“Relevant evidence” means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

We need to parse this definition in order to see what it says and how it applies to intelligence analysis. First, consider the words “any tendency.” What this allows for is evidence being relevant in more than one way. As we will see in Section 4, we can make a distinction between directly relevant evidence and indirectly relevant evidence. Indirectly relevant evidence is often called ancillary, auxiliary, or meta-evidence, since it is evidence about other evidence. For example, in an inference about whether to believe what some HUMINT source tells us, we make use of whatever ancillary evidence we have about the competence and credibility of this source.

Now consider the phrase “any fact that is of consequence to the determination of the action.” This basically refers to the matters to be proved or disproved; i.e. it refers to the hypotheses being considered. In law, the hypotheses will involve some charge in a criminal case or a complaint lodged in a civil case. For example, in a murder case the determination of the action would involve such hypotheses as: “The defendant being charged was the one who unlawfully killed the victim.” In intelligence analysis one hypothesis that might be considered is: “At least one terrorist action will be initiated against homeland USA in the next year.” In both the law and intelligence examples just mentioned, these would be major or upper-level hypotheses. But in constructing arguments bearing on these major hypotheses, there will be any number of lower-level hypotheses involving the sources of doubt we recognize in our arguments. Thus, evidence is relevant if it bears either directly or indirectly on any of our recognized sources of doubt.

Now consider the phrase “more probable or less probable than it would be without the evidence.” What this says is that relevant evidence causes us to change our beliefs, one way or the other, about some hypothesis being tested. But notice that it does not tell us how much we should change our beliefs in these hypotheses. Another way of stating this is to say that relevant evidence has some inferential force or weight, but it does not say how much force or weight it should have. One very good reason why FRE-401 does not say how much force or weight evidence should have is that assessing the force or
weight of evidence is a very complex matter involving the probabilistic strength of our arguments based on evidence that concern both relevance and believability matters. In law and in intelligence analysis, reasonable people may disagree strongly about how forceful a given item of evidence, or some collection of evidence, is on hypotheses of interest.

Defending the relevance of evidence is no easy task especially when we have masses of it to consider, as we do in intelligence analysis. There is a problem associated with what we termed evidential synergism that we discussed in Section 1.1.2. Suppose we have an item of information about event A that, by itself, seems irrelevant or useless as far as an analysis problem we are currently facing and we contemplate discarding it. But someone notices that we also have other items about events B and C that would make item A seem relevant when we take all these three items together. The point here is that the relevance of an item of information often depends on what other items of information we have. Another way of stating this is to say that items of information interact or are dependent in ways that influence their relevance on hypotheses being considered. As we also emphasized, the detection of these interactions producing evidential synergisms depends on how devoted we are to sharing information across agencies and offices in our intelligence services.

3.2.2 Believability

Here is an item of evidence $E^*_{i}$, from source $I$, that all of us believe is relevant on hypotheses we are considering. We strongly believe that we can defend the relevance of event $E$, as reported in our evidence $E^*_{i}$, by the argument we have constructed that we all agree is very strong and free of disconnects or non sequiturs. But the crucial question remains: How certain are we that event $E$ did occur just because source $I$ said it did? Source $I$'s credibility, and perhaps competence, is the major issue here. This is why we have said that source believability considerations form the very foundation for all arguments we make from evidence to our hypotheses. We illustrated this fact in Figure 3 in Section 1.1.3. However strong our relevance argument may be, if it rests on a weak believability foundation, it will falter. Perhaps the best example of inferential calamities known to us in the open-source literature concerns the believability (i.e. competence and credibility) of the human source called “Curveball” (Bruce, 2008).

The Federal Rules of Evidence contain many rules associated with testing the believability of witnesses and the authenticity, reliability, and accuracy of tangible evidence. But there are no rules concerning how we ought to grade believability and how strong it should be. As far as witness credibility is concerned, we have consulted over a hundred works on evidence in law that contain most valuable accumulated strategies for supporting or undermining human testimonial credibility (i.e. HUMINT credibility), and the credibility of various forms of tangible evidence These strategies have been accumulated over six hundred years of experience in our courts and concern the veracity, objectivity, and observational sensitivity of witnesses. We also have accounts of strategies for testing the competence of human witnesses. These accounts of credibility and competence matters allow us to generate experience-tested questions to ask about the competence and credibility of HUMINT sources and of the credibility-related attributes of tangible evidence from a variety of sources. These questions
are discussed in Section 5. We add here that the TIACRITIS system knows what questions you should try to answer regarding the believability of all forms of evidence.

In the TIACRITIS system we have made use of another system we have spent years in developing for the CIA and other intelligence services. This system is called MACE (Method for Assessing the Credibility of Evidence). We have recently described MACE in a paper and mentioned how it rests on over six hundred years of experience in the task of assessing the competence and credibility of HUMINT sources (Schum and Morris, 2007). In addition, the version of MACE we will mention in connection with TIACRITIS makes use of a particular probabilistic system of great use in determining the extent to which we can believe what a source of HUMINT tells us.

There is another very important believability-related matter to be mentioned. It is true that a major origin of our uncertainty or doubt in an intelligence analysis concerns the believability of our sources of evidence, whatever these sources might be. But there are other origins of doubt we are obliged to consider that are not always noticed and incorporated in our assessments of evidence believability. The truth is that lots of things might be done to an item of incoming intelligence information between the time it is first received, and the time it reaches the desk or the computer of intelligence analysts. Any number of persons or devices may have had access to this information item and may have done various things to it. One result is that the intelligence analyst may not have received either an authentic or a complete account of the actual information received from the source.

In law this fact is recognized and so there are elaborate procedures for dealing with what are called chains of custody. Well-qualified persons are designated as evidence custodians who make careful records of every person who had access to an evidence item from the time it was received, what they did with this item, how long they held the item, and who next received the item before it was finally introduced at trial. Although we are not privy to the procedures for dealing with chains of custody of information received in intelligence analysis, and whether there are any persons who act as evidence custodians, we have recently written a paper for intelligence agencies on such matters that also illustrates how a forerunner of the TIACRITIS system can assist analysts to capture doubts associated with chains of custody of intelligence information (Schum et al., 2009a). A detailed discussion of the analysis of the chains of custody is included in Section 5.9.

A final matter here concerns some terms and definitions that have been associated with evidence believability-related matters. So often we hear of persons being described as reliable sources. There is a difficulty associated with using this term with reference to human sources such as for HUMINT. The trouble is that the term reliability is most often used to indicate how consistent or repeatable some process is. You say your car is reliable to the extent to which it will take you where you wish to go for some period of time in the future. A test of any kind is reliable to the extent that it gives the same result over again if it is repeated. But there is so much more to the believability of a human source than mere consistency; we have discussed how attributes of the credibility of sources of HUMINT concern their veracity, objectivity, and observational sensitivity. We are also concerned about the competence of these persons. What counts most is the believability of what these sources tell us. Such judgments rest on all the credibility and competence attributes we have mentioned. The term reliability does not
capture any of these attributes. Where we use the term reliability is with reference only to our sources of tangible evidence such as sensors of various kinds. In our work, we will use the term believability with reference to our sources since, at least with reference to HUMINT sources and other persons involved in the chains of custody we just mentioned, in addition to credibility we have to also be concerned about their competence. What matters in all cases is whether an analyst can believe the information he has received.

### 3.2.3 Force or Weight of Evidence

In a very general sense, the force or weight of evidence indicates how strong the evidence is in favoring or disfavoring hypotheses we are considering. But this is as far as we can go, since there is considerable controversy about what the terms force and weight mean, and especially how these concepts should be assessed and combined. As we noted in Section 1.1.5, Problem 5, there are only two uncontroversial statements we can make about the force or weight of evidence. First, it has vector-like properties indicating the direction and the strength with which evidence favors hypotheses we are considering. Second, the force or weight of evidence is always graded in probabilistic terms. This second statement is actually the greatest source of controversy since a variety of careful scholars in probability, who have given their days and nights to the study of evidence and probability, cannot agree about how force or weight of evidence should be assessed and combined.

Probabilistic judgments can be expressed numerically in several ways, and also in terms of words, as discussed in Section 2.4. Speaking of numerical judgments of probability, a very wise and devoted scholar, Professor Glenn Shafer, has correctly noted that probability is more about arguments than it is about numbers (Shafer, 1976). We add the same concern about verbal assessments of probability, such as “very probable,” “probable,” “unlikely,” and so on. As we have emphasized, the force of evidence depends on the strength of our believability and relevance arguments. If these arguments are not defensible, no one will take seriously any numerical or verbal assessments we make concerning the force or weight of our evidence. This is just one reason why we consider the construction and defense of our relevance andbelievability arguments so carefully in Sections 4 and 5 to follow.

So, we have found it much easier to provide definitions and meaning to the relevance and believability credentials of evidence than we have been able to do so for the force or weight credential. But as we proceed, will provide an assortment of examples about assessing the force or weight of evidence that arise and can be useful in intelligence analysis. Remember that all conclusions in intelligence analysis, in common with all other contexts in which conclusions are based on evidence, must always be hedged probabilistically by some means. As we will again discuss in Section 8, our evidence is always incomplete, usually inconclusive, frequently ambiguous, commonly dissonant, and comes to us from sources having any gradation of believability shy of perfection. As we will observe, alternative views of probabilistic reasoning capture some of these important considerations, but no single view captures them all.
3.3 Arguments Linking Evidence to Hypothesis

To assess a hypothesis, one would need to develop an argument that links the evidence to the hypothesis by establishing the relevance, the believability and the inferential force of evidence. This is illustrated in Figure 26, where the assessment of hypothesis \( H_k \) (problem [P1]) is reduced to the assessment of two simpler hypotheses, \( H_d \) and \( H_e \) (problems [P2] and [P3], respectively). Each of these hypotheses is assessed by considering both favoring evidence and disfavoring evidence (e.g., problems [P5] and [P6]). Let us assume that there are two items of favoring evidence for \( H_d \): \( E_1 \) and \( E_2 \). For each of them (e.g., \( E_1 \)) the agent assesses the extent to which it favors the hypothesis \( H_d \) (i.e., \( [P6] \)). This requires assessing both the relevance of \( E_1 \) to \( H_d \) (problem [P8]) and the believability of \( E_1 \) (problem [P9]).

Relevance answers the question: So what? How does this datum or item of information, whatever it is, bear on what an analyst is trying to prove or disprove?

Believability answers the question: Can we believe what this item of intelligence information is telling us?
Let us assume that TIACRITIS has obtained the following solutions for relevance and believability:

"If we believe E₁, then H_d is almost certain." [S8]
"It is likely that E₁ is true." [S9]

By compositing the relevance and the believability of the evidence E₁ (i.e. solutions [S8] and [S9]), for example through a “min” function, the agent assesses the inferential force or weight of E₁ on H_d:

"Based on E₁, it is likely that H_d is true." [S6]

As illustrated above, the inferential force or weight answers the question: How strong is this item or body of relevant evidence in favoring or disfavoring various alternative hypotheses or possible conclusions being entertained?

Similarly, the agent assesses the inferential force or weight of E₂ on H_d:

"Based on E₂, it is almost certain that H_d is true." [S7]

By composing the solutions [S6] and [S7] (e.g., through a “max” function) the agent assesses the inferential force/weight of the favoring evidence (i.e., E₁ and E₂) on H_d:

"Based on the favoring evidence, it is almost certain that H_d is true. " [S4]

Through a similar process TIACRITIS assesses the disfavoring evidence for H_d:

"Based on the disfavoring evidence it is unlikely that H_d is false." [S5]

Because there is very strong evidence favoring H_d and there is weak evidence disfavoring H_d, TIACRITIS concludes:

"It is almost certain that H_d is true." [S2]

The sub-hypothesis H_e is assessed through a similar process:

"It is an even chance that H_e is true." [S3]

The solutions of H_d and H_e are composed (e.g., through an “average” function) into the evidence-based assessment of H_k:

"It is likely that H_k is true." [S1]
3.4 Case Study: Making Assessments and Assumptions in Arguments

3.4.1 Objective

This case study has two complementary objectives:

- Learning how to make assessments and assumptions in arguments.
- Better understanding the structure of the arguments that link evidence to hypotheses by establishing the relevance, the believability, and the inferential force of evidence.

3.4.2 Summary

The case study uses again the analysis problem “Assess whether the cesium-137 canister is missing from XYZ warehouse” which is part of the analysis example introduced in Section 1.2. This time, however, the analysis is refined to include the assessment of the relevance and the believability of evidence which will be performed by specifying them as assumptions.

You will select this hypothesis and then you will browse its analysis tree to see how it is reduced to assessing the relevance and the believability of the available evidence. After that you will assess these credentials for various item of evidence and see how the inferential force of evidence is automatically determined, at various levels.

Proceed as indicated in the following instructions.

3.4.3 Instructions

1. Start the case study in TIACRITIS.

2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains one or several hypotheses to select from.

3. Select the hypothesis analysis problem: “Assess whether the cesium-137 canister is missing from XYZ warehouse.” Once this hypothesis is selected the Reasoner is automatically invoked to analyze the hypothesis, as shown in Figure 27.
4. Right-click on the top problem in the left panel and select **Expand**. The left panel will show the entire abstract analysis tree.

5. Under “**EVD-002-Ralph: no solution**,” click on “relevance: no solution.” The right panel will show the detailed description of this problem which currently has no solution (see Figure 28). You will read the description of **EVD-002-Ralph**, assess its relevance, and define it as an assumption.

6. In the right panel, click on **EVD-002-Ralph**. **Description** is automatically selected and TIACRITIS displays the description of **EVD-002-Ralph**.

7. Select **Reasoner** and notice that “relevance: no solution” is still selected.

8. Select the **Assumption** menu. As a result you will enter the **Assumption** module and the interface from part (a) of Figure 29 will be displayed, showing the current problem. This is the conditional relevance of **EVD-002-Ralph** to the hypothesis that the cesium-137 canister was in the XYZ warehouse before being reported as missing, assuming that **EVD-002-Ralph** is believable. We will assess this relevance and we will define it as an assumption.

9. Click on the **[NEW]** button, and TIACRITIS will display the pattern of the solution, as shown in part (b) of Figure 29. You will make a specific assessment by replacing “…” with a symbolic probability.

10. Click on “…” and TIACRITIS replaces the “…” with the default symbolic probability “**certain**,” as shown in part (c) of Figure 29.
11. Click on "certain" and then double-click on one of the values (e.g., almost certain) from the displayed selection list (see part (d) of Figure 29). The value "certain" is replaced with "almost certain." You may change again the selected value by clicking on it.

12. Click on the space following “Justification” and, in the opened window, write “Ralph is the administrator of the XYZ warehouse.” Then click outside the window. If you select “Ralph” and “XYZ warehouse” from the selection list, they will appear as known instances, in blue.
### Figure 29. Assessing the relevance of an item of evidence.

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Hypothesis</th>
<th>Reasoner</th>
<th>Evidence</th>
<th>Assumption</th>
<th>Description</th>
<th>Test</th>
<th>Sharing</th>
<th>Arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current problem:</strong> Assess to what extent <strong>EVD-002-Ralph</strong> favors the hypothesis that the <strong>cesium-137 canister</strong> was in the <strong>XYZ warehouse</strong> before being reported as missing, assuming that <strong>EVD-002-Ralph</strong> is believable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Assumptions [NEW]:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Defined new assumption [CANCEL]:** Assuming that **EVD-002-Ralph** is believable, it is ... that **cesium-137 canister** was in **XYZ warehouse** before being reported as missing. (Justification: ...) |

| **Defined new assumption [CANCEL]:** Assuming that **EVD-002-Ralph** is believable, it is **certain** that **cesium-137 canister** was in **XYZ warehouse** before being reported as missing. (Justification: ...) [CREATE] |

| **Defined new assumption [CANCEL]:** Assuming that **EVD-002-Ralph** is believable, it is **certain** that **cesium-137 canister** was in **XYZ warehouse** before being reported as missing. (Justification: ...) [CREATE] |

| **Defined new assumption [CANCEL]:** Assuming that **EVD-002-Ralph** is believable, it is **almost certain** that **cesium-137 canister** was in **XYZ warehouse** before being reported as missing. (Justification: **Ralph is the administrator of the XYZ warehouse.**) [MODIFY] [DISABLE] [DELETE] |
13. Click on [CREATE] to associate your assessment as a solution of the problem. After that you will have the options [MODIFY], [DISABLE] (i.e., keeping it in the system so that it can be associated later with the problem), or [DELETE] the assumption, if you so desire (see part (e) of Figure 29).

14. Select the Reasoner menu, and TIACRITIS will display the updated analysis tree, as shown in Figure 30. Notice the yellow background of the solution, indicating that it was defined as an assumption. Notice also its justification.

15. Click on “believability EVD-002-Ralph: no solution.”

16. In the right panel, right-click on “Assess the believability of EVD-002-Ralph” and select New Assumption (see part (a) of Figure 31). As a result, TIACRITIS makes the default assessment (certain), as shown in part (b) Figure 31.

17. Click on “certain” and, in the displayed list, double-click on “very likely,” which is now used as the new assessment.

Notice in part (c) of Figure 31 that TIACRITIS displays the updated analysis tree, assessing as “very likely” the inferential force of EVD-002-Ralph. This inferential force was obtained by combining the “almost certain” relevance of EVD-002-Ralph with its “very likely” believability, through a “min” function. Notice also that TIACRITIS automatically assesses the hypothesis “cesium-137 canister was in XYZ warehouse: very likely,” based on EVD-002-Ralph.
18. Assess the relevance and the believability of the other items of evidence, EVD-001-Willard, EVD-004-Ralph, and EVD-003-Ralph, and define them as assumptions, as illustrated above. Then notice how TIACRITIS uses these solutions to assess the upper level hypotheses.

At any level in the analysis tree you may define the solution of any problem as an assumption. This allows you to drill down in the analysis as much as desired, based both on the available evidence and on the available time. For example, you may make the assumption that “it is almost certain that the cesium-137 canister is not in the XYZ warehouse,” without evaluating the corresponding evidence. When you define an
assumption for a problem for which TIACRITIS has computed a different solution, the system warns you by showing the assumption with a red border.

19. Select **Case Study**.

20. Click on [SAVE & FINISH] to end it.
4 ESTABLISHING THE RELEVANCE OF EVIDENCE BY ARGUMENTS

4.1 Relevance and the Question: So What?

The first basic question asked about a datum or item of information is: “So what? How is this item linked to any hypothesis or possible conclusion of interest in an intelligence analysis?”

Suppose your intelligence analysis involves inferences about possible forms of terrorist actions that could be taken against targets here in the United States. Here are two items of information you have just received:

Item #1: Professor David A. Schum is the owner of a green 2000 Toyota Corolla vehicle carrying Virginia license plate # TSL-782.

The first question you would ask about Item #1 is: “So what? What conceivable bearing does this bit of information have on any possible conclusions I could reach about possible terrorist incidents here in the United States?” Unless David Schum was associated with any terrorist organization, you would be justified in saying that this datum is totally irrelevant in your present analysis. The concept of relevance concerns our attempts to answer “so what” questions regarding items of information we have. Now consider this second datum:

Item #2: The XYZ company in Baltimore, MD, manufactures devices for sterilizing medical equipment. A person named Willard reported in a Washington Post article that a canister containing powder, including approximately 3000 curies of cesium-137, had gone missing from the company’s warehouse in Baltimore. There were indications that the storage area where this powdered cesium-137 was located showed signs of forcible entry.

Asking the same question, “So what?,” an analyst would give a different answer to this second item than the one given to Item #1. Cesium-137 has all sorts of uses in medicine and in industry. It is used to sterilize food, to manufacture thickness and moisture density gauges, and it is used for various diagnostic purposes in medicine in addition to the sterilization purposes just mentioned. Unfortunately, cesium-137 could be put to other uses including the construction of a dirty bomb. Just a few ounces of this powdered material set off by a conventional explosive in a bomb could contaminate an entire city for decades. Indeed, it is known that the Chechen Mujahidin placed a canister of cesium in a Moscow park in the hopes of spreading radiation throughout the city. Fortunately, this canister was discovered by the police before it was set off. So, Item #2 seems relevant in inferences about what kind of actions terrorist groups may be contemplating here in the United States. In the previous sections and case studies we have shown arguments justifying the relevance of this item.

The arguments concerning the relevance of evidence involve chains of reasoning. There are two species of relevance we must consider. The first, called direct relevance, involves evidence that can be directly linked by an argument or chain of reasoning to some hypothesis or possible conclusion being considered. The second, called indirectly relevance, involves evidence that has no direct linkage itself to
hypotheses but concerns the strength or weakness of any link in a chain of reasoning set up by directly relevant evidence. Sometimes this ancillary evidence is quite appropriately termed meta-evidence since it is evidence about other evidence. We will provide an array of examples of both directly and indirectly relevant evidence as we proceed.

Consider an item of directly relevant evidence and the argument or chain of reasoning an analyst has constructed that links this item to hypotheses being considered. Here starts the initial root of uncertainty in intelligence analysis. In forming this chain of reasoning, each identified link in a relevance chain of reasoning involves a proposition that might be true or untrue; i.e., it is a source of doubt or uncertainty. The argument being constructed thus forms a chain of sources of doubt the analyst believes to be interposed between the evidence and what the analyst is trying to prove or disprove from it. These links or sources of doubt are laid out in a logically consistent order in which one link is inferable from its predecessor.

First question: Where do these links (sources of doubt) come from?

Answer: They come from the analyst’s imagination based upon his/her experience and knowledge of the analytic problem area.

Here we have the roots of disagreements among analysts concerning the relevance of evidence and disagreements about uncertainties in conclusions that may be reached. Different analysts may construct different arguments from the same evidence and thus perceive different sources of uncertainty. Even if they agree about the links in an argument, they may disagree about how strong they are. It is also true, of course, that analysts may generate different possible hypotheses from the same evidence.

Notice, however, that an agent like TIA CRITIS (such as Disciple-LTA) can learn from the relevance arguments initially defined by the analyst. It can then use this knowledge to help the analyst in the generation of arguments that bear some similarities with previous arguments.

A relevance argument having been constructed, it is now time for its evaluation; here is where the necessity for critical reasoning arises. The analyst must ask the following question: Is the chain of reasoning I have just constructed that shows the direct relevance of this evidence item logically coherent? Does it contain any disconnects or non sequiturs?

Here is where the necessity for the defensibility of an analytic argument arises. Should anyone else take an analyst’s argument seriously as far as the relevance of this evidence is concerned? As we will see in a moment, this question also involves the extent to which anyone else should take the analyst’s assessments of uncertainty seriously. An absolutely crucial element in intelligence analysis is the defensibility of arguments constructed by analysts from the evidence available to possible conclusions to be proved or disproved. Of course, it is also true that an argument must be persuasive and that not all defensible arguments are persuasive. One fairly certain way of failing to make an argument persuasive is to have it revealed that it is not defensible on logical grounds. But there is an important point here that needs further elaboration.
There is no such thing as a uniquely correct or perfect argument from evidence. Here is a chain of reasoning an analyst has just constructed to establish the relevance as evidence of an item of information. Someone, another analyst or perhaps another critic, will always be able to find what this person believes to be a missing link or a link that is improperly stated. Perhaps this fellow analyst or critic discovers a disconnect in the analyst’s initial relevance argument. What no one, be they analyst or critic, can say is that they have the “correct” argument justifying the relevance of this item of evidence. Someone can come along later and discover inadequacies in the revised argument proposed by the other analyst or critic. What can be done is to have someone identify defects in an argument. But what no one can do is to say that the argument being proposed is the final or ultimately true argument that anyone could propose. What this says is that someone can correct defects in an argument without ever being able to say that they have the only argument that could ever be made regarding the relevance of evidence. This also accounts for the fact that there will always be some disagreement about the uncertainty that is assessed, combined, and reported among analysts themselves and among persons for whom the analysis was performed. Different persons will construct different arguments from the same bodies of evidence.

The fact that there is no such thing as the ultimately true argument has an important bearing on the many examples we will provide of various evidential and inferential issues. We will never say that the arguments we construct in providing examples are the only correct or true ones. You, the reader, may perceive other reasoning routes from the evidence we present and may indeed see other possible conclusions. Our major hope of course is that you will not see any disconnects or non sequiturs in our arguments.

Let us continue with the example from the previous sections where we have already established that the cesium-137 canister is missing (i.e., $E_i$ in Figure 5). The next step is to consider the competing hypotheses:

- $H_a$: “The cesium-137 canister was stolen.”
- $H_{a1}$: “The cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.”
- $H_{a2}$: “The cesium-137 canister was misplaced.”

As indicated by the reasoning tree in the middle of Figure 4 and discussed in Section 2.3, one has to put each of these hypotheses to work, to guide the collection of relevant evidence. One general strategy to guide the collection of evidence relevant to a given hypothesis $H$ is to look for indicators that the hypothesis $H$ is true. An example of such an indicators-based reasoning tree is provided in Figure 32.

In looking for evidence that the hazardous material locker storing the cesium-137 canister was breached, we talk to a professional locksmith named Clyde who said that the lock had been forced, but that it was a clumsy job (see INFO-003-Clyde in Table 6).
Assess whether there are indicators that the missing cesium-137 canister was stolen from the XYZ warehouse.

Look for evidence that there was suspicious activity suggesting the stealing of the cesium-137 canister from the XYZ warehouse.

Assess whether there are security breach indicators related to the cesium-137 canister missing from the XYZ warehouse.

Look for evidence that the entrance of the XYZ warehouse was breached.

Look for evidence that the hazardous material locker storing the cesium-137 canister was breached.

In looking for evidence that the entrance of the XYZ warehouse was breached, we investigate its security procedures and obtain the information labeled INFO-004-Guard in Table 6, concerning the panel truck having Maryland license plate MDC-578 which was inside the XYZ warehouse on the day before Willard's discovery of the missing cesium-137 canister. This leads us to the identification of the renting company owing the truck, as well as the name and the address of the person who rented the truck (see INFO-005-TRUXINC). Further investigation of the person and the truck reveals the information in INFO-006-SilverSpring and INFO-007-InvestigativeRecord.

In searching for evidence concerning the hypothesis that someone at the XYZ Company had removed this canister and was using the cesium-137 in current work for an XYZ customer, we have contacted Grace, the Vice President for Operations at XYZ. She tells us that no one at the XYZ Company had checked out the canister for work on any project the XYZ Company was working on at the time. She says that the XYZ Company had other projects involving hazardous materials but none that involved the use of cesium-137 (see INFO-008-Grace in Table 6).
Table 6. Additional information on the missing of the cesium-137 canister.

**INFO-003-Clyde:** We talked to a professional locksmith named Clyde, who said that the lock had been forced, but it was a clumsy job.

**INFO-004-Guard:** There is a security perimeter around the XYZ warehouse and employee parking area having just one gate that is controlled by a guard. On the day before the missing canister was observed, the security guard, Sam, recorded that a panel truck having Maryland license plate MDC-578 was granted entry at 4:45PM just before the XYZ closing hour at 5:00PM. The driver of this vehicle showed the guard a manifest containing items being delivered to the XYZ warehouse. This manifest contained a list of packing materials allegedly ordered by the XYZ Company. The vehicle was allowed to enter the parking area. At 8:30PM this same vehicle was allowed to exit the parking area. A different guard was on duty in the evenings and noticed that his records showed that this vehicle had been permitted entry and so he allowed the vehicle to exit the parking area.

**INFO-005-TRUXINC:** Maryland DOT’s record indicates that the panel truck carrying the license plate number MD-578 is registered in the name of a truck-rental company called TRUXINC, located in Silver Spring, MD. The manager of this agency showed records indicating that this truck was rented to a person who gave his name as Omer Riley, having as his listed address: 6176 Williams Ave. in Silver Spring. The truck was rented on the day before Willard’s discovery of the missing cesium-137, and it was returned the day after he made the discovery.

**INFO-006-SilverSpring:** Silver Spring city record according to which there is no residence at 6176 Williams Ave. in Silver Spring, MD.

**INFO-007-InvestigativeRecord:** An examination of the panel truck rented by Omer Riley, using a Geiger counter, revealed minute traces of cesium-137.

**INFO-008-Grace:** Grace, the Vice President for Operations at XYZ, tells us that no one at the XYZ Company had checked out the canister for work on any project the XYZ Company was working on at the time. She says that the XYZ Company had other projects involving hazardous materials, but none that involved the use of cesium-137.

The collected information from Table 6 suggests that the cesium-137 canister was stolen with the panel truck having Maryland license MDC-578. This leads to the development of the analysis tree in Figure 33.

We have to identify the “dots” in the text from Table 6 which are fragments representing relevant items of evidence for the leaf hypotheses in Figure 33. These dots are presented in Table 7. They will be used in the case studies in the following sections.
Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MCD-578 truck.

Assess whether the cesium-137 canister is missing from the XYZ warehouse.

Assess whether the missing cesium-137 canister was stolen with the MDC-578 truck.

Which is possible scenario?

The hazardous materials locker was forced, the MDC-578 truck was inside the company and it transported the cesium-137 canister.

Assess whether the hazardous materials locker was forced.

Assess whether the MDC-578 truck was inside the XYZ company before the discovery of the missing of the cesium-137 canister.

Which is possible scenario?

The MDC-578 truck was not used to transport cesium-137 within the last year and presents traces of cesium-137.

Assess whether the MDC-578 truck was not used to transport cesium-137 within the last year.

Assess whether the MDC-578 truck presents traces of cesium-137.

Figure 33. Analysis of the hypothesis that the cesium-137 canister was stolen with the MCD-578 truck.

Table 7. Dots from Table 6.

EVD-006-Clyde: Locksmith Clyde’s report that the lock was forced.

EVD-007-GuardReport: The record, made by Sam, security guard at the XYZ Company, that a panel truck bearing Maryland license plate number MDC-578 was in the XYZ parking area on the day before Willard’s discovery of the missing cesium-137 canister.

EVD-008-MDDOTRecord: Maryland DOT’s record that the truck bearing license plate number MDC-578 is registered in the name of the TRUXINC Company in Silver Spring, MD.

EVD-009-TRUXINCRecord1: TRUXINC’s record that the truck bearing MD license plate number MDC-578 was rented to a man who gave his name as Omer Riley on the day before Willard’s discovery of the missing cesium-137 canister.

EVD-010-TRUXINCRecord2: TRUXINC’s record that Omer Riley gave his address as 6176 Williams Ave.

EVD-011-SilverSpringRecord: Silver Spring city record according to which there is no residence at 6176 Williams Ave. in Silver Spring, MD.

EVD-012-InvestigativeRecord: Investigative record that traces of cesium-137 were found in the truck bearing license plate number MDC-578.

EVD-013-Grace: Grace, the Vice President for Operations at XYZ, tells us that no one at the XYZ Company had checked out the canister for work on any project.
4.2 Case Study: Evidence-based Hypothesis Analysis

4.2.1 Objective

This case study has the following objectives:

• Learning to associate with a hypothesis in an argument the evidence that is relevant to it.
• Better understanding the process of evaluating the likelihood of a hypothesis based on the available evidence.

4.2.2 Summary

This case study continues the analysis example introduced in Section 1.2. Having been established that the available evidence favors the hypothesis that the cesium-137 canister is missing, the next phase in the analysis is to consider the following alternative hypotheses that may explain the missing of the cesium-137: (1) The cesium-137 canister was stolen; (2) it is used in a project without being checked out from the warehouse; and (3) it has been misplaced. Here you will analyze the first of these hypotheses, that the cesium-137 canister was stolen.

The available evidence suggests a scenario where the XYZ hazardous material locker containing the canister was forced, the MDC-578 truck was inside the XYZ company and it transported the cesium-137 canister. As a result, you will refine the hypothesis, attempting to assess that the missing cesium-137 canister was stolen with the MDC-578 truck.

You will select this hypothesis and then you will browse its analysis tree to see how it is reduced to simpler hypotheses that need to be assessed based on the available evidence. After that you will associate the available evidence to those simpler hypotheses to which it is relevant, estimate the relevance and the believability of each item of evidence, and browse the resulting analysis tree.

4.2.3 Instructions

1. Start the case study in TIACRITIS.
2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains one or several hypotheses to select from.
3. Select the hypothesis analysis problem: “Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.” Once this hypothesis is selected, the Reasoner is automatically invoked to analyze the hypothesis, as shown in Figure 22 (pg. 35).
4. In the left panel, right-click on “cesium-137 canister stolen with MDC-578 truck: no solution” and select **Expand**. As shown in Figure 34, the left panel shows the sub-problems of this problem. You will associate relevant evidence with some of these sub-problems.

5. Select the **Evidence** menu on the top of the window. As a result you will enter the **Evidence** editor.

6. Notice the four modes of operations from the top part of the left panel in Figure 35. Because the selected one is **[AVAILABLE EVIDENCE]**, the left panel shows the current evidence from the knowledge base of TIACRITIS.
8. Click on [COLLECTION GUIDANCE] to display the elementary hypotheses in the reasoning tree and the number of evidence items associated with each of them. Then click on one of these hypotheses. The right panel shows the evidence relevant to the selected hypothesis (see Figure 36). It also allows you to associate search criteria with that hypothesis and to invoke various search engines with those criteria to identify relevant information, as will be practiced in another case study.

9. Click on [COLLECTED INFORMATION] to display the list of collected information items (see the left panel of Figure 37) and then click on INFO-004-Guard to display the content of this information item (see the right panel of Figure 37).
Select mode: [COLLECTION GUIDANCE] [COLLECTED INFORMATION] [AVAILABLE EVIDENCE] [IMPORT EVIDENCE]

Collection guidance
Sorted by: [REASONING] [NAME] [SUPPORT]

the cesium-137 canister was in the XYZ warehouse before being reported as missing (favoring 1, disfavoring 0)
the cesium-137 canister is no longer in the XYZ warehouse (favoring 2, disfavoring 0)
the cesium-137 canister was not moved from the XYZ warehouse to another location (favoring 1, disfavoring 0)
the XYZ hazardous material locker was forced (favoring 0, disfavoring 0)
the MDC-578 truck was inside the XYZ company before the discovery of the missing of the cesium-137 canister (favoring 0, disfavoring 0)
the MDC-578 truck presents traces of cesium-137 (favoring 0, disfavoring 0)

Hypothesis: the cesium-137 canister was in the XYZ warehouse before being reported as missing [REASONING]

Favoring evidence (1): EVD-002-Ralph
Disfavoring evidence (0): No evidence.

Search for relevant evidence:
Search criterion: none [NEW]
Search with: [BING] [GOOGLE] [YAHOO]

Select mode: [COLLECTION GUIDANCE] [COLLECTED INFORMATION] [AVAILABLE EVIDENCE] [IMPORT EVIDENCE]

Collected Information [NEW] [DELETE]
Sorted by: [ID] [DESCRIPTION]

INFO-001-Willard: The XYZ company in Baltimore MD manufactures devices for sterilizing medical equipment. A person named Willard reported in a Washington Post article...
INFO-002-Ralph: Ralph, the supervisor of the warehouse, reports that the cesium-137 canister is registered as being in the warehouse, that no one at the XYZ Company...
INFO-003-Clyde: We have asked a professional locksmith named Clyde who said that the lock had been forced, but it was a clumsy job.
INFO-004-Guard: There is a security perimeter around the XYZ warehouse and employee parking area having just one gate that is controlled by a guard. On the day before...
INFO-005-TRUXINC: Maryland DOT's record indicates that the panel truck carrying the license plate # MD-578 is registered in the name of a truck rental company called...

Figure 36. Information collection guidance.

Figure 37. Collected information.
10. Click on [AVAILABLE EVIDENCE] and then click on **EVD-006-Clyde** in the left panel. As indicated in Figure 38, the upper part of the right panel shows the main characteristics of this item of evidence, followed by all the basic hypotheses in the analysis tree. You will have to decide whether **EVD-006-Clyde** favors or disfavors any of these hypotheses, and indicate this by clicking on [FAVORS] or [DISFAVORS] following that hypothesis.

Figure 38. Selection of the hypotheses that favor or disfavor an item of evidence.
11. Click on **[FAVORS]** following this hypothesis “the XYZ hazardous material locker was forced.” Notice in Figure 39 that this hypothesis was moved under the label **Favors**. Clicking on **[REMOVE]** will move the hypothesis back under the “**Irrelevant to**” label.

![Figure 39. An item of evidence and its relationship with the basic hypotheses.](image-url)
12. Select [REASONING] following the hypothesis “the XYZ hazardous material locker was forced.” The Reasoner is automatically invoked with the favoring evidence for that hypothesis selected.

13. Right-click on “favoring evidence: no solution” and select Expand. Notice in the left panel of Figure 40 that the analysis tree has been extended with the analysis EVD-006-Clyde. You will need to complete this analysis by defining assumptions for the relevance and the believability of this item of evidence.

14. Under “EVD-006-Clyde: no solution,” click on “relevance: no solution” and define the assumption that it is almost certain, by performing the following operations that were illustrated in Figure 29 (pg. 52) and Figure 30 (pg. 53):

   • Select Assumption.
   • Click on [NEW].
   • Click on "...", then click on “certain” and then double-click on "almost certain."
   • Click on [CREATE].

14. Select Reasoner and notice the defined solution for relevance.
15. Click on “believability EVD-006-Clyde: no solution” and define the assumption that it is almost certain, by performing the following operations that were illustrated above and in Figure 29 (pg. 52) and Figure 30 (pg. 53).

16. Select the Evidence menu on the top of the window to return to the Evidence editor.

17. In the left panel, click on EVD-007-GuardReport.

18. In the right panel, click on [FAVORS] following the hypothesis “the MDC-578 truck was inside the XYZ company before the discovery of the missing of the cesium-137 canister” and notice that this hypothesis was moved under the Favors label.

19. Click on other items of evidence in the left panel and associate them with the basic hypotheses that they favor or disfavor, as was illustrated above.

20. Select [REASONING] following those hypotheses or the Reasoner menu, and define assumptions for the relevance and the believability of the above items of evidence.

You will now define an assumption for the hypothesis “MDC-578 truck did not transport cesium-137 within last year.”

21. Select Assumption.

22. Click on [NEW].

23. Click on the first "...", then click on "certain" and then double-click on "very likely".

24. Click on "RDX" and then double-click on "cesium-137".

25. Click on [CREATE].

26. Select Reasoner.

27. Browse the analysis tree.

28. Select Case Study.

29. Click on [SAVE & FINISH] to end the case study.
ASSESSING THE BELIEVABILITY OF EVIDENCE

5.1 Believability: The Foundation of All Arguments from Evidence

The second major credential of evidence involves its believability (sometimes referred also as “credibility”). Here is an item of information an analyst is considering as possible relevant evidence. This credential involves the question: Can we believe what this item of evidence is telling us? Of course this believability question involves considering the source from which this item came. The order in which we ask the relevance question “So what?” and the believability question “Can we believe it?” is immaterial. Which one of the relevance and believability questions we ask first will not affect our discussion of the credentials of evidence. In our view, the evidential and inferential issues surrounding believability assessment form perhaps the most difficult and interesting questions to be asked in intelligence analysis, or in any other context for that matter. One major difficulty is that we must ask different kinds of believability questions depending on the kinds of evidence we have, and upon the sources from which this evidence has come. In the next section, when we discuss basic substance-blind forms of evidence, we will see how different credibility questions we must ask are different for tangible items of evidence such as those provided by IMINT, COMINT, and MASINT than those provided by human informants or assets who provide testimonial evidence in the form of HUMINT. And, in the case of HUMINT, we require additional questions regarding the competence of HUMINT informants; one basic error often made in intelligence analyses is that the competence of a HUMINT source is often construed as evidence about this source’s credibility. As we will show, competence does not entail credibility nor does credibility entail competence; they are entirely separate matters.

Regardless of the form and source of the evidence being considered, we must distinguish between evidence about an event and the event itself. Having evidence about an event does not entail that this event actually occurred. To believe that an event did occur just because we have evidence for that invites all sorts of inferential troubles, primarily because sources of intelligence evidence of any kind have every possible gradation of believability shy of perfection. We can easily distinguish between evidence about an event and the event itself. We let \( E^* \) represent evidence that event \( E \) has occurred. Here is the basic source of doubt that will ground all of our arguments from evidence. We must infer that \( E \) occurred based on our evidence \( E^* \). Clearly, this inference rests upon what we know about the believability of the source of \( E^* \).

5.2 Classification of Evidence Based on Believability

Here is an important question we are asked to answer regarding the individual kinds of evidence we have: How do you, the analyst, stand in relation to this item of evidence? Can you examine it for yourself to see what events it might reveal? If you can, we say that the evidence is tangible in nature. You can examine it and apply your own senses in a determination of what the evidence may be telling you. We might say that in assessing tangible evidence your own senses provide a direct interface with events of interest. As we will discuss momentarily, there are many forms of tangible evidence. But suppose
instead you must rely upon other persons, assets, or informants, to tell you about events of interest. Their reports to you, about these events, are examples of testimonial evidence. You yourself were not privy to the occurrence or nonoccurrence of these events and so you make inquiries of these assets who may have observed these events. It is of vital interest to know how these persons obtained the information they report. And, as we will observe, the human sources of testimonial evidence can express varying degrees of uncertainty about what they have observed.

Figure 41 shows the substance-blind classification of evidence that results from the above discussion and is further discussed below.

5.3 Tangible Evidence

There is an assortment of tangible items we might encounter, and that could be examined by an intelligence analyst. Both IMINT and SIGINT provide various kinds of sensor records and images that can be examined. MASINT and TECHINT provide various objects such as soil samples and weapons that can be examined. COMINT can provide audio recordings of communications that can be overheard and translated if the communication has occurred in a foreign language. We also note that documents are tangible evidence that can be examined by an analyst. These documents might have been captured or revealed by a human asset; but they also include any document obtained from open sources whatever they may be: newspapers, books, websites, etc. We also list as tangible items tabled measurements of any kind including statistical records; charts showing various kinds of scientific or technological relations;
and maps and diagrams or plans of various kinds. Some of these kinds of items might be included in TECHINT or MASINT sources.

One thing we are obliged to note is that the analyst observing these tangible items may need the assistance of other analysts who have expertise in explaining the analyst what a tangible item reveals. For example, an expert in photo analysis may assist another analyst by showing what an image has revealed to us. Analysts whose assistance is required in such cases play the role of “expert witnesses,” so common in both criminal and civil trials. All of this highlights the fact that intelligence analysis is so often a cooperative venture involving teams of analysts each of whom may have particular knowledge and skills.

Two different kinds of tangible evidence have been usefully discerned, at least in the field of law: real tangible evidence and demonstrative tangible evidence (Lempert et al., 2000, 1146 – 1148).

5.3.1 Real Tangible Evidence: Authenticity

Real tangible evidence is a thing itself and it has only one major believability attribute: authenticity. Is this object what it is represented as being or is claimed to be? There are as many ways of generating deceptive and inauthentic evidence as there are persons wishing to generate it. Documents or written communications may be faked, captured weapons may have been altered, and photographs may have been manipulated in various ways. One problem is that it usually requires considerable expertise to detect inauthentic evidence. Further, different kinds of real tangible evidence require different areas of expertise. For example, it would require quite different expertise to detect a forged document than it does to detect an altered photo or a deceptive weapon component.

5.3.2 Demonstrative Tangible Evidence: Authenticity, Accuracy, and Reliability

Demonstrative tangible evidence does not concern things themselves but only representations or illustrations of these things. Examples include diagrams, maps, scale models, statistical or other tabled measurements, and sensor images or records of various sorts such as IMINT, SIGINT, and COMINT. Demonstrative tangible evidence has three believability attributes. The first concerns its authenticity. So, both real and demonstrative tangible evidence have this crucial believability attribute. For example, suppose we obtain a hand drawn map from a captured insurgent showing the locations of various groups in his insurgency organization. Has this map been deliberately contrived to mislead our military forces, or is it a genuine representation of the location of these insurgency groups?

The second believability attribute of demonstrative tangible evidence is accuracy of the representation provided by the demonstrative tangible item. The accuracy question concerns the extent to which the device that produced the representation of the real tangible item had a degree of sensitivity (resolving power or accuracy) that allows us to tell what events were observed. We would be as concerned about the accuracy of the hand-drawn map allegedly showing insurgent groups locations, as we would about the accuracy of a sensor in detecting traces of some physical occurrence. Different sensors have different resolving power that also depends on various settings of their physical parameters (e.g., the settings of a camera). Certain settings of these parameters provide better images
of objects than do other settings, given the conditions under which the image was obtained. Some sensors, such as those employed in ELINT, provide only approximate locations of objects such as the error ellipses provided by ELINT records of radar emissions.

The third major attribute, reliability, is especially relevant to various forms of sensors that provide us with many forms of demonstrative tangible evidence. A system, sensor, or test of any kind is reliable to the extent that the results it provides are repeatable or consistent. You say that your car is reliable to the extent to which it will take you where you wish to go for some specified time in the future. A sensing device is reliable if it would provide the same image or report on successive occasions on which this device is used. A test is reliable to the extent that it provides the same result on repeated applications of it. Speaking of physical sensors, the reliability of any of them depends, of course, on how well they are maintained. The trouble with applying the term reliability to items of HUMINT reported by human sources is that what is at issue is whether or not we can believe what this source has told us; this involves his/her competence and credibility. As discussed in the previous section, the believability of a human source requires questions that are quite different from those we would ask concerning a sensor’s reliability. We could say that a reliable human source is one who will provide us with information whenever we ask for it. But whether we can believe what this source is telling us on any occasion depends on his/her competence and credibility.

Figure 42 expresses the assessment of the believability of demonstrative tangible evidence in the problem reduction/solution synthesis paradigm. First we reduce this assessment to three simpler assessments. Then we combine the solutions of these assessments.

![Figure 42. Assessing the believability of demonstrative tangible evidence.](image-url)
5.3.3 Examples of Tangible Evidence

Here are several examples and questions involving evidence that is tangible and that the analyst can examine personally to see what events it reveals.

Example 1. Have a look at evidence item EVD-009-MDOTRecord in Table 7 on page 61. The Maryland DOT records, in the form of a tangible document, could be given to the analyst to verify that the vehicle carrying MD license plate number MDC-578 is registered in the name of the TRUXINC Company in Silver Spring, MD.

Example 2. Now consider evidence item EVD-007-GuardReport in Table 7. Here we have a document in the form of a log showing when the truck bearing license plate number MDC-578 exited the XYZ parking lot at 8:30 PM on the day in question. This tangible item could also be made available to analysts investigating this matter.

Question 1. What other items of tangible evidence do you see in Table 7?

5.4 Testimonial Evidence

For testimonial evidence we have two basic sources of uncertainty: competence and credibility. This is one reason why it is more appropriate to talk about the believability of testimonial evidence which is a broader concept that includes both competence and credibility considerations.

5.4.1 Competence: Access and Understandability

The first question to ask related to competence is whether this source actually made the observation he claims to have made or had access to the information that he reports. The second competence question concerns whether this source understood what was being observed well enough to provide us with an intelligible account of what was observed. Thus competence involves access and understandability. In several accounts of intelligence analyses we have observed a glaring non sequitur. These accounts all say: “We can believe what this source has reported to us because he had good access to the information he reports.” This source may have had all the access in the world, but still not be credible in his report about what he observed. The problem here is that HUMINT asset competence does not entail the asset’s credibility; competence and credibility are two entirely distinct characteristics. It is also true that a human source’s credibility does not entail his competence. Credibility has entirely different attributes than competence, as we will now explain.

HUMINT asset A tells us that he observed event E to have happened. Suppose, on evidence, we believe A to be a competent source; i.e. we believe A made the observation he says he made. Whether we can believe that event E happened depends on three attributes of A’s credibility: his veracity, objectivity, and observational sensitivity under the conditions of the observation. As we have explained elsewhere, these three attributes of the credibility of human sources of testimonial evidence arise in four different contexts: law, epistemology, signal detection theory, and common experience (Schum, 1989).
5.4.2 Credibility: Veracity, Objectivity, and Observational Sensitivity

5.4.2.1 Veracity or Truthfulness

From experience we learn that people do not always believe what they are telling us. We would not say that a person was being untruthful if this person believed what he/she just reported. So the first question we should ask about the source telling us that event E occurred is: Does this source believe that event E occurred? Assessing veracity or truthfulness has been a problem for centuries and some mistakes have been made in explaining what veracity means. In many old and in some newer works it is said that a source is being truthful only if the event reported actually occurred. There is great trouble here since this explanation confounds veracity with the two other credibility attributes we need to consider. As an example, our source tells us that event E occurred and we later find out that E did not occur. Was this source being untruthful? Not necessarily, since this source might simply have been mistaken. So the veracity of sources of HUMINT who report on what they observe depends on our assessment of whether these sources actually believe what they are reporting to us.

5.4.2.2 Objectivity

From common experience we observe that persons, including ourselves, often believe that some event has occurred because we either expect it to occur or want it to occur, regardless of what our senses are telling us. In such instances, we would say that this source lacks objectivity. An objective observer is one who bases a belief on the sensory evidence he/she received rather than on what this person expected or desired to observe. Suppose we believe that the source telling us that event E occurred is being truthful; he does believe that event E occurred. But now the question is: Was this belief based on the sensory evidence this source received, or was it based on what this source expected or wished to observe? One additional important matter concerns the role of memory. The reason is that our beliefs are elastic in nature; they change over time and often in response to new information we receive. If a HUMINT source made the observation some time ago, we might well question whether this source had the same belief at the time of his/her observation that this person now has while reporting to us. Is this person now telling us what he/she expected or wished to occur instead of basing this report on this person’s recollection of what his/her senses recorded?

5.4.2.3 Observational Sensitivity

Suppose we believe our source to be truthful and objective in their report that event E occurred. This source does believe that E occurred and this source did base this belief on sensory evidence obtained during a relevant observation. But now the question is: How good was the sensory evidence this source received under the conditions in which this observation was made? As we know, none of our senses are perfectly accurate or sensitive, particularly under a variety of ambient conditions such as reduced visibility and high noise levels. The physical condition of the source is also relevant here. We would question the adequacy of the sensory evidence this source obtained if he/she had some sensory defect or was intoxicated at the time the observation was made. Common experience tells us that human senses are not infallible and that we are all prone to make mistakes in our observations.
Figure 43 summarizes the believability credentials for testimonial evidence based upon direct observations, and the questions we need to ask to establish such credentials.

Assess the believability of $E_1$ which is unequivocal testimonial evidence based upon direct observation by the source $S$

Assess the competence of $S$ wrt $E_1$

Assess the understandability of $S$ wrt $E_1$

Assess the access of $S$ wrt $E_1$

Assess the veracity of $S$ wrt $E_1$

Assess the objectivity of $S$ wrt $E_1$

Assess the observational sensitivity of $S$ wrt $E_1$

5.4.3 Types of Testimonial Evidence

As indicated in Figure 41, there are several types of testimonial evidence. If the source does not hedge or equivocate about what he/she observed (i.e., the source reports that he/she is certain that the event did occur), then we have unequivocal testimonial evidence. If, however, the source hedges or equivocates in any way (e.g., “I’m fairly sure that $E$ occurred”) then we have equivocal testimonial evidence. The first question we would ask this source of unequivocal testimonial evidence is: How did you obtain information about what you have just reported? It seems that this source has three possible answers to this question. The first answer is: “I made a direct observation myself.” In this case we have unequivocal testimonial evidence based upon direct observation. The second possible answer is: “I did not observe this event myself but heard about its occurrence (or nonoccurrence) from another person.” Here we have a case of secondhand or hearsay evidence, called unequivocal testimonial evidence obtained at second hand. A third answer is possible: “I did not observe event $E$ myself, nor did I hear about it from another source. But I did observe events $C$ and $D$ and inferred from them that event $E$ definitely occurred.” This is called testimonial evidence based on opinion and it requires some very difficult questions. The first concerns the source’s believability as far as his/her observation of event $C$ and $D$; the second involves our examination of whether we ourselves would infer $E$ based on events $C$.
and D. This matter involves our assessment of the source’s inferential ability. It might well be the case that we do not question this source’s credibility in observing events C and D, but we question the conclusion that event E occurred the source has drawn from his observations. We would also question the certainty with which the source has reported an opinion that E occurred. Despite the source’s conclusion that “event E definitely occurred,” and because of many sources of uncertainty, we should consider that testimonial evidence based on opinion is a type of equivocal testimonial evidence (see Figure 41).

There are two other types of equivocal testimonial evidence. The first we call completely equivocal testimonial evidence. Asked whether event E occurred or did not, our source says: “I don’t know,” or “I can’t remember.” This is an interesting response of the sort we so frequently observe during congressional hearings. There are two possible explanations for this complete equivocation. The first is that the source is honestly impeaching or undermining his own believability; he does not know or cannot remember. A frequent addition to this equivocation might be the further statement: “I’m not a good source here, perhaps you ought to ask X (another possible source).” Unfortunately, there is another possible explanation for this complete equivocation; the source does know or can remember, but refuses to tell us whether E occurred or not. If we had evidence that this source did know or did remember whether or not event E occurred, this would be evidence that our source is a double and has more than one employer.

But there is another way a source of HUMINT can equivocate; the source can provide probabilistically equivocal testimonial evidence in various ways. One way is numerical, as in the following example. Asked whether event E occurred or did not, the source might say: “I’m 60 percent sure that event E happened and 40 percent sure that it didn’t happen.” We could look upon this particular probabilistic equivocation as an assessment by the source of his own observational sensitivity. However, if we had evidence pointing to his underassessment of how sure he was that event occurred, we might be inclined to view this evidence as bearing on the source’s veracity. Another way probabilistic equivocation can be expressed is in words rather than in numbers. Asked whether event E occurred, the source might say such things as: “I’m fairly sure that E occurred”; “It is quite probable that E occurred”; or “It is very unlikely that E occurred.” Here again we would wish to determine whether the source’s stated degree of equivocation was legitimate or not.

5.4.4 Examples of Testimonial Evidence

Here are some examples and questions involving testimonial evidence from human sources that is not hedged or qualified in any away.

Example 3. Evidence item EVD-013-Grace in Table 7 is Grace’s testimony that no one at the XYZ Company had checked out the canister for work on any project. Grace states this unequivocally. You should also note that she has given negative evidence saying the cesium-137 was not being used by the XYZ Company. This negative evidence is very important because it strengthens our inference that the cesium-137 canister was stolen.
Example 4. EVD-006-Clyde in Table 7 is unequivocal testimonial evidence. It represents positive evidence.

Question 2. Table 9 presents additional items of evidence related to the missing cesium-137 scenario. What examples of unequivocal testimonial evidence do you see in this table?

Here are some examples and questions involving testimonial evidence given by human sources who equivocate or hedge in what they tell us.

Example 5. Consider the evidence item EVD-005-Ralph in Table 5. Here Ralph hedges a bit by saying that the lock on the hazardous materials storage area appears to have been forced. He cannot say for sure that the lock had been forced, so he hedges in what he tells us.

Example 6. In new evidence regarding the dirty bomb example, suppose we have a source code-named “Yasmin.” She tells us that she knew a man in Saudi Arabia named Omar al-Massari. Yasmin says she is “quite sure” that Omar spent two years “somewhere” in Afghanistan “sometime” in the years 1998-2000.

Question 3. Give some examples from your own experience when you have heard people providing information about which they hedge or equivocate.

5.5 Missing Evidence

5.5.1 Uncertainties Associated with Missing Evidence

To say that evidence is missing entails that we must have had some basis for expecting we could obtain it. There are some important sources of uncertainty as far as missing evidence is concerned. In certain situations missing evidence can itself be evidence. To begin with, consider some form of tangible evidence, such as a document, that we have been unable to obtain. There are several reasons for our inability to find it, some of which are more important than others. First, it is possible that this tangible item never existed in the first place; our expectation that it existed was wrong. Second, the tangible item exists but we have simply been looking in the wrong places for it. Third, the tangible item existed at one time but has been destroyed or misplaced. Fourth, the tangible item exists but someone is keeping it from us. This fourth consideration has some very important inferential implications including denial and possibly deception. An adverse inference can be drawn from someone’s failure to produce evidence. The failure to produce requested evidence may mean that producing it would not be in the best interests of the person(s) from whom the item was requested. If these interests coincide with those of an adversary, we could conclude that this failure to produce evidence is part of an attempt to deceive us since, if we did obtain this evidence, it would be in our best interests and not the best interests of the adversary.

Now consider missing testimonial evidence. Suppose we expect that a HUMINT asset \( \mathcal{A} \) could tell us about some event of importance to us. There are several interesting possibilities here. First, \( \mathcal{A} \) might never respond to our inquiry; put another way, \( \mathcal{A} \) responds to our inquiry with silence. There are different rules that apply in intelligence analysis than those applying in our courts of law. In law, a
defendant or a witness can claim protection under the Fifth Amendment to our Constitution. He cannot be compelled to testify, and no adverse inference is allowed by his failure to do so. But there is no such privilege in intelligence analysis. We would be entitled to draw an adverse inference about \( A \)'s silence in response to our request for information to which we believe \( A \) has access. Another possibility is that \( A \) acts to impeach his own competence; \( A \) tells us that he never has made any observation of events such as those in which we are presently interested. This may sound like the complete equivocation we discussed above. The difference in this case is that \( A \) gives a particular reason why he does not know whether this event occurred or not; \( A \) says he was never in a position to observe this event or had no access to the information requested of him. If, on evidence, we learned that \( A \) did make an observation or did have access to information about the requested event, we would certainly be entitled to draw an adverse inference concerning \( A \)'s behavior and the inferential consequences of his refusing to reveal the information we are seeking from him.

In summary, there are very important uncertainties associated with missing evidence, either tangible or testimonial in nature. But there is one final matter to consider about which most analysts will already know. We should not confuse negative evidence with missing evidence. To adopt a common phrase, “evidence of absence (negative evidence) is not the same as absence of evidence (missing evidence).” Entirely different conclusions can be drawn from evidence that an event did not occur than can be drawn from our failure to find evidence. We are obliged to ask different questions in these two situations.

5.5.2 Examples of Missing Evidence

The following are some examples and questions about missing evidence that is either tangible or testimonial in nature.

Example 7. Consider our discussion on the cesium-137 canister. Upon further investigation we identify the person who rented the truck as Omar al-Massari, alias Omer Riley. We tell him that we wish to see his laptop computer. We are, of course, interested in what it might reveal about the terrorists he may be associating with. He refuses to tell us where it is. This we referred to as the non-production of evidence.

Question 4. What inferences might we draw from Omar al-Massari’s refusal to provide us with his laptop computer?

Question 5. What other items of evidence are missing so far in our discussion of the cesium-137 case?

5.6 Accepted Facts

There is one final category of evidence about which we would never be obliged to assess its believability. In intelligence analyses, and in many analyses in other contexts, we routinely need information whose believability we would never be expected to defend. In fact, in certain instances we could never establish the believability of this information. Tabled information of various sorts such as
Assessing the Believability of Evidence

tide tables, celestial tables, tables of physical or mathematical results (such as probabilities associated with statistical calculations), and many other tables of information we would accept as being believable provided that we used these tables correctly. In some instances, of course, tabled information might contain errors. For example, tables showing the ranges or explosive power of a weapons system under various conditions might have incorrect entries that are discovered and corrected. Many other items of information are accepted facts whose believability is assumed. For example, an analyst would not be obliged to prove that temperatures in Iraq can be around 120° Fahrenheit in summer months, or that the population of Baghdad is greater than that of Basra.

5.7 Mixed Evidence

5.7.1 Analysis of Mixed Evidence

We have just considered a categorization of individual items of evidence. But there are situations in which individual items can reveal various mixtures of the types of evidence shown in Figure 41. One example involves a tangible document containing a testimonial assertion based on other alleged tangible evidence. As we noted, these forms of evidence are not mutually exclusive; they can occur together in a single item of evidence. We might say that mixtures of them get crowded into the same item of evidence. Figure 44, for example, shows how one would need to assess the believability of testimonial evidence about tangible evidence.

5.7.2 Examples of Mixed Evidence

Here are some examples and questions about mixtures of the forms of evidence discussed above.

Example 8. Here is an obvious example of a mixture of two or more items of tangible evidence; it is called a passport. A passport is a tangible document alleging the existence of other tangible documents recording the place of birth and country of origin of the holder of the passport. In other words, a passport sets up a paper trail certifying the identity of the holder of the passport. In addition to the authenticity of the passport itself, we are also interested in the authenticity of all the other tangible documents on which this passport is based.

Example 9. Here is another mixture of forms of evidence, this time recording a mixture of tangible and testimonial evidence. We return to our asset “Yasmin” who has given us further evidence about Omar al-Massari in our cesium-137 example. Suppose we have a tangible document recording Yasmin’s account of her past experience with Omar al-Massari. This document records Yasmin’s testimony about having seen a document detailing plans for constructing weapons of various sorts that was in Omar al-Massari’s possession. As far as believability issues are concerned, we first have the authenticity of the transcription of her testimony to consider. Yasmin speaks only in Arabic and so we wonder how adequate the translation of her testimony has been. Also, we have concerns about Yasmin’s competence and credibility to consider in her recorded testimony. Finally, we have further interest in the authenticity of the document she allegedly saw in Omar al-Massari’s possession.

Question 6. Do you see any example of mixtures of evidence in Table 7?
Question 7. Can you provide other examples of mixtures of evidence from your own experience?

In this section we have shown that we can classify all evidence, regardless of its substance or content, into just a few categories of recurrent forms and combinations of evidence. That is why this classification is called substance-blind. This classification of evidence is based on its inferential properties rather than upon any feature of its substance or content. Knowledge of these substance-blind forms and combinations of evidence pays great dividends. Such knowledge informs us and TIACRITIS how to evaluate the believability of evidence, based on its type. It allows us to more easily assess evidence coming from different sources and to compare the evidence and conclusions reached from it in different intelligence analyses at different times.

Figure 44. An example of assessing the believability of mixed evidence.
5.8 Case Study: Believability Analysis

5.8.1 Objective

This case study has the following objectives:

- Learning how to represent an item of evidence to be used by TIACRITIS.
- Better understanding the process of believability analysis.

5.8.2 Summary

This case study continues the analysis example introduced in Section 1.2 with the analysis of the problem “Assess whether the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.”

You will select this hypothesis and then you will browse its analysis tree to see how it is reduced to simpler hypotheses that need to be assessed based on the available evidence. After that, you will represent a new item of evidence, will associate it with the hypothesis to which it is relevant, assess its relevance, evaluate its believability by assessing its credentials, and browse the resulting analysis tree. Proceed as indicated in the following instructions.

5.8.3 Instructions

1. Start the case study in TIACRITIS.
2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains one or several hypotheses to select from.
3. Select the hypothesis analysis problem: “Assess whether the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.” Once this hypothesis is selected the Reasoner is automatically invoked to analyze the hypothesis, as shown in Figure 27 (pg. 50).
4. In the left panel, click on the hypothesis “missing cesium-137 canister used in a project: no solution.” We will define and associate an item of evidence with this hypothesis.
5. Select the Evidence menu on the top of the window and then click-on [COLLECTED INFORMATION] at the top of the left panel. The left panel will show the collected items of information. We will define an item of evidence based on INFO-008-Grace.
6. Click on INFO-008-Grace in the left panel. The right panel shows this information (see Figure 45).

7. In the right panel, select the text, “Grace, the Vice President for Operations at XYZ, tells us that no one at the XYZ Company had checked out the canister for work on any project.” You will define a new item of evidence based on this description. If no text is selected, the description of the item of evidence will be the entire text. In any case, you will be able to update the description of the item of evidence.

8. Click on [DEFINE EVIDENCE] located after the description of INFO-008-Grace in the right panel. As a result, the right panel shows a partially defined item of evidence “EVD-013-“ (see Figure 46). You will update the definition of this item of evidence.
5 Assessing the Believability of Evidence

9. Complete the name “EVD-013-” at the top of the right panel with “Grace” and click on [SAVE]. The right side of Figure 47 shows the item of evidence being defined. It should now read “EVD-013-Grace.”

---

**Figure 46.** Partially defined item of evidence.

**Figure 47.** Defining a new item of evidence.

- **EVD-009-TRUXINCRecord1**: TRUXINC’s record that the truck bearing MD license plate number MDC-507 was rented to a man who gave his name as Omer Riley on the day before.
- **EVD-010-TRUXINCRecord2**: TRUXINC’s record that Omer Riley gave his address as 6176 Williams Ave.
- **EVD-011-SilverSpringRecord**: Silver Spring city record according to which there is no residence at 6176 Williams Ave in Silver Spring.
- **EVD-012-InvestigativeRecord**: Investigative record that traces of cesium-137 were found by a Geiger counter in the truck bearing license plate # MDC-578.
- **EVD-013-Grace**: Grace, the Vice President for Operations at XYZ, tells us that no one at the XYZ Company had checked out the canister for work on any project.

- **Selected item of evidence**: EVD-013-Grace
- **Description**: Grace, the Vice President for Operations at XYZ, tells us that no one at the XYZ Company had checked out the canister for work on any project
- **Extracted from**: INFO-008-Grace

- **Irrelevant to**:
  - the cesium-137 canister was in the XYZ warehouse before being reported as missing
  - the cesium-137 canister is no longer in the XYZ warehouse
  - the cesium-137 canister was not moved from the XYZ warehouse to another location
  - the missing cesium-137 canister is used in a project without being checked-out from the XYZ warehouse
10. Click on [EDIT] for Description, click inside the pane and edit the description to “Grace, the Vice President for Operations at XYZ, tells us that no one had checked the cesium-137 canister out.”

11. Click on [SAVE]

12. After “Type: evidence,” click on [CHANGE] to specify the type of this item of evidence (see Figure 48).

Figure 48. Selecting the type of evidence.

13. After “unequivocal testimonial evidence based upon direct observation,” click on [SELECT].

14. After “By the source: not specified,” click on [CHANGE].
15. Type “Grace” and click on [SAVE].

16. Click on [YES].

17. Under the “Irrelevant to” label, and after the hypothesis “the missing cesium-137 canister is used in a project without being checked-out from the XYZ warehouse,” click on [DISFAVORS]. Notice that a Disfavors label was created and the hypothesis was moved under it.

The result of this sequence of operations is shown in the right hand side panel of Figure 49. Notice also that the left panel shows the list of the items of evidence, including the one just defined.

18. Select [REASONING] following that hypothesis. Reasoner is automatically invoked with the disfavoring evidence for that hypothesis selected.
19. Right-click in the left panel and select **Expand**. The left panel shows the credentials of EVD-013-Grace that need to be assessed. Notice the detailed believability analysis in Figure 50 that requires assessing Grace’s access, understandability, veracity, objectivity, and observational sensitivity. You will have to evaluate these believability credentials and define them as assumptions.

20. Click on “access: no solution.”

21. In the right panel, right-click on “Assess the access by Grace to the information in EVD-013-Grace” and select **New Assumption**. As a result, TIACRITIS makes the default assessment certain.

22. Click on “certain” and, in the displayed list, double-click on “almost certain,” which is now used as the new assessment.
23. Select the other evidence credentials for EVD-013-Grace (understandability, veracity, objectivity, and observational sensitivity), assess them, and define them as assumptions for them, as illustrated above, until a solution of the top level problem is obtained. The resulting analysis tree will be similar to that shown in Figure 51. Notice how TIACRITIS evaluated the upper level believability credentials (i.e., competence and credibility), the inferential force of EVD-013-Grace, and the upper level hypotheses.

24. Select Case Study and click on [SAVE & FINISH] to end it.

**Figure 51.** Detailed believability analysis.

### 5.9 Case Study: Self-testing on Believability Analysis

#### 5.9.1 Objective

The objective of this case study is to allow you to test your knowledge on assessing the believability of evidence.

#### 5.9.2 Summary

This case study uses evidence related to the analysis example introduced in Section 1.2, on the missing of the cesium-137 canister from the XYZ warehouse. TIACRITIS will automatically generate test questions of three different types: omission, modification, and construction.
Both an omission and a modification test will show you the reduction of a problem to one or several sub-problems, asking you to characterize the reduction as either:

- Correct (all the sub-problems are present and all of them are correct).
- Incomplete (at least one sub-problem is missing, but the present ones are correct).
- Incorrect (at least one of the sub-problems is incorrect).

A construction test will show a problem and a set of potential sub-problems, asking you to select the complete set of correct sub-problems.

You can request a hint to answer the test question. After answering the test question, TIACRITIS will comment on your answer, either reinforcing a correct answer or explaining an incorrect one.

Proceed as indicated in the following instructions. Notice, however, that the test questions are randomly generated. Therefore, it is unlikely that you will receive the same test questions shown in the next section.

5.9.3 Instructions

1. Start the case study in TIACRITIS.
2. Select the **Hypothesis** menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains several hypotheses to select from.
3. Select the hypothesis analysis problem: “Assess whether Jihad Bis Sayf will set-off a dirty bomb in the Washington DC area.” Once this hypothesis is selected the **Reasoner** is automatically invoked to analyze the hypothesis, as shown in Figure 22 (pg. 35).
4. Select the **Test** menu on the top of the window. As a result, TIACRITIS generates the first test question, as illustrated in Figure 52.

The top part of the right panel in Figure 52 shows the reduction of a problem related to the analysis of the believability of an item of evidence. Under it, it displays the description of the item of evidence and the entire item of information from which it was extracted. This is either an omission or a modification test question. Therefore, as shown in the left panel, TIACRITIS asks you to characterize the reasoning from the right panel either as **[CORRECT]** (meaning that solving the top problem can be reduced to solving the indicated sub-problems), as **[INCOMPLETE]** (meaning that the sub-problems are correct, but some of the sub-problems are missing), or as **[INCORRECT]** (meaning that some of the sub-problems are incorrect).
5. In the left panel, click on **[HINT]**. As a result, TIACRITIS displays a hint to answer the question, as illustrated in Figure 53.
5 Assessing the Believability of Evidence

Figure 52. Sample test question generated by TIACRITIS.

EVD-026-Yasmin-Afghan: Our a source code-named "Yasmin" tells us that she knew a man in Saudi Arabia named Omar al-Massari. Yasmin says she is "quite sure" that Omar spent two years "somewhere" in Afghanistan "sometime" in the years 1998-2000.


6. In the left panel, click on [INCORRECT]. Notice in Figure 54 the explanation provided by TIACRITIS of why this is not the right answer.
7. Notice also the information displayed by TIACRITIS in the top part of the left panel. “Test 1/6” indicates that this was the first question out of a sequence of 6 questions. “Score: 0” indicates how many questions you have answered correctly up to this point.
8. In the left panel, click on [NEXT] to request a new test question, and TIACRITIS will generate the second test question.

In this illustration this happens to be a construction-type question (see Figure 55). However, as mentioned above, the test questions are randomly generated and the questions that you will receive will most likely be different. The right panel shows a problem and several potential sub-problems. You will need to select a complete and correct set of sub-problems.

![Figure 55. A construction-type question generated by TIACRITIS.](image)

9. Click on [SELECT] following the first sub-problem and notice that this sub-problem is copied under the top-level problem.

10. Click on [SELECT] following the fourth sub-problem and notice that this sub-problem is also copied under the top-level problem, as illustrated in Figure 56.
11. Click on [DONE] in the right panel and TIACRITIS will assess your solution, as shown in the left panel of Figure 57.

12. Continue asking for new test questions by clicking on [NEXT] and answers them.

13. When [NEXT] is no longer selectable, you have exhausted the sequence of test questions.

14. Select Case Study.

15. If you wish to end the case study, click on [SAVE & FINISH] at the end of the instructions.

16. If you wish to retake the test with new test questions then perform the following operations:
   - Click on the Case Study.
   - Click on [DISCARD YOUR ANALYSIS AND RESTART] in the right panel.
• Follow the above instructions, starting with “Select Hypothesis.”

Figure 57. Sample TIACRITIS feedback for a correct answer.
6 CHAINS OF CUSTODY

6.1 What Is a Chain of Custody?

In the previous sections we have discussed the different types of evidence (such as testimonial or tangible), and the ingredients of their believability assessment. However, very rarely if ever does the analyst have access to the original evidence. Most often, what is being analyzed is an item of evidence that has undergone a series of transformations through a chain of custody. Here we have borrowed an important concept from the field of law, where a chain of custody refers to the persons or devices having access to the original source evidence, the time at which they had such access, and what they did to the original evidence when they had access to it. The original evidence may be altered in various ways at various links in chains of custody. The important point here is to consider the extent to which what the analyst finally receives is an authentic and complete account of what an original source provided. Uncertainties arising in chains of custody of intelligence evidence are not always taken into account. One result is that analysts are often misled about what the evidence is telling them.

Basically, establishing a chain of custody involves identifying the persons and devices involved in the acquisition, processing, examination, interpretation, and transfer of evidence between the time the evidence is acquired and the time it is provided to intelligence analysts. Lots of things may have been done to evidence in a chain of custody that may have altered the original item of evidence, or have provided an inaccurate or incomplete account of it. In some cases, original evidence may have been tampered with in various ways. Unless these difficulties are recognized and possibly overcome, intelligence analysts are at risk of drawing quite erroneous conclusions from the evidence they receive. They are being misled, not by our original sources of evidence, but by the activities of our own persons or devices who do various things to incoming intelligence evidence.

In civilian and military courts, proponents of evidence, for either side of the matter in dispute, are required to verify the chain of custody of tangible evidence before it is admitted to trial. In many cases, evidence gathered is passed from one person to another, each of whom may examine and process the evidence in various ways. In many situations, proponents are required to select experienced and credible persons who serve as evidence custodians. The major task for these persons is to establish the chain of custody of evidence keeping records of who gathered the evidence, the persons who had access to the evidence, the times at which they had access, and what these persons did with the evidence while they had access to it. A very good account of questions regarding the chains of custody of evidence in our courts is to be found in the book by Lempert, Gross, and Liebman (2000, pp. 1167 – 1172).

Now, we are of course not privy to the actual chains of custody of various forms of intelligence evidence in any of our intelligence organizations. And we do not know whether there are any appointed evidence custodians in these organizations as there are in our legal system. However, we can offer accounts of chains of custody of evidence that seem reasonable and necessary for different forms of
evidence. In our examples of how TIACRITIS can assist analysts to establish the believability of evidence, we have established conjectural accounts of chains of custody for an item of testimonial and an item of tangible evidence in order to illustrate the virtues of TIACRITIS and how it can assist the intelligence analyst to make these very difficult believability assessments.

First, suppose we have an analyst who is provided with an item of testimonial evidence by an informant who speaks only in a foreign language. We assume that this informant’s original testimony is first recorded by one of our intelligence professionals then translated into English by a paid translator. This translation is then edited by another intelligence professional and then the edited version of this translation is transmitted to an intelligence analyst. So, there are four links in this conjectural chain of custody of this original testimonial item: recording, translation, editing, and transmission. Various things can happen at each one of these links that can prevent the analyst from having an authentic account of what our source originally provided.

Then, suppose that an analyst is provided with an account of a tangible item in the form of a digital photo. This photo has been taken by one of our foreign assets. We note that the analyst may see a copy of the photo itself, or just a written account of the events recorded in this photo. Suppose in this case the analyst only receives a written account of what this original photo revealed. We have supposed that this digital photo is first transferred to the computer of one of our intelligence professionals; it is then transmitted to a photo interpreter; the image is interpreted by this person; and then the written interpretation of this photo is transmitted to the analyst. So, in this conjectural chain of custody there is a transference link, an interpretation link, and two transmission links. At any of these links there are possible reasons why what the analyst receives is not an authentic account of what the asset’s original photo depicted.

There are many possible chains of custody, for different types of evidence, as illustrated in Figure 58. However, they can all be characterized by a chain of basic evidence transformation processes (such as translation, editing, or transmission). Moreover, for each such process, one can identify the ingredients and the arguments of its believability assessment, just as for the different types of the evidence. TIACRITIS employs a systematic approach to the assessment of the believability of items of evidence obtained through a chain of custody (Schum et al., 2009a).

With these evidential and chain of custody ideas in mind, we can now show how TIACRITIS can assist intelligence analysts to assess the many sources of uncertainty associated with the authenticity of evidence they receive. We first provide a case study illustrating the matters we have just mentioned.

The cover story for this hypothetical case involves an experienced analyst named Clyde who is involved with intelligence analyses concerning matters in Iraq. Clyde’s present inferential problem involves an Iraqi named Emir Z., a respected official of the existing government in Iraq. Emir Z. has publicly argued on many occasions about the necessity of stopping the sectarian violence that has plagued Iraq and coalition efforts to achieve stability in this country since the U.S. and coalition intervention in 2003. Clyde’s present problem is that he wonders how respectable Emir Z. really is. Clyde has evidence that Emir Z. has been in contact in Iran with representatives of the Iranian Islamic
Revolutionary Guards Corp (IRGC). We already have a variety of strong evidence that the IRGC has been involved in supplying weapons, training, and intelligence to various Shiite militia groups in Iraq. This has certainly not contributed to stability in Iraq, and is against the interests of the coalition forces in Iraq. So, Clyde entertains the hypothesis \( H_1: \) “Emir Z. is collaborating with the IRGC” (i.e., he is not the respected official we have believed him to be).

So far, Clyde has two items of evidence bearing on \( H_1:\)

He first has an item of testimonial evidence from a source code-named “Wallflower” who reports that five days ago he saw Emir Z. leaving a building in Ahwaz, Iran in which the IRGC has offices. Wallflower, an Iranian national, issued his report in the Farsi language that was recorded and then translated into English by a paid interpreter. Then an edited version of this translation is recorded and transmitted to Clyde.

Then Clyde receives an item of tangible evidence in the form of a photograph taken of Emir Z. eight days ago at an IRGC Qods Force base outside Dezful in Iran. This photo was taken by another source, code-named Stovepipe. The identification of Emir Z. in this photo was verified by one of the U.S. intelligence professionals who has had contact with Emir Z. We will assume that Clyde receives this photo together with a written account of what this photo revealed. But we also allow for the possibility that Clyde receives only a written account of the contents of this photo.

Here is a summary account of the inferential problems Clyde faces as he attempts to assess how believable he imagines these two items of evidence to be. We begin by examining the credibility and competence of Clyde’s original sources, Wallflower and Stovepipe.
Wallflower provides testimonial evidence in the form of an assertion he made concerning Emir Z. leaving the IRGC building in Ahwaz, Iran. Wallflower says he based this assertion on his direct observation of these events five days ago. In deciding whether to believe Wallflower, Clyde must first consider both Wallflower’s competence and his credibility, as discussed in Section 5.4. Wallflower’s competence involves his access and his understanding. The basic access question involves asking whether Wallflower was actually in a position to observe what he tells Clyde. The understanding question asks whether Wallflower knew enough about what he was observing to give Clyde an intelligible account of what he observed. His credibility involves the veracity, objectivity, and observational sensitivity attributes we mentioned above.

Stovepipe, on the other hand, supplies tangible evidence in the form of a photo he says he took eight days ago of Emir Z. at an IRGC base outside Dezful, Iran. Considering Stovepipe himself, Clyde must first consider Stovepipe’s competence. What evidence does Clyde have that Stovepipe was actually in Dezful at the time he says he took the photo? In addition, what evidence does Clyde have that Stovepipe knew the person he was photographing? Clyde also has one credibility attribute for Stovepipe to consider, namely his veracity. Was Stovepipe truthful in telling us when, where, how, and why he took this photo? We will assume that we are treating the photo provided by Stovepipe as being demonstrative tangible evidence. There are several reasons why this makes sense: First, we have the believability of the photo itself to consider. Is this photo authentic (Is it what it is represented as being, namely Emir Z. at the IRGC base outside Dezful, Iran)? Second, has this evidence come from a reliable sensing device that would supply us with repeatable information? Third, is the evidence accurate in allowing Clyde or anyone else to tell whether it was really Emir Z. in the photo? These three matters all concern the credibility of the photo itself.

But Clyde has other sources of uncertainty to worry about, ones that concern the chains of custody through which these two intelligence items have passed before Clyde receives accounts of these items. Here we present two conjectural chains of custody, one for the testimonial item from Wallflower and one for the tangible item from Stovepipe. The reader may quickly note other links in these chains of custody that we have overlooked, or have different labels for the ones we have included. Not being privy to any actual chains of custody of intelligence evidence, our conjectural chains of custody may lack realism. But our claim is that they are plausible enough to illustrate the kinds of uncertainties encountered in chains of custody of intelligence evidence and also to illustrate how TIACRITIS can assist analysts in making these kinds of assessments.

First, Clyde has not heard Wallflower’s original testimony and could not possibly have understood it unless Clyde speaks Farsi. We have identified a case officer named Bob who may only speak limited Farsi. Bob records what Wallflower has testified on a Sony XYZ recording device. This recording is transmitted to a paid foreign national named Husam A. who speaks fluent Farsi. Husam’s written translation of Wallflower’s testimony about Emir Z. is then transmitted to a reports officer named Marsha. Marsha edits Husam’s translated version of Wallflower’s testimony and prepares her written edited version for transmission over a (fictitious) system we will call SN 247. What Clyde receives is Marsha’s edited version of Husam A’s translation of Wallflower’s original testimony. This is a tangible item that is only an account of what Wallflower originally said. This account can only be regarded as
demonstrative tangible evidence whose authenticity, reliability, and accuracy are at issue due to the uncertainties arising at each link in the chain of custody through which Wallflower’s original testimony has passed.

Now consider the tangible photo that Stovepipe has provided. First, suppose Stovepipe used an Olympus #AB1 digital camera to take the photo of Emir Z. We suppose that Stovepipe had some means for transferring this digital photo to case officer Bob’s laptop computer. Bob then transmits this stored digital photo to a photo interpreter we shall name Mike. Mike examines the photo to assess its authenticity, and he also verifies that the person depicted in the photo is Emir Z. Mike prepares a written account of his analysis of this photo. Mike then transmits his written account of this photo, and possibly a copy of the photo itself over our (fictitious) SN 247 system. This written account of the photo, and possibly a copy of the photo, is eventually routed to Clyde for his analysis.

The point of this case study is to illustrate the array of uncertainties our analyst Clyde encounters in his efforts to assess the extent to which he and others might believe the testimonial and tangible evidence he has received from Wallflower and Stovepipe. Some of these uncertainties concern these two sources themselves, and others concern what was done to their original evidence in their chains of custody. We now consider how TIACRITIS can assist Clyde in coping with these many uncertainties.

6.2 A Chain of Custody for Testimonial Evidence

As we just noted, several things were done to Wallflower’s and Stovepipe’s evidence before it could be considered by Clyde. Different people had custody of these two items of evidence and did various things to them before Clyde actually saw them. Figure 59 show a specific (hypothetical) example of what might be involved in the chain of custody of Wallflower’s original testimonial evidence.

The major issue here is the extent to which Clyde can believe what he is told Wallflower said. This belief rests not only on evidence regarding Wallflower’s competence and credibility, but also on the competence and credibility issues raised by what was done to Wallflower’s original report about Emir Z. before Clyde received a report of what Wallflower testified. First and foremost, we have the competence and credibility of our primary source of this testimony, Wallflower. Then we are concerned with how authentic is the account of Wallflower’s testimony that is provided for the person, Clyde, who will use this account: Are we sure that this account actually records, completely and accurately, what Wallflower reported? Bear in mind here that Clyde has never seen or talked to Wallflower himself.

Figure 59 is a representation of a possible chain of custody for testimonial evidence such as Wallflower’s. In this example we have three identified persons involved in the chain of custody of Wallflower’s report: case officer Bob, translator Husam A., and reports officer Marsha. Now one thing about this fictitious example is that the analyst, Clyde, may or may not know the identities of these three persons. Obviously, in an actual situation, there may be more or different persons involved in a chain of custody.
The top part of Figure 59 shows the successive transformations suffered by Wallflower’s original testimony (called EVD-001-Wallflower-testimony) until it reaches Clyde, who actually receives the item of evidence called EVD-005-Emir-Iran. The bottom part of Figure 59 shows the competence and credibility issues that can arise regarding the persons and the devices involved in this example.
What follows is the interpretation of the chain of custody shown in Figure 59 and the believability-related issues regarding the processes at each link in this chain.

First Wallflower’s testimony (EVD-001-Wallflower-testimony) was tape-recorded by the case-officer Bob, who interacts with Wallflower. So, we have natural concerns about the fidelity and reliability of this tape recording, as well as about Bob’s competence and veracity. Among other things, is the recording understandable and complete? Was all of Wallflower’s testimony on the recording and did no gaps appear in it? Clyde would also be interested to know whether Wallflower provided his report voluntarily or whether he was asked to report on Emir Z. by Bob. This is quite important since if Wallflower gave this report voluntarily and we believe he is being untruthful, Clyde has to ask why Wallflower told Bob this particular lie in preference to any of the others he might have told. The same question will arise for Stovepipe’s evidence.

As we have specified, Wallflower speaks only Farsi and not English, and Husam A. has translated his recorded testimony (i.e., EVD-002-Bob-recording) into English. We have concerns here about the competence and credibility of Husam A. Competence involves not only knowledge of Farsi and English, but also knowledge of the subject matter being translated. The translated account of Wallflower’s original testimony (i.e., EVD-003-Husam-translation) is then edited by Marsha. We may also have concerns about Marsha’s competence and credibility.

Finally, this recorded, translated, and edited account of Wallflower’s testimony (i.e., EVD-004-Marsha-report) is transmitted through a computer network to Clyde and possibly many other interested persons. What we have here are concerns both about the competence and the credibility of the person who performed the transmission, and also about the fidelity, reliability, and security of the transmission.

6.3 A Chain of Custody for Demonstrative Tangible Evidence

Unfortunately, regarding the photo of Emir Z., allegedly taken outside of Dezful, Iran, eight days ago, we have two possibilities to consider. We have to consider whether Clyde was given a copy of this photo to examine himself, or whether he was just given a written account of what this photo depicted. The major trouble, of course, is that the chains of custody will be different in these two cases. So, we will make some conjectures about what the chains of custody might look like in both of these cases. The first is where Clyde is given the photo to examine; the second is where he is just given a written account of what is in Stovepipe’s photo.

6.3.1 Chain of Custody for a Photo Given Directly to the Analyst

We will begin with the case in which Clyde sees Stovepipe’s photo itself or, more than likely, a copy of Stovepipe’s original photo. The corresponding chain of custody involves the persons and processes shown in Figure 60. The top part of Figure 60 shows the successive transformations suffered by Stovepipe’s original photo of Emir Z. (called EVD-006-Emir-photo-in-camera) until it reaches Clyde (as EVD-010-Emir-Iran). The photo was transferred by Bob on his laptop, and then transmitted electronically to Mike’s computer. Mike interpreted the photo and then transmitted both the photo and its
interpretation to Clyde. The bottom part of Figure 60 shows the competence and credibility issues that can arise regarding the persons and the devices involved in this example.

In this example, we have chosen to have Stovepipe use a digital camera to eliminate the necessity of considering by whom and where the photo was developed. We will also assume that Stovepipe, who knows Emir Z., was instructed to follow Emir Z. eight days ago in Dezful, to see where he went that day.

Additionally, we also will assume that Stovepipe was able to visit Bob, bringing his digital camera with him. There are, of course, other means by which Stovepipe might have communicated with Bob. If Stovepipe had a laptop computer, he could have e-mailed the message to Bob, who could have been anywhere. But this would add additional risks involving the e-mail being intercepted by the Iranian IRGC. Surely, there are risks associated with Stovepipe’s meeting personally with Bob. It took Stovepipe eight days between the time he took the photo and the time he delivered it to Bob. How Stovepipe actually got the photo to Bob is interesting and will eventually bear on Stovepipe’s competence and the authenticity of the photo. Maybe the procedures necessary for Stovepipe to communicate directly with Bob are very complex and have been designed to reduce the risks associated with this direct communication. For example, suppose Bob is in Baghdad, Iraq, but meets with Stovepipe in Al Amara, Iraq. Both cities are near the Iraq-Iran border, about 80 miles from each other. Perhaps it takes several days for Stovepipe to communicate with Bob and then arrange the cover necessary to go into Iraq. These are all matters that bear upon Stovepipe’s competence and may also concern the authenticity of the photo.

But the major assumption underlying this scenario concerns whether or not we can say that Clyde is provided with the original photo that Stovepipe allegedly took. This involves the assumption that the image Bob uploaded on his computer and then transmitted to Mike was not altered in any way, nor was the image that Mike transmitted to Clyde altered. If the image that Clyde received had exactly the same pixels as the one on Bob’s computer, we could probably say that Clyde received the same original photo that Bob received from Stovepipe.
Figure 60. Chain of custody of demonstrative tangible evidence sent to Clyde.
6.3.2 Chain of Custody for a Written Description of a Photo Given to the Analyst

This second case is interesting for the following reason: We are treating the photo as being demonstrative tangible evidence since it is just a possible representation of Emir Z. being outside of Dezful eight days ago. Then, if Clyde is only given a written account of this photo, this is only demonstrative evidence of Stovepipe’s original demonstrative evidence. So, in cases such as this, we have a chain of demonstrative evidence involving two or more sources.

The above discussion shows how complex the processes of analyzing the likelihood of hypothesis \( H_1: \text{Emir Z. is collaborating with the IRGC} \) are, even when we have just a small amount of evidence. However, for a good analysis, one would have to consider many more items of evidence, and to consider both favoring and disfavoring evidence. Unfortunately, the complexity of the analytic process grows so much with the addition of new items of evidence that all the involved probabilities cannot be assessed. There is simply not enough time for the analyst to assess them, or evidence necessary to support these assessments is not available.

However, we now describe how our cognitive assistant TIACRITIS allows the analyst Clyde to perform the complex analysis involved in chains of custody of evidence. Clyde will be allowed to drill-down as much as he wishes; the can make assumptions concerning various verbal assessments of uncertainty, and revise these assumptions in light of new evidence.

6.4 Case Study: Analyzing a Chain of Custody

Let us consider again the process illustrated in Figure 59. As discussed above, the believability of EVD-005-Emir-Iran (the evidence received by Clyde about Emir Z.) is a function of the believability of EVD-004-Marsha-report and that of the transmission process; the believability of EVD-004-Marsha-report is a function on the believability of EVD-003-Husam-translation and that of the editing process; the believability of EVD-003-Husam-translation is a function on the believability of EVD-002-Bob-recording and that of the translation process; and, finally, the believability of EVD-002-Bob-recording a function on the believability of EVD-001-Wallflower-testimony (the original testimony) and that of the recording process. Thus, the believability of the evidence received by Clyde is a function of the believability of the Wallflower’s original testimony and the believability of the recording, translation, editing, and transmission processes.

An important aspect of TIACRITIS is that it has already been taught a great deal about the credentials of evidence and about the ingredients of believability assessments for tangible as well as testimonial evidence so that it can perform the above analysis, as discussed next. TIACRITIS will use the names introduced in Figure 59 to refer to the considered items of evidence, such as EVD-005-Emir-Iran, EVD-004-Marsha-report, etc.

Clyde’s problem is to assess the believability of EVD-005-Emir-Iran (i.e., Wallflower’s alleged testimony about Emir Z. being in Iran, as received through the chain shown in Figure 59).
This problem, which is shown in the upper-right side of Figure 61, is represented as:

“Assess the extent to which EVD-005-Emir-Iran is believable.” \[P1\]

TIACRITIS reduces this problem to two simpler hypothesis analysis problems, guided by a question and its answer:

“How was EVD-005-Emir-Iran obtained?”

“As the transmission of EVD-004-Marsha-report by Marsha with SN 247.”

Therefore I have to

“Assess the extent to which EVD-004-Marsha-report is believable.” \[P2\]

“Assess the extent to which one can believe the transmission of EVD-004-Marsha-report into EVD-005-Emir-Iran by Marsha with SN 247.” \[P3\]

Let us assume that the solutions of problems \[P2\] and \[P3\] are those shown at the bottom of Figure 61:

“It is an even chance that the information provided by EVD-004-Marsha-report is believable.” \[S2\]

“The believability of the transmission of EVD-004-Marsha-report into EVD-005-Emir-Iran by Marsha with SN 247 is almost certain.” \[S3\]

These solutions are combined into the following solution of problem \[P1\] (by taking the minimum of “an even chance” and “almost certain”):

“It is an even chance that the information provided by EVD-005-Emir-Iran is believable.” \[S1\]

As discussed in Section 2.4, TIACRITIS uses symbolic probabilities (see Figure 17 on page 30) to express the solutions of the problems. Notice also that some words appear in blue. They correspond to entities that are represented in the knowledge base of TIACRITIS.

Figure 61 shows only the top part of the problem reduction and solution synthesis tree for problem \[P1\]. The problems from the bottom of Figure 61 (i.e. \[P2\] and \[P3\]) are themselves reduced, in a similar way, to simpler and simpler problems, guided by questions and answers. This problem reduction process continues until the resulting problems are simple enough to find their solutions. Then these solutions are successively combined, from bottom-up, to synthesize the solutions of the upper-level problems, until the solution of the top level problem is obtained. Overall, the entire reasoning tree is quite large.
To help browse and understand such a complex analysis, TIACRITIS displays a simplified version of it, as discussed in Section Error! Reference source not found. and illustrated in the left-hand side of Figure 61. As one can see, under the short name of the initial problem and its solution (i.e. “Believability EVD-005-Emir-Iran: an even chance”), TIACRITIS lists the short names of the bottom problems from the right side of Figure 61 and their solutions:

“Believability EVD-004-Marsha-report: an even chance”
“Believability Transmission: almost certain”
The left hand side of Figure 62 shows a summary of the believability analysis generated by TIACRITIS for EVD-005-Emir-Iran, which corresponds to the scenario from Figure 59.

Because “Believability EVD-004-Marsha-report” was selected in the left-hand side of Figure 62, the right hand side of this figure shows the detailed reduction of this problem.

The left hand side of Figure 63 shows the expansion of the analysis for “Believability EVD-001-Wallflower-testimony,” which takes into account the competence and the credibility of Wallflower.
6.5 Drill-Down Analysis of Chains of Custody

As indicated above, the analyst may not have the time or the evidence to assess all the factors involved. In such a case, TIACRITIS allows him/her to make assumptions with respect to the solutions of the unsolved problems. As illustrated in Figure 64, the analyst may assume that the believability of most of the processes involved in the chain of custody is almost certain, and concentrate his analysis on assessing the credibility of Wallflower. He may further make some assumptions about Wallflower’s competence, veracity, objectivity, and observational sensitivity, and then TIACRITIS will automatically estimate the overall believability of EVD-005-Emir-Iran. Yellow background in Figure 64 indicates that the enclosed solution is an assumption.
But the analyst can drill-down to analyze each of the processes from the chain of custody. For example, Figure 65 shows the analysis of the Recording performed by Bob. TIACRITIS was able to automatically estimate the quality of the recording as “almost certain,” based on its knowledge about the general fidelity and reliability of a Sony XYZ recorder. However, the believability of Bob was assumed by Clyde as “almost certain.” TIACRITIS also allows the analyst to investigate all sorts of “what-if” scenarios. For example, Clyde may consider alternative values for the veracity of Husam A., the translator of Wallflower’s testimony. When this veracity changed from “an even chance” to “unlikely,” the overall assessment of the believability of EVD-005-Emir-Iran changed from “an even chance” to “unlikely.”
As illustrated above, TIACRITIS can automatically generate a detailed and rigorous analysis. However, given the astounding complexity of many intelligence analyses, and the often-limited time to complete them, TIACRITIS also allows the user to perform analytic tasks at several levels of detail; i.e., the analyst can “drill down” to deeper levels depending upon the time available and the evidence necessary to support more detailed levels of analysis. Users are allowed to state various assumptions, to believe “as if,” or to “give benefit of doubt” in these situations.
7 RECURRENT SUBSTANCE-BLIND COMBINATIONS OF EVIDENCE

7.1 Introduction

We have considered a categorization of individual items of evidence but have also mentioned situations in which individual items can reveal various mixtures of the types of evidence shown in Figure 41. We now consider combinations of two or more individual items of evidence. These combinations are also recurrent and do not involve the substance or content of the evidence. One reason for carefully considering these combinations of evidence is that they are often confused or incorrectly identified as leading to mistakes in how the evidence is described in an analysis. But perhaps the most important reason is that there are very important sources of uncertainty lurking in these evidential combinations.

There are three main classes of evidence combinations: harmonious, dissonant, and redundant, all of which we may encounter in a mass of evidence being considered in an intelligence analysis, or an analysis in any other context. However, before we discuss them, let us continue with our dirty bomb analysis from earlier sections which will provide us with examples of various evidence combinations. Having been established that the available evidence favors the hypothesis that the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck, the next step is to identify who has actually stolen it. A natural suspect is Omer Riley who has rented the MDC-578 truck. As indicated by INFO-009-Santa in Table 8, our asset, Santa, has given us significant leads for getting additional information about our suspect. This has led to our obtaining of INFO-010-Test and INFO-011-Walsh. The information from Table 8 and the corresponding dots in Table 9 suggest the following scenario: Omar al-Massari rented the MDC-578 truck, giving his alias, Omer Riley, and a false address, and then used it to steal the cesium-137 canister, which in turn caused it to become contaminated because cesium-137 is a radioactive material. This leads to the development of the hypothesis analysis tree from Figure 66.

Table 8. Information on the presumed stealing of the cesium-137 canister.

| INFO-009-Santa: | An asset code-named “Santa” tells us that the name Omer Riley is one of the aliases used by a person named Omar al-Massari, who came to the USA in 2000, apparently from Saudi Arabia, on an extended work permit. Omar al-Massari is a physicist employed for the past two years by the Ultratech company in Silver Spring. He lives with two other males at 403 Winston Road in Silver Spring. Santa also tells us that Omar al-Massari (alias Omer Riley) is intimately associated with an unnamed jihadist organization in the Washington, DC area. |
| INFO-010-Test: | Omar al-Massari (alias Omer Riley) was apprehended at his place of work at the Ultratech company in Silver Spring. During his questioning, he was given a test called “whole body counting” with a Geiger counter that can detect the gamma radiation emitted by cesium-137. This test indicated the presence of traces of cesium-137 on his skin and hair. |
| INFO-011-Walsh: | The president of Ultratech company, a Mr. John Walsh, reported that Omar al-Massari’s (alias Omer Riley) work at Ultratech does not involve his handling any radioactive substances. |
Table 9. Dots from Table 8.

**EVD-014-SantaAlias**: Santa’s testimony that Omer Riley is an alias used by Omar al-Massari.

**EVD-015-SantaWork**: Santa’s testimony that Omar al-Massari is a physicist employed for the past two years by the Ultratech company in Silver Spring.

**EVD-016-SantaAdr**: Santa’s testimony that Omer Riley lives with two other males at 403 Winston Road in Silver Spring.

**EVD-017-SantaTerOrg**: Santa’s testimony that Omar al-Massari (alias Omer Riley) is intimately associated with an unnamed jihadist organization in the Washington, DC area.

**EVD-018-OmarTest**: “Whole body counting” test result on Omar al-Massari (alias Omer Riley) with a Geiger counter indicating traces of cesium-137 on his skin and hair.

**EVD-019-Walsh**: Walsh’s testimony that Omar al-Massari’s work does not involve handling of radioactive substances.

---

Assess whether the cesium-137 canister was stolen by Omar al-Massari.

Which is possible scenario?

Omar al-Massari rented the MDC-578 truck giving his alias, Omer Riley, and a false address, used it to steal the cesium-137 canister and was contaminated because cesium-137 is a radioactive substance.

What factors should we assess?

The alias, the rental, and the address.

Assess whether Omer Riley is an alias of Omar al-Massari.

Assess whether Omar al-Massari rented the MDC-578 truck giving his alias, Omer Riley, and a false address.

What factors should we assess?

Traces of cesium-137 and their explanation.

Assess whether there are traces of cesium-137 on Omar al-Massari.

Assess whether Omer Riley rented the MCD-578 truck using a false address.

What factors should we assess?

That an address was provided and it was false.

Assess whether Omer Riley provided a certain address to rent the MCD-578 truck.

Assess whether the address provided by Omer Riley to rent the MCD-578 truck is false.

Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.

Assess whether Omar al-Massari was contaminated by being in contact with the cesium-137 canister.

Assess whether the cesium-137 canister was stolen by Omar al-Massari.

Which is possible scenario?

Omar al-Massari rented the MDC-578 truck giving his alias, Omer Riley, and a false address, used it to steal the cesium-137 canister and was contaminated because cesium-137 is a radioactive substance.

Assess whether Omar al-Massari rented the MDC-578 truck giving his alias, Omer Riley, and a false address.

Assess whether Omer Riley is an alias of Omar al-Massari.

Assess whether Omer Riley rented the MCD-578 truck.

Assess whether Omer Riley provided a certain address to rent the MCD-578 truck.

What factors should we assess?

That an address was provided and it was false.

Assess whether the address provided by Omer Riley to rent the MCD-578 truck is false.

Figure 66. Analysis tree for the hypothesis that the cesium-137 canister was stolen by Omar al-Massari.
7.2 Case Study: Hypothesis Analysis Review

It is not necessary to perform this case study in order to understand the combinations of evidence discussed in the follow-on sections of this chapter.

7.2.1 Objective

This case study has two main objectives:

- Improving your understanding of the evidence-based hypothesis analysis process by analyzing a more complex hypothesis.
- Providing an example for illustrating various types of evidence combinations.

7.2.2 Summary

The available evidence suggests a scenario where Omar al-Massari rented the MDC-578 truck giving his alias, Omer Riley, and a false address, used it to steal the cesium-137 canister and was contaminated because cesium-137 is a radioactive substance. As a result, you will assess the hypothesis that the cesium-137 canister was stolen by Omar al-Massari.

Proceed as indicated in the following instructions.

7.2.3 Instructions

1. Start this case study in TIACRITIS.
2. Select the Hypothesis menu and then select the hypothesis analysis problem: “Assess whether the missing cesium-137 canister was stolen by Omar al-Massari.”
3. Browse the analysis of the above hypothesis to see how it is reduced to simpler hypotheses that need to be assessed based on the available evidence.
4. Select Evidence. Then, in the left panel, click on [COLLECTED INFORMATION]. As a result, the left panel shows the collected items of information.
5. Click on the name of each information item you are not familiar with and read its description in the right panel.
6. In the left panel, click on [AVAILABLE EVIDENCE]. As a result, the left panel shows the evidence extracted from the collected information.
7. Associate the evidence items to the hypotheses they are relevant to, estimate their relevance and believability and specify them as assumptions.
8. Browse the final analysis tree.
9. Select Case Study.
10. If you wish to end the case study, click on [SAVE & FINISH] at the end of the instructions. You will be able to resume it at a later time. Otherwise, perform the following operations:
11. Click on the Case Study.

12. Select one of the following commands in the right panel:

- [SAVE & FINISH]
- [CANCEL]
- [FINISH WITHOUT SAVING]
- [SAVE]
- [DISCARD YOUR ANALYSIS AND RESTART]

7.3 Harmonious Evidence

7.3.1 Basic Forms of Harmonious Evidence

Two or more items of evidence are harmonious if they are directionally consistent in the sense that they all point toward, or favor, the same hypothesis or possible conclusion. There are two basic forms of harmonious evidence. The first is called corroborative evidence. In this combination of evidence we first have two or more sources telling us that the same event has occurred. Suppose both of these sources report that event E has occurred. Directional consistency is apparent here since E is consistent with itself. The sources of corroborative evidence may be any combination of the “INTs” we have mentioned. For example, we may have both IMINT and HUMINT telling us that a certain event has occurred at a location at a certain time. Or, we may have IMINT and COMINT both saying that a certain event occurred. This form of corroboration often, but not always, allows us to have greater confidence that the event in question did occur. In such cases we would say that one source has verified what the other source has told us. The exception involves instances in which we have other evidence suggesting that two or more HUMINT sources collaborated in deciding what to tell us, or that one source influenced or coerced another source to report the same event. As we know, HUMINT sources are frequently not independent; they can interact in ways designed to deceive us.

But there is another way evidence can be corroborative in nature involving items of directly relevant and ancillary evidence. Suppose HUMINT asset $A$ reports an event we take to be directly relevant in an analysis. Suppose that in assessing $A$’s believability we have ancillary evidence that we believe supports an attribute of $A$’s believability. Such evidence would be corroborative in the sense that we gain further confidence that the event $A$ reports did in fact occur. An example would involve information about $A$’s track record in his previous reports (if he made any). Such ancillary evidence would support $A$’s veracity or observational sensitivity as far as his present report is concerned. But ancillary evidence can bear upon a human source’s competence as well. In assessing asset $A$’s competence we may have evidence from another asset $B$ who says that $A$ could in fact have made the observation $A$ says he made. We could also verify $A$’s competence by IMINT showing that $A$ was at the place where he says he made his observation.

But there is another combination of harmonious evidence that differs from corroborative evidence of the same event; it is called convergent evidence. This combination of evidence involves two or more
evidence items that concern different events which point toward or favor the same hypothesis. Convergent evidence can involve any of the “INTs.” Suppose we have the following situation. We have IMINT evidence that event E occurred, and we have MASINT evidence that event F occurred. But we believe that both of the events E and F would point to or favor the same hypothesis H. In other words, these two events are directionally consistent; they both point us in the same inferential direction. But convergent evidence can have an additional and most important property that we will now explain.

Convergent evidence can exhibit what is called evidential synergism. In many situations, two or more evidence items, considered jointly, have greater inferential force or weight than they would have if considered separately or independently. Another equivalent way to characterize evidential synergism is to say that one item of evidence can have greater force if we consider it in light of other evidence we have. Suppose again that we have evidence about events E and F that converge in favoring hypothesis H. But when taken together, or considered jointly, these two events have additional force favoring hypothesis H. Additionally, we might observe that evidence about event F seems to have more force or weight when we consider it in light of evidence about event E. One quite tragic example of our failure to exploit evidential synergism involves events that occurred before September 11, 2001. The FBI had evidence of persons from the Middle East who arrived at flying schools here in the U.S.A. paying in cash for their flying lessons. But these students wished only to learn how to steer and navigate heavy aircraft, and not how to make takeoffs and landings in these aircraft. At the same time, our intelligence services had evidence that new attacks would be made on the World Trade Center in New York, this time using airliners. Unfortunately, for various reasons, these items were never considered jointly and hypotheses suggested by these joint events were never considered. What it comes to is that important evidential synergisms will never be recognized unless intelligence evidence is shared among all agencies involved in its collection and analysis. We have written more on the probabilistic underpinnings of evidential synergism (Schum, 1994/2001, pp. 401-409), and have provided additional interpretations of the example just given (Anderson et al., 2005, pp.46-50).

7.3.2 Patterns of Evidential Harmony

Recall our saying the harmonious evidence is directionally consistent because all of it points to the same conclusion. Here are some examples and questions:

**Example 10.** In the cesium-137 scenario we have examples of both forms of evidential harmony. The first involves what we called corroborative evidence, in which two or more sources report the same event. Have a look at evidence EVD-001-Willard and EVD-004-Ralph in Table 5. Here we have both Willard and Ralph telling us that the cesium-137 canister was missing from the XYZ company warehouse. Ralph’s report corroborates Willard’s initial report.

**Example 11.** Convergent evidence involves evidence about different events, all of which point to the same conclusion. Look at evidence items EVD-008-MDDOTRecord, EVD-010-TRUXINCRrecord, and EVD-011-SilverSpringRecord from Table 7, all of which point toward the conclusion that Omar al-Massari was the person who rented the truck from the TRUXINC Company in Silver Spring, MD.
Question 8. Can you make up some examples of evidence that corroborates other evidence in our dirty bomb scenario? Ask yourself what items of evidence we now have that you would like to see corroborated.

7.4 Dissonant Evidence

7.4.1 Basic Forms of Dissonant Evidence

Dissonant evidence involves combinations of two or more items that are directionally inconsistent; they can point us in different inferential directions or toward different hypotheses. There are two basic forms of evidential dissonance; the first involves contradictory evidence. Contradictory evidence always involves events that are mutually exclusive (they cannot have occurred jointly). From one source we learn that event E occurred; but from another source we learn that this same event did not occur. The dissonance seems obvious in this case since event E cannot have both occurred and not have occurred. Contradictory evidence can involve any sources of intelligence evidence and any number of sources. For example, we may have some five sources, three telling us that event E occurred and two telling us that event E did not occur. We must first be a bit careful in discussing the directional inconsistency of contradictory evidence. Suppose we are considering whether hypothesis H is true; an obvious alternative is the hypothesis not-H (H is not true). We further believe that event E, if it occurred, would favor hypothesis H. With some views of probability, which we discuss in Section 9, this means that hypothesis not-H would be favored by event E not occurring. However, with another view of probability we will consider, we may not always believe it necessary to say that the nonoccurrence of E favors the nonoccurrence of H. On other occasions we may not even be sure what the nonoccurrence of E is telling us.

In any case, evidential contradictions are always resolved on believability grounds. There is quite an interesting history concerning how we have come to rely on this form of resolution. As an example, suppose we have three HUMINT sources who tell us that event E occurred, and one HUMINT source who tells us that event E did not occur. In the not so distant past, it was believed that we should always resolve the contradiction by counting heads; i.e. majority rules. So, on this basis we would side with the three sources who tell us that event E did occur. The trouble here is that counting heads assumes that all of the four sources involved in this episode of contradictory evidence have equal believability. This may be a very bad assumption since, on ancillary evidence about these four sources, we may well believe that the one source telling us that E did not occur has greater believability than does the aggregate believability of the three sources who tell us that event E did occur. So, what matters in resolving evidential contradictions is the aggregate believability of the sources on either side of this contradiction.

In some accounts we have read, dissonant evidence is described as being necessarily contradictory in nature; but this is quite erroneous. There is another quite different form of dissonant evidence called divergent evidence. Contradictory evidence involves whether one event occurred or did not occur. But divergent evidence involves entirely different events. The directional inconsistency here means that these events point us toward different hypotheses. In one case, suppose credible evidence
about event E would favor hypothesis H, but credible evidence about event F would favor hypothesis not-H. In a more general case, suppose an analyst is considering four hypotheses \( \{H_1, H_2, H_3, \text{ and } H_4\} \). One body of evidence is consistent in pointing most strongly to hypothesis \( H_1 \), while another body of evidence is consistent in pointing most strongly toward \( H_3 \).

Resolving evidential divergences, or evidential conflicts as it is sometimes called, is a more difficult matter than resolving evidential contradictions. Believability assessment does play an important role in both cases, but there is an additional difficulty with divergent or conflicting evidence. Suppose we return to the simple situation in which we have credible evidence items regarding events E and F. Two analysts agree that evidence of E favors hypothesis H but the evidence of F favors hypothesis not-H. A third analyst observes the two analysts who have just agreed that these two evidence items are divergent or conflicting. This third analyst says, “I don’t agree with your assessment of this evidence. The trouble is that you are considering these two evidence items separately. If you consider them together the apparent conflict disappears. The reason is that the occurrence of event E would effectively swamp the occurrence of event F and so there is no conflict here. These two items of evidence taken together makes their dissonance disappear.” So, dissonance involving divergent evidence always calls for an analyst’s judgments on the directionality of evidence about different events. It is often the case that if we knew more about the situation in which different events have occurred we might be able to explain away divergences or conflicts that seem to appear.

### 7.4.2 Patterns of Evidential Dissonance

We discussed two forms of dissonant, or directionally inconsistent, evidence that point us toward different hypotheses or possible conclusions. Such evidence can be either contradictory or divergent. As we mentioned, one of the unrealistic features about our cesium-137 example is that all the evidence we have so far is harmonious in pointing toward the hypothesis that a dirty bomb containing cesium-137 will be set off somewhere in Washington, DC. In short, we have no contradictory or divergent evidence so far. So, we will have to imagine what some items of dissonant evidence might be.

**Example 12.** Consider the evidence provided by John Walsh, the President of the Ultratech company in Silver Spring, MD, at which Omar al-Massari (alias Omer Riley) works (i.e., EVD-019-Walsh in Table 9). Walsh tells us that Omer Riley’s job does not require him to handle any radioactive materials such as cesium-137. But suppose we interview another executive at the Ultratech Company who is more directly familiar with the work Omer Riley actually performs. This person tells us that Omer Riley has worked recently on devices for measuring soil dampness gradients and this work does involve the use of radioactive materials. This contradicts what Walsh tells us and might be used to reduce the force of EVD-019-Walsh concerning the traces of cesium-137 on Omar al-Massari’s body when he was interviewed.

**Example 13.** Suppose we have evidence from another asset code-named “Wonderboy,” who knows Omar al-Massari very well. Wonderboy tells us that Omar al-Massari has recently put a down payment of $25,000 on a house at 2321 23rd St. in the Georgetown area of Washington, DC. This might be divergent evidence suggesting that our main hypothesis (that a dirty bomb containing cesium-137
will be set off somewhere in Washington, DC) is not true after all. Why would Omar al-Massari invest in a house in a city where a dirty bomb is to be set off? We would obviously be interested in the believability of the evidence Wonderboy has given us. Did he rely only on what Omar al-Massari told him, or did Wonderboy see a contract for the sale of this house? It is very possible, of course, that Omar al-Massari is attempting to mislead Wonderboy, whom Omar may suspect has infiltrated a terrorist organization to which Omar belongs.

**Question 9.** Can you think of any contradicting and divergent evidence we might encounter in the cesium-137 example?

### 7.5 Evidential Redundance

#### 7.5.1 Basic Forms of Redundant Evidence

The final recurrent and substance-blind combination of evidence is in effect the opposite of the possible evidential synergism mentioned above for convergent evidence. We often encounter two or more items of evidence in which the first item acts to reduce the force of subsequent items of evidence. Stated another way, the first item acts to make subsequent items redundant to some degree. There are two ways this can happen as we will see.

The first form of evidential redundance involves the corroborative evidence we discussed above in Section 7.3. In this case we have repeated evidence of the same events. Although having corroborative evidence does add to our confidence that an event of interest did occur, each additional item adds less and less to our confidence. At some point we will surely say, “We already believe that this event occurred, we don’t need any further evidence about this event.” We refer to this situation as **corroborative redundance**. The believability of our sources plays a crucial role in determining how redundant successive reports of the same event will be. To illustrate, suppose event E favors hypothesis H and we have successive items of evidence E* 1, E* 2, and E* 3, all telling us that event E occurred. First, suppose we believe that our first source of evidence, the one who provided E* 1, is perfectly credible. In short, we know for sure that event E occurred. In this case, having evidence E* 2 and E* 3 would tell us nothing we do not already know, so they are perfectly redundant. But now suppose that the first source is not perfectly credible. In this case E* 2 can add to the verification that event E occurred, depending on how credible we believe the second source to be. To the extent that the second source is not perfectly credible, the third source can add some additional verification.

The second form of redundancy involves different events in which evidence about one event, if credible, takes something away from the inferential force of evidence about another event. We have called this **cumulative redundance**. The word “cumulative” is an expression used in law to refer to evidence that does not add anything to what we already know. As an example, suppose asset A tells us that it was Omar, the terrorist, who he saw two days ago planting the shaped explosive device that killed two American soldiers outside of Tikrit. Then asset B tells us that he saw someone who looked like Omar planting this device two days ago at this same location outside of Tikrit. We have two different events here; the first source says it was Omar, but the second source only says it was someone who looked like Omar. Suppose we believe that the first source is perfectly credible. Then the report from
the second source is completely redundant. If Omar was there, it follows necessarily that someone who looked like Omar was there. The report of the second source only springs to life if the first source is not credible.

The importance of considering these two forms of evidential redundancy cannot be overstated. In the case of corroborative redundancy we risk double counting evidence about the same event and ascribing additional weight to the evidence which it does not have. In the case of cumulative redundancy we risk getting more inferential mileage out of the evidence than can be justified.

We have now completed our discussion of the substance-blind forms and combinations of evidence. As far as our emphasis on uncertainty is concerned, this discussion was not idle or off point. Different forms and combinations of evidence each raise uncertainty issues that cannot be ignored. No account of the many uncertainties lurking in intelligence analysis would be even barely adequate if we did not consider the forms and combinations of evidence encountered in every intelligence analysis. But we have one more task to perform regarding uncertainty and evidence. There are five characteristics of evidence that make conclusions drawn from it necessarily probabilistic in nature. They are described in detail later in Section 8.

### 7.5.2 Patterns of Evidential Redundance

We mentioned two forms or redundant evidence which we called corroborative and cumulative redundancy. Corroborative redundancy involves repeated evidence of the same event; cumulative redundancy involves evidence about different events. In either case we have instances in which some evidence can reduce the inferential force of other evidence. Here are some examples and questions concerning redundancy:

**Example 14.** Look again at Willard’s and Ralph’s reports in evidence items EVD-001-Willard and EVD-004-Ralph (see Table 5). If we believed that Willard was completely believable in his report that the cesium-137 canister was missing, then Ralph’s report would tell us nothing we do not already know for sure. This would make Ralph’s report completely redundant. Ralph’s report has value to the extent that Willard is not completely believable. But we could have asked other persons if they believed the cesium-137 canister to be missing. Here comes Joe and then Frank who each tell us that the canister was missing. Each new report of the same event tells us less and less depending on the believability of earlier reports of the same event. This is what corroborative redundancy is all about.

**Example 15.** Here is an example of cumulative redundancy. First, recall the evidence item EVD-014-SantaAdr in Table 9, where Santa is telling us that Omar al-Massari lives with two other males at 403 Winston Road in Silver Spring, MD. We interview a person named Martha, who says she saw a person she knows as Omer Riley (the alias Omar al-Massari uses) park a panel truck in the driveway of the house Omer shares with two other males. This would be additional evidence bearing on the event that the terrorist organization (to which Omar al-Massari belongs) will use, or has used, the stolen cesium-137 to construct a dirty bomb. But we have another neighbor, Paul, who tells us that he saw someone, who looked like Omer Riley, park a panel truck in the driveway of the house at 403 Winston Road in Silver Spring, MD. Martha and Paul report different events: Martha says it was Omer Riley, and Paul says
it was someone who looked like Omer Riley. First, suppose we believe Martha to be perfectly credible when she says that it was Omer Riley who parked the panel truck in the driveway at 403 Winston Road. In this case, what Paul tells us would be inferentially valueless. If it was Omer Riley (alias of Omar al-Massari) who parked the truck in the driveway, then it follows necessarily that someone who looked like Omer Riley parked the truck. However, Paul’s report becomes important to the extent to which we believe Martha not to be credible.

**Question 10.** Can you think of other instances of corroborative and cumulative redundant evidence we might encounter in our investigation of the dirty bomb situation?

Figure 67 summarizes the recurrent substance-blind combinations of evidence discussed above.
8 THE MAJOR SOURCES OF UNCERTAINTY IN MASSES OF EVIDENCE

8.1 Introduction

There are five major reasons why conclusions reached in intelligence analysis based on evidence will be necessarily probabilistic in nature: our evidence is always incomplete, usually inconclusive, frequently ambiguous, commonly dissonant, and with various degrees of believability. Any one of these reasons can lead to uncertain conclusions, but an analyst drawing conclusions based on masses of different forms and combinations of evidence will likely encounter all five of these reasons at the same time. Intelligence analysts who report conclusions with varying degrees of uncertainty are often unjustly criticized for doing so. Persons providing such criticisms are doubtless unaware of many or most of the reasons why it is necessary to hedge conclusions in probabilistic terms. One main reason we have for providing a careful account of these five reasons is that no single view of probability we know about captures all five of these sources of uncertainty. Each view of probability we will mention provides useful insights about some of these sources of uncertainty, but no single view says all there is to be said.

We first continue with our dirty bomb analysis to provide a context for examples of the five major sources of uncertainty in evidence-based reasoning. Then we discuss each of these sources of uncertainty.

We have established that the cesium-137 canister was stolen by Omar al-Massari. Now the question is: Who is Omar al-Massari? Is he someone working for a competitor, someone hoping to sell this valuable material, or someone having terrorist connections?

Figure 68 shows the indicators that guide us in collecting evidence to prove that Omar al-Massari has ties to terrorist organizations. As a result, we collect the information in Table 10.

![Figure 68. Evidence collection guided by indicators of terrorist ties.](image-url)
Table 10. Information on the presumed terrorist ties of Omar al-Massari.

**INFO-012-Laptop:** In further investigation of Omar al-Massari, we tell him that we wish to see his laptop computer. We are, of course, interested in what it might reveal about the terrorists he may be associating with. He refuses to tell us where it is. We referred to this as the non-production of evidence.

**INFO-013-Clark:** As we have learned, Omar al-Massari lives with two other males at 403 Winston Road in Silver Spring, Richard Clark and Fahd al-Quso. We were only able to interview Richard Clark. Clark is an American citizen of Anglo-Saxon origin who was born in 1973 in Lanham, MD, and is the owner of the residence at 403 Winston Road in Silver Spring. He has lived there since 2005, when he purchased the house. He says he had trouble making his house payments and was forced to take in renters who could contribute to his house payment. Clark went on to say that he rented rooms to al-Massari and al-Quso (who came together to look at the rooms) because they were professionals who could pay their rents on time, which Clark says they always did. We told Clark about al-Massari’s detention and asked for further information about him and al-Quso. Clark responded that Fahd al-Quso had suddenly moved out two days ago, and that he had not seen al-Massari for the past two days. However, Clark says that al-Massari had driven up two days ago in a U-Haul panel truck, but had only stayed for a minute before he left. Clark says he wondered why al-Massari was driving around in a U-Haul truck. Finally, Clark says that his two renters kept to themselves most of the time they were home and that he never looked inside their rooms (which would have been an invasion of their privacy), but that he frequently overheard their conversations concerning a place called Allied Import, that Clark guessed was a business of some kind.

**INFO-014-Quso:** The other housemate (besides Richard Clark) of Omar al-Massari is Fahd al-Quso, a Yemeni who, like Omar al-Massari, has been here on an extended work permit. Fahd al-Quso is also a physicist who has been employed for the past three years by a company called Physicom in Laurel, MD. We have not been able to interview him. Just yesterday, Fahd al-Quso boarded Emirates Flight #207 bound for Dubai. He purchased a one-way ticket using a credit card. He was not on any no-fly lists. We have just learned from a trusted source that Fahd al-Quso has been detained by United Arab Emirates authorities for questioning about his association with terrorist incidents in the UAE.

**INFO-015-FBI:** Allied Import is a business at 2121 M Street East in Washington, DC, that deals with a variety of items from various places in the Middle East. FBI contacts tell us that Allied Import has been under surveillance for several months in connection with possible narcotics trafficking. We asked the FBI for any surveillance records they might have about trucks entering and leaving Allied Import. We were shown a surveillance video of a single man arriving two days ago in a U-Haul panel truck with MD license number MDC-578. The driver was positively identified as Omar al-Massari. The video shows al-Massari handing off a single canister-like container to a man. So, Allied Import may be in the terrorist business in addition to being in the narcotics business, since we know from experience that these two activities often go hand in hand. The man in the video accepting the container from al-Massari was identified by the FBI as a Maryland resident named Kenny Derwish. Derwish lists his residence as 113 4th St. in Oxon Hill, MD. Derwish has been with Allied Import for four years.
INFO-016-Yasmin: A source code-named “Yasmin” tells us that she knew a man in Saudi Arabia named Omar al-Massari. Yasmin says she is “quite sure” that Omar spent two years “somewhere” in Afghanistan “sometime” in the years 1998-2000. Yasmin also tells us that she once met Omar al-Massari at a large gathering last August in Bethesda, MD, held (allegedly) to support charities in the Middle East. She said that Omar al-Massari attended this gathering with a person he identified as his roommate and that they were both physicists. Yasmin says that funds collected at this gathering were never intended to be used for charitable purposes, but to support terrorist activities both here and around the globe. Additionally, Yasmin tells us that Kenny Derwish is an alias used by Saeed al-Nami. She says that Saeed was associated with a now-disbanded Islamic Jihad cell in Herndon, VA. She further tells us that Saeed is a now a principal member of an active terrorist cell in Washington, DC, called “Jihad Bis Sayf” (Striving Through the Sword).

The information from Table 10 suggests a scenario where Omar al-Massari, who has ties with terrorist organizations, has stolen the cesium-137 canister and has given it to Saeed al-Nami, alias Kenny Derwish, who is a member of Jihad Bis Sayf. Consequently, we develop the analysis tree in Figure 69 to assess the hypothesis that the terrorist organization Jihad Bis Sayf has the cesium-137 canister. This analysis will be used in the next case study and in the following sections.

Up to now, all the case studies already included both the items of information collected and the items of evidence extracted from them. In the next case study you will have to extract the items of evidence from the collected information yourself. This involves the necessity for parsing incoming information to see what evidential dots or trifles this information reveals. As we have mentioned in Section 2.3, testimonial information or descriptions of tangible items might contain very many details, dots, or trifles. Some of the details might be interesting and relevant evidence, and others not. What we always have to do is to parse the information to extract the information that we believe is relevant in the inference task at hand. Next we look at what can happen if we don’t discuss the necessity for careful parsing:

In so many instances we have seen persons taking a lump of information containing many details, some interesting and some not, and treating it as a single item of potential evidence. There are two problems here. The first is that the relevant individual details in this lump might bear on different inferential issues; they will rarely all bear on the same issue. The second is that the irrelevant details only act to confuse the inferential bearings of the relevant details. Now, the problem is that determining what the relevant and irrelevant details are is a subjective matter. We might not all agree that a particular detail is relevant or irrelevant.

Here comes an example involving INFO-013-Clark from Table 10. In this case Clark tells us a variety of things, some of which seem potentially relevant and others not.
Figure 69. Analysis of the hypothesis that a terrorist organization has the stolen cesium-137.

Looking carefully at this testimony from Clark, we can first identify details that seem irrelevant as far as al-Massari’s terrorist activities are concerned. Here are some of them:

- **Clark had trouble making payments on the house he purchased in 2005. So he had to take in renters.**
- **The renters, al-Massari and al-Quso, always paid their rent on time.**
- **The renters, al-Massari and al-Quso, kept to themselves most of the time when they were home.**

But here are some apparently relevant details, dot, or trifles that bear on different matters.

- **Clark is of Anglo-Saxon origin and was born in 1973 in Lanham, MD.** These details are potentially relevant concerning Clark’s credibility and competence. That he is of Anglo-Saxon origin says that he is probably a kufr, a Muslim word for an infidel. That he is 37 years old might arise in assessments of his competence.
- **Al-Massari and al-Quso roomed together.** This bears on al-Massari’s association with a suspected terrorist.
- **Al-Massari and al-Quso frequently discussed the Allied Import Co.** This bears on where al-Massari might have taken the cesium-137.
• Two days ago al-Massari drove up to their residence in a U-Haul truck. This also bears on where al Massari might have taken the cesium-137.
• Al-Massari only stayed for a minute two days ago when he drove up in the U-Haul truck. This may be relevant on when al-Massari took the cesium to Allied Import.
• Al-Quso suddenly moved out two days ago. This bears on al Quso’s behavior as a possible terrorist.

This analysis above is an example of the necessity for parsing lumps of information to identify what different specific details, dot, or trifles are relevant, and how they are relevant on different issues in an analysis.

8.2 Case Study: Evidence Collection and Hypothesis Analysis

It is not necessary to perform this case study in order to understand the sources of uncertainty discussed in the follow-on sections of this chapter.

8.2.1 Objective

This case study has the following objectives:

• Learning how to extract evidence from the collected information.
• Improving your understanding of the evidence-based hypothesis analysis process by analyzing of a more complex hypothesis.
• Providing an example for discussing the sources of uncertainty in intelligence analysis.

8.2.2 Summary

The available information suggests a scenario where Omar al-Massari, who has ties with terrorist organizations, has stolen the cesium-137 canister and has given it to Saeed al-Nami, alias Kenny Derwish, who is a member of Jihad Bis Sayf terrorist organization. As a result, you will assess the hypothesis that Jihad Bis Sayf has the cesium-137 canister. First you will define evidence based on the available information. Then you will associate it with elementary hypotheses and evaluate them. As a result, you will assess the likelihood of the top-level hypothesis.

Proceed as indicated in the following instructions.

8.2.3 Instructions

1. Start this case study in TIACRITIS.
2. Select the Hypothesis menu and then select the hypothesis analysis problem: “Assess whether Jihad Bis Sayf has the cesium-137 canister.”
3. Browse the analysis of the above hypothesis to see how it is reduced to simpler hypotheses that need to be assessed based on the available evidence.
4. You will define new items of evidence based on the available information, as illustrated in the following.

5. Select the **Evidence** menu and then click on [COLLECTED INFORMATION]. The left panel shows the collected items of information.

6. Click on **INFO-016-Yasmin**. The right panel shows its description from which you may define several items of evidence.

7. Click on [DEFINE EVIDENCE] following the description of **INFO-016-Yasmin**. The right panel shows a partially defined item of evidence “EVD-021-“. You will complete this definition to represent the Yasmin’s testimony that Omar al-Massari spent time in Afghanistan.

8. Complete the name “EVD-018-“ with “Yasmin-Afghan” and click on [SAVE].

9. Click on [EDIT] for Description, click inside the pane and edit the text so that the new description is approximately, “Yasmin testimony that Omar spent two years in Afghanistan in the years 1998-2000.”

10. Click on [SAVE].

11. After “**Type:** evidence,” click on [CHANGE] to specify the type of this item of evidence.

12. After “unequivocal testimonial evidence based upon direct observation,” click on [SELECT].

13. After “**By the source:** not specified,” click on [CHANGE].

14. Type “Yasmin” and click on [SAVE].

15. Click on [YES].

16. After “**Source type:** actor,” click on [CHANGE].

17. After “person,” click on [SELECT].

18. Under the “**Irrelevant to**” label, and after the hypothesis “there is evidence of prolonged presence in an area controlled by a terrorist organization, of Omar al-Massari,” click on [FAVORS]. Notice that the Favors label was created and the hypothesis was moved under it.

19. In the left panel, click on [COLLECTED INFORMATION] and notice that **INFO-016-Yasmin** is still selected.

20. In the right panel, click on [DEFINE EVIDENCE] following the description of **INFO-016-Yasmin**. You will define new items of evidence based on **INFO-016-Yasmin** (for example, the testimony of Yasmin that Kenny Derwish is an alias used by Saeed al-Nami), and associate them with the corresponding hypotheses that will be shown in the right panel.

21. Define additional items of evidence from the collected information and associate them with the corresponding hypotheses.

22. Click on **Reasoner** and browse the analysis tree.
23. Estimate the relevance and believability of all the items of evidence and define them as assumptions.

24. Browse the final analysis tree.

25. When finished, select Case Study.

26. Click on [SAVE & FINISH] to end the case study.

8.3 Incompleteness

8.3.1 What Is Incompleteness of Evidence?

We may have all heard someone say, “I am going to wait until I have all the evidence before I draw a conclusion or make a decision.” This person faces an infinitely long wait because there is no situation in which we can say we have all the possible evidence. The first way of showing that this statement is true is to consider the distinction we have made between directly relevant and ancillary evidence. In doing so, we also referred to ancillary evidence as being meta-evidence, or evidence about evidence. The trouble here is that we face an infinite regress in which we have evidence, ancillary evidence about this evidence, ancillary evidence about this ancillary evidence, and so on, ad infinitum. Suppose we have an HUMINT asset who provides us with some interesting evidence; call this asset our primary source. But then we have a secondary source who provides us with ancillary evidence about the believability of our primary source. But then we have a tertiary source who provides ancillary evidence about the believability of our secondary source. This process could go on and on indefinitely. This fact was noted years ago by the CIA’s James J. Angleton, who encountered situations in which chains of HUMINT sources provided contradictory and divergent evidence about each other’s believability. He described this situation as similar to being in a “wilderness of mirrors” (Martin, 1980).

There are many other situations in which we could have endless chains of evidence, and evidence about evidence, even in empirical statistical situations. It is often said that the conclusions reached by statisticians are always misleading to some extent and that they must choose ways of reporting conclusions that are minimally misleading. Here is an intelligence analyst who reports the results of a statistical analysis of the capabilities of a weapon system of some sort. Her conclusions are challenged by another analyst. In turn, the comments made by this challenger are then challenged by a third analyst. This process could go on forever until someone decides to call a halt to this evidence about evidence situation. This fact is noted in our procedures for trials at law that limit the extent to which we can follow this chain. If this were not the case, a trial might go on for years without any verdict ever being reached.

But there is another even more important reason for our evidence always being incomplete. In how many intelligence analyses could it ever be said that every one of the relevant questions that could have been asked was in fact answered by the evidence that was gathered and analyzed? There probably has never been an intelligence analysis in which there were no lingering unanswered questions at the time a conclusion was required. In the absence of clairvoyance, there may be considerable uncertainty about what questions should be asked in an intelligence analysis. In Section 5.5 we discussed missing evidence
as a possible category of evidence. In such cases we attempted to answer certain questions but were unable to do so. But there will be many questions lingering that we have never even attempted to answer as well as many questions that we may not even recognize as being relevant. In Section 9.5.3 we will discuss a view of probability, called the Baconian View, which uniquely places special emphasis on the extent to which our evidence in an analysis is complete in its coverage of all the questions we recognize as being relevant to the conclusions we must reach. This view requires us to consider the force of evidence we do have, but it also says that this force depends on questions that are unanswered by the present evidence we are considering. This issue of completeness is bound to be of interest to intelligence analysts engaged in current intelligence in which conclusions are often required in a very short time. An issue here concerns the extent to which any analyst could have the time to cover all the questions that might occur to this person as being relevant to the conclusion being requested.

8.3.2 Examples and Questions

Example 16. On various matters concerning events in the past, it might be argued that we have complete evidence. For example, we believe we have evidence that allows us now to conclude, beyond all shadow of doubt, that the twin towers of the World Trade Center in New York City were destroyed on September 11, 2001, and that the then President of the United States, John F. Kennedy, was assassinated in Dallas, Texas, on November 22, 1963. We can go to New York and see for ourselves where the World Trade Center used to be and then view television images of the two aircraft that slammed into the buildings, and the horror of the subsequent collapse of the buildings. Or, we can view the monument to John F. Kennedy in Arlington National Cemetery in Virginia that records the place and time of his death. We can also watch the so-called Zapruder film that shows President Kennedy being struck in the head and then collapsing into his wife Jacqueline’s arms after he was struck. In each of these cases we have what can be regarding as conclusive evidence (more on conclusive evidence in a moment).

There are two points to be made about the two examples we have just provided. First, it does appear that the occurrence of these two events is no longer a topic of analytic interest, since we are certain that they occurred. But there are very many other questions concerning these two events that are now of great interest and will continue to be of interest in future analyses. Concerning the tragedy in New York, we are asking such questions as: “Who were all the persons involved in the planning of this action?” and “Why did these persons take this action at this particular time?” As far as the Kennedy assassination is concerned, it is still being asked: “Did Lee Harvey Oswald act by himself or was he part of a conspiracy to kill President Kennedy?” The evidence on these questions will never be complete. The second point concerns the stability over time of the conclusions we have now reached with certainty. Five hundred years from now, will these two conclusions about the destruction of the World Trade Center and the assassination of President Kennedy still be regarded as certain (if they are, indeed, matters of concern at all)? Perhaps the evidence we now regard as conclusive will have vanished long before the year 2510.

Example 17. Intelligence analysts will not normally be concerned about what will be inferred five hundred years from now about events of interest today. In many cases they are asked to reach
conclusions concerning past events based on evidence that is far from complete. For example, new evidence is coming to light as we write these words on whether Lee Harvey Oswald acted alone in the assassination of President Kennedy. New accounts of the identities and motivations of the nineteen terrorists who destroyed the World Trade Center appear regularly as well. Even more evidence about these events will certainly emerge in the future. Now, consider an intelligence analysis that involves the prediction of some future event, such as whether countries such as Iran, Iraq, Saudi Arabia, Syria, Egypt, and Turkey will engage in all-out war if we remove all of our forces from countries in the Middle East. Unless we have a person who is certifiably clairvoyant and can see into the future we will never know for certain. The only thing certain is that we can only draw inferences about events such as these based on evidence about events in the past and the ever-fleeing present. This evidence will obviously be incomplete, if only because we may not be asking the right questions. In addition, and of the greatest importance, there will always be questions unanswered by the evidence we do have. These is only one view of probabilistic reasoning, the Baconian view, that asks how complete is our coverage of evidence and how many questions remain unanswered by the evidence we have considered.

**Example 18.** This is one final example concerning evidential incompleteness; it involves what we have said about ancillary evidence, or evidence about evidence. We are always facing an infinite regress involving evidence, evidence about the evidence, evidence about the evidence about the evidence, and so on ad infinitum. Consider our source “Santa” in the dirty bomb example. Santa has given us two very important items of evidence: (1) that Omer Riley is an alias used by Omar al-Massari (EVD-014-SantaAlias in Table 9), and (2) that Omar al-Massari is a member of an unnamed jihadist organization in Washington, DC (EVD-017-SantaTerOrg). The question is: what do we really know about Santa’s competence and credibility as far as these two items of evidence are concerned? By the way, it should be obvious that Santa is an informant about terrorist activities in this general area. One question we would ask concerns Santa’s competence in these reports. Has he had any actual contact with Omar al-Massari and any knowledge of who Omar al-Massari associates with? To answer such questions we rely upon another asset code-named “Raindrop.” Raindrop tells us that he is sure that Santa knows Omar al-Massari and also knows about possible terrorist organizations with which Santa has contact. The same questions now arise concerning Raindrop’s competence and credibility concerning what he tells us about Santa’s competence and credibility. To answer these questions we could query yet another source and even another source about this source. There is no end to it.

**Question 11.** For what other evidence items in Table 9 would you wish to have other sources available which could help in deciding whether or not to believe what the items tell us?

We leave the issue of incompleteness with two thoughts we ask you to keep in mind. With the exception of situations like the ones given in Example 16 concerning past events and conclusive evidence, in any other case we have two reasons why our evidence is never complete:

- We will always have some unanswered questions.
- We will always encounter the need for meta-evidence or evidence about evidence, there being no end to this need.
8.4 Inconclusiveness

8.4.1 What Is Inconclusiveness of Evidence?

The evidence encountered in intelligence analysis is commonly inconclusive in nature. This means that evidence is consistent with more than one possibility, hypothesis, or explanation. Conclusions reached from such evidence can only be probabilistic in nature. Another term we might use here is to say that intelligence analysis usually involves circumstantial evidence. Recall that circumstantial evidence, even if credible, supplies only some but not complete grounds for a conclusion. Conclusive evidence, that which is consistent with only one possibility or hypothesis, is usually in very short supply. Conclusive evidence would supply complete grounds for, or make necessary or certain, some hypothesis or possible conclusion.

There is an expression used by intelligence analysts with reference to conclusive evidence on some major hypothesis that comes from a completely credible source; the term nugget is used with reference to such evidence. Here is an example of such a nugget using our dirty bomb (cesium-137) example. Suppose we have a trusted source who reports the following events. This source tells us: “Persons associated with the North American Jihadist Organization (NAJO) in Silver Spring, MD, did acquire the cesium-137 that was stolen from the XYZ warehouse in Baltimore. They are now constructing a dirty bomb in the garage of a residence at 221 Colesville Rd. in Silver Spring, MD, which they intend to set off on the grounds of the capitol building in Washington, DC, next Thursday at 12:00PM.” If we had such a nugget, we could easily prevent this disaster from occurring. Barring the acquisition of such a nugget we must, as the phrase goes, “mine lots of lower grade ore” in the form of inconclusive and circumstantial evidence.

A further comment on the inconclusive nature of evidence is necessary. In the right hand side (green) tree from Figure 4 (p. 15) we illustrated how evidence is connected to hypotheses by chains of reasoning by propositions or events that could be true or false. Each one of these links in a chain of reasoning, indicated by the open circles, is a source of doubt or uncertainty. There are few circumstances in which one proposition in a chain of reasoning makes necessary or certain a following proposition. This says that chains of reasoning are inductive or probabilistic in nature rather than being deductively or necessary in nature.

8.4.2 Examples and Questions

Example 19. Even if Omar al-Massari is a member of a jihadist organization in Washington, DC, (hypothesis H_c in Figure 5), this does not mean that a dirty bomb will be set off somewhere in Washington, DC (hypothesis H_k). In fact, EVD-017-SantaTerOrg in Table 9 (Santa’s report that Omar al-Massari is intimately associated with an unnamed jihadist organization in the Washington, DC area) is only inconclusive as far as source of doubt H_c is concerned. Our source Santa might not be credible; Santa might be lying to us or simply be mistaken. In short, his report is just inconclusive evidence that the event he reports is true.
Example 20. The five evidence items EVD-001-Willard, EVD-004-Ralph, EVD-005-Ralph, EVD-013-Grace, and EVD-006-Clyde (from Table 5 and Table 7) do not conclusively show, taken separately or together, that the proposition “The canister containing cesium-137 was stolen” is true. This evidence does not entitle us to believe with certainty that the cesium-137 canister was stolen from the XYZ warehouse. We may obtain later evidence that Grace was wrong, and that someone at the XYZ company did in fact remove the cesium-137 canister for work on a project for one of XYZ’s customers.

Question 12. Show why the other evidence in Table 5 and Table 7 is also inconclusive.

8.5 Ambiguity

8.5.1 What Is Ambiguity of Evidence?

Evidence is ambiguous to the extent to which we cannot determine what it is telling us. We might also describe ambiguous evidence as being imprecisely stated. In addition, ambiguous evidence goes beyond being merely inconclusive. We may have precisely stated or non-ambiguous evidence that is still circumstantial or consistent with more than one hypothesis or possible conclusion. As an example of ambiguity, we will discuss a conversation we have intercepted between two persons of interest who are involved in known terrorist activities. In this conversation they make use of words used to describe persons and their activities that are designed to conceal their intentions or to mislead others who may be listening. It is well known, for example, that terrorist organizations in the Middle East spend a great amount of time training their operatives to be skillful in disguising their identities, capabilities, and intentions. Even our best efforts to disambiguate evidence we receive are not always successful. A person listening to such a conversation may be perfectly fluent in the language and dialect being used by the two persons overheard, but still be unable to tell us exactly what these two persons were saying.

8.5.2 Examples and Questions

Example 21. Look again at INFO-016-Yasmin in Table 10 in which we have “Yasmin” telling us that she knew a man in Saudi Arabia named Omar al-Massari. Yasmin says she is “quite sure” that Omar spent two years “somewhere” in Afghanistan “sometime” in the years 1998-2000. In addition to her hedging her assessment by saying she is “quite sure,” she is additionally vague or imprecise regarding where and when Omar al-Massari was in Afghanistan. If we knew where and when Omar al-Massari was in Afghanistan we could make a better assessment of what he was doing there and whether he was actually involved in jihadist activities.

Question 13. From your own experience, can you recall other items of ambiguous evidence you have received?

8.6 Dissonance

8.6.1 What Is the Dissonance of Evidence?

We devoted Section 7.4 to a discussion of dissonant evidence as being a recurrent combination of intelligence evidence. We described dissonant evidence as being directionally inconsistent in the sense
that it points us toward more than one hypotheses or possible conclusions. We described the two forms of dissonance as involving contradictory and divergent evidence. Suppose we have an analysis in which it is stated that all of the evidence analyzed was harmonious or directionally consistent in favoring the conclusion reported in the analysis. The first question someone should ask is: “Are you sure you did not gather and analyze just the evidence you believe would favor the conclusion you reported?” In some situations this is called “cherry picking.” At least some pattern of dissonance may be expected in any intelligence analysis, especially one that involves any degree of complexity. To be sure, some of the evidence may be harmonious in pointing in one direction, but on balance we will have other harmonious evidence pointing in another direction. In short, some dissonance will be expected in every intelligence analysis having any degree of complexity. Failure to report this dissonance will arouse justified suspicions of the intentions and the competence of the persons performing the analysis.

8.7 Imperfect Believability

Sources of evidence of any kind (i.e., all of the possible “INTs”) have any possible degree of believability. There are no perfect sensors of any kind; this certainly includes human senses. We have spent a considerable amount of time discussing the believability attributes of the tangible and testimonial forms of evidence. We should also add here the important consideration of the competence of human sources of evidence. We may not always be certain that a source actually had access to the information being reported or made the observation the source claims to have made.

Example 22. In Section 6.2 we considered a human source code-named Wallflower who gave us the report concerning the Iraqi Emir Z. coming out of a building in Ahwaz, Iran that houses offices of the Iranian IRGC Qods Forces. We carefully considered the major attributes of Wallflower’s credibility: veracity, objectivity, and observational sensitivity.

Question 14. The same three attributes need to be considered for all of the human sources in our dirty bomb example in Figure 4 and Figure 5. Pick a human source in this example and state what kinds of questions you would ask about the veracity, objectivity, and observational sensitivity of the person you have chosen.

But we also must be concerned about the believability of any tangible evidence we obtain. These attributes concern the authenticity, reliability, and accuracy of such evidence. In Table 7 we have several items of tangible evidence. Here are some examples of believability-related questions we should ask about this evidence.

Example 23. EVD-012-InvestigativeRecord concerns the traces of cesium-137 that were found in the truck we believe to have been driven by Omar al-Massari. We have examined the chain of custody through which the tangible record of measurements taken of these traces was made. Suppose we are convinced that this record is authentic. But we must also consider the reliability and accuracy of the device used to obtain these measurements. The first question we should ask is: How reliable are these measurements we have? Were repeated measures taken using the same measuring device and did they give the same readings on each measure? The second question involves the accuracy of the device. In particular, what is its hit rate and false-positive rate for detecting cesium-137 traces?
**Question 15.** There are other items of tangible evidence in Table 7. What kind of similar questions would you ask about these other tangible items?

An experienced analyst reading the account of uncertainty in intelligence evidence just provided may easily recognize all five of these characteristics, and will have encountered most of them at one time or another. Any critic of intelligence analysts for expressing their uncertainty in reporting conclusions should be made aware of the five reasons we have mentioned that require intelligence analysts to acknowledge the extent of their uncertainty, which will always be present. But there are additional reasons why uncertainty is evident in all complex activities such as intelligence analysis.

We suspect that one reason for the current interest in uncertainty in intelligence analysis is that analysts have encountered sources of uncertainty that are not captured by conventional views of probability. This is the main reason we have for presenting alternative systems of probabilistic reasoning in the next section.
9 ASSESSING AND REPORTING UNCERTAINTY: SOME ALTERNATIVE METHODS

9.1 Introduction

We have now considered the major sources of uncertainty related to evidence and have shown how uncertainty arises in chains of reasoning linking evidence to hypotheses we entertain. A major credential of evidence we have only mentioned briefly is its inferential force or weight. As we noted, this credential is always expressed in probabilistic terms but is a source of great controversy. In Figure 26, we showed how the force or weight of evidence concerns the strength of all the believability and relevance links in our chains of reasoning. But this illustration just concerns a single chain of reasoning from a single item of evidence. In any intelligence analysis there will be many items of evidence to consider and very many sources of uncertainty or doubt that will be associated with complex arguments linking this mass of evidence to hypotheses at issue in the analysis. It would not be uncommon to be able to identify hundreds or even thousands of sources of doubt arising from masses of evidence being considered.

There are other matters apart from assessing the force or weight of evidence in which uncertainty arises. One way of describing evidence-based reasoning is to say that it involves the revision of probabilistic beliefs about hypotheses based on the evidence we have obtained. To say that we are revising these beliefs suggests that they must have had some initial state in order for them to be revised. The term prior probability is used to indicate the initial conditions of our uncertainty before we consider evidence that begins to emerge. In truth, there has been considerable controversy about prior probabilities and how they can be assessed. When we consider our evidence and its force or weight, we can begin the process of revising these prior beliefs based upon evidence. In the process we revise our prior beliefs to form what are usually termed posterior beliefs, those assessed after we receive and incorporate the evidence we have. But we must take a bit of care concerning the process of belief revision just described.

In the process of discovery or investigation in intelligence analysis and elsewhere, we may have evidence in search of hypotheses and hypotheses in search of evidence all going on at the same time, as discussed in Section 1.2. In other words, it would be quite wrong to suggest that an intelligence analysis always begins with a complete set of hypotheses having been identified. The generation of hypotheses rests on potential evidence we begin to accumulate. Further evidence may suggest new hypotheses or revisions in ones we have generated. In short, evidence not only causes revisions in our probabilistic beliefs about a collection of hypotheses, but it also causes mutations or changes in this collection itself. How this probabilistic belief-revision process proceeds and what its major ingredients are depend vitally upon our view of probability and uncertainty. In the following sections we consider different probability systems. Before that, however, let us proceed with our analysis example, which will be used in discussing these probability systems.
We have concluded that the terrorist organization Jihad Bis Sayf, though its member Saeed al-Nami, has taken possession of the cesium-137 canister. The next hypothesis to evaluate is whether this organization is able to construct a dirty bomb. We direct our intelligence collection efforts on Saeed al-Nami and obtain the items of information from Table 11, which will be used to assess this hypothesis, as indicated in Figure 70.

Table 11. New information related to Saeed al-Nami.

**INFO-017-Miller:** A loading dock worker at Allied Import named Rocky Miller says that Derwish put the object he received from the U-Haul guy in the trunk of his car.

**INFO-018-Garcia:** To learn more about al-Nami (alias Derwish) we interview the management of the Allied Import Company. The first thing we are told by Jose Garcia, a vice president of Allied Import, was that they only knew Kenny Derwish by this name; Garcia says he was very surprised to learn that this name was an alias. Garcia also said that Derwish had worked for Allied Import for five years and is an expert in the evaluation of firearms and explosives that Allied Import purchases from foreign suppliers. Garcia said that Derwish knew more about these items than anyone he had ever known. We asked Garcia what kind of explosives they import. He said that they import only plastic explosives like Semtex, RDX, and C-4 that are very stable and can be shipped safely by ground and sea transport. Many American demolition companies use these explosives but can get them cheaper from China and some European companies. We asked Garcia if any of their imported explosives had gone missing. He said that this has rarely happened, but about two weeks ago, a small amount of RDX, about two pounds, went missing from a storage facility to which al-Nami (Derwish) had access. We then asked Garcia if we could talk with Derwish, Garcia said that Derwish had gone on vacation two days ago.

**INFO-019-Yasmin:** We contacted our source, Yasmin, again. All she has told us so far was that Saeed al-Nami used an alias (Kenny Derwish) and that he was associated with the militant jihadist group Jihad Bis Sayf. We now asked her for more information about al-Nami. She said that the name Derwish was a Yemeni name but al-Nami was a Saudi name. Yasmin said that he took this alias, Derwish, for two reasons. First, because it would sound a much less Muslim name to Americans, and second, because he admired the Yemenis and had spent a year in 2003 in an al Qaeda training camp in Yemen, where he received training in the use and construction of explosive devices. We asked Yasmin if any of this training might have included the assembly of dirty bombs. She says she would not rule this out because al Qaeda wished to have these weapons for many years, and had assembled some stocks of radiological materials.

Finally, we investigate the top-level hypothesis, that Jihad Bis Sayf will set-off a dirty bomb in the Washington, DC area. This reduces to assessing its reasons, desires, and capabilities, as shown in Figure 71. The case study in the next section allows you to assess this top-level hypothesis.
Assessing and Reporting Uncertainty: Some Alternative Methods

Figure 70. Analysis of the hypothesis that Jihad Bis Sayf is able to construct a dirty bomb.

Which a strategy?
Consider the necessary conditions and the direct evidence.

- Assess whether Jihad Bis Sayf is able to construct a dirty bomb, based on conditions analysis.
- Assess whether Jihad Bis Sayf is able to construct a dirty bomb, based on direct evidence.

Which conditions are necessary to construct a dirty bomb?
Possession of radioactive material, explosive material, expertise, and place to construct the dirty bomb.

- Assess whether Jihad Bis Sayf has radioactive material to construct a dirty bomb.
- Assess whether Jihad Bis Sayf has the expertise to construct a dirty bomb.
- Assess whether Jihad Bis Sayf has a secure place to construct a dirty bomb.
- Assess whether Jihad Bis Sayf has the cesium-137 canister which contains enough cesium-137 to construct a dirty bomb.

Which is a scenario?

Jihad Bis Sayf has the cesium-137 canister which contains enough cesium-137 to construct a dirty bomb.

- Assess whether Jihad Bis Sayf has the cesium-137 canister.
- Assess whether the cesium-137 canister contains enough cesium-137 to construct a dirty bomb.

Which is a scenario?
Saeed al-Nami alias Kenny Derwish, a member of Jihad Bis Sayf, has expertise in explosives and has received training in the construction of dirty bombs.

- Assess whether Saeed al-Nami alias Kenny Derwish has expertise in explosives.
- Assess whether Saeed al-Nami alias Kenny Derwish is member of the terrorist organization Jihad Bis Sayf.
- Assess whether Saeed al-Nami alias Kenny Derwish has received training in the construction of dirty bombs.
- Assess whether Saeed al-Nami alias Kenny Derwish had reasons to steal the RDX explosive.

Which is a scenario?
Saeed al-Nami, a member of Jihad Bis Sayf, has stolen 2 pounds of RDX explosive which is enough to construct a dirty bomb.

- Assess whether Saeed al-Nami has stolen 2 pounds of RDX explosive.
- Assess whether Saeed al-Nami alias Kenny Derwish has stolen 2 pounds of RDX explosive which are missing from Allied Import because he had access to it and reasons to steal it.

Which is a scenario?
Saeed al-Nami, alias Kenny Derwish, has stolen 2 pounds of RDX explosive which are missing from Allied Import because he had access to it and reasons to steal it.

- Assess whether 2 pounds of RDX explosive are missing from Allied Import.
- Assess whether Kenny Derwish is an alias of Saeed al-Nami.
- Assess whether Saeed al-Nami alias Kenny Derwish had reasons to steal the RDX explosive.

Which is a scenario?
2 pounds of RDX explosive are missing from Allied Import.

- Assess whether 2 pounds of RDX explosive is enough to construct a dirty bomb.
- Assess whether 2 pounds of RDX explosive were stolen from Allied Import.

Which is a scenario?
Kenny Derwish is an alias of Saeed al-Nami.

- Assess whether Kenny Derwish is an alias of Saeed al-Nami.
- Assess whether 2 pounds of RDX explosive were stolen from Allied Import.

Which is a scenario?
Saeed al-Nami has stolen 2 pounds of RDX explosive.

- Assess whether Saeed al-Nami has stolen 2 pounds of RDX explosive.
- Assess whether Kenny Derwish is an alias of Saeed al-Nami.

Which is a scenario?
Assess whether Saeed al-Nami has stolen 2 pounds of RDX explosive which are missing from Allied Import because he had access to it and reasons to steal it.

- Assess whether Saeed al-Nami has stolen 2 pounds of RDX explosive which are missing from Allied Import because he had access to it and reasons to steal it.
9.2 Case Study: Hypothesis Analysis

It is not necessary to perform this case study in order to understand the probabilistic systems discussed in the follow-on sections of this chapter.

9.2.1 Objective

This case study has the following objectives:

- Practicing with extracting evidence from the collected information.
- Improving your understanding of the evidence-based hypothesis analysis process.
- Providing an example for discussing different probabilistic systems.
9.2.2 Summary

You will analyze the hypothesis that Jihad Bis Sayf will set-off a dirty bomb in the Washington, DC area. First you will define evidence based on the available information. Then you will associate it with elementary hypotheses and evaluate them. Finally, you will define assumptions for the hypotheses that lack evidence. As a result, you will assess the likelihood of the top-level hypothesis.

Proceed as indicated in the following instructions.

9.2.3 Instructions

1. Start the case study in TIACRITIS.

2. Select the Hypothesis menu and then select the hypothesis analysis problem: “Assess whether Jihad Bis Sayf will set-off a dirty bomb in the Washington DC area.”

3. Browse the analysis of the above hypothesis to see how it is reduced to simpler hypotheses that need to be assessed based on the available evidence.

4. Select the Evidence menu and click on [COLLECTED INFORMATION]. The left panel shows the collected items of information.

5. Click on each item of information you are not familiar with and read its description in the right panel.

6. Define evidence items from the new information and associate them with the basic hypotheses they are relevant to.

7. Select the Reasoner menu and browse the analysis tree.

8. Estimate the relevance and believability of all the items of evidence and define them as assumptions.

9. Browse the analysis tree, the collected information, and the evidence items to make sure that all the relevant information has been used in the analysis.

10. Define assumptions for the hypotheses for which there is no relevant evidence.

11. Browse the final analysis tree.

12. When finished, select Case Study.

13. Click on [SAVE & FINISH] to end the case study.

9.3 General Classes of Probability and Uncertainty

A major trouble we all face in thinking about probability and uncertainty concerns the fact that the necessity for probability calculations, estimations, or judgments arises in different situations. In addition, there are many different attributes of our judgments that we would like to capture in assessments of uncertainty we are obliged to make. As we will see, there are some forms of intelligence analyses, or at least parts of them, in which you can estimate probabilities of interest by counting things.
But there are many other situations in which analysts have uncertainty but will have nothing to count. These situations involve events that are singular, unique, or one-of-a-kind. We start with Table 12 below, which categorizes the alternative views of probability we will discuss as we proceed.

Table 12. Some Alternative Views of Probability

<table>
<thead>
<tr>
<th>Enumerative</th>
<th>Non-Enumerative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aleatory (Chances)</td>
<td>Epistemic (1): Subjective Bayesian</td>
</tr>
<tr>
<td>Relative Frequency and Statistics</td>
<td>Epistemic (2): Belief Functions</td>
</tr>
<tr>
<td>Bayesian Statistics (under debate)</td>
<td>Baconian: Eliminative and Variative Inference</td>
</tr>
<tr>
<td></td>
<td>Imprecision and Fuzzy Probability</td>
</tr>
</tbody>
</table>

We begin by discussing two views of probability that involve processes in which we can obtain probabilities or estimates of them by enumerative or counting processes.

### 9.4 Enumerative Probabilities: Obtained by Counting

There are two conceptions of probability that involve counting operations. The first is termed aleatory probability. This term has its roots in the Latin term *alea*, meaning chance, game of chance, or devices such as dice involved in games of chance. Games of chance have two important ground rules:

- There is a finite number $n(S)$ of possible outcomes.
- All outcomes in $S$ are assumed to have equal probability.

For example, in a game involving a pair of fair six-sided dice, where we roll and add the two numbers showing up, there are 36 ways in which the numbers showing up will have sums between 2 and 12, inclusive. So, in this case, $n(S) = 36$. Suppose you wish to determine the probability that you will roll a 7 on a single throw of these dice. There are exactly 6 ways in which this can happen. If $E$ = the sum of the numbers is 7, then $n(E) = 6$. The probability of $E$, $P(E)$, is simply determined by dividing $n(E)$ by $n(S)$, which in this example is $P(E) = 6/36 = 1/6$. So, aleatory probabilities are always determined by dividing $n(E)$ by $n(S)$, whatever $E$ and $S$ are, as long as $E$ is a subset of $S$.

We can dismiss aleatory probability as not being interesting in intelligence analysis since there seem to be no instances in which the two aleatory ground rules will apply. However, we should note that there are frequent instances in which analysts may use the term “chance,” when it may not be appropriate. For example, here is an analyst who says, “The chances are 9 in 10 (probability equals 0.9) that Iran is supplying arms to insurgents in Iraq.” This judgment cannot have arisen by any counting operation in which the two ground rules for aleatory probabilities apply. One rather unfortunate occurrence is that most people are initially introduced to probability theory by use of games of chance to illustrate various concepts. People then often believe that these concepts occur and retain the same
meaning when they are used in entirely different contexts in which uncertainty assessments are required.

Another way of assessing probabilities involves the many situations in which aleatory ground rules will not apply but when we do have empirical methods at hand to estimate probabilities. These situations arise when we have replicable or repeatable processes in which we can count the number of times events have occurred in the past. Suppose that, employing a defensible method for gathering information about the number of times event $E$ has occurred, we determine the relative frequency of an occurrence of $E$ by counting the number of times $E$ has occurred, $n(E)$, and then dividing this number by $N$, where $N$ is the number of observations we have made, or the sample size we have taken. In this case, the relative frequency of $E$, $f(E)$, equals $n(E)/N$. You recognize that this is a statistical process that can be performed in many situations, provided that we assume processes that are replicable or repeatable. It is true, of course, that a relative frequency $f(E)$ is just an estimate of the true probability of $E$, $P(E)$. The reason, of course, is that the number $N$ of observations we have made is always less than the total number of observations that could be made. In some cases there may be an infinite number of possible observations. If you have had a course in probability theory you will remember that there are several formal statements, called the laws of large numbers, for showing how $f(E)$ approaches $P(E)$ when $N$ is made larger and larger.

Probability theory presents an interesting paradox. It has a very long history, but a very short past. There is abundant evidence that people as far back as Paleolithic times used objects resembling dice either for gambling or, more likely, to foretell the future (David, 1962). But attempts to calculate probabilities only date back to the 1600s, and the first attempt to develop a theory of mathematical probability only dates back to 1933 in the work of Russian A. N. Kolmogorov (1933). Kolmogorov was the first to put probability on an axiomatic basis. The three basic axioms he proposed are the following ones:

**Axiom 1:** For any event $E$, $P(E)$ $\geq$ 0. All this says is that probabilities are never negative.

**Axiom 2:** If an event is sure or certain to occur, which we label $S$, $P(S)$ = 1.0. Axioms 1 and 2, taken together, mean that probabilities are numbers between 0 and 1. An event having 0 probability is commonly called an “impossible event.”

**Axiom 3:** If two events, $E$ and $F$, cannot occur together, or are mutually exclusive, the probability that one or the other of these events occurring is the sum of their separate probabilities. In symbols, $P(E$ or $F$) = $P(E) + P(F)$. This axiom is called the additivity axiom and it holds for any number of mutually exclusive events.

Certain transformations of Kolmogorov’s probabilities are entirely permissible and are often used. One common form involves odds. The odds of event $E$ occurring to its not occurring, which we label Odds($E$, not-$E$), is determined by Odds($E$, not-$E$) = $P(E)/(1 - P(E))$. For any two mutually exclusive events $E$ and $F$, the odds of $E$ to $F$, Odds($E$, $F$), are given by Odds($E$, $F$) = $P(E)/P(F)$. Numerical odds scales range from zero to an unlimited upper value. The person who said the chances that Iran is supplying weapons to insurgents in Iraq is 9 in 10, might better have said that the odds favoring Iran supplying the weapons, to their not supplying weapons, are 9 to 1.
What is very interesting, but not always recognized, is that Kolmogorov had only enumerative probability in mind when he settled on the above three axioms. He makes this clear in his 1933 book and in his later writings (Kolmogorov, 1969). It is easily shown that both aleatory probabilities and relative frequencies obey these three axioms. But Kolmogorov went an important step further in defining conditional probabilities that are necessary to show how the probability of an event may change as we learn new information. He defined the probability of event $E$, given or conditional upon some other event $F$, as: $P(E \text{ given } F) = P(E \text{ and } F)/P(F)$, assuming that $P(F)$ is not zero. He chose this particular definition since conditional probabilities, so defined, will also obey the three axioms just mentioned. In other words, we do not need any new axioms for conditional probabilities. Now comes a very important concept you may have heard about; it is called Bayes’ rule.

This rule is named after the English clergyman, the Reverend Thomas Bayes (1702 – 1761), who first saw the essentials of a rule for revising probabilities of hypotheses, based on new evidence (Dale, 2003). He had written a paper describing his derivation and use of this rule but he never published it; this paper was found in his desk after he died in 1761 by Richard Price, the executor of Bayes’ will. Price realized the importance of Bayes’ paper and recommended it for publication in the Transactions of the Royal Society, in which it appeared in 1763. He rightly viewed Bayes’ rule as the first canon or rule for inductive or probabilistic reasoning. Bayes’ rule follows directly from Kolmogorov’s three axioms and his definition of a conditional probability, and is entirely uncontroversial as far as its derivation is concerned. But this rule has always been a source of controversy on other grounds. The reason is that it requires us to say how probable a hypothesis is before we have gathered evidence that will possibly allow us to revise this probability. In short, we need prior probabilities on hypotheses in order to revise them, when they become posterior probabilities. Persons wedded to enumerative conceptions of probability say we can never have prior probabilities of hypotheses since, in advance of data collection we have nothing to count. Statisticians are still divided today about whether it makes sense to use Bayes’ rule in statistical inferences. This is why we have put “under debate” after Bayesian Statistics in Table 12. Some statisticians argue that initial prior probabilities could only be assessed subjectively and that any subjective assessments have no place in any area that calls itself scientific. Bayes’ rule says that if we are to talk about probability revisions in our beliefs, based on evidence, we have to say where these beliefs were before we obtained the evidence.

It is time for us to consider views of probability in situations where we will have nothing to count, either a priori or anywhere else.

9.5 Non-enumerative Probabilities: Nothing to Count

Intelligence analysts will encounter works by some individuals who will argue that the term probability is only applicable to the enumerative situations just described above. In short, we are always out of luck applying Bayes’ rule because of its requirement for subjective prior probabilities; and we are especially out of luck applying probabilities in situations in which the events of concern are singular, unique, or one-of-a-kind, and so we have nothing to count.
It will only be possible for us to provide a very brief account of the following four views of uncertainty assessments. We have chosen to focus on what each one has to tell us about what the force or weight of evidence means.

**9.5.1 Epistemic Probability (1): The Subjective Bayesian View**

We refer to our first non-enumerative view as an epistemic view, since it assumes that probabilities in any case are based on some kind of knowledge, whatever form it may take. In short, probabilities are the result of informed judgments. Many statisticians now favor the use of Bayes’ rule in enumerative or frequentistic situations and have no objection to subjective assessments of prior probabilities. Bayes’ rule requires the assessment of two basic probabilistic ingredients: prior probabilities on hypotheses, and likelihoods or their ratios. As we will illustrate, it is these likelihoods and their ratios that are the ingredients of Bayes’ rule that concern the inferential force of evidence. Furthermore, many persons favor the use of Bayes’ rule for combining subjective assessments of all the prior and likelihood ingredients of Bayes’ rule. But what these persons require is that these assessments be entirely consistent with Kolmogorov’s three axioms and his definition of conditional probabilities we noted above. Since Bayes’ rule rests on these axioms and definition, we must adhere to them in order to say that our assessment process is coherent or consistent.

Here is an example of how likelihoods and their ratios provide a method for grading the force of an item of evidence. This is an example of a situation involving a singular evidence item where we have nothing to count. Suppose an analyst’s interest concerns whether or not the Iranians are supplying parts necessary for the construction of shaped explosive devices to a certain insurgent militia group in Iraq. The new evidence we have is as follows:

Evidence E*: A member of the Qods (Jerusalem) division of the Islamic Republican Guards was captured less than one kilometer away from a location in Iraq at which parts necessary for the construction of these shaped explosives were found.

Suppose the analyst is entertaining the following binary hypotheses:

- **H**: “The Iranians are supplying parts necessary for the construction of shaped explosive devices.”
- **not-H**: “The Iranians are not supplying parts necessary for the construction of shaped explosive devices.”

Figure 72 is a picture of the likelihoods whose ratio Bayes’ rule says we need to indicate the force of evidence E* on H and not-H.

Likelihoods always have the form $P(\text{evidence}, \text{given hypothesis})$. There are two likelihoods as shown in Figure 72: $P(E^*, \text{given } H)$ and $P(E^*, \text{given } \text{not-}H)$. The force of evidence $E^*$ is given by the relative sizes of these two likelihoods. Suppose the analyst judges that $P(E^*, \text{given } H) = 0.50$ and $P(E^*, \text{given } \text{not-}H) = 0.10$. This says that this evidence is five times more likely given $H$ than it is given not-$H$. In short, the evidence favors $H$ over not-$H$ by a factor of five. Likelihood ratios can be any two probability values,
except for the one in the denominator of any likelihood ratio, which must not be zero. Bayes’ rule shows us how to combine likelihoods for multiple evidence items and prior probabilities of hypotheses in order to obtain posterior probabilities of hypotheses, which must sum to 1.0 when we have mutually-exclusive and exhaustive hypotheses, as we do in this example.

**Figure 72. A Bayesian Likelihood Ratio.**

So, using this subjective Bayesian approach, an analyst would be entitled to express the extent of his/her uncertainty in an analysis using numerical probability assessments provided only that they conform to Kolmogorov’s axioms.

### 9.5.2 Epistemic Probability (2): Belief Functions

Both the enumerative and the subjective Bayesian interpretations of probability conform to Kolmogorov’s three axioms. We asserted that these axioms rest on the investigation of replicable or repeatable processes such as statistical analysis of the results obtained in a sample of observations. But there are many reasons for wondering whether these three axioms remain self-evident concerning subjective probability judgments we all make from time to time involving unique events for which no enumerative process can be involved. In a very influential work, the probabilist Professor Glenn Shafer pointed to an array of difficulties associated with Axiom 3 concerning the additivity of enumerative probabilities for mutually exclusive events (Shafer, 1976). In particular, Shafer asserts that this axiom places various constraints on our judgments or beliefs about uncertainty that we may not be willing to accept. Here it is only necessary to mention two of the difficulties Shafer mentions:

- Indecisions we routinely face concerning ambiguities in our evidence.
- Instances in which we encounter what historically has been called “pure” evidence.

In so many instances we may not be sure what evidence is telling us, and so we wish to be able to withhold a portion of our beliefs and not commit it to any particular hypothesis or possible conclusion. A very important element in what Shafer terms belief functions is that the weight of
Assessing and Reporting Uncertainty: Some Alternative Methods

evidence means the degree of support evidence provides to hypotheses we are considering. Shafer allows that we can grade degree of support $s$ on a 0-1 scale similar to the scale for Kolmogorov probabilities; but we can do things with support assignments $s$ that the Kolmogorov additivity Axiom 3 does not allow. To illustrate, suppose we revisit the analyst concerned about whether or not the Iranians are supplying parts necessary for the construction of shaped explosive devices. Her hypotheses are: $H$: The Iranians are supplying parts necessary for the construction of shaped explosive devices, and $\neg H$: The Iranians are not supplying parts necessary for the construction of shaped explosive devices.

At some stage this analyst is required to state her beliefs about the extent to which the evidence supports $H$ or $\neg H$. Here is her assessment:

\[
\begin{array}{ccc}
H & \neg H & \{H \text{ or } \neg H\} \\
\hline
s & 0.5 & 0.3 & 0.2
\end{array}
\]

What does this support assignment mean? She is saying that she believes the evidence supports $H$ exactly to degree $s = 0.5$, and that this evidence also supports $\neg H$ exactly to degree $s = 0.3$. But there is something about this evidence that makes her unsure about whether it supports $H$ or $\neg H$. So, she has left the balance of her $s$ assignment, $s = 0.2$, uncommitted among $H$ or $\neg H$. In other words, she is telling us that she has withheld a portion of her beliefs because she is not sure what some element of her evidence is telling her. She resists doing the following assignment of her beliefs.

If she were required to obey Kolmogorov Axiom 3, she would not be allowed to be indecisive in any way in stating her beliefs. Here is what her support assignment would have to look like:

\[
\begin{array}{ccc}
H & \neg H \\
\hline
s & a & (1 - a)
\end{array}
\]

In this case, she would be required to say that the evidence supports $H$ to degree $s = a$, and supports $\neg H$ to degree $s = (1 - a)$ in agreement with Axiom 3 since $H$ and $\neg H$ are mutually exclusive and exhaustive. In short, Kolmogorov Axiom 3 does not permit the analyst any indecision in stating her beliefs; she must commit all of it to either $H$ and to $\neg H$. This, she believes, would not be a faithful or accurate account of her beliefs.

But Shafer’s belief function approach allows us to cope with another difficulty associated with Kolmogorov’s axioms. For centuries it has been recognized that a distinction is necessary between what has been termed mixed and pure evidence. Mixed evidence has some degree of probability under every hypothesis we are considering. But pure evidence may support one hypothesis but say nothing at all about other hypotheses. In other words, we may encounter evidence that we believe offers zero support for some hypothesis. Here is another example involving our Iran-Iraq situation. Suppose our analyst encounters an item of evidence she believes supports $H$ to a degree, but she believes offers no support at all for $\neg H$. Here is her support assignment $s$ for this evidence:

\[
\begin{array}{ccc}
H & \neg H & \{H \text{ or } \neg H\} \\
\hline
s & 0.5 & 0 & 0.5
\end{array}
\]

147
In this situation the analyst is saying that the evidence supports H to degree $s = 0.5$, but offers no support at all to not-H. The rest of her support she leaves uncommitted between H and not-H. But now we have to examine what $s = 0$ for not-H means; does it mean that not-H could not be supported by further evidence? The answer is no, and the reason why it is no allows us to compare what ordinary probabilities mean in comparison with what support $s$ means. This comparison is shown in Figure 73.

$$
\begin{array}{c}
\text{(a) Conventional Probability} \\
\text{Disbelief or Impossible} & \text{Certain or Complete Belief} \\
0 & 1 \\
\text{Value 0 in conventional probability refers to an event judged to be impossible and one for which you completely disbelieve. We will refer to this scale again in Section 9.5.3 when discussing Baconian probability. But all 0 means on Shafer's $s$ scale is lack of belief, not disbelief. This is very important, since we can go from lack of belief to some belief as we gather more evidence. But we cannot go from disbelief to some belief. On a conventional probability scale, a hypothesis once assigned the probability value 0 can never be resuscitated by further evidence, regardless of how strong it may be. But some hypothesis, assigned the value $s = 0$, can be revised upward since we can go from lack of belief to some belief in this hypothesis when and if we have some further evidence to support it. Thus, $s$ allows us to account for pure evidence in ways that ordinary probabilities cannot do.}
\end{array}
$$

Finally, since one of the Kolmogorov axioms is violated in Shafer’s system, we should not expect to see Bayes’ rule as being the device that allows us to combine support assignments across multiple items of evidence. There is a different rule, called Dempster’s rule, for combining support assignments. Further discussion of the Shaferian and Bayesian views of the weight of evidence are given elsewhere (Schum, 1994/2001, pp. 222 - 243).

### 9.5.3 Baconian Probability and the Importance of Evidential Completeness

Here is a view of probabilistic reasoning that puts particular emphasis on a very important matter not specifically addressed in any other view of probability. In this view the weight of evidence depends on how much relevant and credible evidence we have and upon how complete is our coverage of existing evidence on matters we ourselves have recognized as being relevant in the analysis at hand. This Baconian view of probability and the weight of evidence is perhaps the least well known of any current view of probability, but it deserves much wider recognition. This Baconian view rests on the work of Professor L. Jonathan Cohen from Queens College, Oxford (Cohen, 1977, 1989).
The label “Baconian” on this system of probability acknowledges the work of Sir Francis Bacon (1561 – 1626) who revolutionized the process of inference in science. Bacon argued that attempting to prove some hypothesis by gathering instances favorable to it is mistaken, since all it would take to refute the generality of this hypothesis was one unfavorable instance of it. What Bacon argued was that we ought to design research with the objective of eliminating hypotheses. The hypothesis that best resists our eliminative efforts is the one in which we should have the greatest confidence. As this eliminative process proceeds, it is obvious that we should not keep performing the same test over and over again. What we need is an array of different tests of our hypotheses. The hypothesis that holds up under the most varied set of tests is the one having the greatest probability of being correct. So, Baconian inferences are eliminative and variative in nature.

Several attempts were made in the past, without success, to relate conventional probability to eliminative and variative inferences. Jonathan Cohen was the first person to generate a system of probabilities expressly congenial to this. His Baconian system of probabilities has properties unlike the two we have examined so far. Baconian probabilities have only ordinal properties and cannot be combined algebraically in any way. Figure 74 shows Baconian probabilities on a scale that can be compared with the conventional probability scale shown as (a) in Figure 73.

On the conventional probability scale, 0 means disproof; but on the Baconian scale, 0 simply means lack of proof. A hypothesis now having zero Baconian probability can be revised upward in probability as soon as we have some evidence for it. As noted, we cannot revise upward in probability any hypothesis disproved, or having zero conventional probability.

Figure 75 shows the major point of interest for intelligence analysts in this Baconian system which we illustrate with an example. Professor Cohen argues that in any evidential reasoning situation we are always out on an inferential limb that might be longer and weaker than we may believe it to be. Suppose an analyst has generated three hypotheses \{H_1, H_2, and H_3\}. A body of evidence has been examined and Bayes’ rule is used to combine the likelihoods for this evidence together with stated prior probabilities. The result is that Bayes’ rule shows the posterior probability of H_3, in light of the evidence, to be 0.998, very close to certainty on the Kolmogorov probability scale. Therefore, the analyst confidently reports his conclusion that H_3 is true to an important “customer,” together with its very large posterior probability he has determined. A short time passes and the analyst hears the depressing news that H_3 is not true, a fact his customer will surely let him know about. What can have gone wrong? After all, the analyst performed an analysis that is highly respected by many persons.
A person having knowledge of Cohen’s Baconian probability arrives on the scene of the analyst’s distress and makes the following comments:

You gathered some evidence, fair enough, quite a bit of it in fact. But, how many relevant questions you can think of that were not answered by the evidence you had? Depending upon the number of these unanswered questions, you were out on an inferential limb that was longer and weaker than you imagined it to be (see Figure 75). If you believed that these unanswered questions would supply evidence that also favored $H_3$, you were misleading yourself since you did not obtain any answers to them. The posterior probability you determined by itself is not a good indicator of the weight of evidence. What makes better sense is to say the weight of evidence depends on the amount of favorable evidence you have and how completely it covers matters you said were relevant. In your analysis you completely overlooked the inferential importance of questions your existing evidence did not answer.

Apart from the Baconian system, no other view of evidential reasoning focuses on evidential completeness and the importance of taking into account questions recognized as being relevant that remain unanswered by the evidence we do have. This is why Jonathan Cohen’s Baconian system is so important in intelligence analysis. What we do not take account of in intelligence analyses can hurt us very badly.

As we all know, intelligence analysts frequently have to make inferences about matters for which they often have scant evidence, or no evidence at all. In other instances in which there may be available evidence, analysts may have no time to search for it or consider it carefully. In such cases, analysts say they are forced to make assumptions that may be vigorously challenged. Analysts, and those they serve, usually employ the term “assumption” when there is another term that could be used. There are reasons for arguing that the word “generalization” is preferable to the word “assumption.” All inferences, made by intelligence analysts or anyone else, require generalizations that license inferential steps, and also require ancillary evidence to support the applicability of the generalization in the
particular case in which it is being invoked. This is why we have said that generalizations and ancillary evidence form the “glue” that holds our arguments together. On some occasions, of course, this glue will fail to hold an argument together. The Baconian view being discussed offers much guidance in such matters.

But there is another important consequence of lack of time and evidence. This involves failure to decompose complex arguments into logically consistent or defensible stages. All arguments from evidence to hypotheses, or matters to be proved or disproved, involve chains of reasoning. Each link in such chains involves a source of doubt or uncertainty. Under the pressures of time or lack of evidence, an analyst may not even articulate in any way what these interposed sources of doubt may be. This results in a suppression of uncertainties and can lead to inferential miscarriages of many sorts. In our TIACRITIS system we have used the term “drilling down” to indicate how much detail will be captured by an analyst in the construction of arguments from evidence. TIACRITIS allows an analyst to drill down to various levels depending upon the time and evidential resources available to an intelligence analyst. In many cases this drilling down will be only very slight or nonexistent, in which cases the analysts will say that they must make assumptions. But this amounts to giving a generalization the benefit of the doubt (without supporting it in any way), or to believing as-if some conclusion were true (absent any evidential support for it), or to taking something for granted without testing it in any way. All of these situations involve the suppression of uncertainties.

It happens that only the Baconian probability system provides any guidance about how to proceed when we must give benefit of doubt, believe as-if, or take things for granted. The major reason is that it acknowledges what almost every logician says about the necessity for asserting generalizations and supplying tests of them in evidential reasoning. Search the Bayesian or Belief Function literature and you will find almost no discussion of generalizations and ancillary tests of them. Suppose we are interested in inferring F from E. Bayes’ rule grinds to a halt when we have no basis for assessing the likelihoods P(E given F) and P(E given not-F). Bayesians counter by saying that we will always have some evidence on which to base these judgments. But they never say what this evidence is in particular cases and how credible it might or might not be. The Belief Function approach comes closer by saying that we can assess the evidential support for a body of evidence that may include both directly relevant and at least some ancillary evidence. Following is an account of the Baconian license for giving a generalization benefit of doubt, believing as-if it were true, or taking it for granted, provided that we are willing to mention all of the uncertainties we are suppressing when we do so. Stated another way, we must try to account for all of the questions we can think of that remain unanswered by the absence, or very scant amount, of evidence. This will be crucial in assisting an analyst to defend the assumption this analyst says is being made.

Here are the essentials of Cohen’s Baconian approach to reasoning based on little or no ancillary evidence to either support or undermine a generalization. The first step, of course, is to make sure the generalization is not a non sequitur, i.e., it makes logical sense. In the simplest possible case, suppose we are interested in inferring proposition or event F from proposition or event E. The generalization G in doing so might read: “If E has occurred, then probably F has occurred.” We recognize this if-then statement as an inductive generalization since it is hedged. Generalization G might also be stated in the
future tense: “If E has occurred, then F will probably occur.” Second, we consider various tests of this generalization using relevant ancillary evidence. Third, we consider how many evidential tests of this generalization there might be; suppose we identify N such tests. The best case would be when we perform all N of these tests and they all produce results favorable to generalization G. But we must not overlook generalization G itself; we do so by assigning it the value 1; so we have N+1 things to consider. Now we are in a position to show what happens in any possible case.

First, suppose we perform none of these N evidential tests. We could still proceed by giving generalization G the benefit of the doubt and detach a belief that F occurred (or will occur) just by invoking this generalization G regarding the linkage between events E and F. To do this we assign G the value 1 so that we are considering N + 1 things: the N evidential tests and our generalization G. So, when no evidential tests are performed, we are saying: “Let’s believe as-if F occurred based on E and generalization G.” This would amount to saying that the Baconian probability of event F is $B(F) = 1/(N+1)$. This expression is never a ratio, all it says is that we considered just one thing in our inference about F from E, namely just the generalization G. We could also say, “Let’s take event F for granted and believe that F occurred (or will occur) because E occurred as our generalization G asserts.” However, note that in doing so, we have left all N ancillary evidential questions unanswered. This we represent by saying that our inference of F from E has involved only one of the N+1 considerations and so we have $(N + 1 – 1) = N$, the number of questions we have left unanswered. As far as evidential completeness is concerned, this is when the evidence we have is totally incomplete. But the Baconian system allows us to proceed anyway based on giving a generalization benefit of doubt.

Now suppose we have performed some number k of the N possible ancillary evidential tests of generalization G, as asserted above. The Baconian probability of F in this situation is given by $B(F) = (k + 1)/(N +1)$. The difference between the numerator and denominator in such an expression will always equal the number of unanswered questions as far as the testing of G is concerned. In this case we have $(N + 1) – (k + 1) = N – k$ questions that were unanswered in a test of generalization G. Now, how do we decide whether to detach a belief in proposition or event F based on evidence E, our k tests of G, and G itself? The answer, of course, depends on the results of our k tests of G and how many tests there are. First, suppose that k is very small, say one or two. If both were favorable to G, we would still be giving G the benefit of the doubt since there are N – 1, or N -2 questions remaining about G that we have not answered.

But now suppose that k is larger and that not all answers to these k questions are favorable to generalization G. Under what conditions are we entitled to detach a belief that event F occurred, based on evidence E, generalization G, and the k tests of G? The answer requires a subjective judgment by the analyst about whether the tests, on balance, favor or disfavor G. When the number of the k tests disfavoring G exceeds the number of tests favoring G, we might suppose that we would always detach a belief that event F did not occur, since G has failed more tests than it survived. But this will not always be such an easy judgment if the number of tests G passed were judged to be more important than the tests it failed to pass. In any case, there are N – k tests that remain unanswered. Suppose that k is quite large but the difference between the number of tests favorable to G is only slightly larger than the number of tests unfavorable to G. In such cases the analyst might still give event F the benefit of the
doubt, or believe, at least tentatively, as-if F occurred pending the possible acquisition of further favorable tests of G.

Whatever the basis for an assumption or a benefit of doubt judgment there is, one of the most important things about the Baconian approach is that the analyst must be prepared to give an account of the questions that remain unanswered in evidential tests of possible conclusions. This will be especially important when analysts make assumptions, or more appropriately, give generalizations benefit of doubt, draw as-if conclusions, or take certain events for granted. These are situations in which analysts are most vulnerable and in which Baconian ideas are most helpful. Again, the Baconian system is the only system we know about that is concerned about the completeness of evidence and the importance of considering how many questions remain unanswered by the evidence we have.

9.5.4 Imprecision and Fuzzy Probabilities

The final way an analyst can express uncertainty about a conclusion reached is to use words rather than numbers. The analyst might say: “I am very certain that...”; “What probably will happen is...”; “It is unlikely that...”; and so on. Years ago, Sherman Kent tried his best to relate intelligence analysts’ verbal expressions of uncertainty such as these to specific ranges of numbers on a conventional probability scale (Kent, 1994). One instance we have all heard about involving words was use of the term “slam dunk” to indicate virtual certainty. This illustrates how no less care must be taken in verbal assessments of uncertainty than in the numerical methods just discussed.

Verbal expressions of uncertainty are certainly not confined to intelligence analysis. In the field of law, for example, forensic standards of proof are always employed using words instead of numbers. We all know about standards such as: “beyond reasonable doubt” (in criminal cases); “preponderance of evidence” (in civil cases); “clear and convincing evidence” (in many senate and congressional hearings); and “probable cause” (employed by magistrates to determine whether a person should be held in custody pending further hearings).

All the verbal examples just cited have a current name; they can be called fuzzy probabilities. Words are less precise than numbers. There is now extensive study of fuzzy inference involving what has been termed approximate reasoning, which involves verbal statements about things that are imprecisely stated. Here is an example of approximate reasoning: “Since John believes he is overworked and underpaid, then he is probably not very satisfied with his job.” All the underlined ingredients of this statement are imprecise or fuzzy. We are indebted to Professor Lotfi Zadeh (University of California, Berkeley), and his many colleagues, for developing logics for dealing with fuzzy statements, including fuzzy probabilities (Zadeh, 1983). It is, of course, entirely reasonable to grade the force of evidence in fuzzy terms, such as: “strong force,” “weak force,” “very strong force,” and so on.

We have mentioned that Sherman Kent was concerned with fuzzy probabilities long before Lofti Zadeh began to study them carefully (Kent, 1994). But an American jurist named John H. Wigmore was well ahead of Sherman Kent as far as using words to grade uncertainty in evidential reasoning (Wigmore, 1913; 1937). Wigmore understood that the linkages between propositions in chains of reasoning reveal the sources of doubt or uncertainty we mentioned in connection with Figure 4 and
Figure 5. What Wigmore was concerned about was the inferential force of one proposition on another in these chains of reasoning. But Wigmore was no probabilist and did not consider any numerical methods for grading evidential force. Instead, he used words such as “strong force,” “weak force,” and “provisional force” to indicate the strength of linkages in chains of reasoning. The point here is that verbal assessments of uncertainty in intelligence analysis have a long and very respectable lineage.

Zadeh went a bit farther than Kent did in his methods for relating verbal assessments of uncertainty with numerical equivalents. Zadeh employed what he termed a possibility function, $\mu$, to indicate ranges of numerical probabilities a person might associate with a verbal expression of uncertainty. Zadeh reasoned that a person might not be able to identify a single precise number he/she would always associate with a verbal statement or fuzzy probability. Here is an example of a possibility function for the fuzzy probability “very probable.”

Asked to grade what numerical probabilities might be associated with an analyst’s fuzzy probability “very probable,” the analyst might respond as follows:

For me, “very probable” means a numerical probability of at least 0.72 and at most 0.85. If it were any value above 0.85, I might use a stronger term such as “very, very probable.” I would further say that I would not use the term “very probable” if I thought the probability was less than 0.72. In such cases, I would weaken my verbal assessment. Finally, I think it is most possible ($\mu = 1.0$) that my use of the verbal assessment “very probable” means something that has about 0.82 of occurring.

If the analyst decides that “very probable” declines linearly on either side of $\mu = 1.0$, we would have the possibility function shown in Figure 76.

![Figure 76. Possibilities and fuzzy probabilities.](image)

9.6 A Summary of Uncertainty Methods and What They Best Capture

We regard the alternative views we have discussed for assessing and reporting uncertainty as being not only interesting but also necessary. Each view captures important elements of probabilistic reasoning, but no single view captures all of them. Table 13 presents a summary of things analysts might consider when they contemplate how to assess and report uncertainty that will be associated with their conclusions. We include in this table just the four views we have discussed concerning non-enumerative situations. Analysts can easily find many works on statistics, frequentistic or Bayesian, in enumerative situations.
situations in which they can estimate probabilities from observed relative frequencies. Further explanations of the entries in this table appear below.

Table 13. A Summary of Non-Enumerative Uncertainty Methods.

<table>
<thead>
<tr>
<th>Major Strength</th>
<th>Subjective Bayes</th>
<th>Belief Functions</th>
<th>Baconian</th>
<th>Fuzzy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting for <em>incompleteness</em> of coverage of evidence.</td>
<td></td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Coping with <em>inconclusiveness</em> in evidence.</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Coping with ambiguities or imprecision in evidence, and judgmental indecision.</td>
<td></td>
<td></td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Coping with <em>dissonance</em> in evidence.</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Coping with <em>source believability</em> issues.</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capturing a wide variety of evidential subtleties or complexities</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Applications in current <em>inference network</em> technologies</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Most familiar ways of expressing uncertainty</td>
<td>☑</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The first entry in Table 13 lists a major strength that is exclusive to the Baconian system, its concern about how much favorable evidence was taken into account in an analysis, and how completely this evidence covered matters judged relevant to conclusions that could be reached. A major question this form of analysis allows us to address is the extent to which questions that have not been answered by existing evidence could have altered the conclusion being reached. It would be quite inappropriate to assume that answers to the remaining unanswered questions would, if they were obtained, all favor the conclusion that was being considered. This, of course, requires analysts to consider carefully matters relevant to any conclusion that are not addressed by available evidence. We acknowledge that completeness matters are difficult to manage in current intelligence in which analysts are asked to provide conclusions on very short order. The shorter the time available for the assessment of evidence the more unanswered questions there will be. We hope our customers requiring quick analyses appreciate this fact.

The second entry in Table 13 notes that all four of the uncertainty methods have ways for dealing with the inconclusive nature of most evidence; but they do so in different ways. The Subjective Bayesian does so by assessing non-zero likelihoods for the evidence under every hypothesis being considered, as we observed in the example in Figure 72. Their relative sizes indicate the force the evidence is judged to
have on each hypothesis. But the Belief Function advocate assigns numbers indicating the support evidence provides for hypotheses or subsets of them. We should be quick to notice that Bayesian likelihoods do not grade evidential support, since in belief functions an analyst can say that an item of evidence provides no support at all to some hypothesis. But a Bayesian likelihood of zero under a particular hypothesis would mean that this hypothesis is impossible and should be eliminated. Offering no support in belief functions does not entail that this hypothesis is impossible, since some support for this hypothesis may be provided by further evidence. The Baconian acknowledges the inconclusive nature of evidence by assessing how completely, as well as how strongly, the evidence favors one hypothesis over others. In Fuzzy probabilities it would be quite appropriate to use words in judging how an item or body of evidence bears on several hypotheses. For example, an analyst might say, “This evidence is indeed consistent with $H_1$ and $H_2$, but I believe it strongly favors $H_1$ over $H_2$.”

The third entry in the table first acknowledges the Belief Function and Fuzzy concerns about ambiguities and imprecision in evidence. In the Belief Functions approach, an analyst is entitled to withhold belief for some hypotheses in the face of ambiguous evidence. In such cases the analyst may not be able to decide upon the extent to which the evidence may support any hypothesis being considered, or even if the evidence supports any of them. Judgmental indecision is not allowed in the Bayesian system since it assumes the analyst can say precisely how strongly evidence judged relevant favors every hypothesis being considered. Judgmental indecision, as allowed in the Belief Functions system, seems a natural attribute of many evidential matters encountered by intelligence analysts. Ambiguities in evidence may be commonly encountered. The Fuzzy advocate will argue that ambiguities or imprecision in evidence hardly justifies precise numerical judgments. In the face of fuzzy evidence we can only make fuzzy judgments of uncertainty.

The fourth entry in Table 13 shows that all four probability systems have mechanisms for coping with dissonant evidence in which there are patterns of contradictory and divergent evidence. Recall that dissonant evidence is directionally inconsistent; some of it will favor certain hypotheses and some of it will favor others. In resolving such inconsistencies, both the Bayesian and Belief Functions approach will side with the evidence having the strongest believability, though the mechanisms for doing so differ in Bayes’ rule and Dempster’s rule. The Bayesian approach to resolving contradictions is especially interesting since it shows how “counting heads” is not the appropriate method for resolving contradictions. In times past, “majority rule” was the governing principle. Bayes’ rule shows that what matters is the aggregate believability on either side of a contradiction. The Baconian approach also rests on the strength and aggregate believability in matters of dissonance, but it also rests on how much evidence is available on either side and upon the questions that remain unanswered. In Fuzzy terms, evidential dissonance, and how it might be resolved, can be indicated in verbal assessments of uncertainty. In such instances an analyst might say, “We have dissonant evidence favoring both $H_1$ and $H_2$, but I believe the evidence favoring $H_1$ predominates because of its very strong believability.”

Row five in Table 13 concerns the vital matter of assessing the believability of intelligence evidence. From considerable experience, we find that the Bayesian and Baconian systems are especially important when they are combined. In many cases these two radically different schemes for assessing uncertainty are not at all antagonistic but are entirely complementary. Let us consider a body of evidence about a
HUMINT asset or informant. Ideas from the Baconian system allow us to ask: *How much evidence do we have about this asset, and how many questions about his asset remain unanswered?* Ideas from the Bayesian system allow us to ask: *How strong is the evidence we do have about this asset* (Schum, 1991; Schum and Morris, 2007)?

Row six in Table 13 has just one entry that involves the Bayesian system. The mathematical underpinnings of this system lead to a very rich system for capturing a very wide array of evidential and inferential subtleties or complexities. Many of these complexities are described and analyzed in another work (Schum, 1994/2001, Chapters 6, 7, and 8 in both editions). Some of them can involve single items of evidence while others involve many items in a mass of evidence. In virtually all cases many or most of the probabilistic ingredients of these situations will involve non-enumerative probabilities. The Bayesian system incorporates a concept called conditional dependence that provides the primary means for capturing evidential and inferential complexities for study and analysis. One distinct virtue of Bayesian analyses of evidence is that it prompts us to ask questions of our evidence that we might never have thought of asking if we had not performed this kind of analysis. There are so many important subtleties in evidence that do not meet the eye on casual examinations of evidence.

The seventh item in Table 13 concerns the rapidly emerging technology for the analysis of complex arguments based on many items of evidence; they are referred to as inference networks. Both Bayesian and Belief Function networks have been developed, but it seems fair to say that Bayesian networks have received the most attention in intelligence-related work. Although all inference networks have common properties, there are quite different purposes to which inference networks can be put. In some situations an inference network is constructed in order to make sense out of an emerging mass of evidence. In other instances an inference network is constructed in order to provide a model of some complex process involving many linked probabilistic variables. These models provide a basis for predictions a model allows when we have various combinations of evidence for some of its probabilistic variables. Regardless of the purpose for which an inference network is being constructed, the basic methodology can be described as “divide and conquer” or “task decomposition.” A complex evidence-based inference task is broken down into bits and pieces that are allegedly easier to manage than a “holistic” assessment in which the analyst tries to assess and combine all necessary probabilistic ingredients in his/her head. One should keep in mind that this divide and conquer approach makes necessary the judgment of often huge numbers of probabilities, not all of which may be easy to assess.

The final row in Table 13 simply acknowledges the fact that the subjective Bayesian and the Fuzzy systems make use of uncertainty responses that are the most familiar. We have all been tutored in conventional probabilities and can easily express uncertainty in terms of numbers between zero and one, as percentages when they are appropriate, or in terms of odds. But these same responses, with the exception of percentages, are appropriate for the subjective Bayesian. And, we certainly all know how to use words in the form of Fuzzy probabilities to indicate the extent of our uncertainty; we do it all the time. The responses required in the Belief Functions and Baconian probability systems are certainly less familiar. But in order to take full advantage of what these systems allow in uncertainty assessment, analysts should become more familiar with the works of Professors Jonathan Cohen and Glenn Shafer that we cited above.
9.7 Assessing and Reporting Uncertainty in TIACRITIS

We discussed how the Bayesian system appears in both the enumerative and non-enumerative situations. In this system we have rules for dealing with intersections and unions of propositions or events, but such rules rely on our having specific numerical judgments or statistical estimates of probabilities. One major trouble is that in complex evidential reasoning tasks, such as in intelligence analyses, the task of combining our probabilistic beliefs in Bayesian terms often requires a huge number of specific probability assessments, often many more than intelligence analysts have either the time or resources to provide. In our experience, intelligence analysts usually reject the task of supplying specific probability assessments for the many details that arise in complex analyses. Remember that our approach, in common with Heuer’s, rests on task decomposition, or divide and conquer. When we do this, there is literally no telling how many specific detailed probabilities would be required in a complex problem expressed in Bayesian terms. Analysts, when sufficiently prodded to do so, might be willing to assess one distribution of probabilities across some number of final hypotheses, as Sherman Kent advised years ago, to go along with their natural verbal assessments of uncertainty about these hypotheses. But even Sherman Kent did not advocate assessing the huge numbers of probabilities that would be necessary to combine in order to determine these final probability assessments. It’s clear that Kent did not even know how many probabilities would need to be combined in analyses based on masses of evidence.

Here is precisely where the Baconian and Fuzzy systems arise in importance. First, the probabilities in the Baconian system have only ordinal properties meaning that we can say only that hypothesis H₁ is more likely than H₂, but we cannot say how much more likely H₁ is than H₂. Second, in the Baconian system, it is never necessary to assess subjective probabilities. In our saying that H₁ is more probable than H₂, all we are saying is that there is more favorably relevant evidence on H₁ than there is on H₂. What counts most in the Baconian system is the completeness of our evidence and the extent to which we have questions that remain unanswered by the evidence we have. Here are the two most important Baconian properties of interest to us concerning intersections and unions; there are many other properties of this system that we do not need to consider for our work.

For Baconian Intersections: Suppose we have some events of interest like events F, G, and H. Suppose we have some favorably relevant evidence about each one of these events and have also considered how complete the evidence is for these events. So we determine that the Baconian probabilities (B) for these three events are B(F) ≥ B(G) ≥ B(H). Here’s what these probabilities say: we have more favorably relevant and complete evidence for event F than we do for event G, and more favorably relevant and complete evidence for event G than we have for event H. So, asked what the Baconian probability is for their intersection (F & G & H), we must say that B(F & G & H) = B(H). What this says is that the Baconian probability of the intersection of these three events is equal to the Baconian probability of the event with the least favorably relevant and complete evidence. This is an example of the MIN rule for Baconian intersections. We might compare this with the conventional probability of the intersection of these three events. Suppose that events F, G, and H are independent events where P(F) = 0.8, P(G) = 0.6, and P(H) = 0.4. In this case P(F & G & H) = (0.8)(0.6)(0.4) = 0.192 <
P(H) = 0.4. In the Baconian system the probability of a conjunction of events or propositions can never be less than that of the event having the smallest Baconian probability.

For Baconian Unions: Now consider the same case involving events F, G, and H. Again, suppose that B(F) ≥ B(G) ≥ B(H). Now what we wish to determine is the Baconian probability B(F or G or H). In this case, B(F or G or H) ≥ B(F), where B(F) is the largest of the Baconian probability for the events we are considering. This is the MAX rule for Baconian probability, and what it says is that the probability of a disjunction of events is at least as large as the largest Baconian probability of any of the individual events.

Now consider the Fuzzy probability system in which we have verbal expressions for probabilities. This is exactly what we encounter in so many fields like intelligence analysis, law, history, and others. One of the major matters in these fields is that persons cannot assess probabilities with any degree of precision. In some cases, the events themselves are imprecisely stated. In other situations the probability judgments cannot be stated with any defensible numerical precision. So, in these cases, people are left with the use of words to express the extent of their uncertainty. As an example, suppose we have three events or propositions A, B, and C. We consider the following Fuzzy probabilities (F) for these events, and we say the following:

- Event A is very likely.
- Event B is likely.
- Event C is very unlikely.

We express this by saying that F(A) > F(B) > F(C).

Fuzzy Intersections. In the situation just described, the Fuzzy conjunction of these three events F(A & B & C) = F(C), which is the minimum Fuzzy probability of the three events.

Fuzzy Unions. In the situation just described, the Fuzzy disjunction of these three events F(A or B or C) = F(A), which is the maximum Fuzzy probability of these three events.

So, in both of these very useful systems for reasoning based on evidence, we have MIN/MAX rules for combining probabilities for complex events. Our approach in TIACRITIS is to give examples of various event or proposition combinations using various standard means for expressing fuzzy, or verbally expressed, indications of our uncertainty. The Baconian and Fuzzy systems give us formal license to use the MIN and MAX rules we have just discussed. But there is one other Boolean connector we have not yet discussed: it is negation, where we have some event and its complement, like A and not-A. It is here that the Baconian and Fuzzy views depart.

Fuzzy Negation. Fuzzy negation is complementary. F(A) = 1 – F(not-A).

Baconian Negation. Baconian negation is not complementary. The Baconian rule is quite complex; here’s what it says: If we have A and not-A, if B(A) > 0, then B(not-A) = 0. What this means essentially is that we cannot commit beliefs simultaneously to two events that cannot both occur.
10 COMPETING HYPOTHESES AND ANALYSES

10.1 Problems with Argument Construction

We began our work by dwelling upon attributes of the very complex process of “connecting the dots” in intelligence analysis. Asked to give a one-sentence definition of the process of connecting the dots, we offer the following:

It is the process of marshaling our thoughts and our evidence in order to generate productive hypotheses, and then to form defensible and persuasive arguments on hypotheses that seem most favored by the evidence we have.

As we noted, generating hypotheses as well as arguments rests on imaginative as well as critical reasoning. Further, the arguments we generate rest on evidence having the three credentials: relevance, believability, and inferential force or weight. No evidence ever comes to us with these three credentials already attached; they must be established by the defensible arguments we construct. One thing this means is that the process of intelligence analysis rests on the careful structuring of defensible arguments. How persuasive these arguments will be depends, in large part, on how we assess the inferential force or weight of the evidence we have. As we discussed in Section 9, there are various ways in which this can be done.

We began discussion in Section 0 on the importance and necessity of decomposing evidential reasoning problems by giving you an example of how failure to do so invites all manner of analysis failures. We provided an example of how your own undecomposed and unstructured analysis, based on your “off the top of your head” or holistic analysis, was demolished by your spouse’s penetrating and critical questions that you could not answer. The same thing can and will happen to intelligence analysts facing criticism, not from their spouses, but from policy-making customers or members of the press, who are often eager to demolish an analysis whose results are made public. The best protection an intelligence analyst has against these critics is carefully structured arguments bearing on the conclusions that were reached in an analysis. Such careful structuring, of course, requires the decomposition of a problem in as much detail as is possible. But there are some obvious problems here that we will always have to consider.

The first problem is that there are bound to be disagreements among analysts themselves about which argument patterns are best and, of course, about which conclusions should be reached. Two or more analysts may construct different arguments or chains of reasoning from the same evidence; the result can be that these analysts will draw different conclusions from the same evidence patterns. Remember that argument construction rests in large part on the imaginations of the persons doing the construction. What analyst A imagines an argument to be may be quite different than what analyst B imagines. In many cases, different analysts may consider different patterns of potential evidence to begin with. In other words, their arguments begin from different possible evidential foundations. What analyst A takes to be the essential dots to be connected may be quite different from the dots analyst B
considers. We cannot assess the relative merits of A’s and B’s arguments unless we know what patterns of dots they have each tried to connect. But this requires that they have decomposed their evidential reasoning problems in enough detail so that they can tell us which patterns of dots they have tried to connect.

The second problem endemic in argument construction is that arguments are subject to criticism in various ways. The major issue here is the defensibility of an argument. Here are some examples of how arguments can be criticized.

Suppose an analyst A constructs the following chain of reasoning from evidence E* to hypothesis H. He says, “From evidence E* we can infer that event E did probably occur; from event E we can infer that event F probably occurred; from event F we can infer that event G probably occurred; and finally, if event G occurred, we can infer that hypothesis H is probably true.”

Now along comes a critic, analyst B, who listens to this argument. She says, “You have a disconnect in your argument. I claim that your inference of G from F is non sequitur; G does not follow from F. This makes your whole argument bearing on the relevance of evidence E* on hypothesis H incoherent and indefensible.” All it takes is showing that one of the links in a chain of reasoning breaks. This is enough to uncouple the relevance linkage from E* to H.

But another critic, analyst C, hears this dialogue between analysts A and B. She says, “I agree with B that event G in A’s argument does not follow from event F. But there may be a way of rescuing A’s original argument. If A inserts event J between events F and G, and says event J follows from event F, and G follows from event J, then the rest of the argument would make sense to me.” This whole defensibility dialogue between analysts A, B, and C was possible only because A decomposed his argument from evidence E* to hypothesis H. If A had only said (holistically), “Evidence E* is obviously and strongly relevant to hypothesis H,” critics who disagree would not know where to begin their criticism of A’s argument. The message here is that assessing the defensibility of an argument requires that it can be decomposed.

The third problem we always face in argument construction is that there is never any “true” or “uniquely correct” argument available in any evidential reasoning task. Stated in other words, there is never any “answer key” or “gold standard” against which we can assess the adequacy of any argument. Any argument can be criticized on a number of grounds. No person or system - including TIA CRITIS - can supply you with uniquely correct arguments. A related fact is that intelligence analysts, faced with the task of constructing arguments in defense of the relevance, believability, and force or weight of evidence, will never have any reference sources or persons who can tell them what any argument should be. This may come as a source of comfort to analysts who do not take argument construction seriously. But it is no source of comfort at all because an analyst will always encounter critics who will offer alternative arguments and conclusions at variance with what this analyst believes to be the ones that should be taken most seriously. As we illustrate below, the TIA CRITIS system allows you to compare your arguments against others that might be constructed.
There are other grounds for criticizing conclusions reached in an analysis, even by the most carefully constructed arguments. These are criticisms concerning the inferential strength of arguments and the evidence on which they are based. To illustrate, let’s return to the analysts $A$, $B$, and $C$ who quibbled about the argument or chain of reasoning $A$ constructed originally from evidence $E^*$ to hypothesis $H$. Suppose these three analysts now agree that the revised argument from $E^*$ to $E$, then from $E$ to $F$, then from $F$ to $J$, then from $J$ to $G$, and finally from $G$ to $H$ makes sense. Analyst $A$ is now asked by analysts $B$ and $C$ if he still believes that $E^*$ offers strong support for hypothesis $H$. One thing true is that the force or weight of evidence depends on how strong each of the believability and relevance links in chains of reasoning are, which connect the evidence to the hypotheses. Analyst $A$ now says that he still believes that $E^*$ offers strong support for believing that hypothesis $H$ is true. Asked by $B$ and $C$ why he still believes this, $A$ says, “Thanks to your help, we now have a strong argument regarding the relevance of event $E$ on hypothesis $H$. Since my belief is that the source of evidence $E^*$ is very believable, this justifies my belief since we have a strong argument that rests upon a strong believability foundation.” In reply, both $B$ and $C$ say, “We cannot agree with the strength of your conclusion since we strongly believe that you have too strongly assessed the believability of the source of evidence $E^*$. On the evidence we have, the believability of this source is not nearly as strong as you believe it to be.” But analysts $B$ and $C$ could just as well have challenged the strength of any link in their relevance argument. If analyst $A$ had decomposed the link between evidence $E^*$ and event $E$, analysts $B$ and $C$ could have challenged specific attributes of the believability of the evidence.

10.2 Case Study: Comparison of Analyses of Competing Hypotheses

10.2.1 Objective

The objective of this case study is to learn how to compare the analyses of competing hypotheses in terms of the evidence used and the assessments and the assumptions made.

10.2.2 Summary

This case study continues the analysis example discussed in Sections 1.2 and 1.3 with the comparison of the analyses of the following hypotheses:

“The cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.”
“The cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.”
“The cesium-137 canister was misplaced.”

You will select them from the list of investigated hypotheses, and the system will display their solutions. You will then select any pair, and the system will display the differences in their analyses with respect to the evidence used and the assessments and assumptions made.

Proceed as indicated in the following instructions.
### 10.2.3 Instructions

1. Start the case study in TIACRITIS.

2. Select the **Hypothesis** menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 will be displayed.

3. Click on **[COMPARISON OF COMPETING HYPOTHESES]** for the “Selection mode.”

4. Select the following competing hypotheses by clicking on them:
   - “Assess whether the *cesium-137 canister* was stolen from the *XYZ warehouse* with the *MDC-578 truck*.”
   - “Assess whether the *cesium-137 canister* is used in a project without being checked-out from the *XYZ warehouse*.”
   - “Assess whether the *cesium-137 canister* was misplaced.”

5. The selected hypotheses are moved under “**Selected hypotheses**,” as illustrated in Figure 77.

<table>
<thead>
<tr>
<th>Selected hypotheses:</th>
<th>[HYPOTHESIS ANALYSIS]</th>
<th>[COMPARISON OF COMPETING HYPOTHESES]</th>
<th>[ANALYSES BY DIFFERENT ANALYSTS]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess whether the <em>cesium-137 canister</em> was stolen from the <em>XYZ warehouse</em> with the <em>MDC-578 truck</em>.</td>
<td></td>
<td>[DESELECT]</td>
<td></td>
</tr>
<tr>
<td>Assess whether the <em>cesium-137 canister</em> is used in a project without being checked-out from the <em>XYZ warehouse</em>.</td>
<td></td>
<td>[DESELECT]</td>
<td></td>
</tr>
<tr>
<td>Assess whether the <em>cesium-137 canister</em> was misplaced.</td>
<td></td>
<td>[DESELECT]</td>
<td></td>
</tr>
</tbody>
</table>

Select hypothesis or **[NEW]**:

- Assess whether the *cesium-137 canister* is missing from the *XYZ warehouse*.
- Assess whether the *cesium-137 canister* was stolen from the *XYZ warehouse* with the *MDC-578 truck*.
- Assess whether the *cesium-137 canister* is used in a project without being checked-out from the *XYZ warehouse*.
- Assess whether the *cesium-137 canister* was misplaced.
- Assess whether the *cesium-137 canister* was stolen by *Omar al-Massari*.
- Assess whether *Jihad Bis Sayf* has the *cesium-137 canister*.
- Assess whether *Jihad Bis Sayf* is able to construct a dirty bomb.
- Assess whether *Jihad Bis Sayf* will set-off a dirty bomb in the *Washington DC* area.

Figure 77. Selection of competing hypotheses.
6. Select Reasoner. TIACRITIS displays the hypothesis analysis problems and their solutions, as illustrated in Figure 78. You will need to select two of them to compare their analyses.

Comparison of Competing Hypotheses:

<table>
<thead>
<tr>
<th>[SELECT]</th>
<th>H1: Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</th>
<th>S1: It is very likely that the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SELECT]</td>
<td>H2: Assess whether the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.</td>
<td>S2: It is unlikely that the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.</td>
</tr>
<tr>
<td>[SELECT]</td>
<td>H3: Assess whether the cesium-137 canister was misplaced.</td>
<td>S3: No solution.</td>
</tr>
</tbody>
</table>

7. Click on [SELECT] for H1.

8. Click on [SELECT] for H2.

Because the [EVIDENCE] link under the hypotheses is selected, TIACRITIS compares their analyses with respect to the evidence used (see bottom of Figure 79). Notice the evidence used only in the analysis of H1, the evidence used only in the analysis of H2, and the evidence used both in the analysis of H1 and in the analysis of H2.

9. Click on the [ASSESSMENTS AND ASSUMPTIONS] label under the hypotheses to compare the analyses with respect to the assessments and the assumptions made. The comparisons are made in three regions of an analysis tree. Notice in Figure 80 that there is one assumption made for H1 and none for H2, as far as the top parts (i.e. [UPPER HYPOTHESES]) of the analysis trees are concerned.

10. Click on [BASIC HYPOTHESES] (i.e., the hypotheses to which the evidence is associated) and notice that there is no assumption made for any hypothesis of this type.

11. Click on [EVIDENCE RELATED HYPOTHESES] (i.e., the hypotheses corresponding to the credentials of evidence). Notice in Figure 82 the relevance and the believability assessments made only for H1, those made only for H2, and the ones made for both. This concludes the comparison of H1 and H2.
### Comparison of Competing Hypotheses:

<table>
<thead>
<tr>
<th>Hypothesis (H)</th>
<th>Assumption</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H1</strong>: Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
<td><strong>S1</strong>: It is very likely that the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
<td><strong>EVIDENCE</strong></td>
</tr>
<tr>
<td><strong>H2</strong>: Assess whether the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.</td>
<td><strong>S2</strong>: It is unlikely that the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.</td>
<td></td>
</tr>
<tr>
<td><strong>H3</strong>: Assess whether the cesium-137 canister was misplaced.</td>
<td><strong>S3</strong>: No solution.</td>
<td></td>
</tr>
</tbody>
</table>

**H1 Only:**
- EVD-005-Ralph
- EVD-006-Clyde
- EVD-007-GuardReport
- EVD-012-InvestigativeRecord

**H2 Only:**
- EVD-013-Grace

**Common:**
- EVD-002-Ralph
- EVD-001-Willard
- EVD-004-Ralph
- EVD-003-Ralph

---

Figure 79. Comparison of the analyses of two hypotheses with respect to the evidence used.
**Comparison of Competing Hypotheses:**

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H1</strong></td>
<td>It is very likely that the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
</tr>
<tr>
<td><strong>H2</strong></td>
<td>It is unlikely that the cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.</td>
</tr>
<tr>
<td><strong>H3</strong></td>
<td>No solution.</td>
</tr>
</tbody>
</table>

**Common Assumptions:**

<table>
<thead>
<tr>
<th>Assumptions</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upper Hypotheses</strong></td>
<td><strong>Basic Hypotheses</strong></td>
</tr>
<tr>
<td>H1 Only:</td>
<td>none</td>
</tr>
<tr>
<td>H2 Only:</td>
<td>none</td>
</tr>
<tr>
<td>Common:</td>
<td>none</td>
</tr>
</tbody>
</table>

Figure 80. Comparison of the analyses of two hypotheses with respect to the assumptions made.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H1</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>H2</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>Common</strong></td>
<td>none</td>
</tr>
</tbody>
</table>

Figure 81. Comparison of the analyses of two hypotheses with respect to the assumptions made for basic hypotheses.
<table>
<thead>
<tr>
<th>[UPPER HYPOTHESES]</th>
<th>[BASIC HYPOTHESES]</th>
<th>[EVIDENCE RELATED HYPOTHESES]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H1 Only:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-005-Ralph is believable, it is likely that the XYZ hazardous material locker was forced.</td>
<td>The believability of EVD-005-Ralph is very likely.</td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-006-Clyde is believable, it is almost certain that the XYZ hazardous material locker was forced.</td>
<td>The believability of EVD-006-Clyde is almost certain.</td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-007-GuardReport is believable, it is almost certain that the MDC-578 truck was inside the XYZ company before the discovery of the missing of the cesium-137 canister.</td>
<td>The believability of EVD-007-GuardReport is very likely.</td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-012-InvestigativeRecord is believable, it is almost certain that the MDC-578 truck presents traces of cesium-137.</td>
<td>The believability of EVD-012-InvestigativeRecord is almost certain.</td>
<td></td>
</tr>
<tr>
<td><strong>H2 Only:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-013-Grace is believable, it is almost certain to be false that the missing cesium-137 canister is used in a project without being checked-out from the XYZ warehouse.</td>
<td>The access by Grace to the information in EVD-013-Grace is almost certain.</td>
<td></td>
</tr>
<tr>
<td>The understandability by Grace of the information in EVD-013-Grace is almost certain.</td>
<td>The veracity of Grace with respect to the information in EVD-013-Grace is very likely.</td>
<td>The objectivity of Grace with respect to the information in EVD-013-Grace is very likely.</td>
</tr>
<tr>
<td>The observation sensitivity of Grace with respect to the information in EVD-013-Grace is almost certain.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Common:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-002-Ralph is believable, it is very likely that the cesium-137 canister was in the XYZ warehouse before being reported as missing.</td>
<td>The believability of EVD-002-Ralph is very likely.</td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-001-Willard is believable, it is very likely that the cesium-137 canister is no longer in the XYZ warehouse.</td>
<td>The believability of EVD-001-Willard is likely.</td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-004-Ralph is believable, it is almost certain that the cesium-137 canister is no longer in the XYZ warehouse.</td>
<td>The believability of EVD-004-Ralph is very likely.</td>
<td></td>
</tr>
<tr>
<td>Assuming that EVD-003-Ralph is believable, it is likely that the cesium-137 canister was not moved from the XYZ warehouse to another location.</td>
<td>The believability of EVD-003-Ralph is very likely.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 82. Comparison of the analyses of two hypotheses with respect to the assessments made for the relevance and believability of evidence.

12. Click on [UNSELECT] for H2.
13. Click on [SELECT] for H3.
10 Competing Hypotheses and Analyses

14. TIACRITIS compares the analyses of H1 and H3. Browse the comparison as illustrated above, by successively clicking on the hypothesis classes (i.e., [UPPER HYPOTHESES], [BASIC HYPOTHESES], and [EVIDENCE RELATED HYPOTHESES]), and on [EVIDENCE].

15. Click on [UNSELECT] for H1.


17. Browse the comparison of the analyses of H2 and H3.

18. Select Case Study.

19. Click on [SAVE & FINISH].

10.3 Case Study: Comparison of Competing Analyses of a Hypothesis

10.3.1 Objective

The objective of this case study is to learn how to compare two analyses of the same hypothesis that were performed by different analysts, in order to reveal differences in biases and assumptions.

10.3.2 Summary

This case study continues the analysis example discussed in Sections 1.2 and 1.3. You will compare your analyses of various problems (such as, “Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.”) with the corresponding textbook analyses. You will select a hypothesis analysis problem and TIACRITIS will display both your solution and the textbook solution. The system will also display the corresponding sub-problems in the two analyses that have different solutions and the reasons for these differences, such as different assessments or assumptions made, or different evidence used. Proceed as indicated in the following instructions.

10.3.3 Instructions

1. Start the case study in TIACRITIS.

2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed.
3. Click on [ANALYSES BY DIFFERENT ANALYSTS] for the “Selection mode.” You will have to select a hypothesis to compare your analysis of it with the analysis from the TIACRITIS textbook.

4. Click on “Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.” The hypothesis is highlighted to indicate that it was selected (see Figure 83).

5. Select Reasoner. TIACRITIS displays a comparison between your (student) analysis and the textbook analysis (see Figure 84).

6. Select Hypothesis.

7. Click on “Assess whether the cesium-137 canister is missing from XYZ warehouse.”

8. Select Reasoner. TIACRITIS displays a comparison between your analysis and the textbook analysis.

9. Repeat the above process for other hypotheses.
### Analyses by Different Analysts:

<table>
<thead>
<tr>
<th>Student Analysis:</th>
<th>Textbook Analysis:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hypothesis:</strong> Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
<td><strong>Hypothesis:</strong> Assess whether the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
</tr>
<tr>
<td><strong>Solution:</strong> It is likely that the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
<td><strong>Solution:</strong> It is very likely that the cesium-137 canister was stolen from the XYZ warehouse with the MDC-578 truck.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Differences in Analyses:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H:</strong> Assess the believability of EVD-002-Ralph.</td>
</tr>
<tr>
<td><strong>S:</strong> The believability of EVD-002-Ralph is likely.</td>
</tr>
<tr>
<td><strong>H:</strong> Assess the believability of EVD-004-Ralph.</td>
</tr>
<tr>
<td><strong>S:</strong> The believability of EVD-004-Ralph is likely.</td>
</tr>
<tr>
<td><strong>H:</strong> Assess the favoring evidence for the hypothesis that the XYZ hazardous material locker was forced.</td>
</tr>
<tr>
<td><strong>S:</strong> Based on favoring evidence it is likely that the XYZ hazardous material locker was forced.</td>
</tr>
</tbody>
</table>

**Common Evidence:** EVD-005-Ralph

---

10. Select **Case Study**.
11. Click on **SAVE & FINISH**.
10.4 Case Study: Hypothesis Analyses and Evidence Search

10.4.1 Objective

The objective of this case study is to learn how to use TIACRITIS to analyze hypotheses based on evidence retrieved from the Internet, by associating search criteria with elementary hypotheses, invoking various search engines (such as Google, Yahoo, or Bing), identifying relevant evidence, and using it to evaluate the corresponding hypotheses.

10.4.2 Summary

This case study concerns the following hypothesis analysis problem: “Assess whether the United States will be a global leader in wind power within the next decade.”

You will select this hypothesis and then you will browse its analysis tree to see how it is reduced to simpler hypotheses that you have to assess by searching evidence on the Internet. You will associate specific search criteria with the elementary hypotheses, invoke specific search engines with those criteria, identify and copy relevant web information into TIACRITIS, define evidence from this information, associate evidence with the corresponding hypotheses, evaluate its relevance and believability, with the goal of assessing the likelihood of the top level hypothesis that the be a global leader in wind power within the next decade.

Proceed as indicated in the following instructions.

10.4.3 Instructions

1. Start the case study in TIACRITIS.
2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains one or several hypotheses to select from.
3. Select the hypothesis analysis problem: “Assess whether the United States will be a global leader in wind power within the next decade.” Once this hypothesis is selected the Reasoner is automatically invoked to analyze it, as shown in Figure 22 (p. 35).
4. Click on [HIDE SOLUTIONS].
5. Browse the analysis of the above hypothesis to see how it is reduced to simpler hypotheses that you have to assess by searching evidence on the Internet (see Figure 85).
6. Select the **Evidence** menu and then click-on [**COLLECTION GUIDANCE**]. As a result, the left panel shows the basic hypotheses and their evidential support, which currently is none (see Figure 86). You will select a hypothesis, search evidence on the Internet, and use it to assess the hypothesis.
7. Select the first hypothesis: “the United States imports huge quantities of oil.” The right panel shows that there is no search criteria associated with this hypothesis (see Figure 87).

8. After “Search criteria: none,” click on [NEW].

9. Type a search criterion, such as “oil import by the United States,” and click on [SAVE]. Notice that the defined criterion is automatically selected.

10. After “Search criteria: ...” click on [NEW] to define a new criterion.

11. Type a new search criterion, such as “top oil importing countries,” and click on [SAVE]. Notice in Figure 88 that only one search criterion is selected. You can select another one by clicking on it.
10 Competing Hypotheses and Analyses

12. After “Search with,” click on [GOOGLE] to search the Internet with the selected criterion (i.e., “top oil importing countries”).

13. Browse the documents returned by Google (see Figure 89) and select a relevant one. In this illustration we have selected the second document whose content is shown in Figure 90.

14. Select [COLLECTED INFORMATION] and then click on [NEW]. Both the left and the right panel show a partially defined item of information “INFO-001-“.

15. In the right panel, complete the name (e.g. INFO-001-US-oil-import), and click on [SAVE].

16. After Description, click on [EDIT].
Figure 89. Searching relevant evidence on the Internet.

Figure 90. Selected document providing relevant information.
17. Copy and paste information from the article retrieved with Google into the description pane from TIACRITIS (see Figure 91).

18. Click on [SAVE] following the description panel. You will define one or several items of evidence by selecting relevant fragments from this item of information, as illustrated in Figure 92.

19. Having selected a relevant text fragment in the right panel, click on [DEFINE EVIDENCE]. Notice in Figure 93 that [AVAILABLE EVIDENCE] is automatically selected and a new item of evidence is partially defined.

20. In the right panel, complete the name of the item of evidence (e.g., EVD-001-US-top-oil-importer) and click on [SAVE]. As a result, the right panel shows additional features of the newly defined item of evidence.

21. After Description, click on [EDIT], update the description (e.g., add at the beginning “Daniel Workman provides”), and then click on [SAVE].
22. After "Type: evidence," click on [CHANGE] to define the type of this item of evidence. We will define it as "unequivocal testimonial evidence obtained at second hand," where Daniel Workman is providing us information he has obtained from the U.S. Energy Information Administration.

23. After "unequivocal testimonial evidence obtained at second hand," click on [SELECT].

24. After "By the source," click on [CHANGE].

25. Type "Daniel Workman" and click on [SAVE].
26. Click on [YES].

27. After "Who obtained the information from the source," click on [CHANGE]. Then type “US Energy Information Administration” and click on [SAVE]. Then click on [YES].

28. After "Irrelevant to," click on [FAVORS] following the hypothesis “the United States imports huge quantities of oil.” Notice in the right panel from Figure 94 that the Favors label was created and the hypothesis was moved under it.

<table>
<thead>
<tr>
<th>Select mode: [COLLECTION GUIDANCE] [COLLECTED INFORMATION] [AVAILABLE EVIDENCE] [IMPORT EVIDENCE]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available evidence [NEW] [DELETE]</td>
</tr>
<tr>
<td>Sorted by: [ID] [NAME SUFFIX]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selected item of evidence: EVD-001-US-top-oil-importer [RENAME] [DELETE EVIDENCE]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: Daniel Workman provides revealing stats from the U.S. Energy Information Administration (EIA). Based on 2004 data, the following list shows that...</td>
</tr>
<tr>
<td>Extracted from: INFO-001-US-oil-import [UNLINK]</td>
</tr>
<tr>
<td>Type: unequivocal testimonial evidence obtained at second hand [CHANGE]</td>
</tr>
<tr>
<td>By the source: Daniel Workman [RENAME] [CHANGE]</td>
</tr>
<tr>
<td>Who obtained the information from the source: US Energy Information Administration [RENAME] [CHANGE]</td>
</tr>
</tbody>
</table>

Favors:
- the United States imports huge quantities of oil [REMOVE] [REASONING] [COLLECTION]

Irrelevant to:
- importing huge quantities of oil represents a security threat for the United States [FAVORS] [DISFAVORS] [REASONING] [COLLECTION]
- importing huge quantities of oil represents a big burden on economy of the United States [FAVORS] [DISFAVORS] [REASONING] [COLLECTION]

29. Click on [REASONING] following the hypothesis “the United States imports huge quantities of oil.” As a result, the Reasoner is automatically invoked with the favoring evidence for that hypothesis selected.
30. Right-click in the left pane and select **Expand**. Notice in Figure 95 that the analysis tree has been extended with the analysis the new item of evidence.

![Figure 95. Reasoning tree automatically extended with the analysis of the newly defined item of evidence.](image-url)
31. Assess the relevance and the believability of EVD-001-US-top-oil-importer. Notice that, with respect to the believability of this item of evidence you may choose to drill down as much as desired. For example, you may directly estimate the believability of this item of evidence. Alternatively, you may wish to estimate lower level believability credentials, such as the credibility of Daniel Workman.

32. Select the Evidence menu and then click on [COLLECTION GUIDANCE].

33. Continue with defining search criteria for various hypotheses, searching for relevant evidence on the Internet, representing it in TIACRITIS, and using it to assess the corresponding hypotheses.

34. Select Case Study.

35. If you wish to end the case study, click on [SAVE & FINISH] at the end of the instructions. You will be able to resume it at a later time.

36. If you wish to discard your current analysis and analyze another hypothesis then perform the following operations:

37. Click on Case Study.

38. Click on [DISCARD YOUR ANALYSIS AND RESTART] in the right panel.

39. Continue with the following instructions.

40. Select the Hypothesis menu on the top of the window. We are interested in analyzing whether the United Kingdom will be a global leader in solar power within the next decade. This is not listed as one of the selectable hypotheses.

41. After “Select hypothesis …” click on [NEW]. As a result, TIACRITIS displays a list of hypotheses patterns, in alphabetical order, as shown in Figure 96.

42. Click-on “Assess whether ?O1 will be a global leader in ?O2 within the next decade.” As a result, TIACRITIS will automatically replace the variables with “…”.

43. Click on each "..." and select the desired values (e.g. "United Kingdom" and “wind power”) from the lists displayed by TIACRITIS (see Figure 97).
44. When the hypothesis is instantiated as desired, click-on [CREATE].

45. The Reasoner is automatically invoked with this hypothesis selected (see Figure 98).

46. Select the Evidence menu and then click-on [COLLECTION GUIDANCE]. As a result, the left panel shows the basic hypotheses and their evidential support which currently is none. You will select a hypothesis at a time, search evidence on the Internet, and use it to assess that hypothesis, as was illustrated above.

47. At any time you may click on [SAVE & FINISH] to end this case study which can be resumed later.
Figure 98. Automatic reduction of a new hypothesis.
11 IMPROVING STRUCTURED ANALYTIC METHODS WITH TIACRITIS: THE CASE OF HEUER’S ANALYSIS OF COMPETING HYPOTHESES

The intelligence analysis concepts and methods embedded in TIACRITIS, which are based on the Science of Evidence and Artificial Intelligence, particularly the systematic approach to the development of argumentation structures, the substance-blind classification of evidence and the associated procedure for assessing the believability of evidence, the drill-down analysis, and assumptions-based reasoning, may help the analysts perform better analyses, no matter what analysis methods they use. To justify this claim, we consider in this section what is probably the most popular structured analytic method, Richards J. Heuer’s Analysis of Competing Hypothesis (ACH) (Heuer, 1999, pp.77-78). We show how ACH, which has found favor among many intelligence analysts and it is used in many advanced analysis courses, can be significantly improved by employing some of the concepts and methods embedded in TIACRITIS. Our present comments are based upon a very recent account of a system being developed to implement the ACH approach (Heuer, 2008).

11.1 Using the Substance-blind Classification of Evidence

The basis of ACH consists of a matrix in which various items of interest in an intelligence analysis are recorded, as illustrated in the abstract example from Table 14.

Table 14. An illustration of Heuer’s Analysis of Competing Hypotheses.

<table>
<thead>
<tr>
<th>Evidence</th>
<th>Source Type</th>
<th>Credibility</th>
<th>Relevance</th>
<th>H₁</th>
<th>H₂</th>
<th>H₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>E₁</td>
<td>Inference</td>
<td>medium</td>
<td>high</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>E₂</td>
<td>Assumption</td>
<td>high</td>
<td>low</td>
<td>C</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>E₃</td>
<td>Intel reporting</td>
<td>low</td>
<td>high</td>
<td>I</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>E₄</td>
<td>HUMINT</td>
<td>medium</td>
<td>medium</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>E₅</td>
<td>Liaison</td>
<td>high</td>
<td>low</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>E₆</td>
<td>Lack of intel reporting</td>
<td>low</td>
<td>medium</td>
<td>I</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>E₇</td>
<td>Contrarian hypothesis</td>
<td>high</td>
<td>high</td>
<td>C</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>

In this two-dimensional matrix, analysts first list the substance or content of the evidence in the first column. Then, in the second column, analysts list what Heuer calls “source type,” which should guide them in evaluating the credibility and relevance of evidence (columns 3 and 4).

Here are the actual examples Heuer provides of source types: Inference, Assumption, Intel reporting, HUMINT, Liaison, Lack of intel reporting despite vigorous search, and Contrarian hypothesis. One problem with this classification is that the believability/credibility of evidence in the same category
(e.g., Liaison) is evaluated based on certain credentials, if it is tangible evidence (e.g., authenticity), and on other credentials, if it is testimonial evidence (e.g., veracity, objectivity, etc.). Thus this classification does not help with this evaluation.

As discussed in Section 5, there is a “substance-blind” classification of evidence that emerges precisely from the fact that entirely different believability or credibility questions must be asked of tangible and testimonial evidence. Therefore, an improvement of the ACH method is to use the forms of evidence shown in Figure 41, which will guide the analyst in assessing its believability. In fact, several of Heuer’s types can easily be mapped to these forms. For example, HUMINT is a species of testimonial evidence; Intel Reporting may either involve testimonial or tangible evidence; Liaison evidence (obtained from contacts with representatives of friendly or neutral governments) may be either tangible or testimonial in nature. Heuer’s “Lack of intel reporting despite vigorous search” qualifies as “missing evidence” having potential inferential value, as discussed in Section 5.5.

Heuer uses a very broad interpretation of evidence as “all the factors that influence an analyst’s judgment about the relative likelihood of the hypotheses” (Heuer, 2008, p. 253). However, according to the Science of Evidence (Schum, 2009) and as discussed in Section 3.2, all evidence, regardless of its substance or content, has three credentials that must be established by defensible arguments: relevance, believability or credibility, and inferential force or weight. From this point of view, three of the examples provided by Heuer (inference, assumption, and contrarian hypothesis) do not qualify as evidence. We agree with Heuer that they play an important role in evidential reasoning, but they should be accounted for not as evidence (how do we ever establish the credibility of an assumption or a hypothesis?), but as components of arguments. For example, assumptions could be used to assess the relevance or the believability of evidence, as illustrated in Sections 3.4 and 6.5, as well as discussed below.

11.2 Assessing the Believability of Evidence

In the third column ACH requires the analyst to rate the credibility of the “source type” of an item of intelligence evidence as high, medium, or low. First, as discussed in Section 5.4, we think that it is better to talk about the “believability” of evidence which may also include “competence” considerations in addition to “credibility” ones.

As discussed in Sections 5 and 5.9, believability assessments for some items of evidence may be very complex, especially if these items have been obtained through chains of custody (Schum, 2007; Schum and Morris, 2007). TIACRITIS has a lot of knowledge about the believability of evidence and its constituents, and supports the analyst in making these assessments. For example, it knows about the necessity for determining the authenticity, accuracy, and reliability of the demonstrative tangible evidence. It knows that it has to establish both the competence and the credibility of the human sources of testimony. As discussed in Section 5.4, source credibility and source competence are entirely different characteristics, each with its own ingredients. For example, in order to determine the credibility one has to determine the source’s veracity, objectivity, and observational sensitivity. On the other hand, in order to determine competence, one would need to determine the source’s access and understandability. As
shown by Schum and Morris (2007), each of these assessments may be a very complex. It is therefore important to assist the analysts in performing these assessments, for instance, by incorporating into ACH the TIACRITIS procedures for evaluating the believability of evidence which are discussed in Section 5. In particular, the arguments developed with TIACRITIS for establishing the believability of evidence may include the use of assumptions.

11.3 Assessing the Relevance of Evidence

In the fourth column of the ACH table the analyst has to rate the relevance of an item of evidence as high, medium, or low. However, if the relevance arguments are not specifically constructed they can never be subjected to any form of critical reasoning. TIACRITIS can help with this issue because it involves both the top-down and bottom-up argument-structuring methods (discussed in Section 0), drawing upon and Wigmore’s concern and methods for assessing the relevance of evidence (Wigmore, 1937).

As discussed at the beginning of Section 4, there are two forms of relevance: direct and indirect. Directly relevant evidence is that which can be linked directly to hypotheses being considered by a defensible chain of reasoning or argument. Indirectly relevant evidence has no such direct linkage but bears upon the strength or weakness of links in chains of reasoning set up by directly relevant evidence. Consider, for example, an item of evidence that says nothing about the hypotheses being considered in the ACH method but would allow us to infer that the source of a relevant evidence item is not credible. To use such indirectly relevant evidence, the ACH method would need to be extended to allow the development of arguments for both the believability and the relevance credentials, arguments that could be developed with TIACRITIS.

11.4 Assessing the Likelihood of Hypotheses

The last columns in the ACH table correspond to the hypotheses being considered in the analysis at hand. A significant advancement of ACH over the conventional intuitive analysis approach is precisely the requirement to look at several competing hypotheses. In contrast, conventional intuitive analysis focuses on what is suspected to be the most likely hypothesis and then assesses whether or not the available evidence supports it. This may lead to wrong conclusions because the same evidence may also support other hypotheses.

In the column corresponding to a hypothesis, the analyst grades the bearing of an item of evidence on that hypothesis as either consistent (C) or inconsistent (I). Then the most likely hypothesis is the one with the least evidence against it, that is, the hypothesis with the least number of Is. But there is no indication of how relatively strong any of the Is are. Suppose we have ten items of evidence for which H₁ and H₂ have the same number of Is. How do we decide which hypothesis to accept, given the fact that the evidence items assessed as I under H₁ might be different from the evidence items assessed as I under H₂? In their extension of the ACH method, Good and his colleagues attempted to address this issue by associating numbers to the high, medium, and low gradations of credibility and relevance, and scorings the competing hypotheses (Good et al., 2001). The problem with this approach is that numbers
applied to hypotheses will have little meaning in the absence of any specific relevance arguments, considerations of credibility and competence attributes for different sources of evidence, and characteristics of the evidence itself. This also applies to any ordinary probability assessments under alternative hypotheses that will have little meaning either in the absence of specific arguments justifying them. In that sense, Good’s extension of ACH may do more harm than help because it may provide the analysts with a false sense of confidence rather than encouraging them to give more careful attention to the arguments necessary to justify their conclusions regarding the competing hypotheses.

An additional difficulty with the ACH method is that it requires us to begin with what Heuer calls a full set of hypotheses (Heuer, 2008, p. 256); presumably this means that the hypotheses are mutually exclusive and exhaustive. In some cases, such as in the example Heuer provides, we may consider a set of hypotheses that occur in response to a specific question we have been asked. The analysis example Heuer provides is in answer to the question: What is the status of Iraq’s nuclear weapons program? The three hypotheses he lists as being a full set are:

- $H_1$: “Dormant or shut down.”
- $H_2$: “Has been started up again.”
- $H_3$: “Weapon available within this decade.”

It could, of course, be argued about whether the hypotheses on this list are in fact either exhaustive or mutually exclusive. For example, $H_3$ and $H_2$ are not mutually exclusive. If the weapons program has been started up again ($H_2$) then we might infer that there might be at least one weapon available within this decade ($H_3$). Conversely, for a weapon to be available, Iraq must have started-up its weapons program. What this shows is that it may be difficult to assure that we have a complete set of mutually exclusive hypotheses. However, if the set of hypotheses is not complete, it may just be the case that the most likely hypothesis is among the missing ones. TIACRITIS may help with this issue by estimating the likelihood of each of the competing hypotheses considered or, at least, the one selected through the ACH method. If the ACH-selected hypothesis does not have a high enough likelihood, then this is an indication that additional hypotheses should be considered.

A simplification made by the ACH method is to consider that both the credibility/believability and the relevance of an item of evidence are independent of the particular hypothesis being considered. Let us consider, for example, an item of evidence revealing the number of years needed by North Korea to develop its nuclear program. This item of evidence is relevant to $H_3$ but it is not at all relevant to the other two hypotheses. One way to address this issue is to simply estimate a different believability and relevance for each hypothesis.

James Bruce, who is well-known for his valuable work on the importance of epistemology in intelligence analysis, discusses reasons why the ACH method does represent a significant advance over analytic methods that are entirely unsystematic and have so often resulted in a favored hypothesis being uncritically endorsed on a very shaky evidential foundation (Bruce, 2008). He also mentions various reasons why the ACH method enjoys current popularity among many intelligence analysts. However, the example he provides illustrating the virtues of ACH also illustrates one of its most severe
limitations. He mentions the unjustified conclusions reached about Saddam’s alleged possession and development of WMDs based on the reports provided by “Curveball.” Bruce argues that had these reports been subjected to analysis using ACH, a possibly different conclusion would have been reached, especially regarding bioweapons. There are, however, some good reasons why ACH might not have helped regarding this conclusion. The trouble here is that the ACH method says nothing about the attributes of the competence and credibility of HUMINT or the attributes of the credibility of various forms of tangible evidence, such as the diagrams of bioweapons facilities that Curveball provided. We are just as concerned as James Bruce about the epistemology of intelligence analysis but we are especially concerned that intelligence analysts be provided with appropriate background knowledge regarding such tasks as assessing the credibility of sources of evidence and establishing the relevance of evidence on alternative hypotheses. The MACE system shows the specific competence and credibility attributes we must consider for HUMINT sources (Schum and Morris, 2007). This system would have been especially useful in assessing the competence and credibility of Curveball. Analysts would have been prompted to ask questions they did not ask about Curveball, but for which they did have answers. And TIACRITIS has significant knowledge about the properties, uses, discovery, and marshaling of evidence that it can share with the intelligence analysts who use it. It also knows about the necessary credibility-related questions that form the basis for MACE. This knowledge can be integrated into the ACH method, as suggested above.

There is a problem that seems endemic in intelligence analysis that the ACH method does not address. The problem is that, in so many situations of interest to the Intelligence Community, we have a seamless activity in which we have evidence in search of hypotheses at the same time as hypotheses in search of evidence. Suppose we wish to consider hypothesis H₂, that Iraq’s weapons program has been started up again. There is no mechanism in ACH for putting this hypothesis to use in generating new lines of evidence and inquiry. This mechanism should address the question: What things need to be tested by what evidence in order to sustain this hypothesis? What this amounts to is generating main lines of argument under H₂, showing what evidence would be necessary to prove or disprove the hypothesis that the Iraqis have started up their weapons program. Many possibilities come to mind, such as the acquisition of necessary materials, the bringing together of necessary talented scientific and technical people, and the development of facilities necessary to make weapons of various sorts. You recognize here that this is what we described in Section 1.2 as hypotheses in search of evidence. To put some hypothesis to use requires us to generate arguments from it that will eventually identify classes of observable evidence necessary to sustain this hypothesis. But the world continues to change as we are attempting to understand events in it. The result is that we must continually generate new hypotheses or revise the ones we have constructed. Thus, a major item left out in ACH is the crucial importance of the discovery process in which we have evidence in search of hypotheses at the same time with hypotheses in search of evidence. As discussed in Sections 1.2 and 1.3, TIACRITIS promotes a systematic approach to this complex issue.

A very good feature of the ACH method is that it shows how individual items of evidence relate to the competing hypotheses. This suggests an improvement of TIACRITIS with a module that will
automatically compare the analyses of competing hypotheses, to reveal differences in the evidence used and the assumptions made, including a focus on areas with less evidential support.

Heuer has conceived ACH as a manual method that can be easily used by the analysts and has therefore made many simplifications. The TIACRITIS-inspired improvements suggested above will complicate the original ACH method, but the added complexity will not create any problem if one can use the corresponding components of TIACRITIS. For example, assessing the believability of some item of evidence could easily be done with TIACRITIS, as discussed in Section 5.

Finally, let us notice that many of the improvements suggested above for ACH may be applicable to other evidence-based analytic methods. This suggests that TIACRITIS is an excellent tool for teaching intelligence analysts because the concepts and method for evidence-based reasoning that would be learned with it would help the analysts no matter what specific evidence-based analytic methods they would use.
12 ANALYSIS OF GEOSPATIAL INTELLIGENCE

12.1 Sample Problem: Analysis of Wide-area Motion Imagery

Capabilities exist today to persistently monitor fixed geographic locations (such as conflict areas) as wide as 100 km², for long periods of time, using electro-optic sensors (see Figure 99). This leads to the collection of huge amounts of data to be used either in real-time analysis or in forensic analysis. During real-time analysis, analysts attempt to discover impending threat events (e.g., ambush, kidnapping, rocket launch, false check-point, suicide bomber, IED) in time to react. During forensic analysis, the analysts backtrack from such an event (e.g., an ambush) in order to discover the participants, possible related locations and events, and the specific movement patterns (Desai, 2009). The problem, however, is that the manual analysis of these huge amounts of data would require thousands of analysts.

This section illustrates the analysis methodology discussed in this textbook with a case study involving evidence obtained from wide-area motion imagery (WAMI) and from other sources.

Figure 99. Wide area motion imagery
As discussed in Section 1.2 and summarized in Figure 100, Intelligence Analysis is a process of ceaseless discovery which involves evidence in search of hypotheses (through abductive or imaginative reasoning), hypotheses in search of evidence (through deductive reasoning), and evidential tests of hypotheses (through inductive reasoning), all going on at the same time.

The next sections illustrate this process in the context of real-time analysis of wide-area motion imagery (Tecuci et al., 2010).

Figure 100. Discovery of evidence, hypotheses, and arguments.

### 12.2 Evidence in Search of Hypotheses (Hypothesis Generation)

Let us consider an analyst who performs real-time analysis of the wide area motion imagery (WAMI) of a squared area to the north and west of Al Basra, Iraq, that is approximately 80 km on a side. This area contains main roads from Al Basra north to the cities of Baghdad, Karbala, and Al Hillah. The location of concern to the analyst, shown in Figure 101, is a highway junction near Al Batha, a city about 35 km northwest of An Nasiriyah and about 200 km northwest of Al Basra. In this area, the main north-south highway junctions with several other minor roads. The area west and south of Al Batha is desolate and uninhabited except for scattered small collections of huts and tents as the swamps give way to the desert, south and west of this area. The analyst has just noticed evidence of road work at 1:17AM, at this highway junction located about 1.5 km northeast of Al Batha. Road work at this location at this time is very unusual and the analyst wonders whether it may suggest any threat. Through a flash of insight, the analyst abductively leaps to the hypothesis $H_k$ that there is an ambush threat at that location. Attempting to justify this hypothesis, she generates the abductive inference steps shown in Table 15. Here we have evidence in search of hypotheses where a newly discovered item of evidence searches for hypotheses that would explain it.
12.3 Hypotheses in Search of Evidence (Evidence Collection)

A great challenge in the analysis of wide-area motion imagery is the massive amount of data that needs to be searched quickly, especially during real-time analysis. This is where the analysis methodology described in this book is particularly helpful. Once a hypothesis is formulated, it is used to guide the evidence collection process, as illustrated in Figure 102 and explained in the following.

We have to:

“Assess whether there is an ambush threat to the US forces at the Al Batha highway junction after 1:17AM.”

“What is required for an ambush threat at the Al Batha highway junction?”

“The Al Batha highway junction should be a good location for ambushing the US forces, and there should be some ambush preparation activity.”
Assess whether there is an ambush threat to the US forces at the Al Batha highway junction after 1:17AM.

What is required for an ambush threat at the Al Batha highway junction?
The Al Batha highway junction should be a good location for ambushing the US forces, and there should be some ambush preparation activity.

Assess whether the Al Batha highway junction is a good location for ambushing the US forces.

What are the required features of a good ambush location?
To be on a route used by the US Forces and to have cover.

Assess whether the Al Batha highway junction is on a route used by the US forces.

Search for evidence that the Al Batha highway junction is on a route used by the US forces.

Assess whether there is ambush cover near the Al Batha highway junction.

Search for evidence in WAMI that there is ambush cover near the Al Batha highway junction.

Assess whether people descended at the Al Batha highway junction from a vehicle short before 1:17AM.

Search for evidence in WAMI that people descended at the Al Batha highway junction from a vehicle short before 1:17AM.

Assess whether the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a terrorist facility.

Search for evidence in WAMI that the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a certain facility.

Assess whether the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a terrorist facility.

Search for evidence in WAMI that the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a certain facility.

Assess whether the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a terrorist facility.

Search for evidence in WAMI that the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a certain facility.

Assess whether there is deployment of terrorists at the Al Batha highway junction short before 1:17AM.

Assess whether there is road blocking at the Al Batha highway junction around 1:17AM.

Which are the main components of ambush preparation?
Deployment, road blocking, and movement to cover.

Assess whether there is movement of terrorists from the Al Batha highway junction to cover, after 1:17AM.

What would we need to show by evidence for deployment of terrorists?
That people descended at the Al Batha highway junction from a vehicle that departed from a terrorist facility.

Assess whether the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a terrorist facility.

Search for evidence in WAMI that there is movement of terrorists from the Al Batha highway junction to cover, after 1:17AM.

Which is a strategy for road blocking?
Road work to stop an incoming vehicle.

Search for evidence in WAMI that there is movement of terrorists from the Al Batha highway junction to cover, after 1:17AM.

Search for evidence in WAMI that road work at the Al Batha highway junction at 1:17 AM.

Search for evidence that the departing facility of the vehicle that drove the people to the Al Batha highway junction, if it departed from a facility, is a terrorist facility.

EVD-001-WAMI-RoadWork:
WAMI evidence of road work at the Al Batha highway junction at 1:17 AM.

Search for evidence that the departing facility of the vehicle that drove the people to the Al Batha highway junction, if it departed from a facility, is a terrorist facility.

Figure 102. Evidence collection guidance.
Therefore we have to make two assessments:

“Assess whether the Al Batha highway junction is a good location for ambushing the US forces.”

“Assess whether there is ambush preparation activity at the Al Batha highway junction around 1:17AM.”

Let us now:

“Assess whether the Al Batha highway junction is a good location for ambushing the US Forces.”

“What are the required features of a good ambush location?”

“To be on a route used by the US forces and to have cover.”

Therefore we have to:

“Assess whether the Al Batha highway junction is on a route used by the US forces.”

“Assess whether there is ambush cover near the Al Batha highway junction.”

Consequently, we need to:

“Search for evidence that the Al Batha highway junction is on a route used by the US forces.”

“Search for evidence in WAMI that there is ambush cover near the Al Batha highway junction.”

Based on this guidance we find two items of evidence:

**EVD-002-WAMI-Cover:** WAMI evidence of extensive brush and trees at several locations at the Al Batha highway junction, as well as some ruined buildings that could also provide cover.

**EVD-007-HUMINT-BlueRoute:** Confidential information from the American Forces Command indicating that the highway in the vicinity of Al Batha is the main north-south traffic artery used by the American and Iraqi government forces.

Notice in Figure 102 how the other assessment problems are successively reduced to simpler assessments problems and ultimately to this very precise evidence collection guidance:

“Search for evidence in WAMI that people descended at the Al Batha highway junction from a vehicle short before 1:17AM.”

“Search for evidence in WAMI that the vehicle that drove the people to the Al Batha highway junction short before 1:17AM, departed from a certain facility.”

“Search for evidence that the departing facility of the vehicle that drove the people to the Al Batha highway junction, if it departed from a facility, is a terrorist facility.”

“Search for evidence in WAMI that there is movement of terrorists from the Al Batha highway junction to cover, after 1:17AM.”
The above collection guidance leads us to identify the evidence items in Table 16.

Table 16. Collected evidence from WAMI and other sources as a result of hypothesis decomposition.

<table>
<thead>
<tr>
<th>Evidence ID</th>
<th>Evidence Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVD-001-WAMI-RoadWork</td>
<td>WAMI evidence of road work at the Al Batha highway junction at 1:17AM (AST_0117_24_JUL_2010).</td>
</tr>
<tr>
<td>EVD-002-WAMI-Cover</td>
<td>WAMI evidence of extensive brush and trees at several locations at the Al Batha highway junction, as well as some ruined buildings that could also provide cover.</td>
</tr>
<tr>
<td>EVD-003-WAMI-RiceFarm</td>
<td>WAMI evidence that, at 1:09AM (AST_0109_24_JUL_2010), a Datsun pickup truck left an abandoned rice farm situated in the swamps 3 km west along a minor road leading to the Al Batha highway junction.</td>
</tr>
<tr>
<td>EVD-004-WAMI-PickupTruckArrival</td>
<td>WAMI evidence that, at 1:15AM (AST_0115_24_JUL_2010), a Datsun pickup truck arrived at the Al Batha highway junction.</td>
</tr>
<tr>
<td>EVD-005-WAMI-Personnel</td>
<td>WAMI evidence that, at 1:15AM (AST_0115_24_JUL_2010), personnel descended from the Datsun pickup truck at the Al Batha highway junction.</td>
</tr>
<tr>
<td>EVD-006-WAMI-MoveToCover</td>
<td>WAMI evidence that, at 1:25 AM (AST_0125_24_JUL_2010), the people who blocked the road at the Al Batha highway junction are ducking for cover.</td>
</tr>
<tr>
<td>EVD-007-HUMINT-BlueRoute</td>
<td>Confidential information from the American Forces Command indicating that the highway in the vicinity of Al Batha is the main north-south traffic artery used by the American and Iraqi government forces.</td>
</tr>
<tr>
<td>EVD-008-HUMINT-RiceFarm</td>
<td>Testimony of our Iraqi source, code-named “Meatball,” that the abandoned rice farm, in the swamps 3 km west along the minor road leading to the Al Batha highway junction, has been used by several terrorist groups in the past.</td>
</tr>
</tbody>
</table>

12.4 Case Study: Real-time Ambush Threat Analysis

12.4.1 Objective

The objective of this case study is to practice with evidence-based hypothesis testing by assessing whether there is an ambush threat to the US forces at the Al Batha highway junction after 1:17AM (referred to as AST_0117_24_JUL_2010), based on the evidence from Table 16.

12.4.2 Summary

This case study concerns the analysis of the problem “Assess whether there is an ambush threat to the US forces at the Al Batha highway junction after AST_0117_24_JUL_2010.”
You will select this hypothesis and then you will browse its analysis tree to see how it is decomposed into simpler hypotheses. You will visualize both abstract descriptions of these decomposition operations, as well as detailed ones. You will then study the available items of evidence and associate them to the basic hypotheses to which they are relevant. After that, you will assess the relevance and the believability of each item of evidence with respect to the corresponding hypothesis, and notice its computed inferential force on the upper level hypotheses. Finally, you will browse the entire analysis tree, decide whether you would like to update any of your assessments, and report the result of your analysis as the likelihood that there is an ambush threat to the US forces at the Al Batha highway junction after AST_0117_24_JUL_2010.

Proceed as indicated in the following instructions.

12.4.3 Instructions

1. Start the case study in TIACRITIS.

2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains one or several hypotheses to select from.

3. Select the hypothesis analysis problem “Assess whether there is an ambush threat to the US forces at the Al Batha highway junction after AST_0117_24_JUL_2010.” Once this hypothesis is selected the Reasoner is automatically invoked to analyze it, as shown in Figure 22 (pg. 35). The right panel shows the details of a reasoning step. The left panel shows an abstraction of that step.

4. Browse the analysis tree to see how the top level hypothesis is decomposed into simpler hypotheses.

5. Select the Evidence menu on the top of the window and then select [COLLECTED INFORMATION].

6. Click on each item of information in the left panel and read its description in the right panel.

7. Select the [AVAILABLE EVIDENCE] mode at the top of the left panel. As a result, the left panel displays the evidence extracted from the collected information.

8. Click on an item of evidence in the left panel and read its description in the right panel.

9. Read the hypotheses that are listed under the "Irrelevant to" label.

10. Decide to which of these hypotheses (if any) the current item of evidence is relevant to, and then click on either [FAVORS] or [DISFAVORS] following that hypothesis, to indicate that the current item of evidence favors or disfavors that hypothesis. Notice that a corresponding Favors or Disfavors label was created and the hypothesis was moved under it.

11. Select [REASONING] following that hypothesis. The Reasoner is automatically invoked with the “favoring evidence” or the “disfavoring evidence” for that hypothesis selected, depending on your previous decision.

12. Right-click in the left panel and select Expand. As a result, the left panel shows the credentials of the current item of evidence that need to be assessed.
13. Evaluate the relevance and the believability credentials of this item of evidence and define them as assumptions by using the Assumption module.

14. Notice how TIACRITIS has evaluated the inferential force of the current item of evidence on some of the upper level hypotheses.

15. Select the Evidence menu on the top of the window and repeat the above operations to associate each available item of evidence to a hypothesis and assess its relevance and believability.

16. After all the relevant evidence has been used, browse the entire analysis tree and decide whether you would like to update any of your previous assessments.

17. You have now determined the likelihood that there is an ambush threat to the US forces at the Al Batha highway junction after AST_0117_24_JUL_2010.

18. Click on [SAVE & FINISH]. You will be able to update this analysis later based on additional items of evidence.
13 ANALYSIS OF MILITARY INTELLIGENCE

13.1 Introduction

This chapter uses an Algeria-Tunisia scenario that provides background for military students during the contingency and crisis action planning portions of their course at the Joint and Combined Warfighting School (JCWS) of the Joint Forces Staff College. While using real-world geography and country names, the scenario itself, as well as participants, motives, and actions are fictitious.

The scenario is based on a Tunisia that is deeply divided along North-South lines. A previous president from Southern Tunisia was removed from power in a coup led by the current president from northern Tunisia. The former president fled to Algeria, where he has remained as a guest of the government in Algiers. While the current president has been instrumental in the economic development in Tunisia, many in the south of Tunisia feel they have not benefitted with most of the profits going to the government in Tunis. An organization of disaffected Tunisians has formed in the central part of the country, led by a former military member from the previous president’s regime. The organization has commenced a low-scale campaign against the current government and has publicly stated as their goal, the fall of the current government, to be replaced by a government that truly represents the people. Most targets to date have been governmental infrastructure in the triangle defined by the cities of Sfax, Gafsa, and Medenine. Tunisian security forces have been ineffective in combating this organization.

Tunisian authorities have on numerous occasions publicly voiced their beliefs that the government in Algiers is supplying and funding the insurgent organization and that without such external support, the organization would die. Algeria, has publicly denounced such claims as a means for the government in Tunis to mask their incompetency and lack of public support. This chapter focuses on this specific element concerning evidence favoring Tunisian claims of Algerian support for Tunisian insurgents. The United States interest is two-fold. The scenario has the U.S. in a bi-lateral security treaty with Tunisia. When activated, U.S. forces will deploy to Tunisia to aid in the defense of Tunisia. Secondly, U.S. policy is based on having Tunisia as a strong and vibrant partner in North Africa. In support of these efforts, the United States has permanently stationed U.S. Special Forces and a Geographic Combatant Commander forward element inside Tunisia. Both governments should give attention to the possible role of al Qaeda and other militant jihadists groups who might benefit from any destabilization of the relations between Tunisia and Algeria. The record shows these militant jihadist groups have conducted numerous terrorist actions in Algeria and Tunisia, but many more in Algeria. There are militant Islamists in both of these countries. The basic objective of these groups is very simple: to replace the secular governments in Algeria, Tunisia, and other Maghreb countries with fundamentalist Islamic governments acting under Sharia laws, or what they are interpreted as being. So, we cannot suppose that al Qaeda, for example, would necessarily favor the existing governments of either Algeria or Tunisia as they are depicted in the present scenario. But there is something that should not be overlooked.

The possible actions by the Algerians to support the insurgents in southern Tunisia, as depicted in this scenario, would certainly destabilize this part of the Meghreb and bring forth the presence of
American forces to assist the defense of the Tunisians as the security treaty outlined in the scenario proposes. Tunisia is the smallest country in the Meghreb and is many times smaller than Algeria. But any military action by either the Algerians or the Tunisians would certainly destabilize the area. One plausible thought is that such destabilization would be to the advantage of al Qaeda and the other militant jihadist groups. It would also bring forth the real possibility of Americans now being engaged in three wars including the ones in Iraq and Afghanistan. One consequence would be the continued and enhanced resentment of Americans being involved in wars in Islamic lands. So, these possibilities suggest other evidence that we could consider. The record shows the existence of al Qaeda raids in Tunisia that originated in Algeria. The nature of the al Qaeda operations in Tunisia could be such that they add confusion to the Tunisians about whether these operations were Algerian in nature. Suppose some al Qaeda action in Tunisia prompted the inappropriate military reprisal of the Tunisians against Algeria. More widespread military actions result. So, the Americans intervene and the conflict becomes more intense. In the meantime al Qaeda leaders gloat saying that this is what happens when two neighboring secular and immoral western governments have conflicts; if they were fundamentalist Islamic countries, and acting under Sharia law, this would not have happened (see how necessary it is to change both governments?). Table 17 shows the main participants in our fictitious scenario.

Table 17. Fictitious participants in the Algeria-Tunisia scenario.

<table>
<thead>
<tr>
<th>Leadership - Tunisia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abdullah Mahood – Leader of the Tunisian Liberation Front (TLF).</td>
</tr>
<tr>
<td>Cleric Osama Bin Logan – Radical cleric supporting bin Massie.</td>
</tr>
<tr>
<td>Ali Bin Massie – Former President of Tunisia. Ousted in a coup by al Jucks. Currently in exile in Algeria. He has goals of returning to power in Tunisia.</td>
</tr>
<tr>
<td>Anwar al Jucks – President of Tunisia. Took power in a coup from bin Massie.</td>
</tr>
<tr>
<td>Mounir Klair – Minister of Defense in Tunisia.</td>
</tr>
<tr>
<td>Habib Tekkari – Prime Minister of Tunisia. Long-time ally of President al Jucks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Leadership – Algeria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abdelaziz Madani – President of Algeria.</td>
</tr>
<tr>
<td>Djamel Ghlamallah – Algerian Minister of Defense.</td>
</tr>
<tr>
<td>LTG Ramdi Muhktar – 1st Armored Division Commander, Commander of the el Qued Army Region.</td>
</tr>
<tr>
<td>Darling of the fundamentalist movement inside Algeria. Potential future president of Algeria.</td>
</tr>
<tr>
<td>Mustafa Bassam Yazi – Algerian Vice President.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunisian Government</td>
</tr>
<tr>
<td>Algerian Government</td>
</tr>
<tr>
<td>Tunisian Liberation Front (TLF) – Tunisian insurgency organization with espoused goal of the overthrow of the al Jucks Regime and the return to power of Ali bin Massie.</td>
</tr>
<tr>
<td>Tunisian Military Intelligence</td>
</tr>
<tr>
<td>Algerian Military</td>
</tr>
<tr>
<td>Al Qaeda and other possible militant jihadist groups.</td>
</tr>
</tbody>
</table>
The collected intelligence related to this scenario is shown in Table 18. Two of the hypotheses that are suggested by it are the following ones:

- The Algerian government supports the Tunisian insurgency.
- Al Qaeda acts to make the Tunisian government believe that the Algerian government supports the Tunisian insurgency.

Consequently, the following case study involves assessing the likelihood of these hypotheses based on the available evidence.

Table 18. Intelligence related to the Algeria-Tunisia scenario.

<table>
<thead>
<tr>
<th>INFO-001-HUMINT</th>
<th>Report by a Tunisian border officer on 26 May, 20xx, that an AG-123 diary truck attempting to cross the border from Bir el Ater in Algeria into Tunisia, on 25 May, 20xx, was loaded with weapons and explosive devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFO-002-HUMINT</td>
<td>Testimony on 27 May, 20xx, of Ahmed al-Gadi, the driver of the AG-123 diary truck stating that he is a sergeant in the Algerian military. The truck, which belongs to the Algerian government, departed from the Algerian military installation at Bir el Ater with the destination the city of Gafsa, Tunisia, a stronghold of the Tunisian insurgency.</td>
</tr>
<tr>
<td>INFO-003-HUMINT</td>
<td>Testimony on 28 May, 20xx of Badani, a spokesmen for the Algerian government, that the Algerian government does not supply arms to the Tunisian insurgency. Badani says that al-Gadi’s report is a fabricated incident. A truck was stolen five days ago (23 May, 20xx) from the Algerian military installation at Bir el Ater. Badani also said that Ahmed al-Gadi is not a member of the Algerian military.</td>
</tr>
<tr>
<td>INFO-004-IMINT</td>
<td>Photo of the AG-123 diary truck inside the Algerian military installation at Bir el Ater, taken on 22 May, 20xx.</td>
</tr>
<tr>
<td>INFO-005-COMINT</td>
<td>A recording of an official statement made on 30 May, 20xx, in a speech made in Oran, Algeria by Ali Bin Massie (former President of Tunisia, ousted in a coup by al Jucks and currently in exile in Algeria). Ali Bin Massie said his goal was to return to his opposition to the government of Anwar al Jucks (President of Tunisia). Al Jucks took power in a coup from bin Massie, who claimed that al Jucks is corrupt and uses the oil profits for its own benefit while the people of Tunisia suffer. Ali Bin Massie also calls for the renunciation of the US-Tunisia treaty.</td>
</tr>
<tr>
<td>INFO-006-COMINT</td>
<td>An official statement, recorded on 30 May, 20xx, from Mustafa Bassam Yazi, the Algerian Vice President. Yazi says the Algerian government feels that they should own all the al Burma oil field in spite of the border. The transit rate through the Tunisian pipelines is too high, hurting the Algerian economy. The profits go to the al Jucks cronies. Under bin Massie the rates were much more reasonable.</td>
</tr>
<tr>
<td>INFO-007-HUMINT</td>
<td>Report on 1 June, 20xx, from a Tunisian intelligence source in Algeria, codenamed “Snakebite,” that Algeria is stock piling small arms over and above what their military can use. Snakebite</td>
</tr>
</tbody>
</table>
also says that stockpiles of these weapons in places like Bir el Ater are not well-guarded. Snakebite believes that many of these weapons have been stolen by militant jihadists, in particular by al Qaeda groups.

INFO-008-HUMINT: Assessment on 1 June, 20xx, from the Tunisian Intelligence that the Tunisian Liberation Front (TLF) is trying to solicit additional sources of weapons and is stepping up recruiting.

INFO-009-TECHINT: An IED was discovered on 29 May, 20xx, on a road in Thala, Tunisia. Upon analysis, this IED, of Iranian origin, was very similar to ones used by al Qaeda in their past terrorist actions in Algeria and Tunisia.

INFO-010-HUMINT: A report on 2 June, 20xx, from a Tunisian intelligence source codenamed “Camel,” that he saw two members of the Tunisian Liberation Front (TLF) meeting with two Algerian army officers just outside Tebessa in Algeria.

INFO-011-HUMINT: Report on 3 June, 20xx, from a Tunisian border patrol officer of observing a growing number of probes by the Algerian Army at several places along the Tunisian border.

INFO-012-HUMINT: Report on 4 June, 20xx, from a Tunisian border control officer that a large number of trucks, having dairy markings, have assembled near Bir el Ater and are 10 km from the border from Algeria into Tunisia.

INFO-013-IMINT: A photo taken in Alger, Algeria, on 2 June, 20xx, from a mobile phone belonging to a Tunisian source, codenamed “Cricket,” shows Abdullah Mahood (leader of the Tunisian Liberation Front) in company with bin Massie (former President of Tunisia) in Alger.

INFO-014-HUMINT: Report from Snakebite on 3 June, 20xx, that members of TLF go to Algeria for training.

INFO-015-IMINT: An overhead image, taken on 1 June, 20xx, reveals military training facilities just south of Bir el Ater in Algeria.

INFO-016-HUMINT-and-TECHINT: A man, first thought to be a Tunisian insurgent, was captured in a pickup truck on 2 June, 20xx, near Gafsa in Tunisia. This man was carrying North Korean arms which are imported by Algeria. The man also had a laptop computer in his truck. Analysis of files on this laptop contained messages from an al Qaeda group known to be operating in the vicinity of el Qued in Algeria.

INFO-017-HUMINT: Report from a Tunisian intelligence source, codenamed “Datepalm,” on 6 June, 20xx. Datepalm is a dock worker and gathers intelligence in Oran in Algeria about supplies coming to and going from this Algerian port city. Datepalm says that he recently helped unload several shipments of weapons and explosives from North Korea into Algeria.

INFO-018-COMINT: An intercepted phone message on 7 June, 20xx, from the Algerian Vice-President Mustafa Bassam Yazi to an Algerian Army general in Tebessa. Yazi said that Algeria sympathizes with the people in South Tunisia. Yazi also referred to the TLF as freedom fighters that can no longer support...
oppression from the al Jucks government and desire to liberate the country. Yazi concluded by saying that Algerian forces would be welcomed by the peoples in South Tunisia.

INFO-019-MASINT: A Tunisian Army general was assassinated on 8 June, 20xx, by an explosive device just outside Kasserine in Tunisia. Analysis of the remnants of this device showed it to be virtually identical to the IED that was discovered on 29 May, 20xx, on a road in Thala, Tunisia (see INFO-009-TECHINT). Both devices bear the imprint of al Qaeda.

INFO-020-HUMINT: A man wearing an Algerian army uniform was captured on 10 June, 20xx, just outside Nafta in southern Tunisia near the Algerian-Tunisian border. The man was carrying an Algerian Army ID that, upon analysis, proved to be fraudulent. In addition, the man spoke with a dialect that suggested he was Saudi in origin and not an Algerian.

13.2 Case Study: External Support for Insurgency

13.2.1 Objective

The objective of this case study is to browse a partial analysis of the hypothesis that Algerian government supports the Tunisian insurgency and further extend the analysis.

13.2.2 Summary

This case study concerns the analysis of the problem “Assess whether the Algerian government supports the Tunisian insurgency,” as part of a hypothetical scenario.

You will select this hypothesis and then you will browse its analysis tree to see how it is decomposed into simpler hypotheses and how the solutions of these simpler hypotheses are composed. You will visualize both detailed descriptions of these decomposition and synthesis operations, as well as abstract ones, including an abstract view of the entire tree. You will also visualize the descriptions of the concepts and instances that are referred in the analysis tree. Finally you will extend the analysis by defining new evidence, associating it with the corresponding hypotheses, and assessing these hypotheses.

Proceed as indicated in the following instructions.

13.2.3 Instructions

1. Start the case study in TIACRITIS.

2. Select the Hypothesis menu on the top of the window. As a result you will enter the hypothesis selection module and the interface in Figure 21 (pg. 34) will be displayed. It contains one or several hypotheses to select from.

3. Select the hypothesis analysis problem: “Assess whether the Algerian government supports the Tunisian insurgency.” Once this hypothesis is selected, the Reasoner is automatically invoked to analyze the hypothesis, as shown in Figure 22 (pg. 35). The right panel shows the details of a reasoning step. The left panel shows an abstraction of the step.
4. Select [HIDE SOLUTIONS] link at the top of the window.

5. In the left panel, click on “required conditions for support: no solution” and inspect its decomposition.

6. In the left panel, click on "reasons: no solution" and inspect its decomposition.

7. Browse the rest of the analysis tree.

8. Right-click on top problem in the left panel and select Collapse.

9. Select [SHOW SOLUTIONS] link at the top of the window.

10. In the left panel, click on the top problem, then click on "actual support: likely" and inspect the corresponding problems and their solutions.

11. In the left panel, click on “military equipment support: likely” and inspect the corresponding problems and their solutions.

12. In the left panel, right-click on “AG123 diary truck sent by Algerian government: likely” and select Expand.

13. In the left panel, click on “EVD-003-Ahmed-govtruck: likely” and inspect the corresponding problems and their solutions.

14. Select the Evidence menu. As a result, the left panel shows the defined items of evidence.

15. Click on EVD-003-Ahmed-govtruck and the right panel will show the characteristics of this item of evidence.

16. Browse the other items of evidence.

17. In the left panel, click on [COLLECTED INFORMATION]. As a result, the left panel shows the defined items of information.

18. Click on INFO-002-Ahmed and read its description in the right panel.


20. Select Case Study.

21. Click on [SAVE & FINISH]. You will be able to extend this analysis later by defining new evidence and assessing the corresponding hypotheses.
REFERENCES


Cooper J.R., Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis, Center for the Study of Intelligence, Central Intelligence Agency, Washington, DC, 2005.


APPENDIX: ANSWERS TO QUESTIONS

This appendix contains possible answers to the questions that were posed for the reader throughout this textbook. For many of these questions there will be more than one possible answer. In other words, there are often no unique correct answers. The ones we provide are just examples of answers that seem to make sense.

Question 1 (p. 75) answer. EVD-009-TRUXINCRcord1, EVD-009-TRUXINCRcord2, and EVD-011-SilverSpringRecord are all items of real tangible evidence. EVD-012-InvestigativeRecord is demonstrative tangible evidence. Additionally, Grace could supply documents showing the absence of any use of the cesium-137 in any on-going XYZ project, and those documents would be tangible evidence as well.

Question 2 (p. 79) answer. EVD-019-Walsh is one example, because John Walsh does not equivocate in saying that Omar al-Massari’s work does not involve handling radioactive substances. EVD-014-SantaAlias, EVD-014-SantaWork, EVD-014-SantaAdr, and EVD-014-SantaTerOrg are also items of unequivocal testimonial evidence because Santa does not equivocate in what he is telling us about Omar al-Massari.

Question 3 (p. 79) answer. You should be able to think of many examples. How many times have you heard your spouse say, “I don’t know,” or “I don’t remember” in response to a question you have asked? How many times have you said, “I don’t know” or “I don’t remember” in response to a question your spouse has asked you?

Question 4 (p. 80) answer. We are entitled here to infer that Omar al-Massari has information stored on his laptop about his and others’ activities that he does not wish us to see.

Question 5 (p. 80) answer. What has happened to the cesium-137 canister? Where is it and who has it? How did Omar al-Massari obtain the canister from the XYZ warehouse? Was he assisted by someone at the XYZ company? Did anyone at the XYZ company see Omar al-Massari the day the cesium-137 canister was stolen?

Question 6 (p. 81) answer. EVD-007-GuardReport is tangible evidence about testimonial evidence, because it is a record of Sam’s testimony.

Question 7 (p. 82) answer. The easiest ones perhaps are tangible documents you have received that make reference to other tangible documents, or conversations you have had with persons who tell you about tangible objects they have seen.

Question 8 (p. 118) answer. Our asset, Santa, has told us some very valuable evidence regarding Omar al-Massari. He is obviously an informant or plant inside (what we believe to be) terrorist groups in the area. To be on the safe side, we would like corroborating evidence from other sources concerning what Santa has told us. Additionally, at the risk of being thought paranoid, we might seek corroboration on what John Walsh has told us. Perhaps he is seeking to protect the interests of a valuable employee.
Then of course we have Willard, whose report started this whole thing off. Can we be sure that Willard himself was not involved in some way with the missing cesium-137 canister?

**Question 9 (p. 120) answer.** We might have a source who contradicts Grace’s evidence that no one at the XYZ Company was using cesium-137 on a current project. Alternatively, we might have evidence that the XYZ Company has had radioactive materials stolen in the past by persons working for competitors.

**Question 10 (p. 122) answer.** If we obtain the same reports from two or more sources, these reports will be corroboratively redundant to some degree. Cumulative redundancy involves evidence about different events. We already have evidence of minute cesium-137 traces on the hair and skin of Omar al-Massari, but if we now get evidence of traces of cesium-137 on his clothes we would be inclined to say, “so what?” Finding such traces on his body makes finding traces on his clothes pretty likely and would tell us little we don’t already believe, namely, that Omar al-Massari was exposed to cesium-137.

**Question 11 (p. 131) answer.** We would certainly like to have more evidence concerning the circles Santa travels in, if it is available. We would obviously pump Santa for all the information he can give about this dirty bomb situation.

**Question 12 (p. 133) answer.** To see that all the evidence items in Table 5 and Table 7 are inconclusive, just look at the sources of doubt separating these items from what we are trying to prove from them.

**Question 13 (p. 133) answer.** How about the following: Our wives Anne and Sanda tell us that they are fixing something we will really like for dinner tonight. That’s all they will tell us.

**Question 14 (p. 134) answer.** For a rather complete account of the questions we should ask of human sources of evidence, see: Schum, D. *The Evidential Foundations of Probabilistic Reasoning*. John Wiley 7 Sons, 1994; Northwestern University Press, Evanston, IL, 2001 (paperback ed.), Figure 3.8 on page 107 in both editions.

**Question 15 (p. 135) answer.** What is the authenticity, reliability, and accuracy of the records at XYZ Company logs recording the license numbers of trucks that enter and leave the parking area?