

---

---

## Intelligence Analysis

---

---

July 2009

**DISTRIBUTION RESTRICTION:** Distribution authorized to U.S. Government agencies only because it requires protection in accordance with AR 380-5 and as specified by DCS G-3 Message DTG 091913Z Mar 04. This determination was made on 12 January 2009. Contractor and other requests must be referred to ATTN: ATZS-CDI-D, U.S. Army Intelligence Center and Fort Huachuca, AZ 85613-7017, or via email at [ATZS-FDC-D@conus.army.mil](mailto:ATZS-FDC-D@conus.army.mil).

**DESTRUCTION NOTICE:** Destroy by any method that prevents disclosure of contents or reconstruction of the document in accordance with AR 380-5.

---

---

## Headquarters, Department of the Army

---

---

**FOR OFFICIAL USE ONLY**

**This page intentionally left blank.**

# Intelligence Analysis

## Contents

	Page
<b>PREFACE .....</b>	<b>v</b>
<b>INTRODUCTION .....</b>	<b>vii</b>
<b>Chapter 1 INTELLIGENCE ANALYSIS OVERVIEW .....</b>	<b>1-1</b>
The Intelligence Warfighting Function .....	1-1
The Intelligence Analyst .....	1-1
Intelligence Analysis Process .....	1-2
Characteristics of Effective Intelligence .....	1-2
The Intelligence Process .....	1-2
Intelligence Preparation of the Battlefield .....	1-3
Intelligence Running Estimate .....	1-3
The Military Decisionmaking Process .....	1-3
<b>Chapter 2 ANALYTICAL PROCESSES, METHODOLOGIES, AND TERMS .....</b>	<b>2-1</b>
Overview .....	2-1
Critical Thinking .....	2-1
Types of Reasoning .....	2-8
The Scientific Method .....	2-9
Analysis of Competing Hypotheses .....	2-10
Situational Logic .....	2-18
Applying Theory .....	2-19
Comparison .....	2-19
Modeling .....	2-19
Processes for Intelligence Analysis .....	2-20
Analytical Terms .....	2-21

---

**DISTRIBUTION RESTRICTION:** Distribution authorized to U.S. Government agencies only because it requires protection in accordance with AR 380-5 and as specified by DCS G-3 Message DTG 091913Z Mar 04. This determination was made on 12 January 2009. Contractor and other requests must be referred to ATTN: ATZS-CDI-D, U.S. Army Intelligence Center and Fort Huachuca, AZ 85613-7017, or via email at ATZS-FDC-D@conus.army.mil.

**DESTRUCTION NOTICE:** Destroy by any method that prevents disclosure of contents or reconstruction of the document in accordance with AR 380-5.

\* This publication supersedes FM 34-3, 15 March 1990.

<b>Chapter 3</b>	<b>ANALYTICAL SUPPORT TO SITUATIONAL UNDERSTANDING .....</b>	<b>3-1</b>
	Threat Analysis .....	3-1
	Threat Characteristics Recordkeeping and Database.....	3-12
	Terrain Analysis .....	3-14
	Weather Analysis .....	3-17
	Civil Considerations .....	3-20
	Cultural Database .....	3-24
<b>Chapter 4</b>	<b>ANALYTICAL SUPPORT TO COURSE OF ACTION DEVELOPMENT .....</b>	<b>4-1</b>
	Situation Development.....	4-1
	The Situation Map.....	4-2
	Functional Analysis.....	4-6
	Threat Courses of Action .....	4-9
	Indicators.....	4-11
<b>Chapter 5</b>	<b>ANALYTICAL TOOLS AND PRODUCTS .....</b>	<b>5-1</b>
	Analytical Techniques and Tools .....	5-1
	Automation Support to Intelligence Analysis .....	5-18
<b>Appendix A</b>	<b>ANALYTICAL PITFALLS .....</b>	<b>A-1</b>
<b>Appendix B</b>	<b>THE INTELLIGENCE RUNNING ESTIMATE .....</b>	<b>B-1</b>
<b>Appendix C</b>	<b>INDICATORS.....</b>	<b>C-1</b>
<b>Appendix D</b>	<b>OTHER ANALYTICAL APPROACHES.....</b>	<b>D-1</b>
<b>Appendix E</b>	<b>THREAT CHARACTERISTICS AND INTELLIGENCE ANALYSIS IN COUNTERINSURGENCY OPERATIONS .....</b>	<b>E-1</b>
	<b>GLOSSARY .....</b>	<b>Glossary-1</b>
	<b>REFERENCES.....</b>	<b>References-1</b>
	<b>INDEX .....</b>	<b>Index-1</b>

## Figures

Figure 2-1. Example of analysis of competing hypotheses matrix .....	2-13
Figure 3-1. Grouping mobility corridors to establish avenues of approach .....	3-15
Figure 3-2. Combined obstacle overlay example .....	3-16
Figure 3-3. Example light data chart.....	3-18
Figure 3-4. National Weather Service wind chill factor chart.....	3-18
Figure 3-5. Example of a weather effects chart .....	3-19
Figure 3-6. Example of shared weather effects analysis.....	3-20
Figure 3-7. Example civil considerations product concerning tribes and ethnic groups .....	3-23
Figure 3-8. Example population status overlay.....	3-24
Figure 4-1. Cycle for situational understanding .....	4-2
Figure 4-2. Example of a situation map .....	4-5
Figure 4-3. Depiction of threat functions during an assault .....	4-7

Figure 4-4. Using a complete mission as an enabler for another larger mission..... 4-8

Figure 5-1. Example of a pattern analysis plot sheet..... 5-3

Figure 5-2. Example of an incident overlay ..... 5-4

Figure 5-3. Example of nodes in a network..... 5-5

Figure 5-4. Notional iconic representation of nodal component analysis by activity..... 5-6

Figure 5-5. Example enemy IED network nodal diagram showing relationships..... 5-9

Figure 5-6. Sample time event chart ..... 5-10

Figure 5-7. Example time event chart using Analyst Notebook software ..... 5-11

Figure 5-8. Association matrix symbology ..... 5-12

Figure 5-9. Association matrix example ..... 5-13

Figure 5-10. Activities matrix example ..... 5-13

Figure 5-11. Link diagram concept..... 5-14

Figure 5-12. Example link diagram using Analyst Notebook ..... 5-15

Figure 5-13. Link diagram example using Analyst Notebook software..... 5-15

Figure 5-14. Analyst Notebook link diagram showing information from an activity matrix ..... 5-16

Figure 5-15. Analyst Notebook link diagram showing nonpersonal relationship ..... 5-16

Figure 5-16. Analyst Notebook hierarchy layout ..... 5-17

Figure 5-17. Completed link diagram with supporting matrices ..... 5-17

Figure B-1. Annotated intelligence running estimate format ..... B-2

Figure D-1. CARVER value rating scale (notional) ..... D-2

Figure D-2. Example of DSHARPP matrix tool ..... D-4

Figure D-3. Sample imagery of target area ..... D-5

Figure D-4. Sample sketch of target area ..... D-6

Figure D-5. Sample of labeled target building (rear)..... D-8

## Tables

Table 3-1. Threat characteristics..... 3-2

Table 3-2. Examples of civil considerations ..... 3-22

Table 5-1. Possible nodes located in an improvised explosive device network ..... 5-7

Table C-1. Sample offensive indicators..... C-2

Table C-2. Sample defensive indicators ..... C-4

Table C-3. Sample delaying indicators..... C-5

Table C-4. Sample withdrawal indicators ..... C-5

Table C-5. Sample population indicators ..... C-6

Table C-6. Sample propaganda indicators..... C-8

Table C-7. Sample commodities indicators..... C-9

Table C-8. Environment-related indicators..... C-10

Table C-9. Improvised explosive device indicators ..... C-11

**Contents**

---

Table C-10. Sample threat environment indicators .....C-11  
Table C-11. Recurrence of same clan indicators .....C-12  
Table D-1. Structure analysis matrix.....D-6  
Table D-2. Sample building analysis matrix.....D-7  
Table D-3. Example intelligence requirements for individual buildings .....D-8  
Table D-4. Example intelligence requirements for an individual person .....D-10

## Preface

This circular describes the fundamentals of intelligence analysis. It describes analysis, its use in the intelligence effort, and its role in driving the intelligence running estimate of enemy courses of action and the operational environment.

This circular conforms to the overarching doctrinal concepts presented in FM 3-0 and FM 2-0. It provides doctrinal guidance for the use of analysis in the intelligence effort and its role in supporting the commander and staff. It also serves as a reference for personnel who are developing doctrine; tactics, techniques, and procedures, and institutional and unit training for military operations.

This circular keeps the title “Intelligence Analysis” to describe the process of analyzing the operational environment and the options it presents to threat forces. The use of “battlespace” is replaced by the term “operational environment” or “area of operations,” as appropriate.

The primary audience for this circular is commanders and staffs at battalion level and higher, and military intelligence personnel at all echelons. This circular is also intended to be a resource for trainers.

TC 2-33.4 is not the proponent publication (the authority) for any Army term. For terms defined in the text, the term is italicized and the number of the proponent publication follows the definition.

References to “S” staff sections apply to general, joint, or multinational staffs unless otherwise stated.

This publication contains copyrighted material.

This circular applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

U.S. Army Training and Doctrine Command is the proponent for this publication. The preparing agency is the U.S. Army Intelligence Center and School. Send written comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, ATTN: ATZS-CDI-D, U.S. Army Intelligence Center and Fort Huachuca, 550 Cibequa Street, Fort Huachuca, AZ 85613-7017; or by email to [ATZS-FDC-D@conus.army.mil](mailto:ATZS-FDC-D@conus.army.mil).

## Acknowledgements

The material in paragraphs 2-4 through 2-21 has been used with permission from The Foundation for Critical Thinking, [www.criticalthinking.org](http://www.criticalthinking.org), *The Thinker's Guide to Analytic Thinking*, 2007, and *The Miniature Guide to Critical Thinking: Concepts and Tools*, 2008, by Dr. Linda Elder and Dr. Richard Paul. The copyright owners have granted permission to reproduce material from their works. With their permission, some of the text has been paraphrased and adapted for military purposes.



# Introduction

## THE OPERATIONAL ENVIRONMENT

America has entered an era of persistent conflict where states, nations, transnational actors, and nonstate actors are increasingly willing to use violence to achieve their political and ideological ends. These entities will continue to challenge and redefine the global distribution of power, the concept of sovereignty, and the nature of warfare. Globalization, technology, population growth, urbanization, and demand for natural resources are creating an environment where the location of the next crisis requiring American intervention is not always predictable. Generally with little notice, Army units will be employed in complex and multidimensional environments; usually fought in urban terrain among noncombatant populations. Additionally, they will be called on to conduct full spectrum operations as part of an interdependent joint force conducting simultaneous offensive, defensive, and stability operations. See FM 3-0 for a detailed description of the operational environment.

## THE THREAT ENVIRONMENT

FM 3-0 defines threats as nation-states, organizations, people, groups, conditions, or natural phenomena able to damage or destroy life, vital resources, or institutions. There are four major threat categories intelligence analysts must assist the commander and staff in understanding:

- Irregular threats are characterized as entities seeking to erode U.S. power through protracted struggle. Radical fundamentalists, transnational terrorists, and guerrilla forces are examples of irregular threat. These groups will employ unconventional and asymmetric methods and means to counter U.S. advantages. Irregular warfare includes terrorism, insurgency, and guerilla warfare.
- Traditional threats emerge from states employing recognized military capabilities and forces in understood forms of military competition and conflict.
- Catastrophic threats involve the acquisition, possession, and use of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) weapons.
- Disruptive threats involve an enemy using new technologies to reduce U.S. advantages in key operational domains.

Army units are likely to face any combination of these threats when deployed. By combining irregular, traditional, catastrophic, and disruptive capabilities, adversaries will seek to create advantageous conditions by changing the nature of the conflict from one where U.S. forces can effectively use size, firepower, and technology to its advantage to one where adversaries can use low technology solutions and control of key and decisive terrain to gain and maintain the initiative.

U.S. forces may be employed under the following five types of operational themes across the spectrum of conflict; each with its own unique threat environment:

- Peacetime military engagement comprises all military activities that involve other nations and are intended to shape the security environment in peacetime. Examples include multinational training exercises, security assistance, joint combined exchange training, recovery operations, arms control, and counterdrug operations. Combat is not likely during these operations, but terrorist attacks are always possible and force protection and operations security (OPSEC) are major concerns.
- Limited interventions are executed to achieve an end state that is clearly defined and limited in scope. They are normally conducted by joint task forces. Examples of limited interventions are noncombatant evacuation, raids, show of force, foreign humanitarian assistance, consequence

management, sanction enforcement, and elimination of weapons of mass destruction (WMDs). Like peacetime military engagement, combat is not likely. However, the threat of terrorist attacks is possible, as are attacks from the general population. Force protection, OPSEC, and targeting operations are major concerns.

- Peace operations is a broad term that encompasses multiagency and multinational crisis response and limited contingency operations. The primary purpose of peace operations is to create a safe and secure environment, deter adversaries from overt actions against each other, and provide time for civilian agencies to generate a self-sustaining peace. Peace operations include peacekeeping, peace building, peacemaking, peace enforcement, and conflict prevention. Peace operations normally occur in complex environments. They are characterized by asymmetric threats, a failing government, absence of the rule of law, terrorism, human rights abuses, collapse of civil infrastructure, and the presence of dislocated civilians. Attacks by insurgent and terrorist groups are likely, and U.S. forces may conduct limited offensive operations against these groups in support of stability operations.
- Irregular warfare is a violent struggle among state and nonstate actors for legitimacy and influence over a population. It differs from conventional operations in two aspects. First, it is warfare among and within the people. Second, it emphasizes an indirect approach. Irregular warfare avoids direct military confrontation. Instead, it combines irregular forces and indirect unconventional methods to exhaust the opponent. Types of operations U.S. forces may be employed in to counter irregular warfare are foreign internal defense, support to insurgency, counterinsurgency (COIN), combating terrorism, and unconventional warfare. Traditionally, these missions are conducted by special forces. However, if special forces and host-nation (HN) forces cannot defeat unconventional and irregular threats, conventional Army forces can assume the lead role. Operation Iraqi Freedom and Operation Enduring Freedom are good examples of this.
- Major combat operations occur in circumstances usually characterized by general war and combat between large formations. In this instance, U.S. forces are normally involved in offensive or defensive operations as part of a larger joint force. Major combat operations are the operational theme for which doctrine, including the principles of war, was originally developed. The intelligence analyst provides doctrinal intelligence support to major combat operations in accordance with FM 2-0.

The military intelligence (MI) analyst must understand the four threat categories and the five operational themes previously discussed that prescribe the use of military force. The analyst is the commander's subject matter expert on enemy composition, organization, capabilities, operational art, and tactics, techniques, and procedures (TTP). Each type of threat requires a unique analytical and operational approach to counter it. This circular will discuss these approaches in the context of the intelligence warfighting function and the operational framework under which the analyst is employed. This circular provides examples and additional material in the following appendices:

- Appendix A – Analytical Pitfalls.
- Appendix B – The Intelligence Running Estimate.
- Appendix C – Indicators.
- Appendix D – Other Analytical Approaches.
- Appendix E – Threat Characteristics and Intelligence Analysis in Counterinsurgency Operations.

## Chapter 1

# Intelligence Analysis Overview

This chapter establishes the intelligence warfighting function as the framework for intelligence analysis, discusses the role of the intelligence analyst, and describes the processes used to conduct effective analysis in support of plans and operations.

### THE INTELLIGENCE WARFIGHTING FUNCTION

1-1. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding of the operational environment, enemy, terrain, and civil considerations (FM 3-0). It includes tasks associated with intelligence, surveillance, and reconnaissance (ISR) operations, and is driven by the commander. Intelligence is more than just collection. It is a continuous process that involves analyzing information from all sources and conducting operations to develop the situation. The intelligence warfighting function is comprised of the following four primary Army intelligence tasks that facilitate the commander's visualization and situational understanding of the operational environment:

- Support to force generation.
- Support to situational understanding.
- Perform intelligence, surveillance, and reconnaissance.
- Support to targeting and information superiority.

1-2. Intelligence analysis is a process that is focused by the tasks established by the intelligence warfighting function and described in FM 2-0. Intelligence analysts at all levels must understand the task and purpose of the intelligence warfighting function, be proficient in the subtasks articulated in FM 2-0, and know how intelligence analysis relates to military planning and operations. See FM 2-0 for a detailed discussion of the intelligence warfighting function. See FM 5-0 for a detailed discussion of military planning and operations.

### THE INTELLIGENCE ANALYST

1-3. To effectively execute missions across the full spectrum of military operations, the commander requires intelligence about the enemy and other conditions of the operational environment prior to and during operations. The *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decision of the commander (JP 3-0). The operational environment encompasses physical areas and factors of the air, land, maritime, and space domains. It also includes the information environment and enemy, adversary, friendly, and neutral systems.

1-4. The analyst is directly responsible for aiding the commander's understanding of how current and potential enemies organize, equip, recruit, train, employ, and control their forces. The analyst also aids the commander's understanding of the terrain and weather and their effects upon both friendly and enemy operations. This includes the military aspects of the terrain and weather as well as civil considerations.

1-5. In order to provide the commander the most accurate analysis of enemy disposition and intent, the analyst must—

- Develop detailed threat characteristics.
- Project where and how the enemy is deployed on the battlefield.
- Describe where and how the enemy will maneuver.

- Identify targets.
- Assist in developing an ISR synchronization plan that helps the commander develop the situation out of contact and conduct decisive maneuver to accomplish the commander's objectives.
- Continually assess effects once forces are committed, and recommend modifications to the commander's targeting priorities and intelligence collection operations.

## INTELLIGENCE ANALYSIS PROCESS

1-6. Analysis is the process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current—and attempts to predict the future—impact of the threat, terrain and weather, and civil considerations on operations. It is a disciplined and consistent approach to problem solving that assists the analyst or intelligence staff in determining accurate and unbiased conclusions based on available data. In the Army, intelligence analysis is focused by the intelligence preparation of the battlefield (IPB) process applied during the military decisionmaking process (MDMP) and by the intelligence process throughout Army force generation (ARFORGEN).

1-7. Intelligence analysts must understand that the purpose of intelligence is to provide commanders and their staffs with relevant, analyzed information about the enemy and the environment in a timely manner. Intelligence supports the planning and execution of missions. The most important role of intelligence is to affect, influence, and support the commander's decisionmaking. Intelligence must be timely, relevant, accurate, predictive, and tailored.

## CHARACTERISTICS OF EFFECTIVE INTELLIGENCE

1-8. The effectiveness of the intelligence warfighting function and the intelligence staff's analytical effort is measured against the following standards:

- **Timely.** Intelligence must be provided early enough to support planning, influence decisions and execution of operations, and prevent surprise from enemy action. It must flow continuously to the commander before, during, and after an operation. Regardless of distance and time, intelligence organizations, databases, and products must be available to develop estimates, make decisions, and plan operations.
- **Relevant.** Intelligence must support the commander's concept of the operation and the unit's mission. It must be tailored to the capabilities of the unit and the priorities of the commander, referred to as commander's critical information requirements (CCIRs). Intelligence must be in a usable format which meets the specific needs of the requestor and explains its own significance.
- **Accurate.** Intelligence must give commanders a balanced, complete, and objective picture of the enemy and the operational environment. It should support and satisfy the priorities of the commander. To the extent possible, intelligence should correctly identify threat intentions, capabilities, limitations, and dispositions. It should be derived from multiple sources and disciplines to minimize the possibility of deception or misinterpretation. Alternative or contradictory assessments should be presented, when necessary, to ensure balance and bias-free intelligence.
- **Predictive.** Intelligence should inform the commander about what the enemy is doing, can do, and is most likely expected to do (most likely enemy course of action [COA]). The intelligence warfighting function should anticipate the intelligence needs of the commander.
- **Tailored.** Intelligence must be presented based on the needs of the commanders, subordinate commanders, and staff in a specific format that is clear and concise so they can understand it, believe it, and act on it.

## THE INTELLIGENCE PROCESS

1-9. Intelligence analysts operate within the framework established by the intelligence process. Intelligence operations are executed by performing six steps that constitute the intelligence process:

generate knowledge, plan, prepare, collect, process, and produce. The intelligence process generates information, products, and knowledge about the threat, the area of interest, and the situation, which supports the commander and staff in developing a plan, seizing and retaining the initiative, building and maintaining momentum, and exploiting success. See FM 2-0 for a detailed discussion on the intelligence process.

## **INTELLIGENCE PREPARATION OF THE BATTLEFIELD**

1-10. During planning, intelligence analysis is focused by the IPB process. This process consists of four steps that are performed or at least considered each time the staff plans an operation. Each step in the process is performed or assessed and refined continuously to ensure that the products of IPB remain complete and relevant and that the commander receives the needed intelligence support during current and future operations. The following are the four steps of IPB, which are discussed in detail in FMI 2-01.301:

- Define the operational environment.
- Describe environmental effects on operations.
- Evaluate the threat.
- Determine threat COAs.

1-11. IPB supports the development of the intelligence running estimate and the conduct of MDMP. Most intelligence requirements are generated as a result of the IPB process and the interrelationship of IPB to the MDMP. IPB is a process employed as part of intelligence planning to reduce uncertainties concerning the enemy, terrain, weather, and civil considerations for all types of operations. IPB is conducted during mission planning and throughout the conduct of the operation. It supports the commander's decisionmaking and forms the basis for direction of intelligence operations in support of current and future missions.

## **INTELLIGENCE RUNNING ESTIMATE**

1-12. The result of intelligence analysis is the development and maintenance of the intelligence running estimate. The intelligence running estimate is a logical and orderly examination of the intelligence factors affecting mission accomplishment. It provides commanders with a basis for planning operations and for disseminating intelligence to their staffs and to other headquarters.

1-13. The intelligence running estimate consists of five paragraphs, which outline an analysis of the area of operations (AO), enemy strength, and enemy capabilities that can influence the mission. It may be presented to commanders formally or informally and may be written or oral, detailed or summarized. However, when possible, a written estimate is preferred. The intelligence analyst prepares the intelligence running estimate in accordance with unit standing operating procedures. Appendix B provides an example of an intelligence running estimate.

## **THE MILITARY DECISIONMAKING PROCESS**

1-14. FM 5-0 provides a common understanding of the fundamentals of planning and provides the foundation for developing TTP for planning used in all other Army publications and unit standing operating procedures. It also provides a doctrinal approach to decisionmaking that helps the commander and staff examine a situation, reach logical conclusions, and make informed decisions. To effectively assist in planning, intelligence analysts must understand the purpose, environment, and characteristics of the planning process.

1-15. Knowledge of the concepts stated in FM 5-0 forms the basis of this understanding. In addition, intelligence planners must understand enemy tactics, enemy operational art, the fundamentals of full spectrum operations described in FM 3-0, and the art of tactics described in FM 3-90. Finally, intelligence analysts must be familiar with the operations process (plan, prepare, execute, and assess) and understand

how mission command, the commander's visualization of the situation, and the commander's exercise of command and control influence planning.

1-16. The planning process prescribed in FM 5-0 is built on two central precepts: commanders are responsible for planning, and effective planning incorporates the concept of mission command.

1-17. The commander's knowledge, experience, and personality, along with how the commander interacts with the staff and subordinate commands, drive the planning process. While the staff completes much of the detailed analysis and preparation of plans and orders, the commander plays a central role in planning by giving the staff commander's intent, CCIRs, and planning guidance. This input guides the activities of the staff and subordinate commanders. In turn, the staff assists the commander with the coordination and detailed analysis necessary to convert commander's intent, CCIRs, and planning guidance into a plan or order.

1-18. Just like the rest of the staff, intelligence analysts are focused on helping the commander make decisions and develop effective plans and orders. During mission analysis, the intelligence analyst ensures the commander understands the enemy situation and how the environment may impact operations. During COA development and comparison, the intelligence analyst provides tactically sound recommendations related to ISR operations to support the commander in selecting a COA. After the commander makes a decision, the intelligence analyst prepares and provides input to the intelligence officer in order to complete the intelligence portion of the plan or order; coordinating all necessary details with higher headquarters and subordinate commands.

1-19. During the MDMP, the intelligence analyst is responsible for developing a specific set of intelligence products and tools in accordance with the guidance and timelines established by the intelligence officer. Formal planning begins with the receipt of mission from higher headquarters or as directed by the commander.

## MISSION ANALYSIS

1-20. Most of intelligence analyst's products are developed during mission analysis. Both the process and products of mission analysis help commanders refine their situational understanding and determine their mission. Accurate situational understanding enables commanders to better visualize the operation. The 17 separate tasks associated with mission analysis are listed below. The intelligence analyst is involved in all of them.

- Analyze higher headquarters order.
- Perform initial IPB.
- Determine specified, implied, and essential tasks.
- Review available assets.
- Determine constraints.
- Identify critical factors and assumptions.
- Perform risk assessment.
- Determine initial CCIRs and EEFIs.
- Determine the initial ISR plan.
- Update the operational timelines.
- Write the restated mission.
- Deliver a mission analysis briefing.
- Approve the restated mission.
- Develop the initial commander's intent.
- Issue the commander's planning guidance.
- Issue a warning order.
- Review all facts and assumptions.

1-21. Generally, the intelligence portion of mission analysis is an evaluation of the following effects within the AO: threat, terrain, weather, and civil considerations. Additionally, it includes an analysis of the higher headquarters' plan or order to determine critical facts and assumptions; specified, implied, and essential tasks; and constraints that affect ISR operations. End state is the development of an initial ISR plan, the commander refining the estimate based on a clear understanding of the situation, and the staff refining running estimates based on that same understanding.

1-22. To ensure there is a clear and common understanding of what information is fact and what is assumption, it is at this point that the intelligence analyst tells the commander and staff what is known, what is thought, and what is yet unknown. Analysts should also be prepared to explain and present information that led them to their conclusions. This interaction promotes critical thinking and generates the staff discussion required to formulate sound COAs.

### **COURSE OF ACTION DEVELOPMENT**

1-23. The purpose of COA development is to present the commander with options of response to possible or probable enemy action. The staff develops friendly COAs based on facts and assumptions identified during IPB and mission analysis. Incorporating the results of IPB into COA development ensures that each friendly COA takes advantage of the opportunities the environment and threat situation offer.

1-24. The intelligence analyst works closely with the rest of the staff to analyze relative combat power and develop friendly COAs that can defeat enemy operations. All friendly COAs are developed off the enemy situation template and enemy event template or matrix the intelligence analyst produced during mission analysis. At the conclusion of COA development the staff has completed draft information requirements for each friendly COA as well as a draft ISR overlay and synchronization matrix in preparation for COA analysis.

### **COURSE OF ACTION ANALYSIS (WAR-GAMING)**

1-25. COA analysis is a disciplined process that includes rules and steps followed in sequence. It relies heavily on an understanding of doctrine, tactical judgment, and experience. Each staff member participating must come prepared with the full knowledge of the warfighting function represented. The intelligence analyst may have two functions in the war game: the analyst may role-play the enemy commander and may act as the unit intelligence planner.

- First, as the enemy commander, using the enemy situation template as a start point and the event template or matrix as a guide, the analyst develops critical enemy decision points in relation to friendly COAs; projects enemy reactions to friendly actions; and projects enemy losses.
- Second, as the intelligence planner, the analyst identifies new information requirements; assists the staff in developing priority intelligence requirements (PIRs); refines the situation and event templates; develops the ISR overlay and synchronization matrix; and assists in the development of the high-payoff targets (HPTs) and the decision support template. At the conclusion of the war game, pending COA approval by the commander, every intelligence product that must be published with the order is complete.

1-26. At the conclusion of the war game the staff identifies its preferred COA and makes a recommendation to the commander. This is the COA decision briefing. During this briefing the intelligence analyst will brief any changes to the current enemy situation and any environmental factors that have changed since the commander was last briefed.

### **ORDERS PRODUCTION**

1-27. The staff, led by the S-3 prepares the order by turning the selected COA into a clear, concise concept of operations and supporting information. The order provides all the information subordinate commands need to plan and execute their operations. However, this is not the first time subordinate commanders and their intelligence staffs have seen this data.

1-28. As stated previously, within the brigade's parallel and collaborative planning process, planners at all echelons have been involved in the brigade orders process. Brigade and separate battalion S-2 sections have been reviewing brigade intelligence staff products as they were developed and, at this point, are clarifying changes and submitting requests for additional information and product support. Prior to the order being issued the brigade S-2 will conduct an orders crosswalk with the rest of the staff as directed by the brigade S-3.



## Chapter 2

# Analytical Processes, Methodologies, and Terms

This chapter addresses common analytical processes, methodologies, and terms used during the conduct of intelligence analysis.

## OVERVIEW

2-1. Intelligence analysis requires higher order thinking. Higher order thinking involves learning complex skills such as critical thinking and various problem-solving techniques. Effective use of these skills and techniques will improve an analyst's ability to provide clear and accurate assessments of complex situations.

2-2. Analysts may be inclined to draw inclusions and make decisions based on personal knowledge and experience. Personal experience provides what most would call "know-how." Learning from experience is characteristic of intelligent behavior. However, there are problems associated with knowledge gained from experience. The major problem is that experience is subjective and often leads to flawed conclusions. (See analytical pitfalls discussed in appendix A.) To avoid this, analysts strive to provide reasonable and justifiable conclusions based on unbiased evaluation of fact and assumption.

2-3. While there is no "right way" to solve a problem in each and every circumstance, there are several processes and methodologies analysts may use to increase accuracy in their evaluations. The foundation upon which the analyst performs those processes and methodologies is critical thinking. The processes and methodologies include—

- Reasoning types.
- Scientific method.
- Analysis of competing hypotheses (ACH).
- Situational logic.
- Applying theory.
- Comparison.
- Modeling.

## CRITICAL THINKING

2-4. Critical thinking is essential to improved analysis because critical thinking is disciplined reasoning whereby individuals formulate ideas about what to believe or do. Cognition is the broad term that includes all the ways by which we come to know things. Some of our knowledge is instinctive; some we acquire by various means; some we generate ourselves. Thinking is the deliberate part of cognition. When we think critically, we impose structures to ensure rigor and thoroughness without needlessly limiting creativity.

2-5. Researchers Richard Paul and Linda Elder of the Foundation for Critical Thinking developed three useful guides to improve thinking:

- The elements of thought, which provide a checklist to help ensure reasoning is thorough.
- The standards of thinking, which serve as a guide to check the quality of thinking.
- The essential intellectual traits, which describe the individual who carefully and habitually applies the elements and standards.

2-6. Striving to incorporate the elements of thought, standards of thinking, and developing essential intellectual traits is beneficial even when dealing with entry-level analysis. However, to fully develop critical thinking skills analysts require training and deliberate practice. Recommended readings provided by The Foundation for Critical Thinking are listed in the references.

### THE ELEMENTS OF THOUGHT

2-7. There are eight basic elements present in all thinking. Whenever we think, we think for a purpose within a point of view based on assumptions leading to implications and consequences. We use ideas and theories to interpret data, facts, and experiences in order to answer questions, solve problems, and resolve issues. This section discusses these eight elements in more detail:

- **Element 1 – Purpose.** All thinking has a purpose. A critical thinker will state the purpose clearly. Being able to distinguish your purpose from other related purposes is an important skill a critical thinker possesses. Checking periodically to be sure you are still on target with the purpose is also important.
- **Element 2 – Question.** All thinking is an attempt to figure something out, to settle some question or to solve some problem. A critical thinker is able to state questions clearly and precisely, express the questions in several ways to clarify their meaning and scope, and break the questions into subquestions. There are three general types of questions: fact based, opinion, and preference. Fact-based questions generally have one verifiably correct answer; opinion questions are answered subjectively, and questions of judgment have better and worse answers.
- **Element 3 – Assumptions.** All thinking is based on assumptions. Critical thinkers clearly identify their assumptions and work to determine if they are justifiable. In addition, it is important to realize that your assumptions are shaping your point of view.
- **Element 4 – Point of View.** All thinking is done from some point of view. To think critically you must recognize your point of view, seek other points of view, and look at them fairly for their strengths and weaknesses.
- **Element 5 – Information.** All thinking is based on data, information, and evidence. Critical thinkers should restrict their claims to those supported by the relevant information. Be open to actively searching for information that supports as well as contradicts your position. Make sure that all information is as accurate, clear, and relevant.
- **Element 6 – Concepts.** All thinking is expressed through, and shaped by, concepts and ideas. Critical thinkers must identify key concepts and explain them clearly. Consider alternative concepts or alternative definitions of concepts in your thinking.
- **Element 7 – Inferences.** All thinking contains inferences or interpretations by which we draw conclusions and give meaning to data. Be careful to infer only what the evidence implies and to crosscheck inferences with each other. Clearly identify the assumptions which led you to the inferences you are making. Consider alternative inferences or conclusions.
- **Element 8 – Implication.** All thinking leads somewhere or has implications and consequences. Take the time to think through the implications and consequences that follow from your reasoning. Search for negative as well as positive implications.

### Checklist for Reasoning

2-8. By applying the eight elements of thought, analysts can develop a checklist for reasoning. Developing and using a reasoning checklist, as shown below, will help analysts focus their efforts to a specific problem and avoid wasting time on irrelevant issues or distractions:

- All reasoning has a PURPOSE:
  - Express the purpose clearly.
  - Distinguish the purpose from similar purposes.

- Check regularly to ensure the analysis is still on target.
  - Choose meaningful and realistic purposes.
- All reasoning is an attempt to find an answer, to resolve some QUESTION, and to solve some problem:
  - State the question at issue clearly and precisely.
  - Express the question in several ways to clarify its meaning and scope.
  - Break the question down into subquestions.
  - Determine if the question has only one correct answer; decide if it is a fact or an assumption; assess whether it requires reasoning from more than one point of view.
- All reasoning is based upon facts and ASSUMPTIONS:
  - Identify assumptions and determine whether they are justifiable.
  - Consider how assumptions are forming the point of view.
  - Ensure the facts are true.
  - Verify facts with multiple sources if possible.
- All reasoning is done from some POINT OF VIEW:
  - Identify a point of view.
  - Evaluate other points of view and identify strengths and weaknesses.
  - Strive to be open-minded in evaluating all points of view.
- All reasoning is based upon raw data and INFORMATION:
  - Restrict claims to those supported by the data.
  - Search for information that opposes the position as well as information that supports it.
  - Make sure that all information used is clear, accurate, and relevant to the question at hand.
  - Make sure sufficient information is collected.
- All reasoning is formed by CONCEPTS and ideas:
  - Identify key concepts and explain them logically.
  - Consider alternative concepts or alternative definitions to concepts.
  - Develop ideas clearly and precisely.
- All reasoning contains INFERENCES or interpretations by which we draw conclusions and give meaning to data:
  - Infer only what the information implies.
  - Confirm assumptions which lead to inferences.
  - Verify inferences for their consistency with each other.
- All reasoning leads somewhere or has IMPLICATIONS and consequences:
  - Trace the implications and consequences that follow from reasoning.
  - Search for negative and positive implications.
  - Consider all possible consequences.

### The Intellectual Standards

2-9. When critical thinkers take apart their thinking and examine its parts, they use standards of quality we refer to as the intellectual standards or standards for thought. While the elements of thought provide a framework for analyzing thinking, the standards of thought provide criteria critical thinkers use to assess the quality of thinking. Here are some essential intellectual standards—clarity, accuracy, precision, relevance, depth, breadth, logic, significance, and fairness. These standards are discussed below:

- **Standard 1 – Clarity.** Clarity is a gateway standard. If the questions we are trying to answer and such things as the information we are using, the inferences we are making, the assumptions that guide our thinking are unclear, we cannot determine whether they are accurate, relevant, logical, justifiable, and so forth.

- **Standard 2 – Accuracy.** To be accurate is to represent something in accordance with the way it actually is. People often describe things or events inaccurately. Critical thinkers listen carefully to statements and, when there is reason for skepticism, they question whether what they hear is true or accurate. A statement describing an implication, assumption, inference, or the very question we are trying to answer may be clear but not accurate. At the same time, because we tend to think from an egocentric perspective, assessing the accuracy of our own ideas can be difficult. We often tend to believe that our thoughts are accurate just because they are ours; therefore, the thoughts of those that disagree with us are inaccurate. We also often fail to question statements others make that agree with what we already believe.
- **Standard 3 – Precision.** To be precise is to give the details needed for someone to understand exactly what is meant. Precise thinking seeks out more details and greater specificity when necessary. You can apply the standard of precision to evaluate how detailed the question is that you are answering, or how detailed it needs to be. Precision is also standard to determine if assumptions and facts contain enough detail to evaluate them using the standards of relevance, clarity, and accuracy.
- **Standard 4 – Relevance.** Something is relevant when it is connected with and bears upon the question we are reasoning through. Something is also relevant when it is pertinent or applicable to a problem we are trying to solve. Relevant thinking also encourages us to identify facts, information, questions, assumptions, implications, and points of view that we should set aside as not being pertinent to the main issue. Thinking that is relevant stays on track. People are often irrelevant in their thinking because they lack discipline. They wander into side issues that may be intellectually satisfying to discuss but have no bearing on the issue or question.
- **Standard 5 – Depth.** We think deeply when we get beneath the surface of an issue or problem. Depth of thinking is also present when we identify its inherent complexities, and then deal with those complexities not superficially but in an intellectually responsible way. Even when we think deeply to identify the complexities in a question, we may find the question difficult to address.
- **Standard 6 – Breadth.** When we consider the issue from every relevant viewpoint, we think in a broad way. Multiple points of view that are pertinent to the issue are given due consideration. You think broadly about an issue when you recognize other viewpoints and intellectually empathize with those contrary viewpoints so as to understand them.
- **Standard 7 – Logic.** When we think, we bring together thoughts in some order. When the combined thoughts are mutually supporting and make sense, the thinking is logical. If information, inferences, and so forth, are contradictory, if they do not make sense together, they are illogical.
- **Standard 8 – Significance.** When we reason, we want to concentrate on the most important information and take into account the most important ideas or concepts to answer the question. Too often, we fail in our thinking because we do not recognize that, though many ideas may be relevant to an issue, they are not equally important.
- **Standard 9 – Fairness.** When we think through problems, we want to make sure that our thinking is fair in the context. To think fairly is to think in accordance with reason and take into account the views of relevant others. Fairness as a standard helps us deal with our propensity for self-deception. Personal biases and ego creep easily into our thinking. When gauging the fairness of a decision, the critical thinker asks, “Do my selfish interests distort this thinking or is my decision fair to all concerned?” The fairness standard seeks to prevent egocentric thinking. As one’s ego enters the thought process, critical thinking becomes poisoned.

2-10. Critical thinkers evaluate their thinking with questions such as: “Am I being clear? Accurate? Precise? Relevant?” “Am I thinking logically?” “Am I dealing with information of significance?” “Is my thinking justifiable in context?”

2-11. Critical thinkers employ these standards to evaluate the quality of their own thinking as well as the thinking of others—anywhere thinking produces a judgment, opinion, or conclusion. Ordinary thinkers,

often those who believe they are good thinkers, usually assess their thinking in vague terms with no clear standards. The standards for thought enable us to use explicit definitive standards to assess thinking. The nine standards above are essential intellectual standards, but they are only some of the many intellectual standards existing in human thought and language.

### **Applying the Elements and Standards**

2-12. When an analyst exercises self-discipline and thoughtfully analyzes thinking (using the elements of thought) and then assesses the quality of the elements using intellectual standards, the result is a solid foundation for critical thinking. It is important to remember that critical thinking is a deliberate choice. Critical thinking requires self-discipline and a commitment to improve the skills that support this approach. While critical thinking cannot necessarily solve every problem an analyst may face (because some are so complex), it can ensure that every analyst is more effective and efficient while conducting the different intelligence tasks, especially those that are the most complicated or ambiguous. The example on page 2-6 addresses a hypothetical mission that involves effective use of critical thinking.

### **THE ESSENTIAL INTELLECTUAL TRAITS**

2-13. Repeatedly applying and practicing the elements of thought and intellectual standards develop intellectual traits. These traits are essential to excellence of thought. They influence with what insight and integrity we think. This section contains brief descriptions of the essential intellectual traits, along with related questions that foster their development. By routinely asking these questions of yourself, you develop these dispositions.

#### **Fair-Mindedness**

2-14. A fair-minded thinker strives to treat every relevant viewpoint in an unbiased, unprejudiced way. Fair-mindedness entails an awareness that we tend to prejudge the views of others, placing them into “favorable” (agrees with us) and “unfavorable” (disagrees with us) categories. We tend to give less weight to a contrary view than to our own. This is especially true when we have selfish reasons for opposing such views. Fair-minded thinkers try to see the strengths and weaknesses of any reasoning they assess. Fair-mindedness entails a conscious effort to treat all viewpoints alike in spite of one’s own feelings or selfish interests, or the feelings of one’s friends, company, community, or social organization.

#### **Intellectual Humility**

2-15. Intellectual humility is knowledge of ignorance, sensitivity to what you know and what you do not know. It means being aware of your biases, prejudices, self-deceptive tendencies and the limitations of your viewpoint. Questions that foster intellectual humility include—

- What do I really know (about myself, about the situation, about another person, about what is going on in the world)?
- To what extent do my prejudices or biases influence my thinking?

#### **Intellectual Courage**

2-16. Intellectual courage is the disposition to question beliefs you feel strongly about. It includes questioning the beliefs of your culture and the groups to which you belong, and a willingness to express your views even when they are unpopular. Questions that foster intellectual courage include—

- To what extent have I analyzed and questioned the beliefs I hold?
- To what extent have I demonstrated a willingness to give up my beliefs when sufficient evidence is presented against them?
- To what extent am I willing to stand up against the majority (even though people ridicule me)?

### Example

An Army unit is given a mission to support the local population in building a well in a village within the AO. The intelligence staff could apply the elements and standards as they work through the analytical process in order to provide information and situational understanding to the commander before undertaking the mission. The section below provides an example of how the critical thinking elements and standards might apply.

Analysts begin reviewing the mission: one of the first things they must do is to define the purpose. What is the purpose for building this well? Is it purely a humanitarian mission, or is there a desire to gain a military advantage by doing so? Let's say that the purpose of the well project builds positive relations with the local population. Once this purpose is established, the analyst would have to work on clearly and accurately defining what is meant by "positive relations." This example will show just a few of the complexities that are inherent in this project. Without the disciplined approach that a critical thinker uses, some of these complexities may be ignored, thus compromising the mission.

Once the purpose is defined, the analyst will probably have many questions that need answers. Some questions have a single correct answer: Is there a need for the well? Some are questions of opinion: What type of well will the villagers prefer? And some are questions of judgment: Will building this well likely achieve desired results?

Analysts can use questions to get the information needed to best proceed with this mission. They should gather information from multiple sources. The townspeople, higher headquarters, hydrologists, cultural awareness experts—all of these will have information to share. Part of the analyst's job will be to judge the relevance and significance of the information. An analyst could certainly find out the average age of citizens in the town, and cross-check records to verify the accuracy of this information, but would it be relevant to the mission? Is it significant enough to be meaningful in this project?

This mission will have to be considered from multiple points of view. This ensures that all thoughts about the well have breadth. Analysts should consider this project from the point of view of a villager who will want the well in a location that is convenient to use, but recognize that this might conflict with the point of view of the Soldiers building the well who want it built in the most convenient location in terms of logistics and security.

Analysts also have to consider the point of view of the local leaders in the selected village and neighboring village. What are the implications of working with one village over the other to future missions?

In addition to this level of critical thought, maybe in spite of it, analysts are operating from their own point of view, and as such they bring their own assumptions to the work being done on this well project. While there are literally hundreds of assumptions that are likely at play in this scenario, let's focus on one.

The unit analysts are working under the assumption that the entire town will be grateful to U.S. forces if the well is successfully built. This perhaps comes from the western concept of community-shared resources, but if the locals are operating from the concept that the local leader "owns" the well, then there could be problems with the project achieving the desired purpose.

Assumptions will lead directly to inferences or conclusions made about the project. The assumption just discussed might lead analysts to believe that U.S. forces will be able to move, effectively operate, and protect themselves within the town after completion of this project. That belief might cause the unit to go forward with the project when a further logical review of it might contradict the assumptions made. If analysts do not take time to check their thinking, these assumptions can hold too much weight in the analytical process and lead to undesired consequences.

### Intellectual Empathy

2-17. Intellectual empathy is awareness of the need to actively entertain views that differ from our own, especially those we strongly disagree with. It is to accurately reconstruct the viewpoints and reasoning of our opponents and to reason from premises, assumptions, and ideas other than our own. Questions that foster intellectual empathy include—

- To what extent do I accurately represent viewpoints I disagree with?
- Can I summarize the views of my opponents to their satisfaction? Can I see insights in the views of others and prejudices in my own?
- Do I sympathize with the feelings of others in light of their thinking differently than me?

### Intellectual Integrity

2-18. Intellectual integrity consists of holding yourself to the same intellectual standards you expect others to honor (no double standards). Questions that foster intellectual integrity include—

- Do I behave in accordance with what I say I believe, or do I tend to say one thing and do another?
- To what extent do I expect the same of myself as I expect of others?
- To what extent are there contradictions or inconsistencies in my life?
- To what extent do I strive to recognize and eliminate self-deception in my life?

### Intellectual Perseverance

2-19. Intellectual perseverance is the disposition to work your way through intellectual complexities despite the frustration inherent in the task. Questions that foster intellectual perseverance include—

- Am I willing to work my way through complexities in an issue or do I tend to give up when I experience difficulty?
- Can I think of a difficult intellectual problem with which I have demonstrated patience and determination in working through the difficulties?

### Confidence in Reason

2-20. Confidence in reason is based on the belief that one's own higher interests and those of humankind are best served by giving the freest play to reason. It means using standards of reasonability as the fundamental criteria by which to judge whether to accept or reject any belief or position. Questions that foster confidence in reason include—

- Am I willing to change my position when the evidence leads to a more reasonable position?
- Do I adhere to principles of sound reasoning when persuading others of my position or do I distort matters to support my position?
- Do I deem it more important to “win” an argument or see the issue from the most reasonable perspective?
- Do I encourage others to come to their own conclusions or do I try to force my views on them?

### Intellectual Autonomy

2-21. Intellectual autonomy is thinking for oneself while adhering to standards of rationality. It means thinking through issues using one's own thinking rather than uncritically accepting the viewpoints of others. Questions that foster intellectual autonomy include—

- To what extent am I a conformist?
- Do I think through issues on my own or do I merely accept the views of others?
- Having thought through an issue from a rational perspective, am I willing to stand alone despite the irrational criticisms of others?

## TYPES OF REASONING

2-22. Reasoning is the process of forming conclusions, judgments, facts, opinions, or inferences. Reasoning assists in forming arguments based upon evidence about observed activities. There are several reasoning types. For the purposes of this circular, discussion is limited to deductive and inductive reasoning.

### DEDUCTIVE REASONING

2-23. Deductive reasoning, sometimes called deductive logic, is reasoning where a conclusion is a logical consequence of the premise. Deductive reasoning, however, can lead to false conclusions if the premise is inaccurate. Deductive reasoning depends on everything being known about a problem set before a conclusion can be drawn. To some degree, deductive reasoning is used in all problem solving; some problems rely on little more than deductive reasoning. The challenge for intelligence analysts is to recognize what problem sets may be solved using deductive reasoning and apply the process effectively. For example, deductive reasoning is very useful in pattern and link analysis when there is an accurate volume of information to analyze.

#### Example

- Historical reporting and incident overlays show that the enemy is mining main supply route (MSR) Blue with improvised explosive devices (IEDs) in the same area every day.
- Time-event charts show the IED activity is occurring every day between the hours of 0100 to 0400.
- Current human intelligence (HUMINT) reporting states that the enemy believes its IED operations on MSR Blue are very effective and U.S. forces cannot stop the attacks.

**Conclusion: The enemy will continue to mine MSR Blue with IED every night from 0100 to 0400 hours.**

2-24. Based upon information provided in the above example, the analyst can deduce that the enemy will continue its improvised explosive device (IED) operations on MSR Blue. This conclusion is supported by the fact that the enemy has a history of conducting IED operations at a certain place and time. In addition, related reporting indicates the enemy is confident in its ability to successfully continue its IED attacks.

### INDUCTIVE REASONING

2-25. Inductive reasoning, sometimes called inductive logic, is the process of reasoning in which a person uses a number of specific established facts to draw a general conclusion. Inductive reasoning is generally conducted in four stages:

- Observation (collect facts without bias).
- Analysis (classify facts by establishing patterns of regularity).
- Inference (from the patterns, infer generalizations about the relationship between facts).
- Confirmation (test the inference through further observation).

2-26. Inductive reasoning is useful when there is limited information about a problem. Enemy situation templating when the exact disposition of the enemy is unknown is a good example of the use of inductive reasoning. Based on what is known about the enemy's threat characteristics, operational art, tactics, and previous operations, the analyst can extrapolate how the enemy will generally organize and maneuver on the battlefield.



**Example**

- Reporting indicates the enemy will attack the battalion's defensive position.
- The enemy normally attacks with no less than a 3 to 1 combat power ratio in its favor, will attempt to exploit seams between elements belonging to different units, and prefers to attack during daylight hours to minimize its opponent's superior night-vision capability.
- The battalion's right flank is the boundary with a battalion from another brigade combat team.

***Conclusion: The enemy will attack with a brigade-sized force during daylight hours. The enemy main effort will be our right flank.***

2-27. Based upon information provided in the above example, the analyst can infer the enemy's most likely COA from what is known about the enemy's past operations.

**THE SCIENTIFIC METHOD**

2-28. The scientific method refers to the various techniques used for investigating phenomena, acquiring new knowledge, or correcting and integrating previous knowledge. Generally, the scientific method follows a six-step process. However, even though the scientific method consists of a series of steps, new information or thinking may cause an analyst to back up and repeat steps at any point during the process.

**STEP 1 – DEFINE THE PROBLEM**

2-29. The most difficult step in the scientific method is defining the problem. In most instances the analyst will not be required to define the problem, which will be presented in the form of PIRs or other "intelligence gaps" identified by the commander or intelligence officer. Whatever the form, the problem must be stated in such a way that observation or experimentation can provide an answer. The problem must be stated in an objective way without preconceptions or bias.

**STEP 2 – GATHER DATA**

2-30. The analyst must gather all available data relating to the problem. For the intelligence analyst, this generally includes reviewing historical databases or data files as well as current intelligence reporting on the problem.

**STEP 3 – FORM A HYPOTHESIS**

2-31. Based on a review of gathered data, the analyst develops a hypothesis that provides a tentative explanation of the problem. It is making an educated guess at how to solve the problem which was defined in step 1. The hypothesis must be focused on providing a solution that would be a contribution to the overall intelligence picture. The hypothesis should lead to new problems thus demanding further research.

**STEP 4 – TEST THE HYPOTHESIS**

2-32. Testing the hypothesis is the action of confirming or rejecting the hypothesis through investigation. Intelligence analysts use various methods to investigate their hypothesis:

- Pattern analysis (time and event).
- Link analysis.
- Research.
- Case studies.

### STEP 5 – DRAW A CONCLUSION

2-33. Intelligence analysts formulate conclusions by reviewing available facts as well as considering relevant and reasonable assumptions when analyzing a hypothesis. When formulating a conclusion, the analyst must be unbiased. If the facts and assumption do not support the hypothesis, a new hypothesis must be formed and investigated.

### STEP 6 – COMMUNICATE RESULTS

2-34. Intelligence analysts report results of investigation in several ways. The most common are answering information requirements through clear and concise statements, formulating detailed assessments relating to effects within the AO, developing threat COAs, conducting intelligence briefings, and preparing intelligence summaries.

2-35. Each of these vehicles for communication is centered around the analyst's assessment of the situation based on available data. They are not just compilations of facts. When communicating, analysts must explain what they know and why they know it; what they think and why they think it; what they do not know and what they are doing about it. In doing this, the analysts provide an unbiased framework for the commander to conduct an independent analysis of the situation.

## ANALYSIS OF COMPETING HYPOTHESES

2-36. The ACH is a method which helps analysts make determinations on important issues requiring careful weighing of alternative explanations or conclusions. ACH helps an analyst overcome, or at least minimize, some of the cognitive limitations that make predictive intelligence analysis so difficult to achieve. ACH is a very time-consuming method, best used by a large staff of analysts at operational or strategic echelons. This does not mean that tactical units cannot use this method; however, significant time is required. ACH—

- Is an eight-step procedure grounded in basic insights from cognitive psychology, decision analysis, and the scientific method.
- Is a surprisingly effective, proven process that helps analysts avoid common analytic pitfalls.
- Because of its thoroughness, ACH is particularly appropriate for controversial issues when analysts want to leave an audit trail to show what they considered and how they arrived at their conclusion.
- Requires an analyst to identify all the reasonable alternatives and have them compete against each other for the analyst's favor, rather than evaluating their probability one at a time. (Appendix A provides examples of analytical pitfalls.)

2-37. Most analysts pick out what is suspected intuitively as the most likely answer. They then look at the available information from the point of view of whether or not it supports that answer. If the evidence seems to support the favorite hypothesis, analysts tend to look no further. If the evidence does not support the analyst's hypothesis, the analyst either rejects the evidence as misleading or develops another hypothesis and goes through the same procedure again. The main issue is that if analysts focus on trying to confirm one hypothesis thought as probably true, then the analyst can easily be led astray because there is so much evidence to support that point of view. An analyst can fail to recognize that most of this evidence is also consistent with other explanations or conclusions, and that these other alternatives have not been disproved.

2-38. Simultaneous evaluation of multiple, competing hypotheses is difficult. To retain three to five or even seven hypotheses in working memory and to note how each item of information fits into each hypothesis is beyond the mental capabilities of most people. It takes greater mental agility than listing evidence supporting a single hypothesis that was prejudged as the most likely answer. It can be accomplished, though, with the help of the procedures discussed here.

2-39. Psychological research into how people go about generating hypotheses shows that people are actually rather poor at thinking of all the possibilities. If analysts do not even generate the correct hypothesis for consideration, obviously they will not get the correct answer.

### STEP-BY-STEP OUTLINE OF ANALYSIS OF COMPETING HYPOTHESES

2-40. The following is an outline with step-by-step procedures for ACH:

- Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.
- Make a list of significant evidence and arguments for and against each hypothesis.
- Prepare a matrix with hypotheses across the top and evidence down the side. Identify which items are most helpful in judging the relative likelihood of the hypotheses.
- Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.
- Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.
- Analyze how sensitive a conclusion is to a few critical items of evidence. Consider the consequences for the analysis if that evidence was wrong, misleading, or subject to a different interpretation.
- Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.
- Identify milestones for future observation that may indicate events are taking a different course than expected.

#### Step 1 – Identify Possible Hypotheses

2-41. Identify all hypotheses that merit detailed examination. At this early hypothesis generation stage, it is useful to bring together a group of analysts with different backgrounds and perspectives.

2-42. Brainstorming in a group stimulates the imagination and may bring out possibilities that individual members of the group had not thought of. Initial discussion in the group should elicit every possibility, no matter how remote, before judging likelihood or feasibility. Only when all the possibilities are on the table should an analyst then focus on judging them and selecting the hypotheses to be examined in greater detail in further analysis.

2-43. When screening out the seemingly improbable hypotheses that the team of analysts does not want to waste time on, it is necessary to distinguish hypotheses that appear to be disproved from those that are simply unproven. For an unproven hypothesis, there is no evidence that it is correct. For a disproved hypothesis, there is positive evidence that it is wrong. Early rejection of unproven, but not disproved, hypotheses biases the further analysis, because one does not then look for the evidence that might support them. Unproven hypotheses should be kept alive until they can be disproved.

2-44. One example of a hypothesis that often falls into this unproven but not disproven category is the hypothesis that an enemy is trying to deceive the U.S. An analyst may reject the possibility of denial and deception because there is no evidence of it, but rejection is not justified under these circumstances. If deception is planned well and properly implemented, one should not expect to find evidence of it readily at hand. The possibility should not be rejected until it is disproved or, at least, until after a systematic search for evidence has been made and none has been found.

2-45. There is no “correct” number of hypotheses to be considered. The number depends upon the nature of the analytical problem and how advanced you are in the analysis of it. As a general rule, the greater the level of uncertainty, or the greater the policy impact of the conclusion, the more alternatives the analyst may wish to consider. More than seven hypotheses may be unmanageable; if there are this many alternatives, it may be advisable to group several of them for an initial cut at the analysis.

### Step 2 – Make a List

2-46. Make a list of significant evidence and arguments for and against each hypothesis. In assembling the list of evidence and arguments, these terms should be interpreted broadly. They refer to all the factors that have an impact on judgments about the hypotheses. Analysts should not limit themselves to concrete evidence in the current intelligence reporting. Also include assumptions or logical deductions about another person's, group's, or country's intentions, goals, or standard procedures. These assumptions may generate strong notions as to which hypothesis is most likely. Such assumptions often drive the final judgment, so it is important to include them in the list of "evidence."

2-47. First, list the general evidence that applies to all the hypotheses. Then consider each hypothesis individually, listing factors that tend to support or contradict each one. Analysts will commonly find that each hypothesis leads to asking different questions and, therefore, to seeking out somewhat different evidence.

2-48. For each hypothesis, ask these questions: If this hypothesis is true, what should be expected to be seen or not seen? What are all the things that must have happened, or may still be happening, and that one should expect to see evidence of? If the evidence is not there, why not? Is it because it has not happened, it is not normally observable, it is being concealed from collection assets, or because analysts or intelligence collectors have not looked for it?

2-49. Note the absence of evidence as well as its presence. For example, when weighing the possibility of military attack by an adversary, the steps the enemy has not taken to ready the enemy's forces for attack may be more significant than the observable steps that have been taken. This recalls the Sherlock Holmes story in which the vital clue was that the dog did not bark in the night. Most analysts tend to focus their attention on what is reported rather than what is not reported. It requires a conscious effort to think about what is missing, but should be present if a given hypothesis were true.

### Step 3 – Prepare a Matrix

2-50. Step 3 is perhaps the most important element of this analytical procedure. It is also the step that differs most from the natural, intuitive approach to analysis, and therefore the step analysts are most likely to overlook or misunderstand.

2-51. The procedure for step 3 is to take the hypotheses from step 1 and the evidence and arguments from step 2 and put this information into a matrix format, with the hypotheses across the top and evidence and arguments down the side. Identify which items are most helpful in judging the relative likelihood of alternative hypotheses. This gives an overview of all the significant components of the analytical problem.

2-52. Analyze how each piece of evidence relates to each hypothesis. This differs from the normal procedure, which is to look at one hypothesis at a time to consider how well the evidence supports that hypothesis. That will be done later in step 5. At this point in step 3, take one item of evidence at a time, then consider how consistent that evidence is with each of the hypotheses. Here is how to remember this distinction:

- In step 3, work across the rows of the matrix, examining one item of evidence at a time to see how consistent that item of evidence is with each of the hypotheses.
- In step 5, work down the columns of the matrix, examining one hypothesis at a time, to see how consistent that hypothesis is with all the evidence.
- Fill in the matrix by taking the first item of evidence and asking whether it is consistent with, inconsistent with, or irrelevant to each hypothesis.
- Then make a notation accordingly in the appropriate cell under each hypothesis in the matrix.

2-53. The form of these notations in the matrix is a matter of personal preference. It may be pluses, minuses, and question marks. It may be consistent (C), inconsistent (I), or not applicable (NA). Or it may be some textual notation. In any event, it will be a simplification, a shorthand representation of the

complex reasoning that went on as the analytical team thought about how the evidence relates to each hypothesis.

2-54. After filling in the matrix for the first item of evidence, go on to the next item of evidence and repeat the process until all cells in the matrix are filled. Figure 2-1 shows an example of how such a matrix might look. It uses as an example the intelligence question that arose after the U.S. bombing of Iraqi intelligence headquarters in 1993: Will Iraq retaliate? The evidence in the matrix and how it is evaluated are hypothetical, fabricated for the purpose of providing a plausible example of the procedure. The matrix does not reflect actual evidence or judgments available at that time to the U.S. intelligence community.

<b>Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?</b>			
<b>Hypotheses:</b>			
<b>H1 - Iraq will not retaliate.</b>			
<b>H2 - Iraq will sponsor some minor terrorist actions.</b>			
<b>H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.</b>			
	<b>H1</b>	<b>H2</b>	<b>H3</b>
<b>E1. Saddam public statement of intent not to retaliate.</b>	<b>+</b>	<b>+</b>	<b>+</b>
<b>E2. Absence of terrorist offensive during the 1991 Gulf War.</b>	<b>+</b>	<b>+</b>	<b>-</b>
<b>E3. Assumption that Iraq would not want to provoke another US attack.</b>	<b>+</b>	<b>+</b>	<b>-</b>
<b>E4. Increase in frequency or length of monitored Iraqi agent radio broadcasts.</b>	<b>-</b>	<b>+</b>	<b>+</b>
<b>E5. Iraqi embassies instructed to take increased security precautions.</b>	<b>-</b>	<b>+</b>	<b>+</b>
<b>E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.</b>	<b>--</b>	<b>+</b>	<b>+</b>

**Figure 2-1. Example of analysis of competing hypotheses matrix**

2-55. This example shows that H2 is the most likely COA, followed by H3 and finally H1. Intelligence analysis, however, is not that simple. Any particular piece of evidence may be a deception, an assumption may not prove true, or, especially in the case of extremist leaders, those leaders may do something completely unexpected. While the “science” of intelligence analysis indicates H2 is most likely, the “art” of analysis may lead the intelligence Soldier to believe H1 is most likely. This hypothesis is discussed further in step 5.

2-56. Evidence is diagnostic when it influences the judgment on the likelihood of the various hypotheses identified in step 1. If an item of evidence seems consistent with all the hypotheses, it may have no diagnostic value. A common experience is to discover that most of the evidence supporting what is believed the most likely hypothesis really is not very helpful, because that same evidence is also consistent with other hypotheses. When you do identify items that are highly diagnostic, these should drive your judgment. These are also the items for which accuracy must be rechecked and other interpretations considered.

2-57. In the hypothetical matrix dealing with Iraqi intentions, note that evidence designated “E1” is assessed as consistent with all of the hypotheses. In other words, it has no diagnostic value. This is because the team of analysts did not give any credence to Saddam’s public statement on this question. Saddam might say he will not retaliate but then do so, or state that he will retaliate and then not do it. On the other hand, E4 is diagnostic: increased frequency or length of Iraqi agent radio broadcasts is more likely to be observed if the Iraqis are planning retaliation than if they are not. The double minus for E6 indicates this is considered a very strong argument against H1. It is a primary assumption that drives the conclusion in favor of either H2 or H3. Several of the judgments reflected in this matrix will be questioned at a later stage in this analysis.

2-58. In some cases it may be useful to refine this procedure by using a numerical probability, rather than a general notation such as plus or minus, to describe how the evidence relates to each hypothesis. To do this, ask the following question for each cell in the matrix: If this hypothesis is true, what is the probability that evidence of this item would be seen? Make one or more additional notations in each cell of the matrix, such as—

- Adding a scale to show the importance of each item of evidence.
- Adding a scale to show the ease with which items of evidence could be concealed, manipulated, or faked, or the extent to which one party might have an incentive to do so. This may be appropriate when the possibility of denial and deception is a serious issue.

#### **Step 4 – Refine the Matrix**

2-59. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value. The exact wording of the hypotheses is obviously critical to the conclusions one can draw from the analysis. By this point, the analyst will have seen how the evidence breaks out under each hypothesis, and it will often be appropriate to reconsider and reword the hypotheses. Are there hypotheses that need to be added or finer distinctions that need to be made to consider all the significant alternatives? If there is little or no evidence that helps distinguish between two hypotheses, should they be combined into one?

2-60. Also reconsider the evidence. Is your thinking about which hypotheses are most likely and least likely influenced by factors that are not included in the listing of evidence? If so, put them in. Delete from the matrix items of evidence or assumptions that now seem unimportant or have no diagnostic value. Save these items in a separate list as a record of information that was considered.

#### **Step 5 – Draw Tentative Conclusions**

2-61. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove hypotheses rather than prove them. In step 3, the team worked across the matrix, focusing on a single item of evidence or argument and examining how it relates to each hypothesis. Now, work down the matrix, looking at each hypothesis as a whole. The matrix format gives an overview of all the evidence for and against all the hypotheses, so that analysts can examine all the hypotheses together and have them compete against each other for their favor.

2-62. In evaluating the relative likelihood of alternative hypotheses, start by looking for evidence or logical deductions that either enable the rejection of a hypothesis or at least determine that a hypothesis is unlikely.

2-63. No matter how much information is consistent with a given hypothesis, an analyst cannot prove that hypothesis is true because the same information may also be consistent with one or more other hypotheses. On the other hand, a single item of evidence that is inconsistent with a hypothesis may be sufficient grounds for rejecting that hypothesis. People have a natural tendency to concentrate on confirming hypotheses already believed to be true, and analysts commonly give more weight to information that supports a hypothesis than to information that weakens it. This is wrong; an analyst should do just the opposite. Step 5 again requires doing the opposite of what comes naturally.

2-64. In examining the matrix, look at the minuses, or whatever other notation used to indicate evidence that may be inconsistent with a hypothesis. The hypothesis with the fewest minuses is probably the most likely one. The hypothesis with the most minuses is probably the least likely one. The fact that a hypothesis is inconsistent with the evidence is certainly a sound basis for rejecting it. The pluses, indicating evidence that is consistent with a hypothesis, are far less significant. It does not follow that the hypothesis with the most pluses is the most likely one, because a long list of evidence that is consistent with almost any reasonable hypothesis can be easily made. What is difficult to find, and is most significant when found, is hard evidence that is clearly inconsistent with a reasonable hypothesis.

2-65. The initial ranking by number of minuses is only a rough ranking, as some evidence obviously is more important than other evidence, and degrees of inconsistency cannot be captured by a single notation such as a plus or minus. By reconsidering the exact nature of the relationship between the evidence and the hypotheses, an analyst can judge how much weight to give it. Analysts who follow this procedure often realize that their judgments are actually based upon few factors rather than on the large mass of information they thought was influencing their views.

2-66. The matrix should not dictate the conclusion. Rather, it should accurately reflect an analytical judgment of what is important and how these important factors relate to the probability of each hypothesis.

---

*Note.* The analyst, not the matrix, must make the decision.

---

2-67. The matrix serves only as an aid to thinking and analysis, to ensure consideration of all the possible interrelationships between evidence and hypotheses and identification of those few items that really swing judgment on the issue. Again, this is an example of the difference between the science and the art of intelligence analysis.

2-68. When the matrix shows that a given hypothesis is probable or unlikely, analysts may disagree. If so, it may be because the analysis omitted from the matrix one or more factors that have an important influence on the analytical problem. Go back and put those factors in, so that the analysis reflects the team's best judgment. New evidence may be present that only recently came to light. Include this evidence and continue to refine the matrix. If following this procedure has caused the consideration of things otherwise overlooked, or has caused the revision of an earlier estimate of the relative probabilities of the hypotheses, then the procedure has served a useful purpose. However, an analyst may not have answered the question. If time allows, go through the process again. When done, the matrix serves as a shorthand record of the analyst's thinking and as an audit trail showing how the conclusion was arrived at.

2-69. This procedure forces the analyst to spend more analytical time than most analysts otherwise would on what were thought to be the less likely hypotheses. This is desirable. The seemingly less likely hypotheses usually involve plowing new ground and, therefore, require more work. What an analyst started out thinking was the most likely hypothesis tends to be based upon a continuation of their own past thinking. A principal advantage of the ACH is that it forces analysts to give greater thought to all the alternatives.

### **Step 6 – Analyze Conclusion Sensitivity**

2-70. Analyze how sensitive the conclusion is to a few critical items of evidence. Consider the consequences of the analysis if that evidence were wrong, misleading, or subject to a different interpretation.

2-71. In step 3 the analyst identified the evidence and arguments that were most diagnostic, and in step 5 the analyst used these findings to make tentative judgments about the hypotheses. Now, go back and question the few basic assumptions or items of evidence that really drive the outcome of the analysis in one direction or the other. Are there questionable assumptions that underlie your understanding and interpretation? Are there alternative explanations or interpretations? Could the evidence be incomplete and, therefore, misleading?

2-72. If there is any concern at all about denial and deception, this is an appropriate place to consider that possibility. Look at the sources of key evidence. Are any of the sources known to the authorities in the foreign country? Could the information have been manipulated? The analysts must put themselves in the shoes of a foreign deception planner to evaluate motive, opportunity, means, costs, and benefits of deception as they might appear to the foreign country.

2-73. When analysis turns out to be wrong, it is often because of key assumptions that went unchallenged and proved invalid. It is a truism that analysts should identify and question assumptions, but this is easier said than done. The problem is to determine which assumptions merit questioning. One advantage of the ACH procedure is that it tells the analyst what needs to be rechecked.

2-74. In step 6 the team may decide that additional research is needed to check key judgments. For example, it may be appropriate to go back to check original source materials rather than relying on someone else's interpretation. In writing a report, it is desirable to identify critical assumptions that went into the interpretation of information and to note that the conclusion is dependent upon the validity of these assumptions.

### Step 7 – Report Conclusions

2-75. Discuss the relative likelihood of all the hypotheses, not just the most likely one. It will be helpful for the commander to know the relative likelihood of all the alternative possibilities. Analytical judgments are never certain. There is always a good possibility of their being wrong. Commanders need to make decisions on the basis of a full set of alternative possibilities, not just the single most likely alternative. Contingency or fallback plans may be needed in case one of the less likely alternatives turns out to be true.

2-76. When analysts recognize the importance of proceeding by eliminating rather than confirming hypotheses, it becomes apparent that any written argument for a certain judgment is incomplete unless it also discusses alternative judgments that were considered and why they were rejected. In the past, at least, this was seldom done.

2-77. The narrative essay at strategic level—or the intelligence running estimate at operational and tactical levels, which is the dominant form for the presentation of intelligence judgments—does not lend itself to comparative evaluation of competing hypotheses. Consideration of alternatives adds to the length of reports and is perceived by many analysts as detracting from the persuasiveness of argument for the judgment chosen. Analysts may fear that the reader could fasten on one of the rejected alternatives as a good idea. Discussion of alternative hypotheses is nonetheless an important part of any intelligence appraisal, and ways can and should be found to include it.

### Step 8 – Identify Milestones

2-78. Identify milestones for future observation that may indicate events are taking a different course than expected. Analytical conclusions should always be regarded as tentative. The situation may change, or it may remain unchanged while new information is received that alters the appraisal. It is always helpful to specify in advance things one should look for or be alert to that, if observed, would suggest a significant change in the probabilities. This is useful for intelligence consumers who are following the situation on a continuing basis. Specifying in advance what would cause analysts to change their minds will also make it more difficult to rationalize such developments, if they occur, as not really requiring any modification of the final judgment.

### TESTS OF COMPETING HYPOTHESES

2-79. A final step in any analytical effort is to test the truth of premises. Both deductive and inductive reasoning involve three basic tests of truth. These tests include—

- Correspondence test of truth.
- Coherence test of truth.
- Pragmatic test of truth.



## Correspondence Test of Truth

2-80. While studying a response to the commander's PIR, an analyst notices that all presented information is the result of firsthand observation. Knowing the source to be reliable, the analyst assumes that every statement in the response corresponds to reality. The correspondence test of truth is the theory in which the truth is a statement that corresponds to reality.

### Example

- Pilots returning from a close air support mission reported destruction of three enemy tanks. The debriefing officer debriefed each pilot separately, and all pilots gave essentially the same report.
- Despite the fact that all pilots of one flight reported destruction of three tanks, the brigade commander wanted more supporting evidence. To gain supporting evidence, the brigade S-2 requested a post-strike unmanned aircraft system (UAS) imagery mission through the division ISR manager. The ISR manager granted the request and ordered the mission. Both the brigade S-2 and the commander placed more credibility in the photographic evidence because they believe that it is more objective, and less prone to human error. As such, the S-2 felt that it would eliminate the chance of human error.
- The S-2, believing that video and photography eliminated any possibility of subjectivity, failed to consider that photographs require interpretation and this interpretation involves a degree of subjectivity.
- Post-strike results: The UAS mission revealed three badly damaged tanks in hull-defilade positions. The intelligence analyst considered the imagery reports, along with the pilot debriefs. Based upon this information, the analyst reported three tanks confirmed damaged, but cannot confirm they were destroyed.

2-81. In the example above, the statements or other evidence corresponded to reality. To test the degree of correspondence, observations are required. The chief criterion in observations is objectivity. Using a mix of ISR assets can attain greater objectivity during collection operations.

2-82. Analysts naturally place more confidence in data collected from multiple sources than data collected from a single source. In the case of the unmanned aircraft system (UAS) mission report, versus the pilots' reports, the analyst had more confidence in the UAS's ability to observe the target from multiple angles. The UAS-derived information had more credibility than the pilots' report because the pilots may only have a fleeting glimpse of the target while attempting to egress. When a variety of collectors corroborate with each other, confidence in the conclusions increases. If there are conflicts between reports from multiple sources, analysts tend to rely on the least subjective source.

2-83. The correspondence test of truth requires observations to test whether or not, and to what extent, statements correspond to reality. One problem with this theory is that the enemy seldom permits direct observations, and often goes to great lengths to prevent direct observations or to deceive those observing.

## Coherence Test of Truth

2-84. This test of truth uses consistency with ideas or facts to validate statements. Where direct access to the threat is denied, the coherence test of truth becomes necessary. The coherence theory refers to how consistent different pieces of information are in relation to each other. An analyst considering a new piece of information that corroborates known information would place more credibility in the new information and the conclusions drawn from it.

**Example**

In the latter part of September, theater level staff intelligence officers considered the following information:

- The Southern League (Parma, Corinth, Lythia, and Samar) normally concludes their training cycles with a large-scale, combined exercise (historical record).
- Visitors to Parma reported being denied access to certain areas in the vicinity of Ides, in the western Daematia Province (confirmed report).
- Reports indicate certain infantry, armor, and engineer units from all four League member nations have moved from their garrison locations (unconfirmed report).
- All commercial air traffic to Thesulis will be restricted for a period of two weeks, starting 1 October (confirmed report).

The intelligence staff concluded that this year's League exercise will take place in, or near Thesulis, bordering Parma's Daematia province, during the period 1 to 14 October. Although no one piece of information pointed directly to this conclusion, all pieces of information seemed consistent with each other as well as with the conclusion.

2-85. In the realm of theory, intelligence usually works with some factual basis for most inferences or conclusions. The coherence test of truth supplements the correspondence test of truth.

**Pragmatic Test of Truth**

2-86. The pragmatic test of truth proposes that a statement is true if it works in practice. Although a practical tool, the pragmatic test of truth has some weaknesses. First, the results may only appear to justify the means used to achieve them. Second, a successful outcome may be attributed to other factors that could have produced the same outcome in a different situation.

**Example**

Before the Battle of Cape Esperance in World War II, U.S. Navy Admiral Norman Scott organized a task force into a long, single column. He believed this line-ahead formation would be effective against the Japanese units' night tactics. In the ensuing battle, Admiral Scott sank two Japanese destroyers and severely damaged two cruisers. After the battle, Admiral Scott concluded that the line-ahead formation theory was indeed effective. By combining radar-controlled fire control systems with the line-ahead formation, Admiral Scott believed he could master any night battle situation.

2-87. In the above example, the use of radar-controlled fire control systems may have produced the same result no matter what formation was used. Lastly, an unsuccessful outcome does not necessarily imply that the means used were unsound; again, other unknown factors may have contributed to the unsuccessful outcome.

**SITUATIONAL LOGIC**

2-88. The most common method of intelligence analysis is "situational logic," sometimes called the "area studies" approach. This involves generating different hypotheses on the basis of considering concrete elements of the current situation. Broad, global generalizations are avoided. Even though most analysts know this to be untrue, every situation is treated as one-of-a-kind, to be understood in terms of its own unique logic. A single country is looked at, although on multiple interrelated issues.

2-89. Next, the analyst seeks to identify the logical antecedents and consequences of the situation. This is called “building a scenario,” and the analyst may work backwards to explain the origins of the current situation or forward to estimate the future outcome. Situational logic is cause-and-effect logic, based on the assumption of rational, purposive behavior. The analyst identifies the goals being pursued by the enemy and explains why the enemy believes certain means will achieve certain goals. One of the major risks with this approach is projecting personal values onto an enemy.

## APPLYING THEORY

2-90. Another methodology of intelligence analysis is “applying theory,” sometimes called the “social science” approach. Theory is not a term used much in the intelligence community, but “applying theory” involves drawing conclusions from generalizations based on the study of many examples of something. Theory enables the analyst to see beyond transient developments, to recognize which trends are superficial and which are significant. For example, suppose an event occurs in Turkey. The analysts apply what they know about developing countries in precarious strategic positions to predict how Turkey will react militarily and politically. Multiple countries are looked at in terms of a single overriding issue.

2-91. Sometimes situational logic and applying theory contradict one another. Consider Saudi Arabia, for example. A theoretical approach would apply the axiom that economic development and massive infusion of foreign ideas lead to political instability. It would suggest that the days of the Saudi monarchy are numbered, although analysts using a situational logic approach would conclude that no such threat exists to the Saudi royal family.

## COMPARISON

2-92. Comparison is the analytical methodology where the analyst seeks to understand current events by comparing them with historical precedents in the same country or with similar events in other countries. It differs from theory in that conclusions are drawn from a small number of cases, whereas theory is generated from examining a large number of cases. This approach is quite useful when faced with an ambiguous and novel situation because it looks at how the country handled similar situations in the past or how similar countries handled similar situations. Historical precedent is influential, but one must be careful in arguing from analogies with the past.

## MODELING

2-93. Mathematical modeling is considered to be a process by which analysts weigh and combine information on relevant variables. Studies have shown that statistical models, built on regression analysis, are superior to conceptual models built on analysts trying to describe in words what they do. However, once an analyst has constructed a mathematical model, the accuracy of the analytical judgment is determined mostly by the accuracy and completeness of the data. Mathematical modeling is also known as “data-driven” analysis, and it is entirely appropriate for some uses, but not for others. An example of appropriate use is in MI, for example, estimating combat readiness. In this case, the rules and procedures for estimating combat readiness are relatively well established, so a mathematical model would help arrive at accurate judgments depending upon how accurate the source of the data is.

2-94. Conceptual modeling is considered “conceptually driven” analysis and therefore does not rely upon any agreed-upon schema. Analysts are left to their own devices. Other analysts examining the same data may reach different conclusions. The daily routine of an analyst is driven by incoming spot reports, higher headquarters and adjacent unit intelligence summaries and running estimates, HUMINT-derived reporting and open-source information. Interpretation will be ongoing and based on an implicit model in the analyst’s head about how and why events normally transpire in the country for which the analyst is responsible. Accuracy of judgment depends almost exclusively on accuracy of the mental model, not the data.

2-95. Mental models are neither good nor bad but are unavoidable. When information is lacking, analysts often have no choice but to lean heavily on mental models. They must remain open to new ideas, while ensuring they avoid mental blocks and ruts. To accomplish this, creativity exercises are sometimes useful. Sometimes agencies implement peer review, where at least one of the reviewers is not from the branch that produced the report or is required to play the “devil’s advocate.” Mirror-imaging, or thinking “if I were a Russian intelligence officer,” is also useful but dangerous. Another creativity technique is the “crystal ball” where you imagine some “perfect” intelligence source (such as a crystal ball) has told you a certain assumption is wrong. If analysts can develop a plausible alternative scenario, it suggests the original estimation is open to some question. Gaming simulation also serves the purpose of creativity.

2-96. Analysts should keep a record of unexpected events and think about what they might mean; they should not disregard them or explain them away. They should pay attention to any unexpected developments that might signal an impending event. Any such tactical indicators that are inconsistent with strategic assumptions should trigger an alert to higher level intelligence organizations.

## **PROCESSES FOR INTELLIGENCE ANALYSIS**

2-97. The earlier part of this chapter discussed various methods an analyst can use to conduct intelligence analysis. Now the discussion will shift to specific processes that enable an analyst to organize information and produce intelligence and therefore knowledge that the commander can use to make decisions on the battlefield.

### **PREDICTIVE ANALYSIS**

2-98. Predictive analysis is a process allowing the intelligence analyst to predict future events based upon previous enemy activities and events. Predictive analysis is not guessing; its basis is the use of common sense and solid analysis using the methods discussed in chapter 1, and the appropriate analytical tools and methodologies for the situation. It is a key component in the IPB process, situation development, and indications and warnings. Predictive analysis often focuses on determining a threat’s capabilities, intent, vulnerabilities, and most probable COA. It requires the analysts to stretch their intellects to the limit and understand that the predicted event, or COA, can hinge on many variables. For specific information concerning predictive analysis, see chapter 5.

### **FUNCTIONAL ANALYSIS**

2-99. Functional analysis is based on the concept that while every battle or action is unique, certain functions must be performed to bring about mission accomplishment. Functional analysis provides a framework for understanding how a specific threat will make use of its capabilities—whatever they may be—to accomplish its goals. Functional analysis is a method for determining likely threat COAs.

2-100. Analysis involves the separation of useful information from misleading information, using experience and reasoning, and reaching a conclusion based upon fact and sound judgment. Functional analysis is a framework in which the analyst chooses which enemy capabilities best or most likely accomplish a certain function. This practice allows the commander to plan for full spectrum operations. Functional analysis is not a step in the IPB process; it is an updated thought process for analysts to use. For more information on functional analysis, see chapter 4.

### **LINK ANALYSIS**

2-101. Link analysis is the process of identifying and analyzing relationships between personnel, contacts, associations, events, activities, organizations, and networks to determine significant links. Analysts use link analysis to determine who is involved, how they are involved, and their significance concerning a particular situation. Some types of link analysis tools include—

- Association matrices.
- Activities matrices.

- Link diagrams.
- Network diagrams.

2-102. For more information on link analysis, see chapter 5.

### NODAL COMPONENT ANALYSIS

2-103. A node is a point at which subsidiary parts originate or center. Nodal component analysis is the analysis of how the nodes of a designated system function in relation to one another. Similar to functional analysis, nodal component analysis assists in identifying critical nodes of the system. A critical node is an element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct operations.

2-104. Analysts working with nodes will spend a great deal of time working with various pieces of information to assist them in understanding relationships. Relationships can exist between people, organizations, entities, locations, or any combination of the above. How the various groups interact is as important as knowing who knows (or should know) who. Relationships are also present within a network itself. A network is a complex, interconnected group or system which, in some manner, concerns itself with a specific operation or mission such as mortar fire or IEDs.

### PATTERN ANALYSIS

2-105. Pattern analysis is the process of deducing the doctrinal principles and TTP that enemy forces prefer to employ by carefully observing and evaluating patterns in their activities. When using this technique, the premise that enemy activities reflect certain identified and interpreted characteristic patterns is its primary basis. Pattern analysis can be critically important when facing an enemy whose doctrine is undeveloped or unknown and it is necessary to create a new threat model and threat templates. Combating insurgency operations is a prime example of this type of analysis. For further information on pattern analysis, see chapter 5.

### ANALYTICAL TERMS

2-106. In order to fully understand intelligence analysis and analytical methodologies used to develop intelligence products, it is essential to understand the following terms that support analytical production:

- *Correlation* is the process of gathering like or associated information and data. This includes the use of automated systems to receive data, display data, and parse information into databases. Under most circumstances computer networks or systems are used to conduct correlation. For example, reports from a collection system about the 28th Mechanized Infantry Division will be collected and put into a database on the 28th Mechanized Infantry Division.
- *Collation* is the process of gathering or arranging information in proper sequence and comparing critically in order to verify and integrate. Computers receive data and collate like items in order to compare points of agreement or disagreement. Computers can often do a large amount of work in order to assemble data into a logical arrangement, but it takes an analyst to look at the information and draw conclusions about the data. It also requires an analyst to provide meaning to the data, turning it into information and knowledge. Collation is a function conducted by both humans and computers.
- *Fusion* is the process of taking information from similar or different sources or intelligence disciplines and creating knowledge. Fusion requires a human to conduct analysis and the correlation and collation efforts of automated systems to do fusion quickly and effectively. For example, an analyst may receive reports from a HUMINT source, a UAS, and a SIGINT system about a particular enemy unit. Taking all three reports, the analyst uses fusion to identify the unit type and location on the battlefield.

2-107. Analysis is always done by a human. Analysis requires using thought processes by which collected information is evaluated and integrated with existing information that requires taking multiple pieces of information, thinking through their related connections, and determining a particular conclusion. Computers can assist in analysis, but do not conduct analysis. All-source intelligence analysts conduct analysis to create intelligence products, briefings, and reports.

## Chapter 3

# Analytical Support to Situational Understanding

Support to situational understanding is the task of providing information and intelligence to commanders to assist them in achieving a clear understanding of the force's current state with relation to the enemy and the environment. It supports the commander's ability to make sound decisions. Intelligence analysts provide the commander the most current information on the enemy, terrain and weather, and civil considerations. All information, assessments, and products the intelligence analyst develops are used by commanders and staffs throughout the organization. This includes enemy force organization, disposition, and intent; current weather and weather effects; military aspects of the terrain and its effects on operations; and civil considerations. The enemy situation overlay, event template, and running estimate displayed as part of the common operational picture (COP) provide focus for fires and maneuver as well as ISR operations. Additionally, detailed geospatial and other topographic products are used to enhance the unit's ability to maneuver decisively.

### THREAT ANALYSIS

3-1. Threat analysis is the most important part of intelligence analysis at all levels. Intelligence analysts consider threat characteristics and integrate them with other intelligence pertaining to the mission variables of mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC) to determine threat capabilities, vulnerabilities, and probable COAs. Table 3-1 (page 3-2) shows examples of threat characteristics for full spectrum operations.

3-2. Data development occurs in many fields outside the scope of threat characteristics, but ultimately all intelligence relates to it. For example, technical intelligence produces intelligence on the capabilities of weapons systems, but threat characteristic intelligence determines the effect of weapons capabilities and characteristics on threat tactics, combat effectiveness, and organization.

3-3. Threat characteristics consist of evaluated information on the threat. This information is broken down into basic categories. The threat characteristics are a common analytical framework for recording, sorting, and interpreting information to describe a threat. In some cases analysts will not use all threat characteristics, and in other situations analysts may discover a need to modify existing categories or create additional ones.

### COMPOSITION

3-4. Composition is the identification of threat cells or forces and their affiliated political, religious, or ethnic organizations. In conventional military units, the analyst looks at what equipment and personnel make up the unit. It applies to specific units, organizations, or commands as well as types of units or organizations. Unit or organization identification is a key intelligence requirement because it answers several questions concerning the enemy. Composition provides answers to "Who" questions like, "Who is out there?" "Who are friendly forces fighting?" and "Who is supporting the threat?" Unit or organization identification consists of the complete designation of a specific unit or organization by name or number, type, relative size or strength, and subordination.

Table 3-1. Threat characteristics

<b>Threat Characteristic</b>	<b>Examples</b>		
<b>Composition</b>	Regular Army Unit history	Militia Uniforms	Unit designation Type of unit
<b>Disposition</b>	Historic	Current	Proposed future
<b>Tactics</b>	Method of operations Conventional Terrorism	Intent Unconventional	Propaganda Asymmetric
<b>Training</b>	Individual Source of training Specialized training	Team Uniforms	Unit Insignia
<b>Sustainment</b>	Food Spare parts Maintenance status	Transportation Water	Fuel Ammunition
<b>Finance</b>	State-sponsored Taxes	Support from allies Donation	Criminal activity
<b>Operational Effectiveness</b>	Strength Morale Equipment	Goals Weapons Chain of command	Personnel Leadership Loyalty
<b>Communications</b>	Written Verbal and live drop Electronic	Internet Emitter type	Signal Frequency range
<b>Intelligence</b>	Surveillance Reconnaissance	Countersurveillance Electronic warfare (EW) capability	Deception
<b>Recruitment</b>	Local International Motivation	National Coercion	Regional Volunteers
<b>Support</b>	Financial National International	Media Regional Popular	Local Religious Tribal or ethnic
<b>Intelligence Reach</b>	Databases Architecture	Assets Access	Connectivity Informal networks
<b>National Agencies</b>	Loyalties Capabilities	Agenda Relationships	Leadership
<b>Law Enforcement Agencies</b>	Loyalties Capabilities	Agenda Relationships	Leadership
<b>International Organizations and NGOs</b>	Loyalties Capabilities	Agenda Relationships	Leadership Areas of operations
<b>Personality</b>	Key leaders	Education level	Idiosyncrasies
<b>Other Threats</b>	Natural diseases Chemical hazards Criminal activity	Biohazards Wildlife	Radiological Toxic industrial material



3-5. Once analysts identify a unit or organization, they can develop a history of its composition, training, tactics, and combat effectiveness. The identification of a specific unit or organization within an organization alerts the analyst to the possible presence of other unidentified or unlocated units or organizations of the same parent organization; this can lead to the identification of other previously unidentified units or organizations.

3-6. Analysts can modify the considerations for the composition factor to describe various types of unconventional threat forces. Often the focus starts with individuals or cells, such as the “Ba’quibah IED cell,” the “Mahdi Militia Company,” or the “Balad indirect fire cell.” The cellular structure of some organizations like terrorist or insurgent groups should also be considered under the category of composition. Most terror cells will have a sustainment cell, surveillance cell, operational cell, and a leadership cell. Each of these cells is a part of the composition of the terrorist organization. Composition includes—

- Operational and support cells (similar to sections in a military unit).
- Echelons.
- Staff elements.
- Internal and external command and control.
- Operational organizations.
- Unit history and insignia.
- Individual uniforms.

3-7. Composition includes factors such as how many tanks are in a platoon, company, and battalion. It is essential to know a threat force composition to calculate how much of a force a friendly unit may have to face in battle. Knowing composition helps an analyst learn if friendly forces are facing an elite unit (Republican Guards or Revolutionary Guards), religious militia force, paratroopers, commandos, or conscripts. Understanding composition can also indicate how hard a threat force will fight or how quickly it may capitulate. Analysts and collectors must look for distinctive unit insignia such as airborne wings, particular uniforms not worn by the rest of the force, or unit patches which will indicate the composition of the threat force.

## DISPOSITION

3-8. Disposition consists of the geographic location of threat forces. It includes the recent, current, and projected or probable movements of threat units or organizations. Disposition provides answers to “Where” questions, such as “Where is the threat?” “Where will the threat attack?” “Where will the threat mass forces?” “Where will friendly forces engage the threat?”

3-9. Location refers to a geographic area or position occupied by a unit or organization. Knowledge of the strength and location of a threat force assists the analyst in determining the capabilities of the force and its effects on the friendly mission. For example, an analyst assessing disposition during the initial phase of an enemy offensive operation may consider such data as—

- Enemy line of departure.
- Left and right boundaries.
- Immediate and subsequent objectives.
- Attack routes.
- Avenues of approach (AAs) (including air AAs).
- Enemy ISR units.
- Artillery firing positions (initial and subsequent).
- Artillery range fans.
- Point of penetration.
- Special munitions.

- Main effort and shaping efforts (maneuver units).
  - Enemy decision points.
  - Enemy attack timeline.
- 3-10. During enemy defensive operations, consider the following when building an intelligence product:
- Position of known enemy defensive positions.
  - Position of known enemy obstacles.
  - Template the remaining unlocated units (based on known enemy composition).
  - Template the remaining enemy obstacles.
  - Plot known or templated enemy artillery locations and their range fans.
  - Draw direct fire system range fans.
  - Template the targets of special munitions, such as chemical agents.
  - Locate unit boundaries.
  - Consider locations of enemy decision points and the associated decision.

## TACTICS

3-11. Tactics include strategy, methods of operation, and doctrine. Each refers to the threat's accepted principles of operation. Tactics also involve political, military, psychological, and economic considerations. The use of IEDs is a method the threat chooses to carry out their tactics. Tactics, on the other hand, describe the manner in which units or organizations conduct an operation. From knowledge of tactical doctrine, the analyst knows how the threat may employ forces under various conditions and in certain types of situations or special operations. Analysts usually expect conventional threat units or organizations to perform according to certain patterns within the framework of their tactical doctrine.

3-12. All conventional armies establish basic principles and patterns for the employment of their types of units or organizations (infantry, armor, artillery, sustainment) in both offense and defense. Of a more specific nature, intelligence personnel analyze the specialized tactical doctrine a certain unit or organization, or even a certain commander, employs in given situations during combat or training activities because it indicates possible changes in the overall threat doctrine. Threat templating, as detailed in FMI 2-01.301, is one method of graphically portraying enemy tactics.

3-13. Insurgent tactics are techniques and procedures which support strategy. Tactics involve political, military, psychological, and economic considerations. Insurgent tactics vary in sophistication according to the level of training the individual or organization has received. Insurgents carefully plan and train for individual and small-group operations. Typical insurgent tactics include, but are not limited to—

- Assassination.
- Arson.
- Bombing.
- Hostage taking.
- Kidnapping.
- Intimidation or blackmail.
- Seizure.
- Raids or attacks on facilities.
- Sabotage.
- Hoaxes.
- Use of technology.
- Use of CBRNE weapons.
- Psychological operations (PSYOP).

3-14. Nonmilitary hazards such as chemicals, radiological material, biological waste, disease, and toxic industrial materials must not be dismissed. The threat may sabotage an industrial complex thereby releasing deadly chemicals in an attempt to inflict mass casualties and blame the deaths on the HN government or friendly forces. The capability of the threat to use naturally occurring diseases or a natural disaster such as a flood to their advantage must be considered.

3-15. Short-range or medium-range ballistic missiles must be considered, as well as the possibility of the threat's firing them at a neutral or neighboring country in order to cause political instability within any coalition that is facing the threat country. Mines and minefields left over from previous conflicts must be considered when analysts conduct the IPB process. How flooding changes the landscape near suspected or known minefields is another consideration when analyzing the operational environment.

## TRAINING

3-16. Individual and unit or organization training contribute significantly to the combat effectiveness of any military organization or insurgent group. The thoroughness, degree, and quality of individual training that the recruit, specialist, noncommissioned officer, and officer receive are major factors in determining the overall efficiency of an armed force. Unit or organization training, normally conducted in seasonal cycles from small-unit or organization exercises to large-scale maneuvers, is an essential part of the training necessary for a unit or organization to operate at its full potential.

3-17. Each type or phase of training a unit or organization accomplishes increases its capabilities and effectiveness. Specialized training that a unit or organization receives (air assault, river-crossing) may point to its ability to undertake certain missions beyond its normal doctrinal capabilities or responsibilities. Therefore, it is easier to appraise the combat effectiveness of a unit or organization when the degree and quality of its training are known, as well as any specialized training it undertakes. Whether a unit is composed mostly of seasoned veterans or recent conscripts will also indicate its level of training and therefore its operational effectiveness.

3-18. The type and depth of individual and collective (unit) training that insurgents receive is tied to their tactics and operations. Higher education also plays a role in insurgent training, as many insurgents have a college education in technical areas such as engineering. Insurgent training may include, but is not limited to—

- Indoctrination and strategy (political, ideological, or religious).
- Operations.
- Tactics.
- Weapons (individual and crew served), including such specialties as demolitions, weapons, snipers, and assassinations.
- Communications.
- Sustainment.
- Transportation (covert movement).
- ISR.
- PSYOP.
- Media manipulation.

3-19. Insurgents may be very well trained and experienced fighters, which could range from previous commando units or youths with minimal weapons training. Analysts must not underestimate a poorly trained force. It is essential that analysts study the threat's level of training so that friendly forces can determine important aspects of the threat force. Even a poorly trained threat force can cause significant casualties to friendly forces when operating in operational environments favorable to the enemy.

## SUSTAINMENT

3-20. Sustainment is the procurement, maintenance, distribution, and replacement of all types of material including transport of personnel. The ability of a fighting force to operate effectively is a direct reflection of the ability to support the force. The adoption of a COA depends on the logistic system supporting the action. Knowledge of the current capabilities of a unit's or organization's sustainment support structure enables analysts to more accurately evaluate its capabilities, strengths, and combat effectiveness. In addition, the locations of elements of a unit's or organization's logistic support structure indicate the disposition of maneuver formations and sustainment elements.

3-21. Modern fighting forces have enormous supply needs. As the scale and complexity of military operations increase, the importance of sustainment to their success increases. Generally, the more complex and equipment heavy a military force is the more sustainment support it needs. A light infantry unit or organization may require only food for its Soldiers and ammunition for their individual weapons. An armor unit or organization, however, requires the same food and ammunition for its Soldiers, plus specific ammunition for the main gun and machine guns; maintenance support; repair parts; and fuel for its tanks and other vehicles.

3-22. Categories of sustainment information include—

- All classes and types of supply (food, water, ammunition, spare parts, fuel).
- Supply lines of communication (LOCs).
- Procurement methods.
- Distribution priorities and procedures.
- Transportation networks and modes.
- Installations and sustainment control points.
- Ports and terminals.
- Evacuation and salvage procedures.
- Maintenance and transportation.
- Method of delivery of goods and services (rail, ship, river boats, truck, or mule).

3-23. The effectiveness of insurgent operations depends heavily on sustainment. This dependency fluctuates horizontally and vertically between the various groups and levels of operation. The intensity of logistic activity is based upon operations. Critical components of sustainment include, but are not limited to—

- Food.
- Water.
- Weapons and ammunition.
- Bomb-making components.
- PSYOP materials (paper, ink, printing press).
- Medical supplies.
- Transportation (on-hand and required).
- Financial support.
- Sanctuary locations.

## OPERATIONAL EFFECTIVENESS

3-24. Operational effectiveness describes the overall ability and fighting quality of a unit, organization, or insurgent group. Numerous tangible and intangible factors impact operational effectiveness. Combat effectiveness is a subjective judgment, which usually comes after actual combat encounters with the threat by friendly forces. Analysts predict how combat effectiveness affects the capabilities of a unit, organization, or army by analyzing—

- Personnel strength, including estimated losses.
- Amount and condition of weapons and equipment.
- Status of training.
- Efficiency of the officer and noncommissioned officer corps.
- Quality of leadership.
- Combat experience of individuals (or lack thereof).
- Length of time a unit or organization has been committed in combat.
- Traditions and past performance.
- Personality traits of the unit or organization commanders.
- Geographic area in which committed.
- Morale, esprit de corps, health, discipline, and political reliability (or belief in the cause for which they fight).
- Status of technical and logistic support of the unit or organization.
- Adequacy of military schooling at all levels.
- National characteristics of the people.

3-25. Combat effective strength is the adjusted strength after deducting combat losses of personnel, weapons, and equipment. Combat effective strength is the most important strength figure when conducting combat assessment. Combat effective strength is expressed in a percentage of baseline strength. Compute the combat effective strength by dividing the number remaining after deducting losses by the starting strength.

### Example

The commander needs a calculation of the combat effective strength for the personnel of a specific threat infantry company. For purposes of this example, assume that the baseline strength of the company is 126 personnel. However, analysts receive information, which confirms that 5 of the personnel from that company deserted before combat. The effective strength is 121 ( $126 - 5 = 121$ ) personnel or 96% ( $121/126 = .96 = 96\%$ ). During combat operations, analysts receive additional information that the same company lost 10 more personnel to injury or death. The combat effective strength is now 88% ( $121 - 10 = 111$ ;  $111/126 = 88\%$ ).

## COMMUNICATIONS

3-26. During operations, threat forces may use a variety of communication methods. Plans, orders, or information may be passed using radios, land line telephones, cellular phones, Internet, mail, couriers, face-to-face meetings, or the drop system. Communications equipment available to insurgents range from the most primitive to the most modern. Insurgent forces can use the methods available to more conventional threat army units or the others listed above. Insurgents may use specific radio frequencies for remote detonation of improvised weapons and explosives. Communications come in the forms of—

- Written.
- Verbal.

- Personal.
- Internet.
- Electronic. Special attention should be paid to—
  - Emitter type.
  - Frequency range.
  - Location (direction finding).

3-27. Generally, there are three general types of communication:

- **Common.** The primary means of communication among members of the organization; the assumption is that it is not monitored.
- **Stand-by.** Back-up or alternate communication to be used if the common communication means is compromised.
- **Alarm.** Used when either an operation or a member is compromised.

3-28. The lack of an obvious formal organizational structure or architecture in some unconventional threat organizations may impede development of an extensive threat electronic database and an electronic technical database. The sophistication of a threat's communications networks indicates how quickly threat forces can react to changing conditions on the battlefield. The threat that must rely on couriers to communicate will be less likely to react quickly to friendly force actions; however, intercepting threat communications becomes extremely difficult in this case.

## INTELLIGENCE

3-29. Intelligence is a very important function of a threat organization. Just like any U.S. intelligence organization, the threat conducts a variety of intelligence tasks in preparation for a mission. Intelligence personnel and leaders on the ground, along with the assistance of counterintelligence personnel, must understand the political and physical strengths and weaknesses of the threat intelligence capabilities and leadership as well as how best to exploit those weaknesses. Analysts must always remain vigilant to the possibility that the threat is using deception tactics. The analyst should consider the following information:

- How is the threat conducting target reconnaissance?
- What assets or personnel is the threat keeping under surveillance?
- What factors is the threat evaluating when choosing a target?
- What type of propaganda is the threat using?
- What ideology is the leadership dedicated to?
- How will the organization continue to function effectively without key leaders?

3-30. Threat intelligence capabilities may include spy satellites, reconnaissance aircraft, EW, and other sophisticated systems, or may include children watching U.S. forces and running to tell insurgent fighters what is happening in a village. Analysts must pay attention to the intelligence gathering and processing capabilities of threat forces whether facing an insurgency or general war.

## RECRUITMENT

3-31. Recruiting is a main source of sustainment in a threat's organizational structure. Recruiting deals not only with selecting people to become members of the cell but also with developing a network of supporters of the organization who may or may not claim membership. Threat forces may recruit members from local, regional, national, or even international sources. Many insurgent cells are suspicious of people wanting to volunteer to become a member of their organization. The suspicion lies in the fear of having their organization infiltrated by someone who has ulterior motives or is a foreign intelligence agent. Because of this fear, some organizations have a very structured, long process to become a full-fledged member of the cell. Other threat units may use coercion to force recruitment or may use children or mentally handicapped persons to their advantage. At a minimum, analysts should evaluate the following:

- How potential members are identified.

- Once identified as potential members, how they are assessed for loyalty and how they are vetted for reliability.
- How the organization uses fear and intimidation to aid their recruitment.
- How potential recruits are reached.
- Which, if any, particular ethnic or religious groups are recruited.
- What media or means are used for recruitment propaganda.
- What the organization does with supporters who become disloyal. The answer to this question will assist the analyst in determining the organization's power over the local population.

## SUPPORT

3-32. Threat networks depend on support from the local population. Of the activities conducted by a threat organization, generating local support may be one of the most important for the insurgency's short-term effectiveness. While the support may or not be voluntary, it is a means of fulfilling the needs of the organization. These needs may include but are not limited to finance, medical support and supplies, and transportation. In today's highly connected world, the effect of the media as a supporter or nonsupporter of the threat unit or network must be critically examined. As with member recruitment, threat forces may receive support from local, regional, national, or even international sources. An analyst should evaluate the following:

- How potential supporters are identified.
- Once identified as potential supporters, how they are assessed for loyalty and how are they vetted for reliability.
- The type of support being provided to the organization.
- Whether the support is voluntary.

3-33. Operations that support threat forces, whether conventional army or insurgent forces, fall into five general categories:

- **Local support.** Threat networks depend on support from the local population. Of all the activities conducted by a threat organization, generating local support is one of the most important to ensure the threat's sustainability.
- **Regional support.** Regional support of a threat organization can come in a variety of venues. Regions may have a greater ability than the local population to provide certain services and support to the threat; for example, sanctuary, security, secrecy, or transportation.
- **National support.** Generating national support has a great impact on the threat's long-term viability. This is almost always the backbone of a threat force. National support may come in a variety of ways; for example, morale, physical, or financial.
- **International support.** Activities conducted by any threat organization generating international support often have the greatest impact on the threat's long-term effectiveness. International support may include technical, financial, transportation, sanctuary, or support of the threat government and its policies.
- **Popular support.** Popular support applies locally, regionally, nationally, and internationally. Popular support results in safe havens (sanctuary), freedom of movement, logistic support, financial support, intelligence, and recruitment of new personnel for the threat. Generating popular support has positive feedback effects on a threat organization and its morale.

3-34. Financial sustainment is a main source of viability to a threat's organizational structure. When researching a threat organization's financial standing, analysts should realize the importance of not only how the organization pays for services rendered or items purchased but also with how the organization is going to sustain its operations and continue to draw in needed financial support.

3-35. When considering the financial support of a nation's army or other forces, an analyst needs to consider the strength and ability of the national government to raise funds through taxes, oil revenues (or other resources), and international support from nations friendly to that country. The informal money

transfer system of some areas is extremely difficult to track. Bank robbing, kidnapping, extortion (collecting illegal taxes), narcotics, and smuggling are examples of how insurgent organizations obtain financial support.

## REACH

3-36. The ability of the threat to obtain data on friendly forces is a force multiplier. The threat will use every method available to gather information on all aspects of friendly force operations. Depending on the technological capabilities of the threat, the reach capability may be very rudimentary or it may be highly technical. Information automation and retrieval capabilities of the threat will help the analyst shape an opinion as to the threat's intelligence capabilities. When facing a more conventional force, the analyst must consider that the threat may have access to high technology automation tools that may parallel our own. The threat's communications architecture must also be considered for the purposes of disseminating data and intelligence.

3-37. Threat use of Internet access will give the threat an enhanced reach capability. The threat can use Internet sites to conduct research on the friendly units in their AO; learn about personalities, weapons capabilities, and certain friendly TTP; or download imagery of their AO in order to plan attacks and conduct ISR operations. Even very remote areas of complex terrain, such as mountains in Afghanistan or Southeast Asian jungles, can have Internet access if the appropriate technology is available.

## NATIONAL AGENCIES

3-38. The threat's ability to leverage national agencies to assist in the military fight is an important force multiplier to consider. For example, the threat's force may be able to use its own or another nation's national intelligence agencies or other agencies which can influence the military fight to the threat's advantage.

3-39. Insurgents normally will not have the ability to receive support from HN national agencies as these agencies most likely are hostile to the insurgency. This does not eliminate the need to analyze the relationship between the insurgents and HN national agencies. Some personnel within the national agencies may be supportive of the insurgents and may use their access to provide information to the insurgents. In a more conventional scenario, threat forces would likely have at least partial or even full support from national agencies. The analyst should examine, at a minimum, the following aspects of national agency support to threat forces:

- To whom the agency is loyal, both the leadership and members.
- The mission and agenda of the agency.
- The capabilities of the agency and how the threat force can bring them to bear.
- The agency's relationship with the threat force, both historic and current.

## LAW ENFORCEMENT AGENCIES

3-40. A threat nation's national, regional, or local LEAs may impact the threat forces' military capabilities by providing information or other support. This support could come in the way of arrests, personality profiles, data, or by influencing court systems. The examination of the relationships between the threat and civilian LEA is vital. The analyst must determine which LEAs are sympathetic to the insurgency and which are not. The insurgents may be secretly getting key information or supplies through these agencies. The analyst must also examine whether former law enforcement personnel have joined the insurgency. In a more conventional scenario, threat forces likely have at least partial support from local LEAs. The analyst should examine, at a minimum, the following aspects of LEA support to threat forces:

- To whom the agency is loyal, both the leadership and members.
- The agenda of the agency.
- The capabilities of the agency and how the threat force can bring them to bear.
- The agency's relationship with the threat force, both historic and current.



- How aggressively the police forces will enforce the law in order to maintain stability and the rule of law in the country.
- How corrupt law enforcement officers are; whether they harass certain ethnic groups, minorities, or women.

3-41. LEAs can provide many functions such as traffic control, detaining suspicious persons or arresting hardened criminals. An analyst must understand that law enforcement officers may support occupying friendly forces or insurgent or threat forces. Under some circumstances, it is possible that law enforcement officers and leaders will tell both U.S. forces and insurgents whatever is necessary to maintain the power base and control they hold in their community.

## INTERNATIONAL AGENCIES AND NONGOVERNMENTAL ORGANIZATIONS

3-42. The threat's ability to influence benevolent organizations to their advantage must be studied. The threat may use these organizations as cover for intelligence gathering. The analyst must determine which organizations are in danger of being attacked by the threat and which are not. Organizations that provide food and medical care can be coerced into providing these services to threat forces, or may provide them willingly.

3-43. Sometimes employees of the organizations are kidnapped or killed by the threat in an attempt to influence friendly forces or the policies of friendly nations. This has often resulted in the organizations departing the area, leaving the general populace in need of the support previously supplied. International agencies and NGOs may also be unwittingly providing third-party support to the threat through legitimate organizations. Some organizations may provide a portion of all charitable contributions to the militant part of their causes. Donors may or may not know that their contributions are going to supply support to the militants or terrorists. Threat forces may use a combination of international agencies, NGOs, and the local, national, or regional media in an attempt to influence global opinion.

## PERSONALITY

3-44. Personalities are a critical factor when analyzing intelligence in an AO. Attention must often be focused on individuals in an attempt to link them to other known or unknown elements of threat groups. Insurgent organizations should be depicted through multidimensional link analysis. (See chapter 5 for information on determining relationships between critical personalities and then their group association.) This applies to virtually any threat represented in COIN operations. Once relationships and the level of contact or knowledge the personalities have on each other are known, their activity can be determined. It is paramount to identify the leaders and their relationships at all levels to accurately establish an initial organizational chart. Personality files include, but are not limited to—

- Leaders (political, ideological, religious, military).
- Staff members.
- Organization's spokesperson.
- Family members (immediate and extended, tribal affiliation).
- Key members who bring expertise to the organization (demolitions, special weapons, assassinations, indirect fire).
- Media manipulation and propaganda campaign personnel.
- Specialized trainers.
- Code names, nicknames, brevity codes.
- Cultural idiosyncrasies.

3-45. Analysts and troops on the ground must also understand the political and physical strengths and weaknesses of the threat force leadership and how best to exploit those weaknesses. Considerations include—

- Who are the leaders? Is there a single, dominant charismatic leader?
- Is the leadership highly dedicated to an ideology?

- Are the leaders committed to a specific organizational and operational pattern?
- Are there differences of opinion among leaders as to purpose and methods? Will discord or other events occur as a result?
- What is the relationship between the leadership and the operational and support elements?
- What is the decisionmaking process of the insurgent leadership? Are decisions centralized or decentralized?
- Will the organization continue to function effectively without key leaders?

### **OTHER THREATS**

3-46. Examples of other threats are natural diseases, chemical hazards, biological hazards, wildlife, radiological hazards, and toxic industrial material.

### **THREAT CHARACTERISTICS RECORDKEEPING AND DATABASE**

3-47. Keeping accurate records on threat forces and organizations is critical to the success of intelligence analysts. There are a number of methods to do this, and most methods today use the power of computers to quickly organize and retrieve data. Each threat force, whether a nation's army or an insurgent force, will have its own idiosyncrasies. Therefore, it is important to understand that one solution on organizing the information about a threat force will not fit every situation. Some threat forces will change and evolve over the extent of a conflict with that force.

3-48. During Operation Iraqi Freedom, for example, initially U.S. forces fought the Iraqi Army. After the defeat of that force, some Iraqi soldiers formed an insurgent and terrorist organization supported by outside terrorist organizations and foreign fighters. This change occurred over a very short time causing intelligence analysts to change their thinking on what to look for and how to organize threat characteristic information.

3-49. A threat characteristics database is a summary of all basic intelligence concerning a nation's military forces. While it will address all the threat characteristics, if applicable, it will concentrate most of its attention on the composition, disposition, identification, subordination, and combat effectiveness. It includes all units from the various services that function in a ground or ground support role, including naval and air forces. It is normally published at national level intelligence centers.

3-50. However, as a threat force evolves from an organized army into a guerrilla or insurgent force, that information will become outdated and those national level intelligence centers will rely on information from the intelligence analysts on the ground at brigade and battalion levels to build the new threat characteristics database. This is why it is extremely important for intelligence analysts to understand the principles of threat characteristics relative to all four threat categories in the operational environment. Change on today's battlefield happens quickly, and the analyst must keep pace with a dynamic enemy.

3-51. A threat characteristics database should include the following information for each unit:

- Unit identification, to include numerical designator and type of unit (armored brigade, infantry battalion, artillery regiment).
- Subordination (parent unit).
- Subordinate units.
- Location—city and province or state, military installation stationed at, military geographic region (if a large country like Russia or China), grid location if deployed.
- Combat effectiveness (usually indicated in strength percentage or known capabilities).
- Nickname or unofficial name (such as “the Medina Division” or “Qods Force”).
- Unit insignia.
- Signature equipment (T-72s, Type 59s, SA-2s).
- Turret numbers, registration or bumper numbers, or other identifying features of the unit.

- Any other pertinent data:
  - Each threat characteristics database must contain explanatory notes and a glossary of terms, acronyms, and abbreviations used in the product. It must also contain formations or units grouped by subordination and echelon. For example, units assigned to a particular military district or region should immediately follow those headquarters units that exercise command over the subordinate units.
  - Other methods of recalling data must also be used. It may be necessary to identify each armor unit in an area; organizing the database so that it can be searched by “armor” or by equipment type (“T-62”) is an important element of database development. Databases should also contain additional summaries or products such as orientation maps of the nation or region concerned. For large countries like Iran, Russia, and China an orientation map for each military district should also be included in the analyst’s threat characteristics holdings.
  - The analyst should periodically amend or update threat characteristics databases. While the timing and degree of updates are at the discretion of the originator or highest headquarters in the case of a theater of operations, updates should be published when substantial changes to threat characteristics are detected.

3-52. In irregular warfare the analyst databases threat characteristics in the same manner used for the other three threat categories discussed above. Each situation will vary during an insurgency or asymmetric battle, and the analyst must quickly identify what is and is not an important data element in order to understand the threat. Even though a piece of information may not seem significant, analysts must keep a record of it. New information acquired later may show that data which originally seemed insignificant is important. The analyst must have kept that data in some file location so it can be retrieved later. In irregular warfare, rather than tracking battalions or companies an analyst at higher echelons may be tracking small groups of people or even individuals.

3-53. During irregular warfare the analyst should consider information such as the location of possible safe houses for the team or individual, meeting times, and known locations of relatives and business associates. Use of the threat characteristic “disposition” may be an appropriate way to categorize a safe house or café used for planning insurgent operations. The level of military training between one individual and another may be similar providing a link to understanding how the insurgent or terrorist cell is organized. Where a subject went to college and what languages the subject speaks may provide links to understanding the enemy’s TTP. Creativity is important and no details should be left out when compiling threat data during an insurgency or asymmetric battle.

3-54. Personality files or data contain information on certain individuals. The data in these files should include the person’s military rank or position in government, date and place of birth, civilian and military education, political, religious, and tribal or ethnic affiliation, nicknames (for example, Chemical Ali), demonstrated performance in leadership positions, speeches, or published articles. Often the personality file or database is the most difficult to build because the subject often does not want to be known, particularly in an insurgency. Again, in the case of personality data no detail is too small to be included, especially in the case of a hostile individual or a high-value target (HVT) which is being sought to be killed or captured.

3-55. The number of items that must be considered when studying cultural aspects of an operational environment are innumerable, but the following provides some aspects of culture to consider:

- Language differences.
- Tribal, ethnic, or racial tensions between groups.
- Religious groups and the friction or harmony that may exist between them.
- Tribal boundaries that may extend beyond political boundaries (such as the Kurdish area known informally as “Kurdistan” that includes parts of Turkey, Iran, and Iraq).
- Leadership within the culture or tribe and how it is obtained.
- Educational differences between tribes or groups and between men and women in the society.
- History of the tribe or ethnic group and its propensity to use violence to resolve disputes rather than negotiation to resolve matters.

- Whether a particular ethnic or religious group had a favored status in the government and if other groups are resentful of that favored status.

## TERRAIN ANALYSIS

3-56. Terrain analysis is the study and interpretation of natural and manmade features of an area, their effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continuous process. Changes in the terrain may change the analysis of its effect on the operation or enemy COA.

3-57. The best terrain analysis is based on a reconnaissance of the AO and area of interest. Analysts should identify gaps in knowledge of the terrain which the study of a map or image cannot satisfy and use those identified gaps as a guide for reconnaissance planning. If there are time constraints, focus the reconnaissance on the areas most important to the commander and the unit mission.

3-58. Most of terrain analysis focuses on the military aspects of terrain: observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, and cover and concealment (OAKOC). These OAKOC factors discussed below are general guidelines when analyzing and defining the battlefield.

## OBSERVATION AND FIELDS OF FIRE

3-59. Observation is the condition of weather and terrain that permits a force to see personnel, systems, and key aspects of the environment. Commanders evaluate their observation capabilities for electronic and optical line of sight surveillance systems, as well as for unaided visual observation. The highest terrain normally provides the best observation. For this reason, elevated terrain often draws the enemy's attention. A field of fire is the area that a weapon or group of weapons may cover effectively from a given position. A unit's field of fire is directly related to its ability to observe. Evaluation of observation and fields of fire identifies—

- Potential engagement areas.
- Defensible terrain and specific equipment or equipment positions.
- Areas where friendly forces are most vulnerable to observation and fires.
- Areas of visual dead space.

## AVENUE OF APPROACH

3-60. An AA is an air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. The identification of AAs is important because all COAs which involve maneuver depend on available AAs. Figure 3-1 is an example of grouping mobility corridors to establish AAs. During offensive operations, the evaluation of AAs leads to a recommendation on the best AA to a command's objective and identification of avenues available to the enemy for counterattack, withdrawal, or the movement of reinforcements or reserves. In a defense operation, identify AAs that support the enemy's offensive capabilities and avenues that support the movement and commitment of friendly reserves. To develop AAs, use the results developed during obstacle evaluation to—

- Identify mobility corridors.
- Categorize mobility corridors.
- Group mobility corridors into AAs.
- Evaluate AAs.

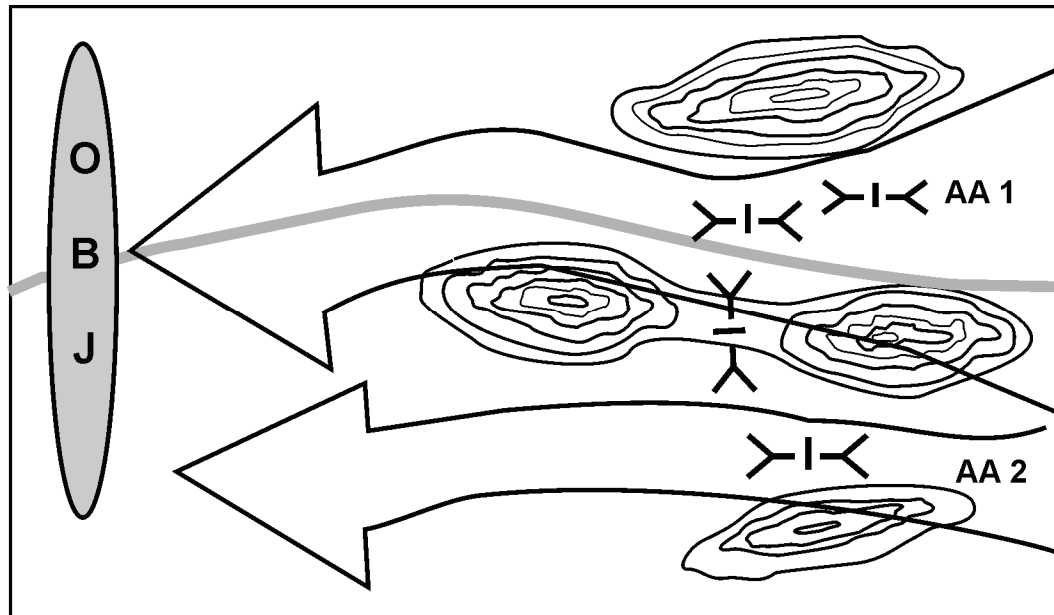


Figure 3-1. Grouping mobility corridors to establish avenues of approach

### KEY AND DECISIVE TERRAIN

3-61. Key terrain is any locality or area whose seizure, retention, or control affords a marked advantage to either combatant. In an urban environment, key terrain can be tall structures, choke points, intersections, bridges, industrial complexes, or other facilities. High ground can be key terrain because it dominates an area with good observation and fields of fire. In an open or arid environment, a draw or wadi could be viewed as key terrain. Tactical use of terrain is often directed at increasing the capability for applying combat power and at the same time forcing the threat into areas in order to reduce their ability to apply combat power.

3-62. Decisive terrain is key terrain that has an extraordinary impact on the mission. The successful accomplishment of the mission depends on seizing, retaining, or denying the terrain to the threat. It needs to be understood that key terrain is not necessarily decisive terrain. Commanders designate decisive terrain to communicate to their staff and subordinate commanders how important that terrain is to their concept of operation.

### OBSTACLES

3-63. An obstacle is any obstruction designed or employed to disrupt, fix, turn, or block the movement of an enemy force, and to impose additional losses in personnel, time, and equipment on the threat. Obstacles can be natural, manmade, or a combination of both. Some examples of obstacles to ground mobility are buildings, mountains, steep slopes, dense forests, rivers, lakes, urban areas, minefields, trenches, certain religious and cultural sites, and wire obstacles (concertina, barbed wire).

### COVER AND CONCEALMENT

3-64. Cover is physical protection from bullets, fragments of exploding rounds, flame, nuclear effects, and biological and chemical agents. Cover and concealment can be provided by (but are not limited to) ditches, caves, riverbanks, folds in the ground, shell craters, buildings, walls, and embankments.

3-65. Cover does not necessarily provide concealment. An example of cover without concealment is a bunker in plain sight that is intended for the protection of personnel. Concealment is protection from observation. It denies the threat the ability to observe forces, equipment, or position. Trees, underbrush, snow, tall grass, cultivated vegetation, as well as manmade camouflage, can provide concealment. Concealment does not necessarily provide cover.

3-66. Combine the several factor overlays into a single product known as the combined obstacle overlay. Figure 3-2 is an example of a combined obstacle overlay. These overlays are integrated with the evaluations of various other factors (for example, into a single product known as the modified combined obstacle overlay that depicts the operational environment's effects on mobility).

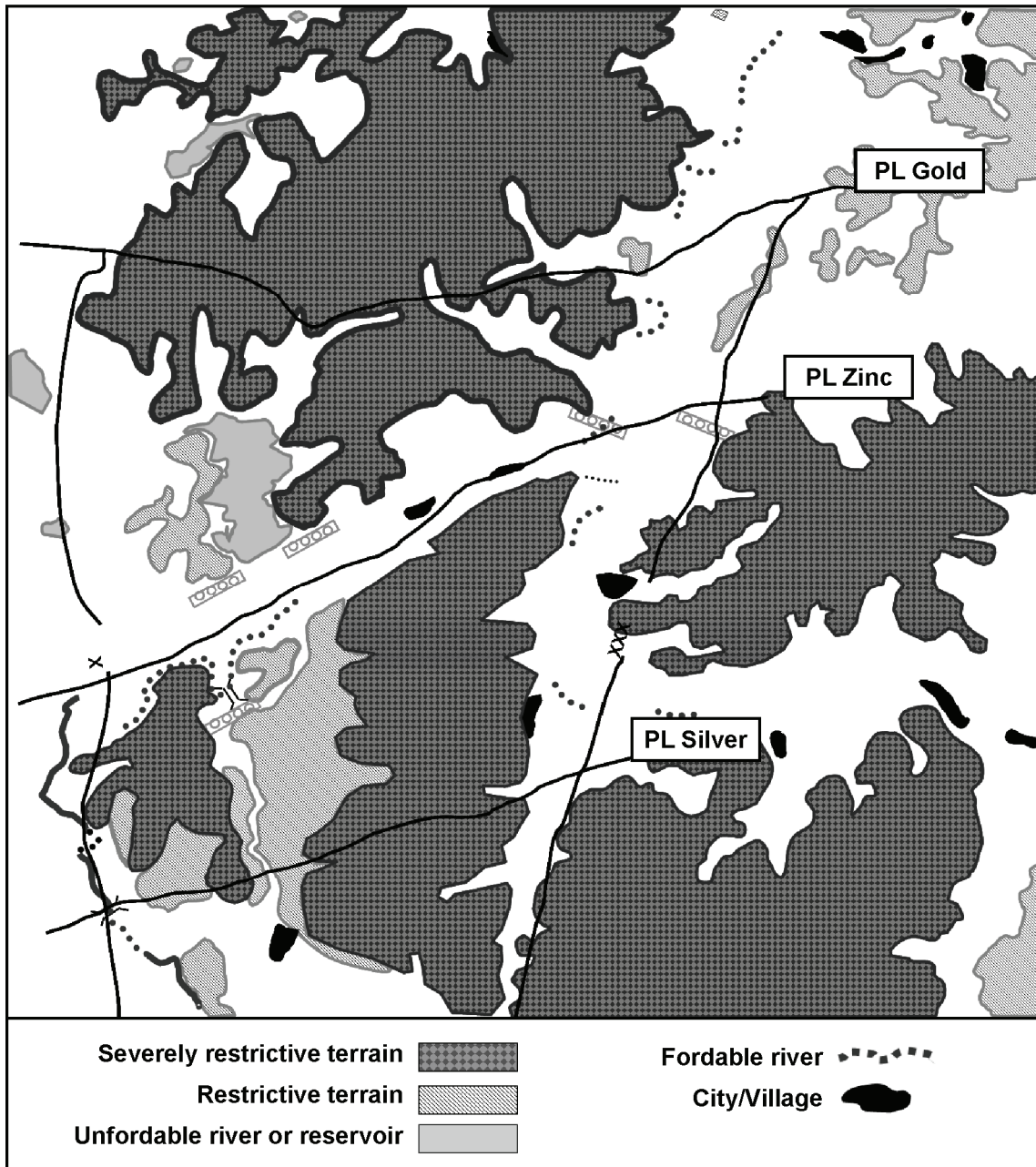


Figure 3-2. Combined obstacle overlay example

3-67. The geospatial engineers at brigades, divisions, corps, and theater armies conduct the major portion of the terrain analysis, combining extensive database information with the results of reconnaissance. The geospatial engineer teams work closely with the Air Force weather detachment or weather specialty team to incorporate the effects of current and projected weather conditions into their terrain analysis. Geospatial engineers have access to terrain databases, such as the theater geospatial database and national level geospatial databases, allowing automated support of the terrain analysis process.

3-68. Geospatial engineer teams also work closely with the G-2/S-2 in order to exploit imagery, reconnaissance information and reports, as well as other all-source data collected by the G-2/S-2, to supplement their standard terrain databases and to provide direct support to the unit. Automated terrain software and, to a limited extent, Distributed Common Ground System-Army (DCGS-A) offers two- or three-dimensional terrain analysis capabilities. These databases should be supplemented with a physical (leader's) reconnaissance of the terrain in question when feasible. The automated terrain programs address but are not limited to such factors as—

- Cross-country mobility.
- LOCs (transportation, communications, and power).
- Vegetation type and distribution.
- Surface drainage and configuration.
- Surface materials.
- Subsurface (bedrock) materials.
- Obstacles.
- Infrastructures.
- Flood zones.
- Helicopter landing zones.

3-69. Terrain analysis should include the effects of weather on the terrain. Analysts should consider the existing situation as well as conditions forecasted to occur during mission execution. Express the results of evaluating the terrain's effects by identifying areas of the operational environment that favor, disfavor, or do not affect each COA. Drawing conclusions about the terrain will help the staff evaluate the terrain for places best suited for use. For further information about terrain analysis, see FMI 2-01.301, FM 3-34-230, FM 5-33, and JP 2.03.

## WEATHER ANALYSIS

3-70. Analysis of the weather must include a study of its direct effects and its effects on terrain, weapons, and equipment as well as other aspects of the environment. Weather analysis integrates climate, forecasts, and current weather data with terrain analysis and the overall analysis of the environment. Air Force weather specialty teams (if available) at brigades, division, corps, and Army Service component command work together with geospatial engineer teams and the G-2 section during much of the analysis process. Weather specialty teams can provide detailed descriptions of the weather's effect on each equipment system and subsystem. Terrain and weather aspects of the environment are inseparable. The analyst should include the weather's effect on terrain during terrain analysis.

3-71. The military aspects of weather are visibility, wind, precipitation, cloud cover, temperature, and humidity.

## VISIBILITY

3-72. Visibility is defined as the greatest distance that prominent objects can be seen and identified by the unaided, normal eye. It is important that visibility be evaluated in accordance with METT-TC. A major factor in evaluating visibility is the amount of available light during night; the analyst must consider if the moon is in the night sky and how much illumination it provides. Figure 3-3 (page 3-18) is an example of a light data chart and figure 3-4 (page 3-18) is a National Weather Service wind chill factor chart.

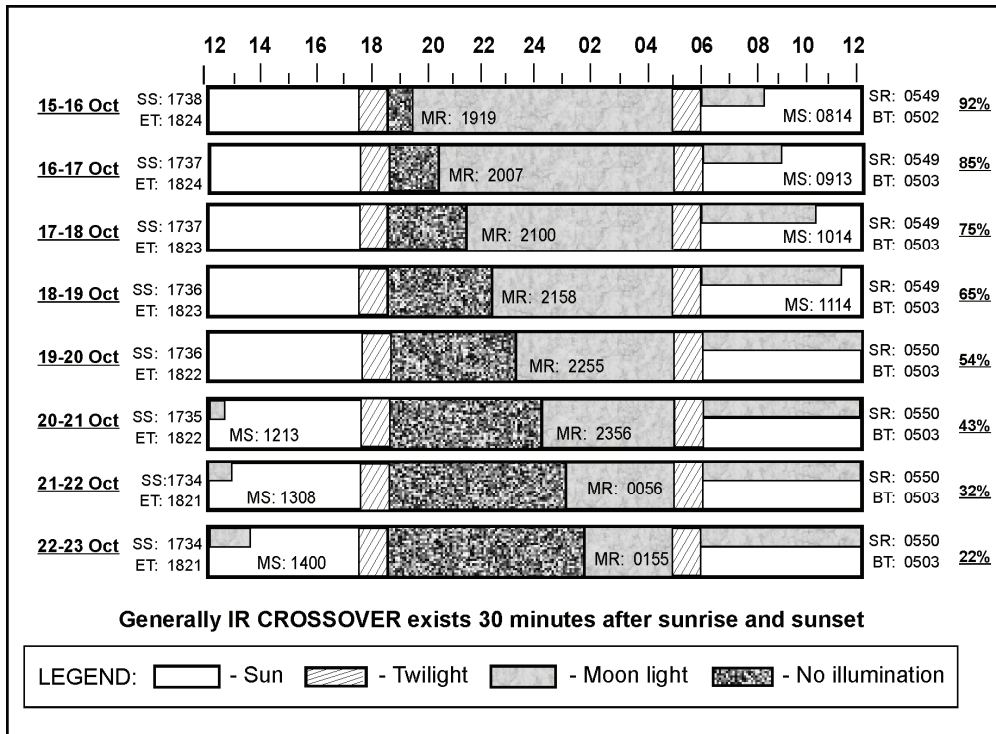


Figure 3-3. Example light data chart

ESTIMATED WIND SPEED (in mph)	Actual temperature reading											
	50	40	30	20	10	0	-10	-20	-30	-40	-50	-60
	Equivalent chill temperature (F)											
Calm	50	40	30	20	10	0	-10	-20	-30	-40	-50	-60
5	48	37	27	16	6	-5	-15	-26	-36	-47	-57	-68
10	40	28	16	4	-9	-24	-33	-46	-58	-70	-83	-95
15	36	22	9	-5	-18	-32	-45	-58	-72	-85	-99	-112
20	32	18	4	-10	-25	-39	-53	-67	-82	-96	-104	-121
25	30	16	0	-15	-29	-44	-59	-74	-88	-109	-113	-133
30	28	13	-2	-18	-33	-48	-63	-79	-94	-116	-129	-140
35	27	11	-4	-20	-35	-51	-67	-82	-98	-113	-132	-145
40	26	10	-6	-21	-37	-53	-69	-85	-100	-116	-132	-148
(Wind speeds greater than 40 mph have little additional effects.)	<b>LITTLE DANGER</b> is < hr with dry skin. Maximum danger of false sense of security.			<b>INCREASING DANGER</b> Danger from freezing of exposed flesh within 1 minute.				<b>GREAT DANGER</b> Flesh may freeze within 30 seconds.				
Trenchfoot and immersion foot may occur at any point on this chart.												
Developed by U.S. Army Research Institute of Environment Medicine, Natick, MA.												

Figure 3-4. National Weather Service wind chill factor chart



**PRECIPITATION**



















3-73. Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types of precipitation. Precipitation affects soil trafficability, visibility, and the functioning of many electro-optical systems. Heavy precipitation can have an effect on sustainment, communications, personnel, military operations, and many civilian activities. Figure 3-5 is an example of a weather effects chart, and figure 3-6 (page 3-20) is an example of weather effects analysis.

**CLOUD COVER**

3-74. Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many ISR and target acquisition systems and general aviation operations. Conversely, low cloud cover may increase the available level of light when there are ground-based lights such as what is available in urban areas.

Weather Effects										
Operation		06-09	09-12	12-15	15-18	18-21	21-24	00-03	03-06	Comments
I N T E L	EAC RECON									Transitional period between northeast and southwest monsoons. Northeast monsoons provide favorable weather for operations with decreased rain and thunderstorms. Also during the transitional period tropical cyclone frequency increases.
	TACTICAL RECON				C	C	C			
	UA - Hunter				C	C	C			
	UA - Predator				C	C	C			
	GROUND RECON									
MANEUVERABILITY (ARMOR/INFANTRY)					P	P				
A V I A T I O N	HELO, CAS (A-10), C-130 (Non-AWADS) AI (Vis Deliveries)									
	CAS (Non A-10)									
	AI (Radar Deliveries) C-130 (AWADS)									
AIRBORNE OPS										
ARTILLERY/AIR DEFENSE										
ENGINEERS					P	P				
LASER OR THERMAL OPERATION				P	P	P				
MOPP IV			T	T	T	T				
LEGEND: <span style="display: inline-block; width: 15px; height: 15px; background-color: #cccccc; border: 1px solid black;"></span> – Moderate degradation      T – Temperature      V – Visibility      C – Ceiling <span style="display: inline-block; width: 15px; height: 15px; background-color: #808080; border: 1px solid black;"></span> – Severe degradation      W – Wind      P – Precipitation										

Figure 3-5. Example of a weather effects chart

	<b>PREDOMINANT</b>	<b>TEMPORARY</b>	
LIGHT INFANTRY			Temperature, Rain
MECHANIZED INFANTRY			Temperature, Rain
SMOKE/CHEMICAL			Temperature, Rain
PSYOP			Temperature, Rain
SOF			Temperature, Rain
AIR ASSAULT			Ceiling, Visibility
CAS/AI			Ceiling, Visibility
AIR DEFENSE			Temperature, Rain
ATTACK AVIATION			Ceiling, Visibility




<b>LEGEND:</b>	 - Favorable	 - Marginal	 - Unfavorable
----------------	---	--	--

Figure 3-6. Example of shared weather effects analysis

### TEMPERATURE

3-75. Temperature extremes can reduce effectiveness of troops and equipment capabilities. They may affect the timing of combat operations. For example, extremely high temperatures in a desert environment may require dismounted troops to operate at night, reduce the length of their patrols, and increase the amount of water and thus the amount of weight each Soldier must carry on the mission.

### HUMIDITY

3-76. Humidity is the state of the atmosphere with respect to water vapor content. Automated sensors are often inaccurate when relative humidity exceeds 90 percent or is under 20 percent. High humidity affects the human body's ability to cool off. Hence, troops in tropical areas may become less effective because of higher humidity levels. Humidity is usually expressed as—

- Relative humidity. This is the ratio between the air's water content and the water content of the saturated air.
- Absolute humidity. This is the measure of the total water content in the air. It is high in the tropical ocean areas and low in the arctic regions.

### CIVIL CONSIDERATIONS

3-77. Civil considerations comprise the influence of manmade infrastructure, civilian institutions, and attitudes and activities of civilian leaders, populations, and organizations within an AO on the conduct of military operations. The acronym ASCOPE refers to the areas, structures, capabilities, organizations, people, and events within an operational environment. They are a factor in all types of military operations: offense, defense, stability, and civil support. If the military's mission is to support civil authorities, civil considerations define the mission.

3-78. Civil considerations generally focus on the immediate impact of civilians on military operations in progress; however, they also include larger, long-term diplomatic, informational, and economic issues at higher levels. At the tactical level, they directly relate to key civil considerations within the AO. Discounting these can tax the resources of follow-on elements. The world's increasing urbanization means that the attitudes and activities of the civilian population in the AO often influence the outcome of military operations. Civil considerations can either help or hinder friendly or enemy forces; the difference lies in which commander has taken time to learn the situation and its possible effects on the operation. These considerations can influence the choice of a COA and the execution of operations.

3-79. Some effects of civil considerations may impede overall force activities; others affect Soldiers directly, preventing them from functioning to their full capability. Anticipation and preparation can often overcome these effects, or even turn them to friendly advantage. This is particularly true for civil considerations, where careful preparation can turn parts of civil populations into advantages for friendly forces and disadvantages for enemy forces.

3-80. An appreciation of civil considerations—the ability to analyze their impact on operations—enhances several aspects of operations: among them, the selection of objectives; location, movement, and control of forces; use of weapons; and protection measures. Civil considerations comprise six characteristics (expressed as ASCOPE).

3-81. Organize ASCOPE information both by listing the facts and by viewing some form of visual aid. Two related products are recommended to accomplish this for each ASCOPE element—a matrix and a map overlay. Both products are based on the same information. The matrix provides detailed information, while the overlay plots the location on a map.

3-82. Table 3-2 (page 3-22) provides information on the elements of ASCOPE. Figures 3-7 and 3-8 (pages 3-23 and 3-24) provide examples of intelligence products that indicate the civil considerations for a particular AO. An overlay provides insights to the area. This includes items such as sectarian lines, areas of violence, and other fault lines. The analyst uses this to provide the commander with predictive analysis on where violence may erupt next and provide a better understanding of the different demographic clusters and their issues.

Table 3-2. Examples of civil considerations

<b>Area</b>	<b>Structures</b>	<b>Capabilities</b>	<b>Organizations</b>	<b>People</b>	<b>Events</b>
Tribe	Cemeteries	Sewer	Tribal	Phones	Weddings
Family or clan	Religious shrines	Water	Family or clan	Speeches	Birthdays
Ethnicity	Houses of worship	Electrical	Religious	Face-to-face meetings	Religious gatherings
Religion	Bars and tea shops	Academic	Ethnic	Media – radio	Funerals
Economic districts	Social gathering places	Trash	U.S. and multinational forces	Media – television	Major religious events
Smuggling routes	Print shops	Medical	Governmental agencies	Media – print	Anniversaries of wars and battles
National boundaries	Internet cafes	Security	Farmers or merchants	Visual – graffiti, signs	Birthdays or remembrance
Social classes – rich, middle, poor	Television stations	Market (use and controls)	Community organizations	Visual – videos, digital video disks (DVDs)	Harvest of plantings
Political districts	Radio stations	Employment and commerce	Military and militia units	Audio – pirated or illegal radio	Reconstruction openings
Military districts	Hospitals	Crime and justice	Illicit organizations	Rallies or demonstrations	Town council meetings
School districts	Banks	Basic needs	Insurgent groups	Restaurants	Elections
Road system	Dams	Public health	Gangs	Door-to-door	Sports events
Water sources	Gas stations	Religion	Nomads	Sports	
Construction sites	Military barracks	Displaced persons and refugees	Displaced persons and refugees	Religious gatherings	
Gang territory	Jails	Political voice	Volunteer groups	Parks	
Safe areas and sanctuaries	Water pumping stations	Civil rights , individual rights	Intergovernmental organizations	Family gatherings	
Trade routes	Oil and gas pipelines		Political	Gas lines	
Power grids	Water lines		Contractors	Bars and tea shops	
	Power lines		Nongovernmental organizations	Food lines	
	Storage facilities		Labor unions	Job lines	
	Electric substations		Indigenous groups	Speaking to reporters	

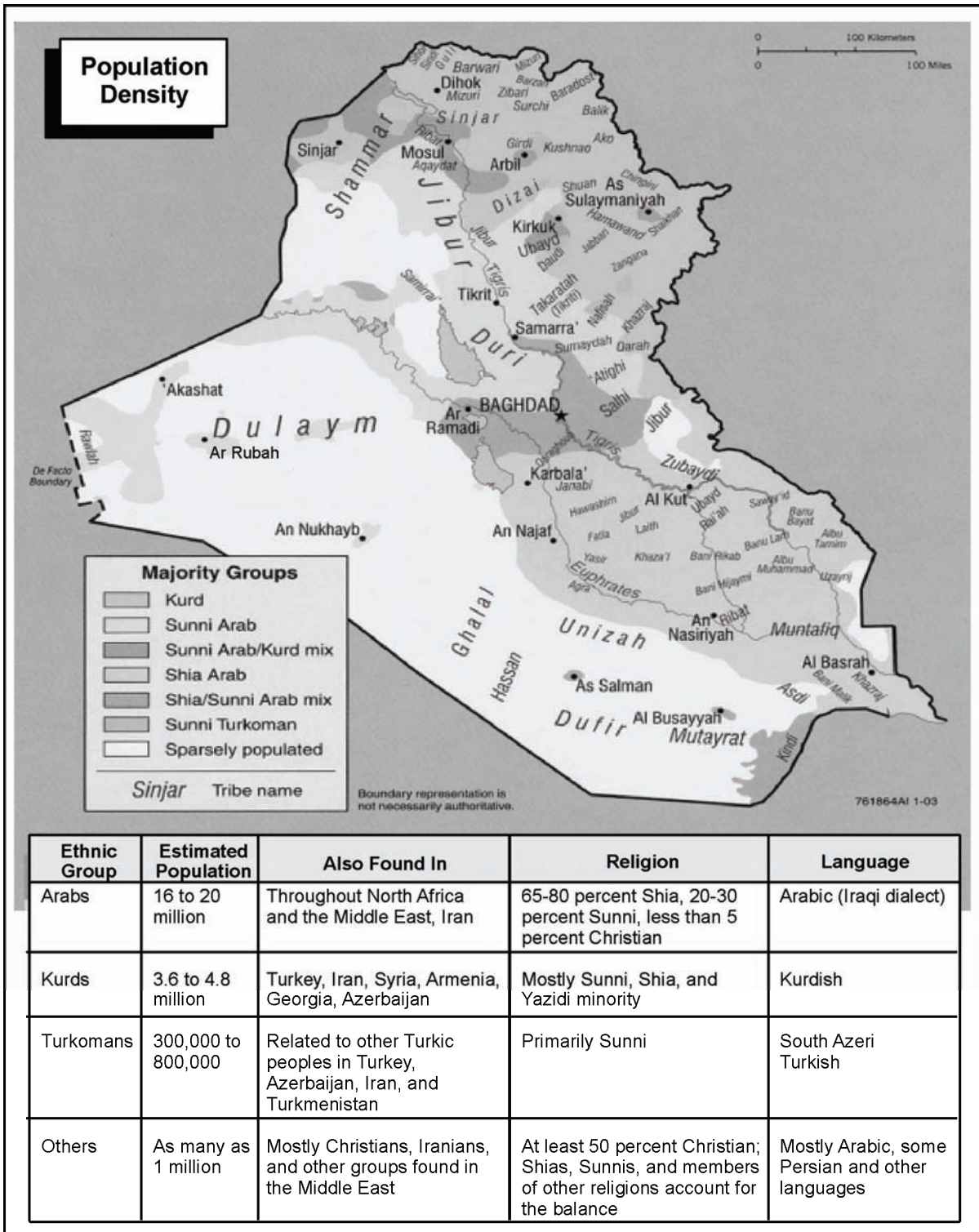


Figure 3-7. Example civil considerations product concerning tribes and ethnic groups

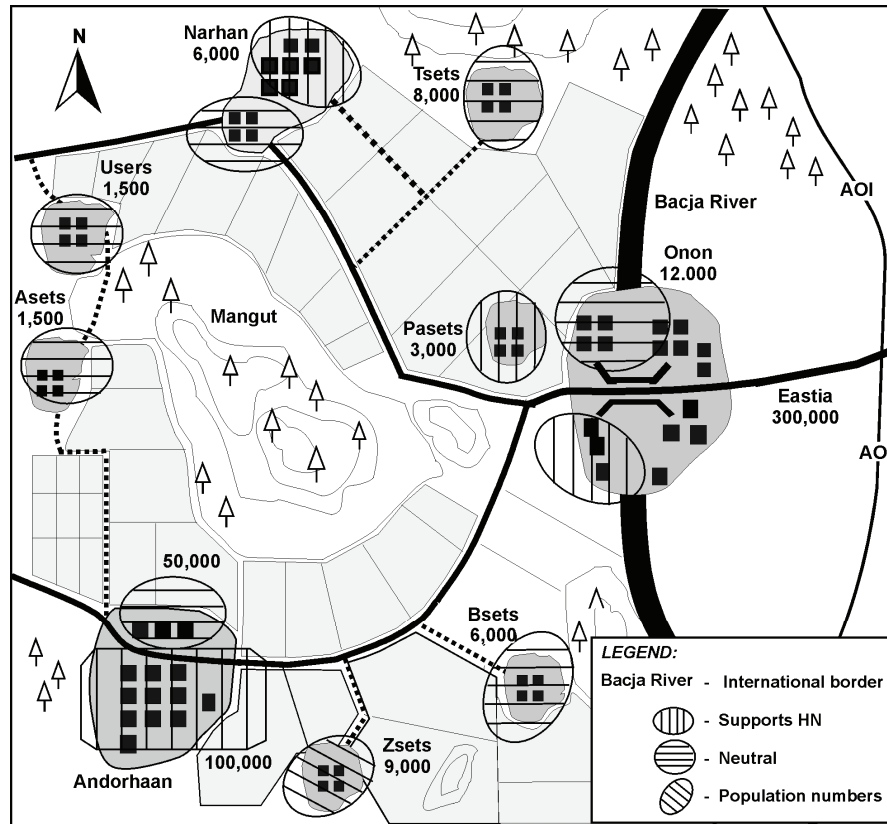


Figure 3-8. Example population status overlay

## CULTURAL DATABASE

3-83. The cultural database includes things of cultural or ethnic significance, such as tribes, religious groups, and languages or dialects spoken. The analyst must realize that the cultural diversity of a country or area may be larger than the country or area being studied. Large cities in which friendly forces operate will also have cultural diversity. It is essential the analyst understands the particular nuances of each ethnic or cultural group. Cultural information may be related not only to the threat but also to the entire operational environment.

3-84. The number of items that must be considered when studying cultural aspects of an operational environment are innumerable, but the following list provides some aspects of culture to consider:

- Language differences.
- Tribal, ethnic, or racial tensions between groups.
- Religious groups and the friction or harmony that may exist between them.
- Tribal boundaries that may extend beyond political boundaries (such as the Kurdish area known informally as “Kurdistan” that includes parts of Turkey, Iran, and Iraq).
- Leadership within the culture or tribe and how it is obtained.
- Educational differences between tribes or groups and between men and women in the society.
- History of the tribe or ethnic group and its propensity to use violence to resolve disputes rather than negotiation to resolve matters.
- Whether a particular ethnic or religious group had a favored status in the government and if other groups are resentful of that favored status.

## Chapter 4

# Analytical Support to Course of Action Development

This chapter provides processes which the intelligence analyst may use in order to provide analytical support to situational understanding. The use of situation development, situation maps (SITMAPs), functional analysis, and the development of threat COAs and indicators all assist the analyst in supporting situational awareness for a unit's battle staff and situational understanding for commanders.

### SITUATION DEVELOPMENT

4-1. This section describes the analysis phase of situation development and how the analyst converts information into intelligence to satisfy CCIRs. Analysis in support of situation development continues the IPB process and portrays significant aspects of the enemy, terrain, weather, and civil considerations in support of the MDMP and ongoing operations. The basis of this portrayal is the analysis of information from all previously recorded, cataloged, and evaluated sources in a manner to facilitate effective analysis. The analyst's updates are continuously posted, which automatically updates the database with current and accurate information.

4-2. The primary product of intelligence analysis is the intelligence running estimate. The estimate provides a continuous description of the enemy, terrain, weather, and civil consideration impacts on operations. The estimate is dynamic and changes constantly with the situation. Thus, analysis is a continuous process using the information available. The available information is usually incomplete. Analysts use known information about the enemy, terrain, weather, and civil consideration factors from the IPB process to estimate and determine information gaps. In addition, analysts determine the threat's capabilities, which are the basis for predicting probable threat COAs. (See appendix B for a sample format for the intelligence running estimate.)

4-3. Situation development is a process for analyzing information and producing current intelligence about the threat and operational environment during operations. Situation development—

- Enables commanders to visualize the AO and understand the current situation, broadly define the future situation, assess the difference between the two, and envision the major actions that link them.
- Provides commanders sufficient time, information, and detail to make sound tactical decisions.
- Helps intelligence analysts locate threat forces; determine their strength, combat effectiveness, capabilities, and significant activities; determine their objectives and intentions; and predict their probable COAs.
- Reduces the possibility of surprise and increases a commander's flexibility to effectively employ and adjust available combat assets and resources in response to enemy COAs.
- Confirms or denies enemy COAs.
- Identifies threat disposition (location).
- Explains enemy actions in relation to the friendly force operations.
- Provides an estimate of threat combat effectiveness.
- Enables intelligence analysts to quickly identify information gaps and explain threat activities in relation to the unit's or organization's own operations, thereby assisting the commander in gaining situational understanding.
- Helps the commander make decisions and execute detailed plans. This reduces risk and uncertainty in the execution of the plan.

4-4. The intelligence analyst maintains, presents, and disseminates the results of situation development through intelligence input to the COP, the SITMAP, and other intelligence products. Figure 4-1 shows the information cycle for situational understanding.

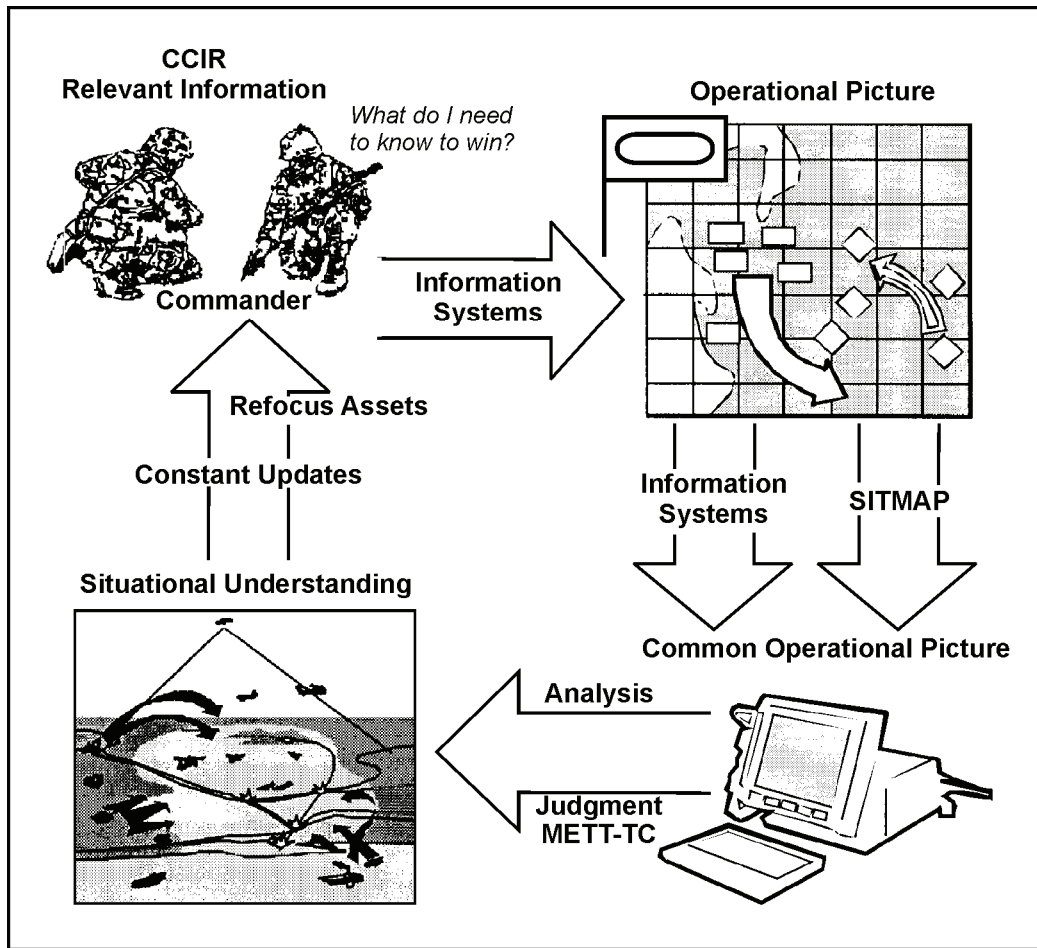


Figure 4-1. Cycle for situational understanding

## THE SITUATION MAP

4-5. The primary means the analyst uses for situation development is the SITMAP. The SITMAP is a map showing the tactical or the administrative situation at a particular time. The G-2/S-2 staff creates the SITMAP to aid in situation development and analysis. The SITMAP is the basic analytical tool at all levels of command; it contains both friendly and enemy unit symbols, their composition and disposition, the locations of obstacles, and friendly graphics that depict the AO and other graphic control measures for the current operation.

4-6. The analyst contributes to situation development by maintaining the SITMAP which integrates information from all intelligence sources and conducts analysis of the situation and how it might change in the future. Intelligence analysts monitor the ISR effort using the SITMAP and inform the commander or appropriate operations, fire support, sustainment and other personnel in the command post (CP) as to the current situation and predictive intelligence on the future situation. When using a SITMAP to monitor ISR, the map must have appropriate friendly graphics such as unit boundaries and named areas of interest on the SITMAP.



4-7. The SITMAP is not to be confused with the COP. A *common operational picture* is a single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (FM 3-0). The COP features a scale and level of detail that meets the information needs of that commander and staff. It varies among staff sections and echelons. Separate echelons create a COP by collaborating, sharing, and refining relevant information. The G-2/S-2 includes information from the intelligence running estimate in the COP. The COP relies on enhanced ISR and dissemination by modern information systems, which provide an accurate, near real-time perspective and situational awareness for commanders throughout the force.

4-8. DCGS-A provides access to data from ISR sensors at various echelons in near real time to provide a COP that is interoperable with other battle command systems. Information from the COP, transformed into situational understanding, allows commanders to better utilize the six warfighting functions: movement and maneuver, fires, intelligence, sustainment, command and control, and protection. Modern information systems help leaders at all levels make better decisions faster. Better decisions rapidly communicated allow Army forces to mass the effects of combat power more rapidly and effectively than the enemy.

4-9. Do not confuse the SITMAP with the situational template, which is a product of the IPB process. The situation template is a depiction of a potential enemy COA as part of a particular enemy operation. Situation templates are developed using the enemy's current situation, based on enemy doctrine and the effects of terrain, weather, and civil considerations. For more information on situation templates, see FMI 2-01.301.

4-10. All intelligence records are used with the SITMAP to develop the enemy situation and intelligence running estimate. The analyst posts all practical information to the SITMAP. Such information may include strength, activity, or last known location of an enemy unit. All information must have an "as of" time denoted by the use of the date-time group (DTG) of the time of observation posted on the map with the unit symbol. This allows for outdated information to be removed and assists in monitoring the movements of enemy forces. An analyst must maintain other intelligence reports and information that cannot be posted and uses this information to create situational awareness of the enemy and their most likely COAs.

4-11. Analyst use the SITMAP to—

- Evaluate, compare, and integrate information and intelligence from all sources.
- Track enemy forces.
- Identify indicators of particular enemy COAs.
- War-game possible enemy COAs.
- Conduct predictive analysis of likely enemy COAs.
- Identify intelligence gaps and new information requirements.

4-12. By comparing known information about an enemy unit or organization (plotted on the SITMAP) with the appropriate event template and the known threat characteristics, the analyst identifies unknown elements of an enemy force. For example, if an analyst identifies, locates, and plots two North Korean armor battalions, subordinate to a particular armor regiment on the SITMAP, doctrinally the analyst should expect to locate the third armor battalion near the other two battalions. The IPB process helps the analyst determine the most likely location of the third armor battalion. This comparison also helps the analyst identify and locate enemy HVTs, such as CPs, and air defense artillery weapon sites.

4-13. SITMAPs cannot show sufficient intelligence information during operations to use exclusively; therefore, the analyst must use other analytical tools such as time event charts, pattern analysis plot sheets, link diagrams, and association matrices in conjunction with the SITMAP. For example, if analysts are templating a possible IED attack, they would find a likely location where friendly forces would traverse and then consider locations where an observer could execute the command detonation of the IED. Conducting terrain analysis in accordance with the IPB process is the most reliable method to use.

4-14. Figure 4-2 shows a SITMAP appropriate for use by an intelligence analyst working within a battalion or brigade AO. It has a title, “2BCT SITMAP” along with a DTG. Always ensure a DTG accompanies SITMAPs and enemy activities on the SITMAP. In this example, the population in the area is divided into five different areas, mostly along tribal affiliations but also including religious preferences.

4-15. The SITMAP has areas of “attack zones” in which friendly forces often encounter attacks such as small arms fire and IEDs. There are also areas in which sectarian violence and sectarian fault lines are present. Various terrorist, religious, militia, and criminal groups operate in the areas as indicated by the diamonds with the appropriate markings within them. The ovals that encompass the enemy symbols indicate the general vicinities in which those groups have influence. Explosively formed penetrators are smuggled along the routes indicated by the arrows. Finally, the text box at the bottom left of the SITMAP has bullet comments on the primary problems within the area.

4-16. The intelligence analyst uses a SITMAP to identify patterns, hot spots of enemy activity, and other concerns such as ethnic or sectarian fighting and places where religious militia may become violent within the battalion’s AO. Coupling the SITMAP with an incident overlay (discussed in chapter 5), pattern analysis chart, or a link diagram can draw a picture for the analyst of the situation within the AO and help the staff develop possible enemy COAs. None of the analytical tools will stand alone, but together they are useful for situational awareness and predictive analysis.

4-17. The maintenance of the SITMAP is challenging during fast paced combat operations. The intelligence staff must maintain the SITMAP carefully and constantly update it as the situation changes. In most cases this will require several analysts working on the SITMAP at the same time with an officer or senior noncommissioned officer analyst coordinating the effort of the staff.

4-18. The SITMAP provides a record of the latest reported locations of enemy forces or activities, such as IED strikes, rocket attacks, or ambushes. As new information is received, the analyst compares it with information on the last known location and updates the SITMAP accordingly. This updated information indicates the direction and rate of enemy movement. It can also help determine the accuracy of intelligence reporting. For example, if a new report is received on a previously identified unit and it indicates an unusually rapid movement, then either the earlier or the current report may be incorrect. The analyst must confirm reporting with the source, or if there is not sufficient time to confirm the report, make a judgment about the new location. This is another example of the art of intelligence analysis.

4-19. A SITMAP is vital in recognizing and evaluating intelligence indicators. Many indicators are associated with patterns of enemy activity which can become apparent once posted to the SITMAP. An indication of an impending enemy attack can be the forward massing of artillery or finding a tank battalion in an assembly area refueling. A careful analysis of the SITMAP and comparison of it with known threat characteristics and event templates developed during the IPB process may reveal significant patterns of enemy activities.

4-20. IPB products are important analytical tools when used with the SITMAP. Comparison of templates and the SITMAP systemizes analysis and increases the accuracy of the intelligence running estimate. Situation and event templates depict projected enemy activities while the SITMAP depicts known enemy locations according to intelligence reports and unit observations. By comparing and integrating the two, the analyst can better predict future enemy activities with greater accuracy.

4-21. The SITMAP is also well suited for war-gaming. War-gaming integrates friendly and enemy capabilities and possible COAs with terrain and weather information. An analyst supports the MDMP by war-gaming enemy COAs against friendly COAs. This helps the unit’s battle staff in analysis prior to an operation and is vital to preparing the intelligence running estimate. It also helps the analyst predict threat reactions to friendly actions.

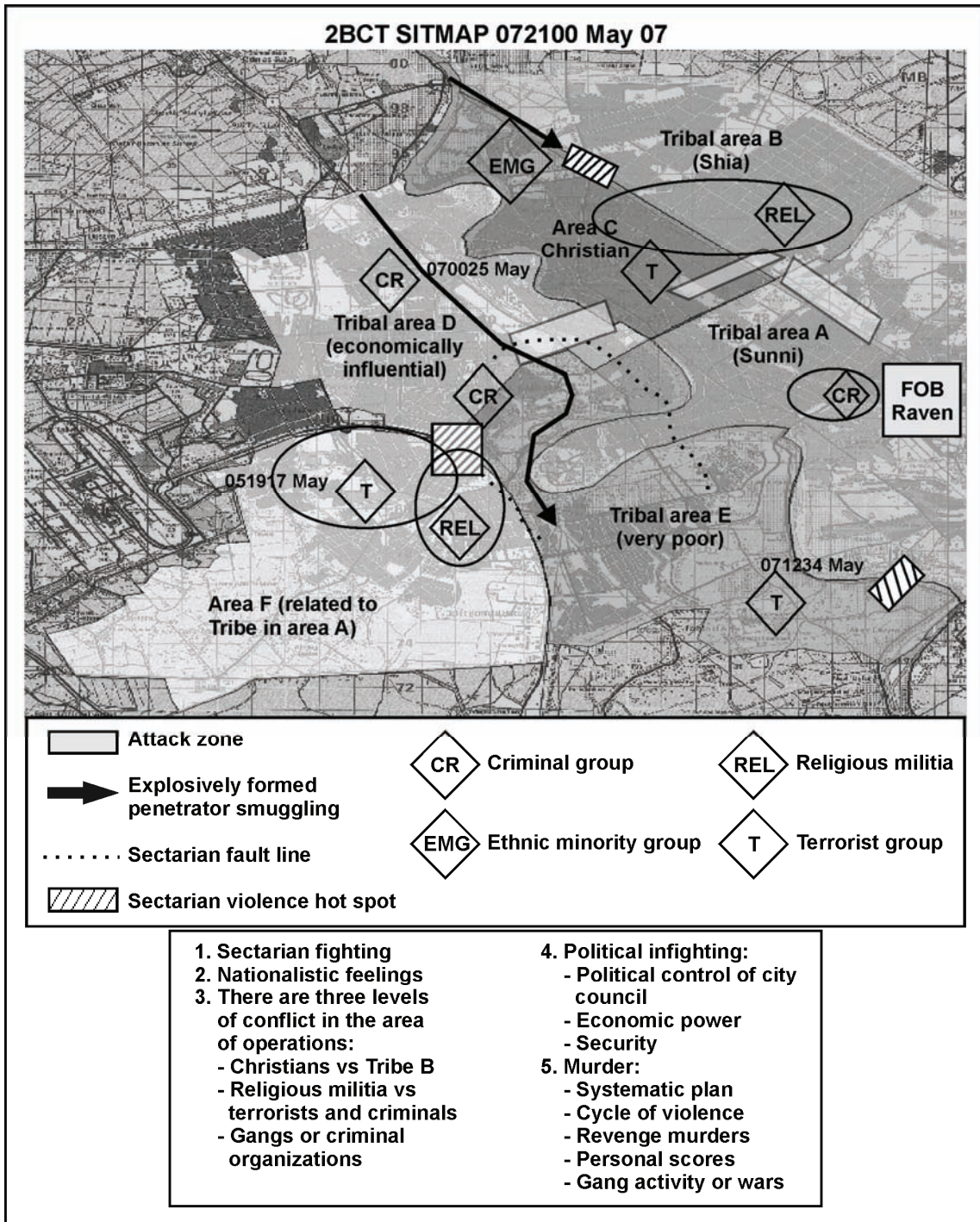


Figure 4-2. Example of a situation map

4-22. Generally, enemy units are posted to the SITMAP two echelons below that of the friendly unit. For example, an infantry battalion S-2 would post enemy units to the platoon level, while a division G-2 would post units to the battalion level. Enemy units that are behind the forward line of own troops in a conventional battle situation must be plotted regardless of size because of the threat they pose to sustainment operations and troops. In asymmetric or insurgency situations, however, it may be necessary to

plot activities of very small groups of people or even individuals in order to maintain the SITMAP. An analyst's experience and judgment, along with input from the commander, will dictate to what level of detail a SITMAP is maintained.

4-23. Care must be taken to prevent overcrowding the SITMAP. One method of doing this is to group entries by categories on a series of overlays. A typical separate overlay may include obstacles or suspected safe houses in a unit's AO. An enlarged sketch map can also assist the analyst in ensuring readability on the SITMAP. The SITMAP can be represented by using a standard map with overlay or can be projected by electronic means such as DCGS-A, Maneuver Control System, or command and control personal computer. The analyst has many tools available to assist them, such as FalconView, Imagine, or ArcGIS. The analyst maintains separate records of information that cannot be posted and uses them to support and expand information depicted on the SITMAP.

## FUNCTIONAL ANALYSIS

4-24. Functional analysis provides a framework for understanding how a specific threat will make use of its capabilities, whatever they may be, to accomplish its goals.

### DETERMINE THE THREAT OBJECTIVE

4-25. Functional analysis begins with a determination of what goal or goals the threat is trying to achieve (enemy objectives). Threat objectives are often, but not always, what the friendly unit's mission is trying to prevent and, conversely, are also often actions taken by the threat to prevent friendly mission accomplishment. Threat objectives will be specific to the type of threat force and to the friendly unit's AO, composition, mission, and other factors. The following are some example threat objectives:

- Cause friendly unit casualties to weaken political resolve in the United States and among coalition partners.
- Destroy friendly aircraft while on the ground during a refueling operation.
- Kidnap and ransom a civil leader friendly to U.S. forces.
- Prevent friendly security forces from discovering a hidden drug laboratory.
- Seize an important crossroads to facilitate maneuver of a larger force.
- Distract friendly forces to draw forces from the primary objective.

### DETERMINE THREAT FUNCTIONS

4-26. A number of different functions must be executed each time a threat force attempts to accomplish a mission. While the various functions required to accomplish any given mission can be diverse, they can be broken down into four very broad categories: action, enabling, fixing, and security:

- **Action function.** The action function (also known as the exploitation, decision, or mission function) is performed by the set of capabilities that actually accomplish a given mission. If the threat objective is to destroy a city with a WMD, then the WMD is performing the action function. If the threat objective is to seize a friendly capital city and it employs a WMD in another area to force a response by friendly forces that leaves the capital exposed, then the force used to seize the capital is performing the action function and the WMD is performing an enabling function.
- **Enabling function.** The enabling function is performed by a set of capabilities that acts to assist those capabilities performing the action function. If the mission is to enter a U.S. base and set off an explosive device, an enabling function would be to penetrate the perimeter defenses of the base or to assist in its infiltration.
- **Fixing function.** The fixing function is performed by a set of capabilities that acts to prevent opposing capabilities from interfering with mission accomplishment. If the mission is to ambush a convoy moving through an urban area, a fixing function would be to delay the arrival of a

quick reaction force. If the mission is to destroy a force in a defensive battle position, a fixing function would be to prevent the opposing reserve forces from maneuvering.

- **Security function.** The security function is performed by a set of capabilities that acts to protect other capabilities from observation, destruction, or becoming fixed.

4-27. Figure 4-3 provides an example of an enemy operation being carried out with all four functions. An action element is using the cover or distraction of a rioting crowd to attempt to seize a traffic control point. Snipers on either side of the enabling element will attempt to fix the crew-served weapons positions in place and not allow them to engage targets. The observer or sniper elements in the rear act as the security element and both watch for and engage or delay reinforcements.

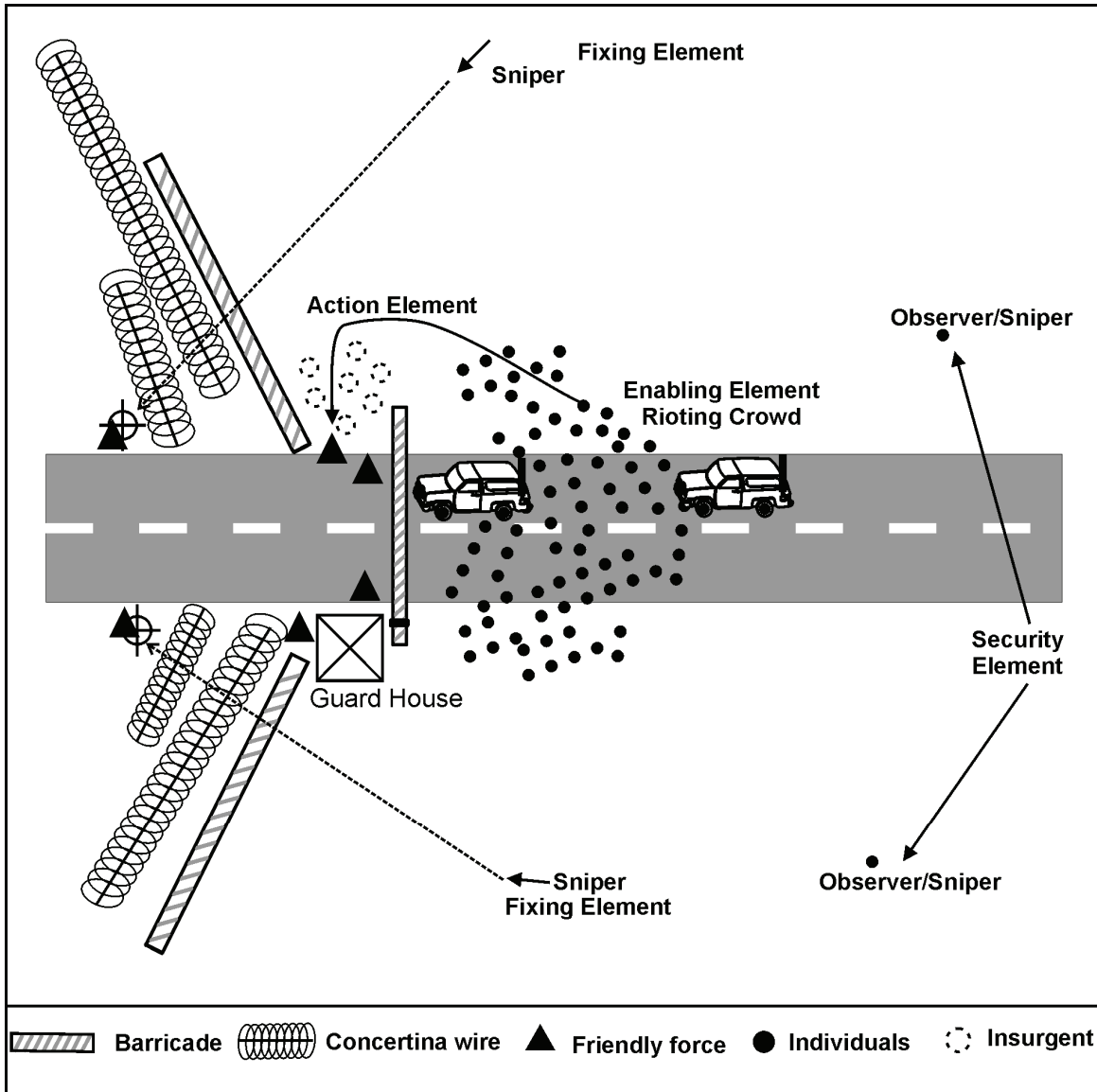


Figure 4-3. Depiction of threat functions during an assault

4-28. In the example at figure 4-4, consider that the engagement on the traffic control point in figure 4-3 (page 4-7) is merely an enabling function, a ruse, or a supporting effort for another operation which involves using IEDs to ambush the reaction force. This is what is meant by analysts having to consider secondary and tertiary actions.

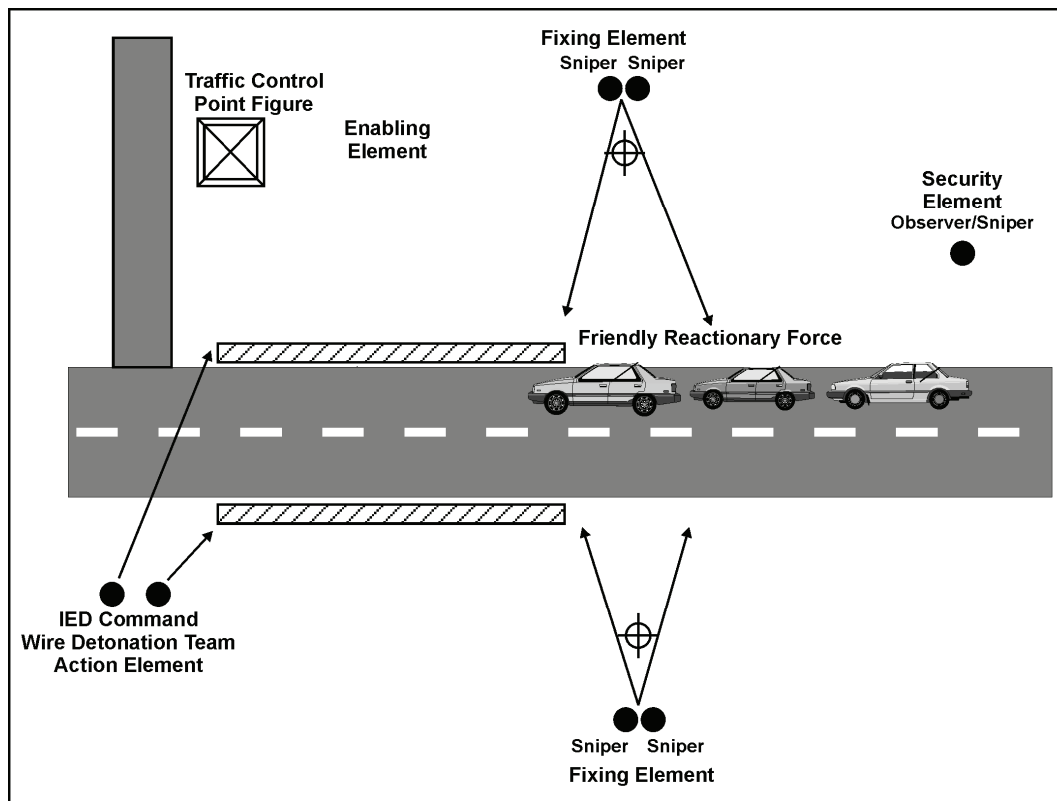


Figure 4-4. Using a complete mission as an enabler for another larger mission

## DETERMINE THREAT CAPABILITIES

4-29. Once the analyst knows which functions the enemy unit needs to perform to accomplish its goal, the last step is to identify what capabilities the enemy has to execute each function. While the functions required to have a high chance of success in achieving a military goal are universal, the means through which they may be accomplished will vary widely from theater to theater, enemy to enemy, environment to environment. Indeed, they may even vary from street to street. In one battle, the enemy may employ an infantry platoon equipped with infantry fighting vehicles and sophisticated thermal sensors to execute the security function. In another fight, that same function may be performed by a female civilian in a third floor apartment window using a cell phone.

4-30. Threat capabilities are potential actions and supporting actions which the threat can use to influence the accomplishment of the friendly mission. Define the capabilities with the use of statements. The following are examples of capability statements:

- “The threat has the capability to attack with up to eight divisions supported by 150 daily sorties of fixed-wing aircraft.”
- “The criminal organization has the ability to pay off local LEAs.”
- “The terrorists have the capability to send destructive viruses over the Internet, which can destroy computer files and archives.”

- “The threat can establish a prepared defense by 14 May.”
- “The terrorists have the capability of using CBRNE.”
- “The drug smugglers have the ability to conduct three drug-smuggling operations at the same time.”
- “The terrorists have the ability to conduct multiple car bombings simultaneously.”
- “The threat has the ability to target friendly convoys along main supply routes using remotely detonated IEDs.”

4-31. Supporting threat capabilities include the following:

- Use of CBRNE.
- Intelligence collection.
- EW operations.
- Use of air assets (fixed and rotary).
- Countermobility operations.
- Air assault or airborne operations.
- Amphibious operations.
- River operations.
- PSYOP.
- Deception operations.
- Car bombings, bomb scares, and suicide bombers.
- Raids on weapon storage facilities.
- Carjacking or hijacking of vehicles used in transporting personnel, weapons, or drugs.
- Theft of chemicals related to drug manufacturing.
- Threat information operations.

4-32. When identifying threat capabilities and COAs, consider the threat’s ability to conduct each operation based upon the current situation and its own METT-TC. Most situations will not present the threat with ideal conditions.

4-33. The threat could be under strength in personnel and equipment, may be short of logistic support, or the Soldiers or other personnel may be inexperienced or poorly trained. For example, a terrorist group’s normal tactics may call for the use of car bombs as a diversionary tactic to conduct other operations elsewhere. An evaluation of the threat’s sustainment might indicate a critical shortage of explosives. The following are additional considerations:

- Do not limit the threat capabilities strictly to threat conventional military forces. For example, student rioters during a noncombatant evacuation operation may be or may become a threat during the operation.
- During any discussion of the threat, cultural awareness is an important factor to consider. By developing an awareness of the culture, friendly units can identify groups or individual members of the population that may be friendly, a threat, somewhere in between, or both.

4-34. Functional analysis is the application of the knowledge of common and necessary military functions to specific threat capabilities. While it requires a strong understanding of the threat and threat TTP, it is one of the best processes of analysis for intelligence Soldiers to use. It is readily understood by combat arms Soldiers and creates excellent intelligence products that commanders and combat unit staffs will understand. Functional analysis is an excellent method for use by the intelligence Soldier serving at the tactical level.

## **THREAT COURSES OF ACTION**

4-35. The ultimate objective of intelligence analysts is to support the commander’s decision making and mission success. This normally involves a determination of the enemy’s most likely COAs and the

probability the enemy adopts those COAs. Like capabilities, the analyst determines the threat's COAs in terms of what, when, where, and in what strength. The probable COAs provide the basis for predicting enemy intentions. By accurately estimating the enemy's intentions, the analyst provides the answers to critical uncertainties (usually expressed as PIRs), which affect the commander's tactical decisions. In determining asymmetric threat COAs, it is important for the analyst to consider the motivations and objectives of insurgents in order to accurately describe what is truly driving their actions. Some of the characteristics of the asymmetric force that will determine the COA employed by them are their means of generating popular support or tolerance, their affiliation with local and regional ethnic, tribal, religious, political, and social groups; and their access to weapons, explosives, or IED construction and emplacement networks.

4-36. Understanding threat capabilities and vulnerabilities are necessary to develop COAs that the threat may take. The analyst uses knowledge of threat characteristics to provide predictive intelligence on—

- What the threat can do.
- How the threat will do it.
- When the threat can do it.
- Where the threat will do it.
- In what strength (element size) the threat can do it.
- What the threat's military and political objectives are.

4-37. Estimates of threat capabilities and their probability of adoption of a COA significantly affect the friendly commander's scheme of fire and maneuver for accomplishing the mission. Analysts estimate threat capabilities with a reasonable degree of confidence by integrating the enemy's tactical doctrine and operational effectiveness, the characteristics of the operational environment, and the time and space factors as developed through IPB. For example, a threat force may want to attack across a river in a particular location. Flooding in the area and the destruction of a bridge over the river, however, make a river crossing exceptionally difficult. Therefore, an enemy attack across the river is unlikely.

4-38. Some threat capabilities refer specifically to the support of combat forces rather than the capabilities of the actual forces. Support capabilities are constant considerations, especially when the enemy's implementation of them will significantly affect the accomplishment of the friendly mission. Enemy support capabilities consist of fuel, transportation of supplies and materiel, and the replacement of casualties among others. If friendly forces have interdicted enemy supply lines and a tank division cannot get fuel, it will significantly affect the options the enemy commander has. The analyst must consider the sustainment of enemy forces while developing intelligence on operational capabilities.

4-39. When determining enemy capabilities, time is a critical factor. Analysts must consider when the enemy can implement a capability. The friendly commander relies on time to defeat the enemy as well as follow-on forces or reinforcements. The friendly commander needs an accurate estimate of when enemy forces are employed to decide how to fight the battle. Analysts should consider the following factors when estimating when the enemy will employ its forces:

- Mobility capabilities.
- Disposition.
- Doctrinal rates of movement (if a conventional force).
- Established patterns and enemy TTP (trend analysis).
- Characteristics of the terrain, LOCs, trafficability, and obstacles.
- Time required for displacement, assembly, emplacement, and closing on the battle area.

4-40. In asymmetric environments, the analyst must consider the following factors when estimating when and how the enemy will employ enemy forces:

- Insurgent lines of infiltration and exfiltration.
- Safe house locations and weapons caches.
- Methods of engagement and denial.



- Force generation and sustainment.
- Historical patterns of activity.

4-41. Integrating information on the threat and the battlefield environment determines where the threat implements a capability. The enemy's composition, disposition, weapons, and equipment dictate how well the enemy moves, shoots, and communicates—the activities vital to most enemy COAs. Analysis of existing and forecasted weather conditions and military aspects of the terrain (OAKOC factors, see chapter 5) reveals how they affect enemy capabilities in various parts of the AO. In addition, the location of suitable defensive positions determines where the enemy attacks, defends, or adopts unconventional considerations. Terrain factor overlays, developed during IPB, identify specified aspects of the terrain. They assist the analyst in determining where the threat implements various capabilities.

4-42. Analysts use all-source databases as the key in determining enemy capabilities. When considering a conventional enemy force, doctrinal and situation templates assist the analyst in developing enemy COAs. During irregular warfare attempts to apply traditional threat characteristics and templates is challenging. Commanders and analysts require knowledge of difficult-to-measure characteristics. These may include the following:

- Insurgent goals.
- Grievances insurgents exploit in the local population.
- Means insurgents use to generate support.
- Organization of insurgent forces.
- Accurate locations of key insurgent leaders.

4-43. Using these and other threat characteristics to assess the unconventional (asymmetric) force will assist the analyst in determining how, when, where, and in what strength an insurgent force will employ its capabilities. In either case, conventional or unconventional, the event template and event analysis matrix help the analyst determine when and where the threat can implement a COA. The analyst follows the friendly operation to determine which threat capabilities have the greatest effect on the friendly operation. For a more in-depth discussion of warfare in asymmetric environments and specific IPB products for it, see FM 3-24 and FMI 2-01.301.

## INDICATORS

4-44. Indicators are the basis for situation development. The analyst integrates information from all sources to confirm indications of threat activities. Detection and confirmation of enables analysts to answer the CCIRs (PIRs and friendly force information requirements).

4-45. Indicators are clues that point toward enemy activities, capabilities, vulnerabilities, or intentions. Indicators, however, may not be factual and can lead the analyst to develop an incorrect intelligence estimate. Analysts must remember that an estimate is not certain, but is an opinion based on the facts and analysis of a particular situation. If an indicator is a ploy (part of a deception plan), then the conclusions based upon it may be incorrect.

4-46. An individual indicator cannot be allowed to stand alone. Integration of multiple indicators and other factors is essential before the analyst can detect patterns and enemy intentions. Other staff elements will assist intelligence analysts in developing indicators. The development of indicators is instrumental in answering commander's PIRs and information requirements. Indicators serve as a means of prediction across all operational levels from tactical to strategic. The analyst—

- Needs to be able to connect a series of tactical alarms to point to a higher indicator.
- Uses indicators to evaluate particular events or activities with probable enemy COAs.
- Uses indicators to determine what events or activities will likely occur for an enemy force to follow a particular COA.

4-47. The ability to recognize deceptive indicators is as important as recognizing true indicators of threat activity. See appendix C for sample indicators.

### Example

During both the American Civil War and World War II, there were a number of instances when documents captured by one side or the other held key information regarding the opponent's force composition or plans. The question in these cases was, were they authentic? If not, then most likely they were part of the threat's deception plan. Taken alone, as most were, there was little to validate the captured documents. They stood or fell on their own merits.

On the eve of the Battle of Antietam, during the American Civil War, Union forces captured a complete set of General Lee's plans for the engagement. The Union forces discounted the plans because they believed that they were part of a deception plan.

During the days preceding the Normandy Invasion in World War II, the Germans acquired plans revealing that the Allies would attack Normandy while the operations around Calais were to be a feint. Adolph Hitler, as a result of Operation Fortitude South II—a deception operation—believed the real attack would come at Calais and ignored this information.

In both cases, the recipients held the plans in great suspicion; it was just too easy, and the consequences of successful deception were too great. A conclusion built on an incremental framework of small indirect indicators is far more reassuring than one based upon one or two direct indicators, especially in the absence of significant associated indicators.

4-48. A threat may attempt to create false or misleading patterns of their intentions by providing friendly forces with false indicators. Analysts detect these false indicators, and then analyze them to determine what actual COA the threat is attempting to initiate. Analysts discover deception by comparing indicators, intelligence, and combat information from all sources to create an accurate picture of the battlefield. Because the use of indicators is such an important part of determining threat COAs, it is imperative that analysts carefully weigh all indicators.

### WEIGHTING INDICATORS

4-49. Weighting indicators helps resolve uncertainty. In combat, intelligence analysts will often encounter conflicting indicators. Conflicting indicators result from—

- Deliberate deception.
- Poor mission execution.
- Temporary indecision.
- Transition between missions.
- Random activity.
- Incomplete or inaccurate information.
- Uncertainty or doubt of the indicator itself.

4-50. When confronted with doubtful or conflicting indicators, analysts weigh some indicators more heavily than others to determine the enemy's actual intent. This is not a simple mathematic equation; it takes time and experience to become proficient in associating indicators with COAs.

4-51. The G-2 staff develops a list of indicators and places a priority on each. This prioritization establishes the relative weight of one indicator in comparison to another.

**Example**

Airborne reconnaissance low-multifunction (ARL-M) identifies three moving target indicators along avenue of approach (AA) #2. From the disposition of the MTIs, an analyst is able to identify elements of an insurgent reconnaissance force. There is not, however, any confirming data and there is a 50 percent chance that this could be a deception operation. At the same time, ARL-M identifies an assembly point for a significant number of what appears to be sustainment vehicles along AA #4. The U.S. Navy Advanced Tactical Airborne Reconnaissance System F/A-18D flies a mission to verify the targets, as the Hunter unmanned aircraft system simultaneously launches. Both confirm the site as a large sustainment supply base and staging area along AA #4, and far from AA #2.

**Analysis:** While some weight was given to a possible reconnaissance force along AA #2, much greater weight is placed on the location and confirmation of a large sustainment supply point and staging area along AA #4. The most likely enemy COA is an attack on AA #2.

4-52. Despite the heavy weight, or value placed on the sustainment indicators above, it is always dangerous to draw conclusions from a single indicator. The analyst integrates each indicator with other indicators and factors then defines patterns and establishes threat intentions. The analyst may develop standing or specific indicators to answer the commander's PIRs and information requirements. The information collected and intelligence provided through the indications and warnings effort drives operational-level planning and long-term PIRs and information requirements. The analyst uses these indicators to cross-reference specific events and activities with probable enemy trends and COAs.

4-53. The most obvious indicators are not necessarily the best depiction of a particular enemy COA. The obvious indicators may actually serve as elements of a deception plan. The successful analysis of indicators can help confirm or deny enemy COAs, and is therefore essential to supporting the commander. However, it is very important not to search for indicators of an expected COA or to expect a certain COA at all. Leaders must use indicators as a tip-off that something is occurring but demand that intelligence analysts dig deeper into the why or what of the situation and develop an indicator list specific to the situation.

4-54. The event matrix and ISR synchronization plan serve as important tools in the analyst's noting of developing events. By developing these products in a logical, progressive, or step-by-step manner, they often provide easy answers for the G-2/S-2 during the initial phases of an event; however, there may be a tendency to overrely on them. Indicators also tend to discourage analytical thinking because a bird's-eye view of the event is so readily apparent.

4-55. While it is important to understand and look for indicators of military activity, analysts cannot ignore specific indicators that might not fit a military category. The availability of resources such as funding, fuel, and the ability of a country to sustain its military must be considered by analysts at the operational and strategic levels.

**FISCAL RESOURCES**

4-56. A fiscal resource is one of the very best indicators of a country's or organization's ability to support a limited or protracted military mission or its willingness to militarily, overtly or covertly, support another country's military or terrorist action. Fiscal resources underline the two main indicators of a terrorist group COA, intentions, and capabilities.

4-57. Countries that are not fiscally independent may be willing to allow their territory to be used for training or a holding area and use their military in a mercenary role in return for monies, equipment, or advanced technology. If a country undertakes an action or program requiring a significant commitment of fiscal resources, this is a strong indication of a serious intent, capabilities, and commitment to that action or program. Fiscal resources can support the analyst theory of a country's commitment, intent, or ability to

commit to a military action. Fiscal independence also adds credence to a country's verbal threats and political and economic influence.

### RESOURCE SCARCITY

4-58. If a country commits a scarce resource in support of a military action this may indicate its intent to project a false commitment to achieve a military solution while attempting to force another country to seek a peaceful solution (which usually involves forcing the other country to make some concessions). A country that has scarce resources may place such a high value on the resources that it may not use them unless it is forced to. Countries with a scarce resource (technology, military equipment, military experts) may be willing to employ a resource which they have an abundance of (military personnel, training areas, raw minerals) to acquire more of the scarce resources. All of these indicators must be analyzed to correctly answer CCIRs and PIRs and to help facilitate situational understanding for the commander.

#### Example

If a nation has a fleet of 50 warships, sending 1 to stand off another nation's coast is a less reliable indicator than if they sent the only warship they had, especially if there was a chance that they could lose this ship.

4-59. If an enemy element makes a preparation that is not reversible by cheap and efficient means, they may be unintentionally signaling intent. If an artillery brigade dumps more ammunition at its gun locations than it has the organic transport to carry in one lift, then there is a problem if the unit moves. This may indicate that the unit does not anticipate moving with the ammunition, which could mean that they plan to fire it or leave it in place.

### DEVELOPING INDICATORS

4-60. When developing indicators, start from the event, work backwards, and include as many indicators that can be thought of. Analysts can always remove some later if decided that they are unnecessary. These indicators form the basis of an ISR plan.

4-61. Common knowledge and understanding of threat characteristics and the operational environment are often very useful to ensure that all avenues are covered. This can be as simple as using threat characteristic factors in a more conventional scenario. If presented with a PIR, the thought process can follow—

- Threat characteristics, particularly composition, disposition, tactics, training, sustainment, and combat effectiveness.
- Electronic characteristics (formerly electronic order of battle). Electronic characteristics are the identification of enemy digital and analog communication links, systems, and associated units.
- Personalities.
- Where on the battlefield to expect a particular enemy activity.
- In stability operations or support missions, it might be more applicable to use who, what, when, where, why, how, and in what strength.

### ANALYZING INDICATORS

4-62. Analysis of indicators requires a number of actions. First, analysts examine collected information and intelligence. They then ensure that any information pertaining to the indicators has footnotes that include details of the event. Next, look for the development of patterns. If the analyst notices that one set of indicators is being satisfied, but another is not, watch closely to detect deception operations. An analyst must recheck the validity of the indicators and verify that the staff did not miss any relevant information. If the indicators are valid, report the findings. The commander will need to know whether the threat is conducting an actual combat operation or a deception operation. (See appendix C for examples of indicators.)

## USING INDICATORS

4-63. Develop indicators by placing them in a logical order and at different levels or stages. In this methodology, there is often a logical sequence or order of indicators. Although the indicators may overlap, avoid using them in isolation. In some cases, it may be more advantageous to develop indicators as a series of milestones leading up to an action or event in a sequential manner. Analysts should consider probability and priority when describing these indicators.

**This page intentionally left blank.**

## Chapter 5

# Analytical Tools and Products

Analysts use a myriad of techniques and tools to assist in providing intelligence support to operations. This chapter will address use of predictive analysis, pattern analysis, nodal analysis, and other methods, tools, and products that can help analysts illustrate their understanding of the situation to operations officers and commanders. This chapter contains examples of products created using the Analyst Notebook software.

### ANALYTICAL TECHNIQUES AND TOOLS

5-1. Intelligence personnel analyze, organize, and make estimates based upon data collected on a specific area or subject to support the commander's decisionmaking process. There are a number of techniques to facilitate analysis. These include—

- Predictive analysis.
- Pattern analysis.
- Nodal component analysis.
- Time event analysis.
- Link analysis.

5-2. Automation can assist intelligence analysts in the techniques listed above. DCGS-A, for example, has software applications specifically designed for each of these techniques.

### PREDICTIVE ANALYSIS

5-3. Predictive analysis is a process allowing the intelligence analyst to predict future events based upon previous enemy activities and events. Predictive analysis is not guessing; its basis is the use of common sense, solid analysis using the methods discussed in chapter 2, and the appropriate analytical tools and methodologies for the situation. It is a key component in the IPB process, situation development, and indications and warnings. Predictive analysis often focuses on determining a threat's capabilities, intent, vulnerabilities, and most probable COA. It requires the analysts to stretch their intellects to the limit and understand that the predicted event, or COA, can hinge on many variables.

5-4. Prediction is not guessing. Predictions must be based on solid analysis of information using specific tools and methodologies. The commander needs to know who the enemy is, what they can do, where they are, and, most importantly, what they are going to do next. Staying ahead of the enemy is the primary focus of the combat commander. Predictive analysis allows the commander to maintain the initiative.

5-5. Conventional analysis examines, assesses, and compares bits and pieces of raw information and synthesizes findings into an intelligence product that usually reflects enemy capabilities and vulnerabilities. Predictive analysis goes one step further because the objective is not just to establish capabilities. The goal is to determine enemy intentions and probable COAs.

5-6. Predictive analysis is a continuous analytical process which focuses on determining a threat's capabilities, intent, and most probable COA and reactions to friendly operations. Even with the most sophisticated analytical tools and a wealth of information, it is possible that the prediction will not happen. This is often seen as a failure of MI for those who do not understand true analysis. However, the analyst

must be able to present to the commander every possible intention of the threat along with the capabilities. Performing predictive analysis and producing intentions intelligence is required for commanders to make informed decisions.

### Example

Information from aerial reconnaissance indicates the location of approximately 31 MTIs. The MTI locations and times of imaging are annotated on the mission report. Based upon this report, you will conduct several mental functions (analysis), attempt to fuse this information into what is happening in the operational environment, and predict enemy intentions. The following steps are taken:

- Plot the MTI locations on a SITMAP and annotate the DTG recorded on the mission report. Indicate direction of movement. Be sure to post the DTG of the observation, not the DTG the report was sent.
- Once plotted, look for any relationships to previously reported units in the area. If the answer is that there is no relationship, consider what must be done to answer the “who, what, when, where, and why” questions.
- If there is a relationship, an analyst can probably determine what type of unit it is (tanks, armored personnel carriers, trucks). Consider the direction of movement along with the unit’s speed to determine where the unit may be going.
- With this information, now analyze the bigger picture: does the movement indicate where the threat force will be committed? Is this part of a threat’s main offensive? Specifically, try to analyze what this information really means, its cause and effect, and draw conclusions.

With the combination of analysis, adjunct information, and seeing what it means overall, the analyst is now prepared to state the threat’s intentions (predict). The prediction in this case should specify what the equipment is, the unit designator, rate of march, and when and where engagement may occur. It is answering the when and where, in this case, that is predictive.

## PATTERN ANALYSIS

5-7. Pattern analysis is the process of deducing the doctrinal principles and TTP that enemy forces prefer to employ by careful observation and evaluation of patterns in their activities. When using this technique, the premise that enemy activities reflect certain identified and interpreted characteristic patterns is its primary basis. Pattern analysis can be critically important when facing an enemy whose doctrine is undeveloped or unknown and it is necessary to create a new threat model and threat templates. Combating insurgency operations is a prime example of this type of analysis. However, the tool presented here also applies in support of conventional operations.

5-8. The pattern analysis plot sheet, as shown in figure 5-1, shows patterns in time. It helps the analyst to identify when the threat tends to conduct specific types of activities. By analyzing the patterns, the intelligence staff may be able to anticipate upcoming attacks and likely targets. Intelligence staff may also be able to draw conclusions about the threat forces’ capabilities and vulnerabilities.

5-9. Build the pattern analysis plot sheet by creating a circular product. The circle is divided into sections to annotate time around the edge of the circle. Subsequent circles indicate the day of the month or the day of the week. Squares, circles, stars, different colors, or other symbols indicate particular enemy activities. By plotting the particular enemy activity on the time and date that corresponds to the circular plot sheet, patterns may emerge.



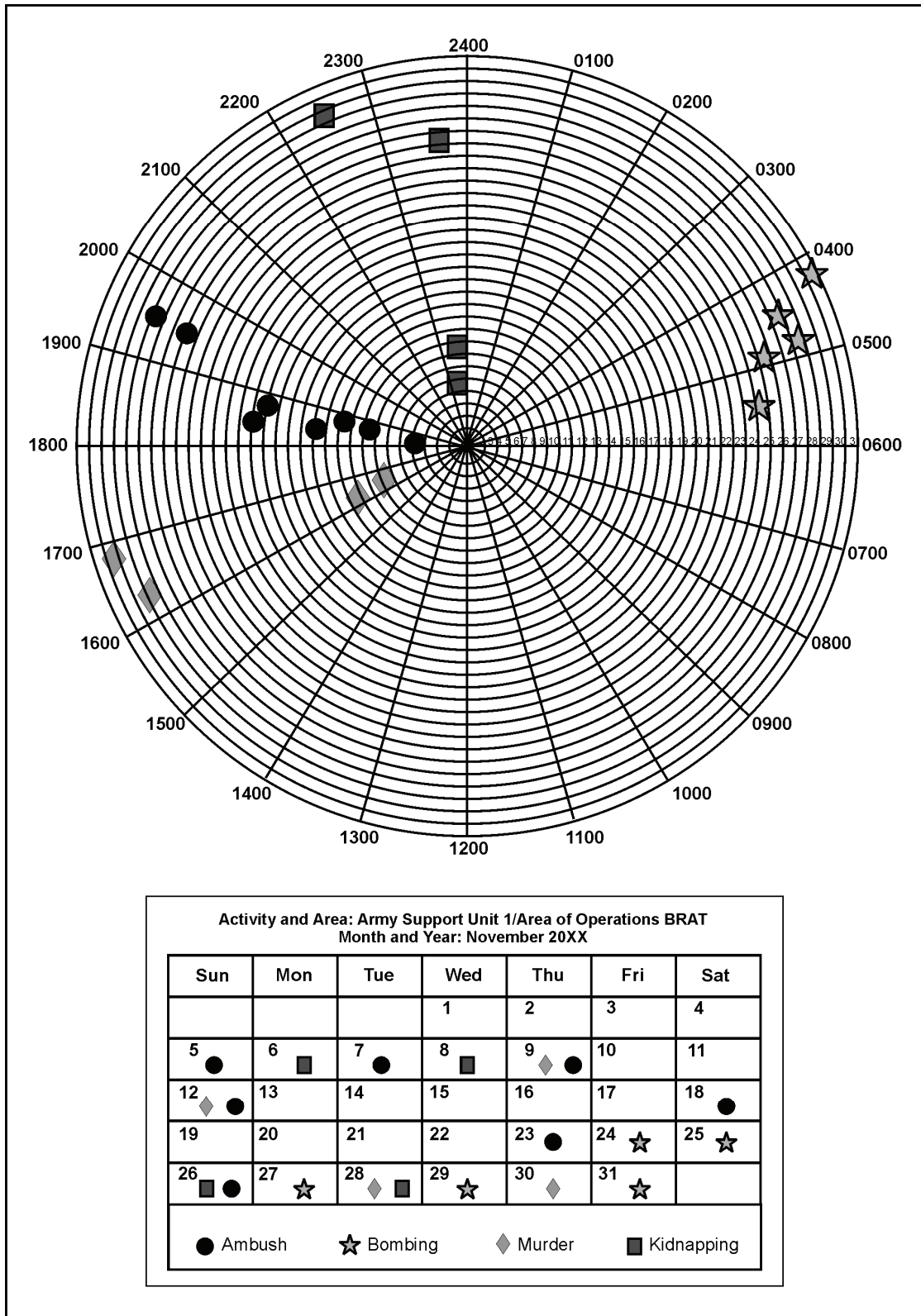


Figure 5-1. Example of a pattern analysis plot sheet

5-10. In the example in figure 5-1 (page 5-3), six enemy ambushes occurred in the month between 1800 and 1900. However, later in the month two ambushes occurred between 1900 and 2000. This could indicate a shift in threat TTP to conducting ambushes later in the day. However, an analyst must also consider if friendly forces caused the change by not being in the area between 1800 and 1900. Using the pattern analysis plot sheet can help illustrate timeframes of enemy activity, but it does not mean the analyst can stop thinking. Using the chart in figure 5-1 the analyst can clearly see that bombings occur in the early morning, but ambushes are an evening event, while kidnappings take place very late at night.

5-11. An incident overlay, as shown in figure 5-2, is another tool used in pattern analysis and is similar to the SITMAP. It displays activities spatially. It is useful to gauge spatial patterns; however, it does not provide any visual representation of temporal patterns. Just as the SITMAP cannot stand alone without further intelligence products or written reports to fill in the details, the incident overlay can only illustrate on a map or image what and where an event took place. It is critical to include a legend on the incident overlay and a time period covered. Just as with the SITMAP, the analyst must be sure not to overcrowd the map and make it unreadable.

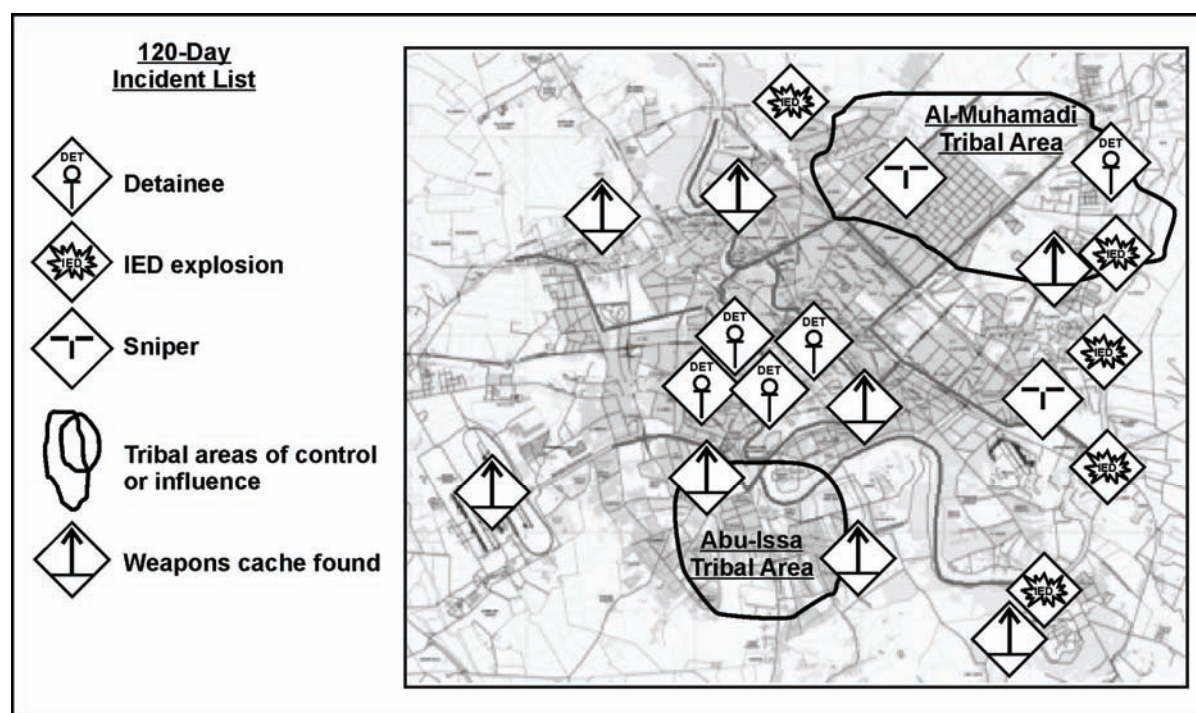


Figure 5-2. Example of an incident overlay

5-12. Build the incident overlay by plotting specific activities on the map using appropriate symbols. Asymmetric environments may require using many unfamiliar symbols, so it is critical to have a legend in the margin of the map. Symbols listed in FM 1-02 or MIL-STD-2525C should be used as much as possible. Maps can either be imagery or standard military maps. Use whichever map the commander prefers. Incident overlays are excellent briefing tools to update the enemy situation within a unit's AO.

## NODAL COMPONENT ANALYSIS

5-13. A node is a point at which subsidiary parts originate or center. Nodal component analysis is the analysis of how the nodes of a designated system function in relation to one another. Similar to functional analysis, nodal component analysis assists in identifying critical nodes of the system. A critical node is an element, position, or command and control entity whose disruption or destruction immediately degrades

the ability of a force to command, control, or effectively conduct operations. For illustrative purposes, a notional IED network will be used as the example threat network.

5-14. Analysts working with nodes will spend a great deal of time working with various pieces of information to assist them in understanding relationships. Relationships can exist between people, organizations, entities, locations, or any combination of the above. How the various groups interact is as important as knowing who knows (or should know) who. Relationships are also present within the IED network itself. An IED network is a complex, interconnected group or system which in some manner concerns itself with IEDs.

5-15. The analysis of any type of network involves the use of models designed to graphically display the system or network components. Models of various complexities are useful to different command levels. The upper echelons will employ the use of a smaller, less complex diagramming model while the lower echelons will use a more complex and detailed model. Figures 5-3 and 5-4 (page 5-6) depict the same network using different representations in order to show varying levels of complexity. The reason there are different levels of complexities is due to the operational focus of the echelon.

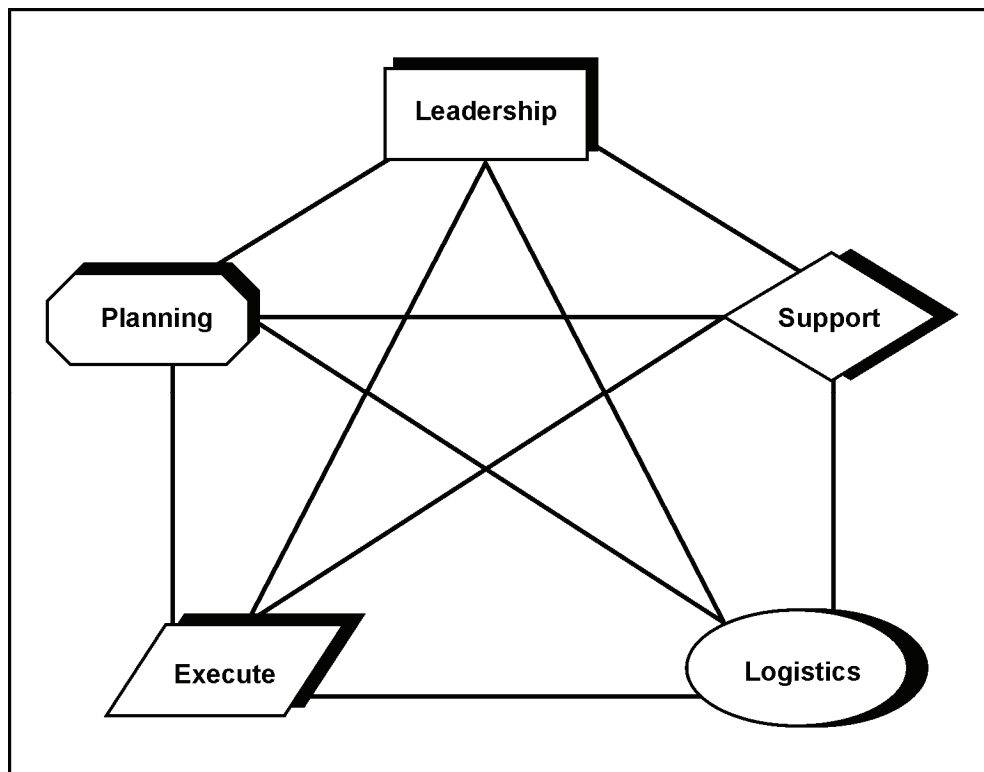
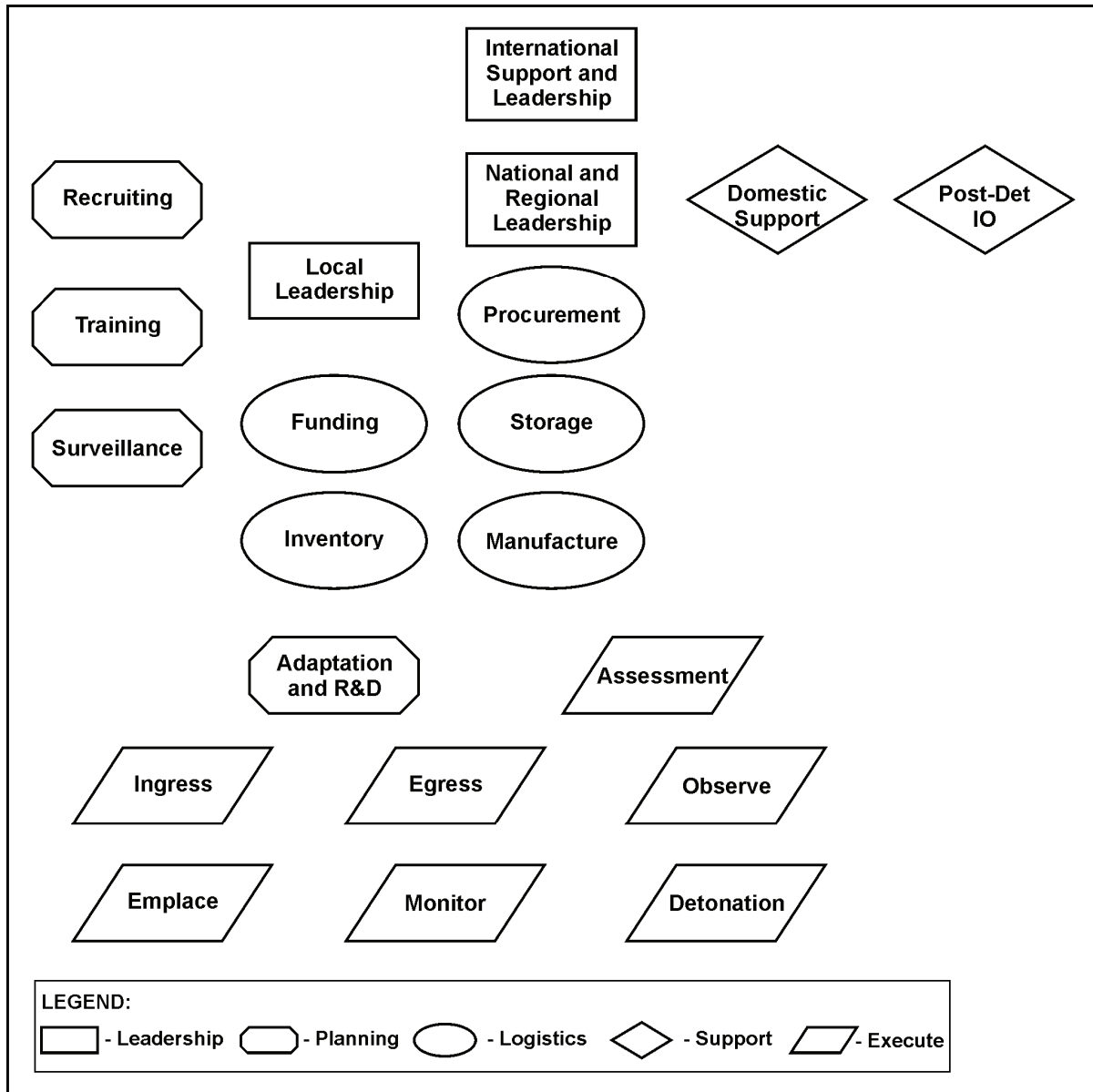


Figure 5-3. Example of nodes in a network



**Figure 5-4. Notional iconic representation of nodal component analysis by activity**

5-16. Once analysts have determined the functional nodes within an IED network, they can then begin to dissect the system even further by breaking down each of the functions into activities which take place within that functional node. Some possible nodes located in an IED network are discussed in table 5-1. This is by no means an all-inclusive list. It is not necessary for a network to contain each node listed. Conversely, there may also be networks that contain nodes not mentioned.

*Note.* It is imperative for the analyst to understand that each network will be structured differently.

Table 5-1. Possible nodes located in an improvised explosive device network

<b>When determining what type of activities may take place in the LEADERSHIP function, consider the following:</b>	
<b>International Support and Leadership</b>	Emir- or front commander-level leader of a country directing the political agenda, directing information operations (IO), directing funds to the nodes.
<b>Local Leadership</b>	Leadership of a cell that carries out processes contained in the other nodes. Facilitation of the factory to make improvised explosive devices (IEDs) includes training grounds, money transfers, and messengers. Target selection to produce the desired effects for the information campaign.
<b>National or Regional Leadership</b>	Emir- or front commander-level leader of a region directing the political agenda, directing IO, directing funds to the nodes. Knowledge of the local populations and terrain providing efficient use of resources. Local target type selection for the information campaign.
<b>When determining what type of activities may take place in the PLANNING function, consider the following:</b>	
<b>Adaptation/Research and Development</b>	Take ideas from the assessment node and try out the concepts. Research and development will include adapting to effective coalition force countermeasures.
<b>Recruiting</b>	People at all levels that recruit willingly or force coerced people into performing tasks in the other nodes. Looking for all skill levels. Finding and smuggling militants into the joint operations area who are willing to be messengers, emplaces, or suicide bombers.
<b>Surveillance</b>	Watching multinational and U.S. forces for target selection opportunities and viability of locations. Surveillance also verifies or denies timelines and friendly and enemy tactics, techniques, and procedures.
<b>Training</b>	Willing or coerced people are evaluated and trained to act in other nodes.
<b>When determining what type of activities may take place in the SUSTAINMENT function, consider the following:</b>	
<b>Inventory</b>	Storage and maintenance of completed IEDs while waiting for orders to ingress and emplace.
<b>Manufacture</b>	Bomb makers take raw materials from storage and construct the desired type of IED and deliver it to the inventory node.
<b>Funding</b>	Use of banks and other funding sources to purchase materials.
<b>Procurement</b>	Acquisition and production of bomb components, purchased or stolen. Local support directly related to construction, emplacement, detonation, and expertise on new bomb-making techniques.
<b>Storage</b>	Secure storage of components before they are used to build an IED.
<b>When determining what type of activities may take place in the EXECUTE function, consider the following:</b>	
<b>Assessment</b>	Use the cataloged effects collected in the observation node to quantify the performance of the device type. Generate ideas on how to make the device better and provide it to the adaptation or research and development node.
<b>Detonation</b>	Initiation of the IED using arming signals from monitoring node and fusing signals from victim. Output is the physical effect on the victim.
<b>Egress</b>	After detonation, or after friendly forces arrives, removal of evidence and personnel to a secure location. Movement post detonation of the personnel who carried out the detonation includes anyone who was there to observe the attack and report damage assessment.
<b>Emplace</b>	Burying or disguising the IED, running the wires for arming switches, placing the antenna, for reception from the monitoring point. For vehicle-borne IEDs, parking or driving the car next to the target. For suicide bomber, walking the IED to the target.

Table 5-1. Possible nodes located in an IED network (continued)

<b><i>Ingress</i></b>	Moving the IED from the inventory location to the detonation point using a secure transport mechanism and using care not to detonate IED.
<b><i>Monitor</i></b>	Observation of IED location from a secure vantage point. Output is the arming signal to the IED. Performed to keep the IED secure and protect assets until target is present.
<b><i>Observe</i></b>	Observation and cataloging of the effect on the target,—simply data collection, not assessment or analysis.
<b><i>When determining what type of activities may take place in the SUPPORT function, consider the following:</i></b>	
<b><i>Domestic Support</i></b>	Local populace support and supporting infrastructure that are involved with dual use items. Noncombatant support in the form of food, shelter, and water that supports activities in other nodes.
<b><i>Postdetonation IO</i></b>	Use of media images to engender support for international fundraising and local support. Any use of the media to lend support to the local threat. Use of speeches by international leaders, footage from recent attacks, or interviews with citizens.

5-17. As analysts begin to look at the network by its functional components, they must be cognizant of the different types of nodes within that network. Nodal component analysis attempts to break down a network into nodes where the same type of function is performed.

5-18. After the analyst determines which activities are taking place within the network being analyzed create a model using those activities. The activities can be depicted graphically using an iconic diagram or any similar type of diagramming tool to facilitate understanding. The functional analysis and the activity node model can be layered (or the information melded together) to show how the activities fit within the functional analysis scheme. Figure 5-5 utilizes shapes to depict the various functional areas. Color, if available, may also be used to distinguish between the functional areas. This figure also shows an example IED model annotated to show the type of commodities moving between the nodes.

5-19. Once the analyst has determined how the IED network is constructed, it is also important to understand how the various activity nodes interact with one another. The goal is to produce a model of the enemy IED operations that captures the processes present in the network. Intelligence briefs on enemy activity within each node should be analyzed to produce signatures and vulnerabilities. This mapping will produce a list of capability gaps that will be the basis for funding priorities.

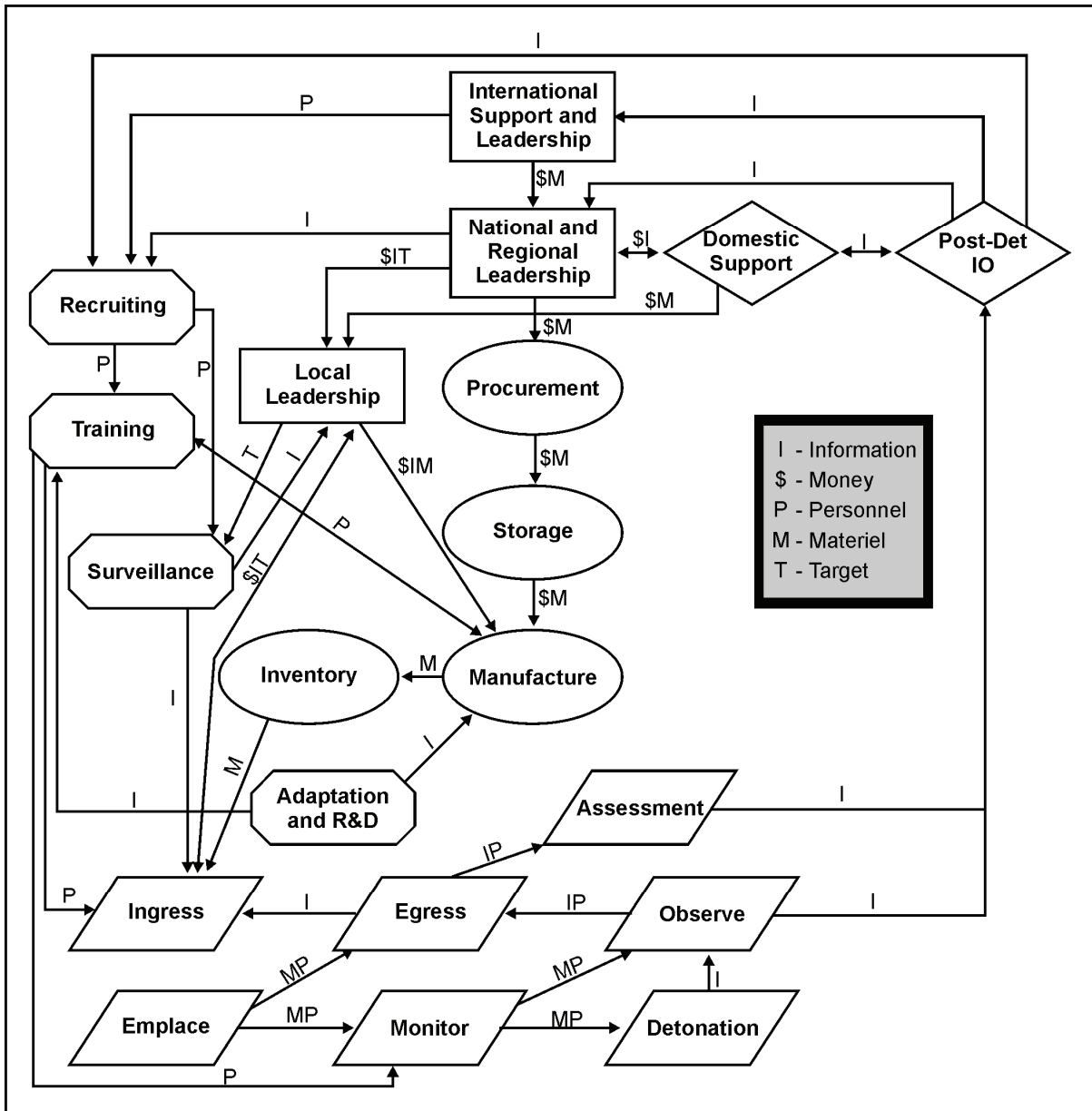


Figure 5-5. Example enemy IED network nodal diagram showing relationships

5-20. The nodes are processes that can operate independently of each other. The nodes take commodities as they become available, process them, and produce an output for the next node to use. Enemy networks are opportunistic and therefore operate asynchronously. The amount of synchronization between the nodes in figure 5-5 is purposely left out as a parameter to keep the model generic. For example, there may be enough volunteers for daily tasks that recruiting does not need to be active, but has to be ready to process volunteers when they show up, and direct them to the proper training locations. The timelines within nodes can vary greatly, from months in the leadership type nodes to minutes in the monitor and detonate nodes.

5-21. While all of this modeling may seem like a one-size-fits-all effort—and to some extent it is—by varying the levels of abstraction, the desired size of the same model can be produced for the current need. Once modeling has taken place, the result should assist in understanding a specific AO for a specific

snapshot in time. The models are constantly evolving and can be adapted by the analyst to assist in understanding any AO.

### TIME EVENT ANALYSIS

5-22. A time event chart is a method for placing and representing individual or group actions chronologically. It uses symbols to represent events, dates, and the flow of time. Normally, triangles are used to depict the beginning and end of the chart and may be used within the chart to indicate particularly critical events such as an ideological shift or change. Rectangles, used as events, store administrative data and indicate events or activities. An "X" through an event highlights a significant event or activity. Each symbol (event) contains a sequence number and date. An incident description is written below the event node providing a brief explanation of the incident. This explanation should include the size of the enemy force and the type of incident. Figure 5-6 is an example of a time event chart. Figure 5-7 shows a time event chart using Analyst Notebook.

5-23. By using these symbols and descriptions it is possible to analyze a group's activities, transitions, trends and operational patterns in both time and activity. If desired, the event nodes may be color coded to indicate a particular event or type of event to aid in pattern recognition. The time event chart also serves as a chronological record of an individual's or group's activities designed to store and display large amounts of information. The tool is easy to prepare, understand, and use. It is also an excellent briefing aid and flexible analytical tool. The time event chart is used most frequently both as part of a terrorist database and in preparation of threat assessments. Several automation tools, such as Analyst Notebook, may be used to create the time event chart.

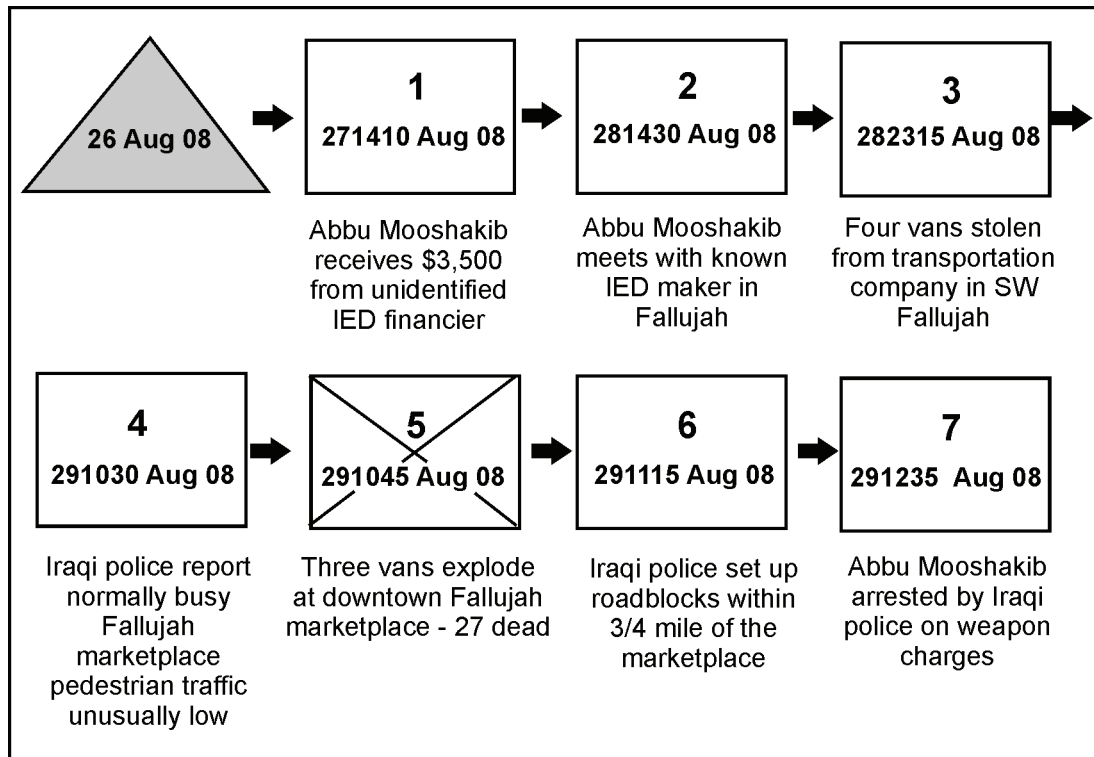


Figure 5-6. Sample time event chart



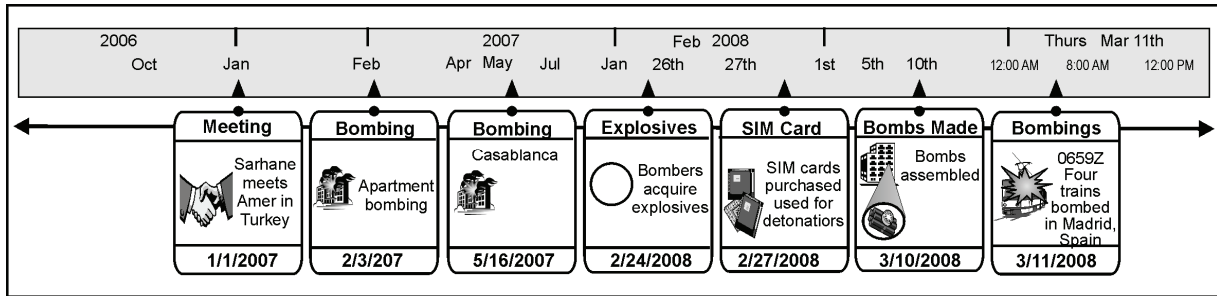


Figure 5-7. Example time event chart using Analyst Notebook software

## LINK ANALYSIS

5-24. Link analysis is the process of identifying and analyzing relationships between personnel, contacts, associations, events, activities, organizations, and networks to determine key or significant links. Analysts use link analysis to determine who is involved, how they are involved, and their significance concerning a particular situation. Some types of link analysis tools include—

- Association matrices.
- Activities matrices.
- Link diagrams.

5-25. Construction of a matrix is the easiest and simplest way to show the relationships between numbers of similar or dissimilar associated items. The items can be anything that is important to the analyst, such as people, places, organizations, automobile license plates, weapons, telephone numbers, or locations. In HUMINT analysis, matrices are often used to identify “who knows whom,” or “who has been where or done what” in a clear concise manner.

5-26. There are two types of matrices used in HUMINT analysis:

- The association matrix—used to determine existence of relationships between individual humans.
- The activities matrix—used to determine connectivity between individuals and any organization, event, address, activity, or any other nonpersonal entity.

5-27. The graphics involved in constructing the two types of matrices differ slightly, but the principles are identical.

## Association Matrix

5-28. A known association is determined by “direct contact” between individuals. Direct contact is determined by a number of factors, including but not limited to—

- Face-to-face meetings.
- Confirmed telephonic conversation between known parties.
- All members of a particular organizational cell.

---

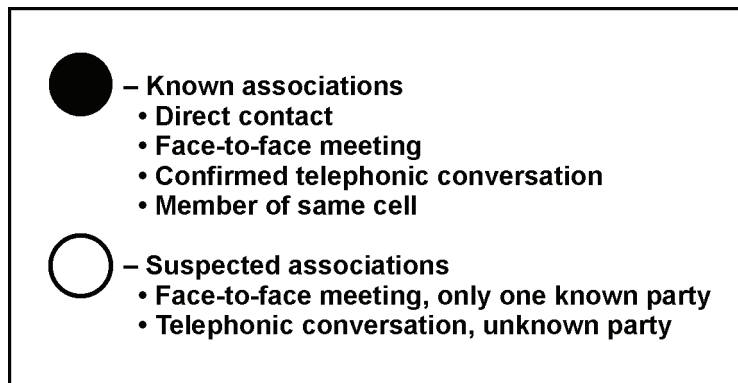
**Note.** An important point to remember about using the association matrix is that it will, without modification, show only the existence of relationships not the nature, degree, or duration of those relationships.

---

5-29. A known association between individuals is depicted on the matrix by a dot or filled-in circle. See figure 5-8 (page 5-12) for association matrix symbology. Suspected associations are depicted on the association matrix by an open circle. The rationale for depicting suspected associations is to get as close as

possible to an objective analytic solution while staying as close as possible to known or confirmed facts. If a suspected association is later confirmed, the appropriate adjustment may be made on the association matrix simply by filling in the open circle. A secondary reason for depicting suspected associations is that it may give the analyst a focus for requesting to task limited intelligence collections assets in order to confirm the suspected association. Suspected associations between persons of interest are considered to be associations which are possible or even probable, but cannot be confirmed using the above criteria. Examples might be—

- A known party calling a known telephone number (the analyst knows to whom the telephone number is listed) but it cannot be determined with certainty who answered the call.
- A face-to-face meeting where one party can be identified, but the other party can only be tentatively identified.



**Figure 5-8. Association matrix symbology**

5-30. The association matrix is constructed in the form of an equilateral triangle having the same number of rows and columns. Personalities must be listed in exactly the same order along both the rows and columns to ensure that all possible associations are correctly depicted. As shown in figure 5-9, an alternate recommended method is to list the names along the diagonal side of the matrix.

---

*Note.* In the event that a person of interest is or becomes deceased, a diamond is drawn next to his or her name on the matrix. The purpose of the association matrix is only to show the analyst who is associated with whom.

---

### Activities Matrix

5-31. The activities matrix determines connections between individuals and any organization, event, entity, address, activity, or anything other than persons. The activities matrix is a rectangular array of personalities compared against activities, locations, events, or other appropriate information. The kind and quantity of data that is available to the analyst determines the number of rows and columns and their content. The analyst may tailor the matrix to fit the needs of the problem at hand or may add to it as the problem expands in scope.

5-32. The activities matrix normally is constructed with personalities arranged in a vertical listing on the left side of the matrix with events, activities, organizations, addresses, or any other common denominator arranged along the bottom of the matrix. Figure 5-10 shows an example. The activities matrix is critical for the study of a group's internal and external activities, external ties and linkages, and even modus operandi.

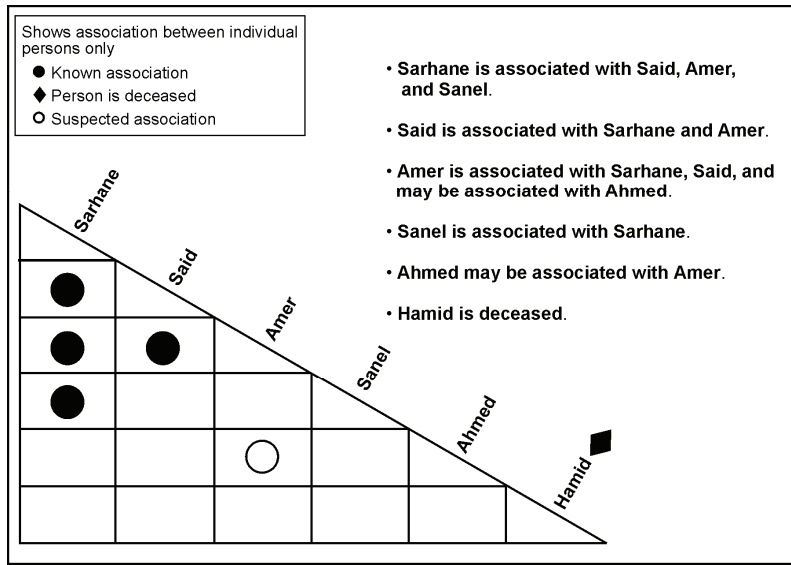


Figure 5-9. Association matrix example

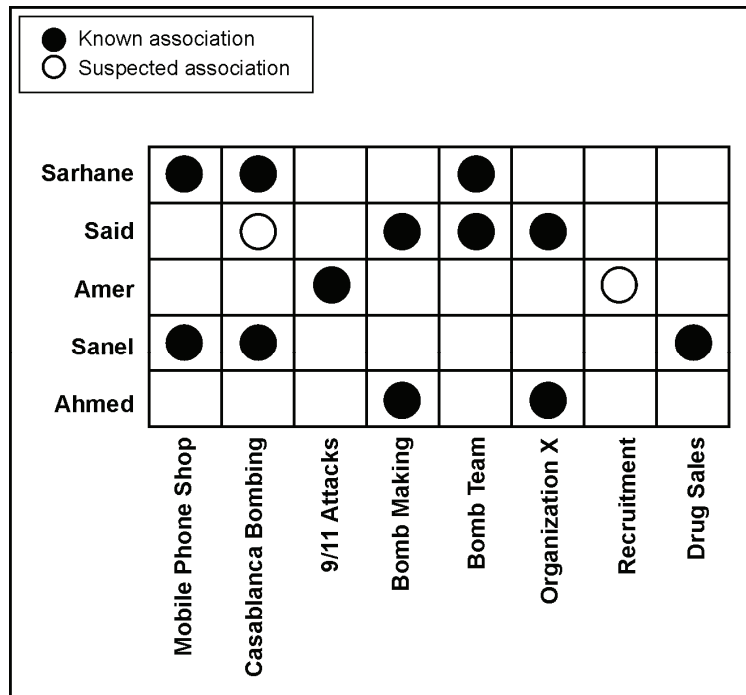


Figure 5-10. Activities matrix example

5-33. Similar to the association matrix, confirmed or “strong” associations between individuals and nonpersonal entities are shown with a solid circle or dot, while suspected or “weak” associations are illustrated by an open circle. Using matrices, the analyst can pinpoint the optimal targets for further intelligence collection, identify key personalities within an organization, and considerably increase the analyst’s understanding of an organization and its structure. Matrices can be used to present briefings,

evidence, or to store information in a concise and understandable manner within a database. Matrices do not replace standard reporting procedures or standard database files.

---

*Note.* It is possible, and sometimes productive, to use one matrix for all associations, personal and nonpersonal; this is done routinely using automated systems. However, when an analytical problem includes more than approximately fifty entities (persons and other things), experience has shown the use of one manual matrix to be extremely cumbersome and difficult to comprehend and manage.

---

## Link Diagram

5-34. The link diagram shows the connections between people, groups, or activities. The difference between matrices and link analysis is roughly the same as the difference between a mileage chart and a road map. The mileage chart (matrix) shows the connections between cities using numbers to represent travel distances. The map (link diagram) uses symbols that represent cities, locations, and roads to show how two or more locations are linked to each other.

5-35. Link diagrams can show organizations, membership within the organization, action teams or cells, or participants in an event. Construct the appropriate association matrices showing who knows whom, who participated in what, who went where, and who belongs to what group.

5-36. To create the link diagram, draw information from the database and intelligence reports and relationships from the matrices. Persons should be grouped into organizations or cells based on information about joint association, activities, or membership. Draw lines representing connections between individuals, organizations, or activities to complete the diagram. See figures 5-11, 5-12, and 5-13 for various degrees of link diagramming.

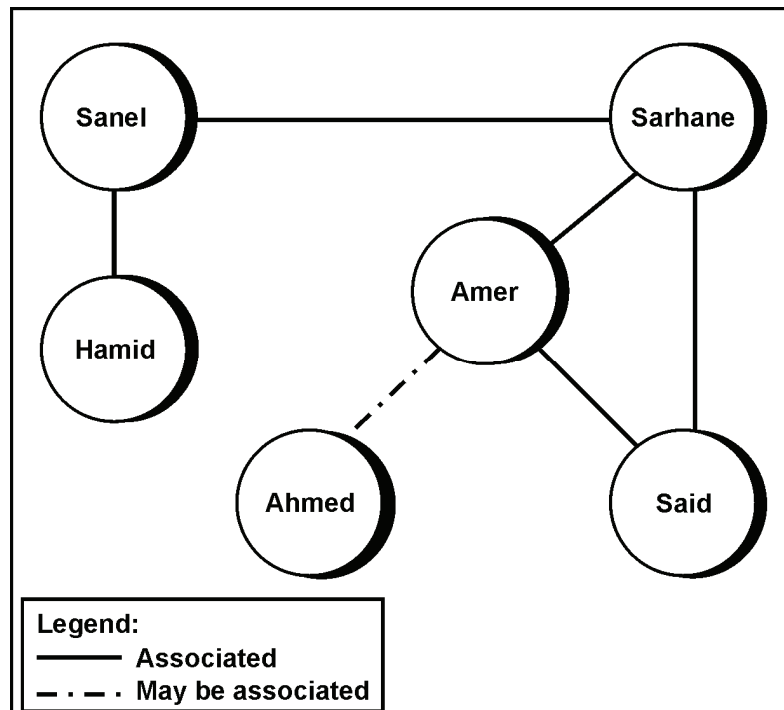


Figure 5-11. Link diagram concept

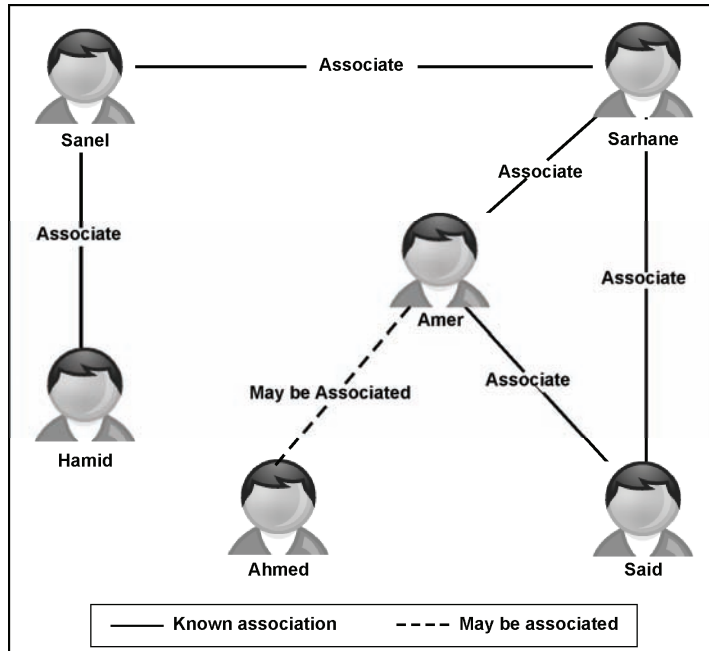


Figure 5-12. Example link diagram using Analyst Notebook

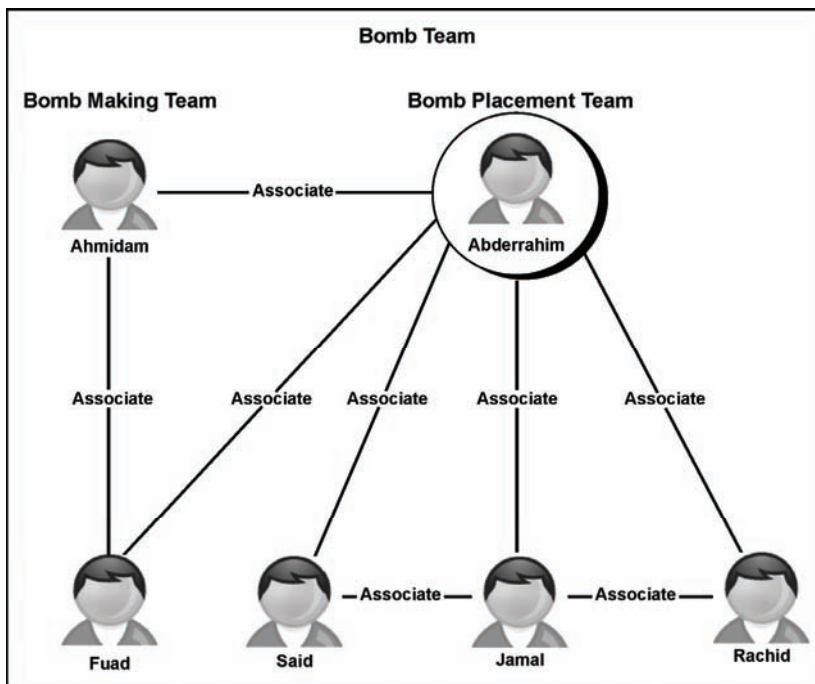


Figure 5-13. Link diagram example using Analyst Notebook software

5-37. Since each individual depicted on a link diagram is shown only once, and some individuals may belong to more than one organization or take part in more than one event, squares or rectangles

representing nonpersonal entities may overlap. Figures 5-14 and 5-15 are examples of Analyst Notebook link diagrams showing information from an activity matrix and nonpersonal relationship, respectively.

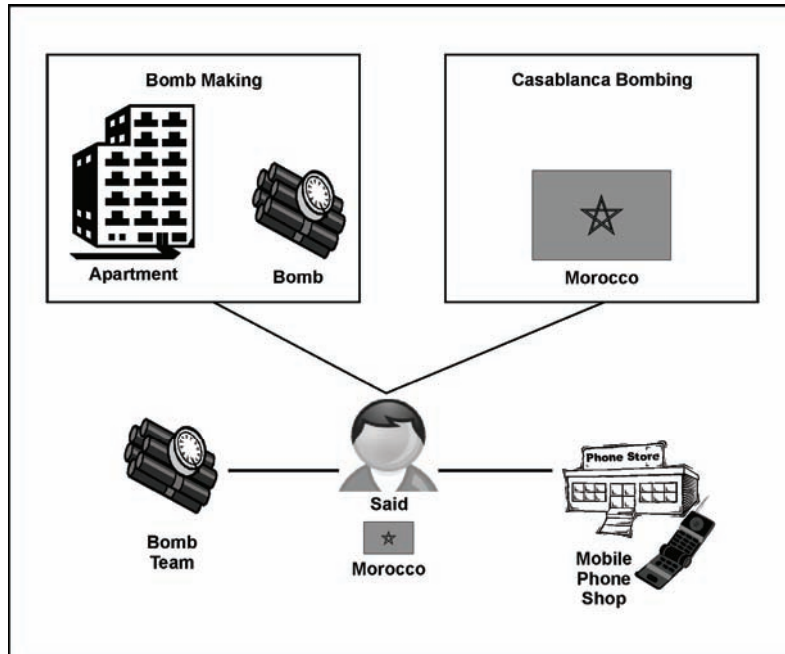


Figure 5-14. Analyst Notebook link diagram showing information from an activity matrix

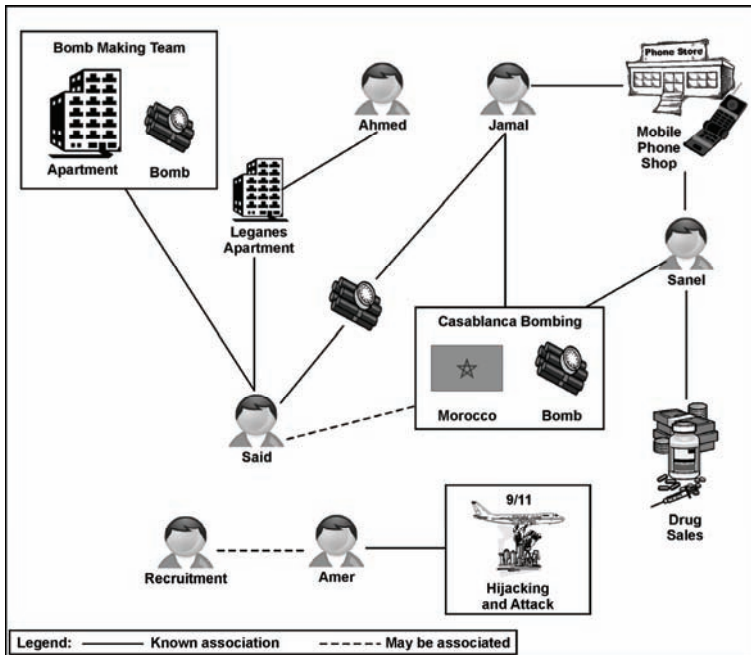


Figure 5-15. Analyst Notebook link diagram showing nonpersonal relationship

5-38. Another type of possible graphic depiction in Analyst Notebook combines link diagramming and the association matrix into a hierarchy layout. Figure 5-16 shows the hierarchy layout entities arranged into a tree structure to reveal hierarchical relationship and figure 5-17 shows a completed link diagram with supporting matrices.

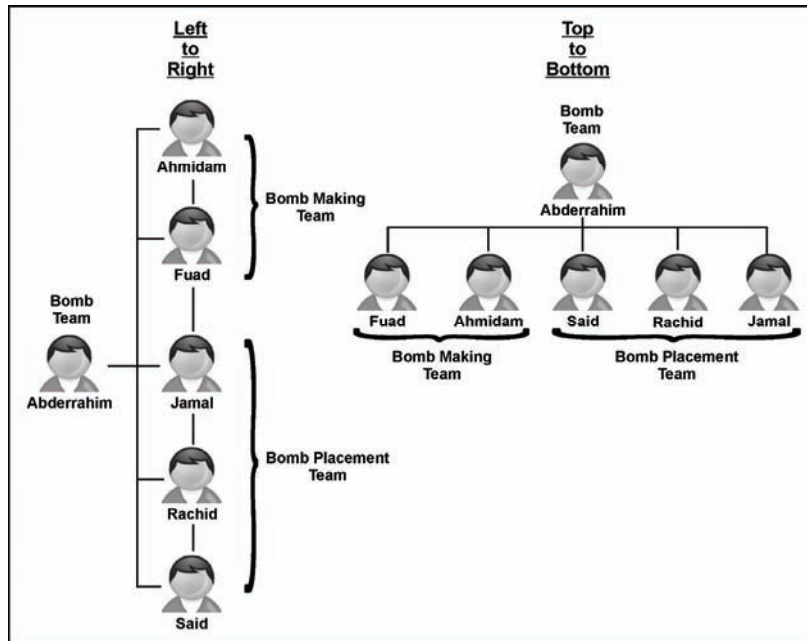


Figure 5-16. Analyst Notebook hierarchy layout

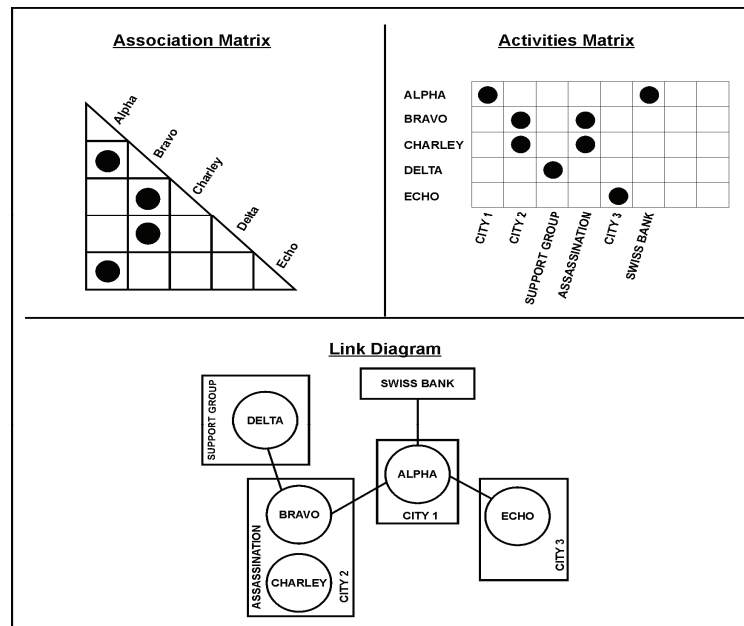


Figure 5-17. Completed link diagram with supporting matrices

## AUTOMATION SUPPORT TO INTELLIGENCE ANALYSIS

5-39. Modern automation and communications systems are vital to intelligence analysis. Real-time collaboration, detailed operational planning, and ISR integration, as well as enhanced collection and source exploitation tools, must support team efforts. Emerging technology continues to allow the entire intelligence analysis system to operate more effectively. Commanders must be prepared to supply their intelligence sections with the best possible technology and training not only to enhance collection but also to optimize the survivability of Soldiers.

5-40. Intelligence analysis automation uses common hardware and software solutions with a flexible interactive user interface to provide standardization of equipment and processes across all operational environments and conditions. Analysis automation systems must be deployable and scalable to fit the mission, or force package. System components must be capable of intelligence reach to support forward-deployed elements.

### ANALYTICAL AUTOMATION REQUIREMENTS

5-41. There is a requirement for a robust, web-based communications capability. DCGS-A will provide this ability. Web-based visual analytical tools allow maximum analyst participation and collaboration in the development of products geared to mission planning, targeting, and information analysis at all echelons.

5-42. Analytical products must be responsive to the special needs of a specific ISR operation, project, or element. DCGS-A is the Army's ISR ground processing system for all disciplines. It provides weather and terrain analysis support as well. DCGS-A is an integration of existing and new ISR system hardware and software that produces a common net-centric, modular, scalable, multisecurity, multidiscipline, interoperable ISR architecture to operations. DCGS-A provides access to data from tactical to national sensors across the Army Intelligence Enterprise as well as facilitates intelligence reach with collaboration capabilities for deployed elements.

### AUTOMATED ANALYSIS TOOLS

5-43. Automation of analytical tools, such as time event charts, association matrices, activity matrices, and link analysis diagrams dramatically increase predictive analysis capabilities. Automation permits more rapid access to more information which, upon further critical analysis, produces a more accurate and timely product. Automated analysis techniques, aided by virtual-viewing programs, allow the analyst to generate better battlefield visualization.

5-44. Automated analysis tools such as DCGS-A are linked to databases, include artificial intelligence programs and computer-assisted analytical programs, and reduce time required for analysis. These programs assist the analyst in developing predictions and identifying information gaps to support targeting and collection. Automation and web-based tools allow the analyst to—

- Track and cross-cue reports.
- Incorporate data extraction technology, retrieval, automated data organization, content analysis, and visualization.
- Share analytical decisions with other units and other analysts in real time.
- Apply multidimensional technologies, content analysis techniques, and web-based collaborations.
- Display analytical results and view operations in real time.
- Share resources such as models, queries, visualizations, map overlays, and tool outputs through a common interface.
- Apply clustering (a nonlinear search that compiles the results based upon search parameters) and rapid spatial graphical and geographic visualization tools to determine the meaning of large informational streams.



- Rapidly discover links, patterns, relationships, and trends in text to use in predictive analysis.
- Capture analytical conclusions and automatically transfer them to intelligence databases and systems.

## SEARCH ENGINES

5-45. Search engines provide access to previously collected or known information; they facilitate the development of comprehensive analytical and intelligence products, and avoid unnecessary collection tasking redundancy. A tool set for data visualization, search, and discovery is required, which is embedded with several software programs for manipulating data from multiple databases.

5-46. The types of modules in visualization packages should include search engines and knowledge discovery (semantic clustering) for unformatted data, applications for extracting and organizing formatted data, and data labeling. The package should also include a model-building tool to enable users to make their archives more efficient with respect to search, retrieval, and compatibility to other applications, as well as archiving and maintenance tools to support what will eventually become a large data warehouse. Search engines should be—

- Multilingual and able to query multiple classified and unclassified databases.
- Capable of developing, querying, and manipulating stored information.

## WEB-BASED REPORTING

5-47. Web-based reporting employs current Internet technology. It employs an interactive graphic interface, using client browser technology, search engines, hyperlinks, and intelligent software agents for searching, finding, viewing, and maintaining databases and supporting analytical work, data, and information flows. It supports collaborative analysis at multiple echelons through connectivity on the secure Internet protocol router network and Joint Worldwide Intelligence Communications System. The following pertains to web-based reporting:

- Web-based databases work with any computer hardware, operating system, or software.
- Firewalls and information access are controlled at each level with an approving systems administrator at each level conducting quality control through release authority procedures.
- Graphic user interface uses standard Army and Department of Defense report formats.
- Graphic user interface walks the user through a critical task, and is able to identify Army and Department of Defense reports as required. Reports must be Army and Department of Defense platform compatible, and transferable through and to their respective systems.
- Multimedia support applications for attaching, associating, and hyperlinking video, still photographs, voice, scanned objects, graphics, and maps to records and files.

5-48. Web-based reporting and web pages developed for specific products allow the user to—

- Leverage their effort and expertise against all requirements, not just the ones that must be met immediately.
- Identify timely intelligence gaps and the leads to fill those gaps.
- Ensure immediate analytical feedback on collector reports to—
  - Post questions directly to a web page to enable all operators to answer, or be cued to the specific request.
  - Identify or request clarification on questionable data for quality control.
- Fuse information from specific intelligence disciplines and create all-source intelligence as required.
- Focus collection teams supporting maneuver commanders' requirements more effectively.
- Immediately extract information for crisis reaction.

## DATABASES

5-49. Without databases information is difficult or impossible to retrieve quickly, especially under adverse conditions. Databases support many complex analytical functions and requirements, to include—

- Initial databases, which must include enemy, terrain, weather, and civil considerations.
- Mission deconfliction.
- Requests for information.
- Summary, report, and assessment preparation.
- Threat and friendly situation tracking.
- Targeting.

5-50. Databases that interact with other tools support predictive analysis, prepare graphic analytical products, and provide situational awareness down to unit commanders. These databases—

- Support time event charts, association matrices, link analysis, and other analytical tools.
- Require a designated systems administrator at each echelon. To ensure a high degree of integrity, the metadata must be verified for accuracy and completeness. Without accurate metadata, databases cannot be easily searched for their information.
- Allow operators, managers, and analysts to—
  - Compartment (protect) source-sensitive, operational database segments, files, records, and fields.
  - Create, update, and maintain databases from locally generated information.
  - Import complete or partial databases from larger, or peer databases.
  - Share databases between peers, subordinates, or higher with appropriate access authorization.
- Provide systematic processing and automated parsing, using intelligence operations standardized forms, into appropriate databases for information storing, sharing, retrieval, and analysis.
- Allow query functions for decision making, as well as operational and analytical support.
- Provide analytical programs able to correlate data that facilitate information retrieval from any data repository.
- Incorporate information retrieval functions, such as browsing, Boolean functions, key word searching, concepts, and similar functions.

## Appendix A

# Analytical Pitfalls

This section addresses the thought processes applied to the analysts' data, focusing specifically on the errors they may commit during the process. The errors, referred to as fallacies, are usually committed accidentally although sometimes they are deliberately used to persuade, convince, or deceive. There are two categories of logical fallacies—omission and assumption. This appendix will enable an analyst to recognize these fallacies and to avoid falling prey to them.

### FALLACIES OF OMISSION

A-1. Fallacies of omission leave out something important. The arguments may omit a consideration of many cases; they may omit a consideration of other hypotheses that would account for the same conclusion; or they may omit something unfavorable to a prevailing argument.

### OVERSIMPLIFICATION

A-2. Oversimplification is a generality that fails to adequately account for all the complex conditions under consideration. Oversimplification includes omitting facts, using generalities, and applying an inadequately qualified generalization to a specific case. Oversimplification results when considerations of all the complex conditions that give rise to a certain situation or condition are omitted.

#### Example

The M1A1 is the tank that won the Gulf War.

**Remarks:** The M1A1 tank was one of many weapons used during the Gulf War.

### HASTY GENERALIZATION

A-3. Hasty generalizations are conclusions drawn from samples that are too few or from samples that are not truly representative. Hasty generalization results when the conditions of sampling have not been met; that is, when the samples are nonrepresentative or too small.

#### Example

After receiving a single interrogation report from a front-line force in contact with a threat force, an intelligence analyst concluded and reported that the threat's morale was extremely low and that capitulation was only a matter of time.

**Remarks:** The analyst demonstrated the fallacy of hasty generalization because he based his conclusions on one report from a single source's point of view.

## FALSE CAUSE

A-4. A false cause is the fallacy committed when an argument assumes casual relationship without sufficient grounds.

### Example

An aircraft equipped with a new electronic attack pod was not fired on while flying over threat territory. It was concluded that, since the aircraft was not intercepted or fired upon, the countermeasures were extremely effective in suppressing threat electronic systems.

**Remarks:** The conclusion may or may not account for the aircraft's not being attacked. Other considerations include—

- The threat was collecting data on this new configuration.
- The threat recently moved several surface-to-air missile units and radars and did not want to reveal the new positions.

## FALLACIES OF ASSUMPTION

A-5. Fallacies of assumption relate to begging the question (also referred to as reasoning in a circle), stating hypotheses contrary to fact, and misusing analogies. All of these fallacies implicitly or explicitly involve assumptions. An assumption is a belief. Like all beliefs, an assumption may or may not be true.

## REPHRASING THE QUESTION

A-6. Rephrasing the question occurs when speakers assumes they are giving a legitimate response to a query when in fact they may be merely restating the question in different terms.

### Example

(Pilot to debriefing officer) "In response to your questions about whether or not all my bombs landed on target, I'd like to say that as soon as I completed my pass there were two tremendous secondary explosions."

**Remarks:** The fallacies in this response include the following:

- It did not answer the question.
- It shifted attention from the primary issue to a secondary one.
- The answer was not appropriate for the question asked.

## STATING HYPOTHESES CONTRARY TO FACT

A-7. A hypothesis contrary to fact is another type of fallacy involving faulty assumptions. This fallacy occurs when someone states decisively what would have happened had circumstances been different.

**Example**

"If we had not supported Castro in his revolutionary days, Cuba would be safe for democracy today."

**Remarks:** The weakness of the hypothesis-contrary-to-fact fallacy is that the assumption expressed in the statement cannot be verified.

**MISUSING ANALOGIES**

A-8. In the absence of other evidence, intelligence analysts may reason from analogy. When reasoning from analogy, an analyst assumes the object or event that is being analyzed is similar to the object or event in the analogy. As such, the strength of a conclusion drawn from analogy is proportional to the degree of similarity between two objects or two events. One of the more dangerous assumptions in reasoning from analogy is the notion that because objects, events, or situations are alike in certain aspects they are not necessarily alike in others.

**Example**

In 1942, Winston Churchill argued for an invasion of Sicily by stating that, "An attack against Sicily would be the first in a series of thrusts at the soft belly of the Axis."

**Remarks:** The error of analogy committed by Winston Churchill was in thinking that human characteristics could be attributed to a nonhuman entity.

A-9. Conclusions drawn from analogy are inappropriately used when they are accepted as evidence of proof. Often situations (objects or events) may be similar in certain aspects but not in others. When one generalizes indiscriminately from analogy to other situations, one commits the fallacy of misusing analogies. One way in which arguments can be weakened is by citing a counteranalogy. Like all analogies, a counteranalogy is only as good as the similarity between objects or events being compared. The most that can be said about the counteranalogy is that it points out weaknesses in the original analogy by citing other comparisons that can be made on the same basis. Reasoning by analogy can be extremely profitable, particularly when firsthand information is denied to the investigator and analyst.

**Example**

One reply that may have summed up American thoughts on Winston Churchill's ideas may have been, "What good does it do to strike at the belly of the Axis in Sicily, while the heart of the battle is in France?"

**Remarks:** Note that though a counteranalogy, the same error was made in thinking that human characteristics could be attributed to a nonhuman entity.

A-10. The fallacies discussed above all involve assumptions in some form or another. For example, in begging the question, speakers may assume they are responding to a query when in fact they are either reasoning in a circle or shifting attention from a primary issue to a secondary one. In the hypotheses contrary to fact fallacy, one assumes that if certain conditions prevailed, the outcome would have been different. The danger in this case is not so much the assumption as it is the decisiveness in which one asserts the results of what did not occur. "Poisoning the well" attempts to discount evidence before it is presented. The assumption here is that what is to be presented will be of little value; hence, discounting it in advance can save time. The last fallacy is related to the misuse of analogy. Analogies are misused when one assumes that because two objects or events are similar in certain respects, they will necessarily be similar in all respects. This is where people get the phrase, "You're comparing apples to oranges."

## MISUSE OF LANGUAGE

A-11. Asking leading questions and lifting statements out of context are two pitfalls that involve the misuse of language. Leading questions are questions used to elicit desired responses. Very often the response is intended to implicate the person responding to the query. Lifting statements out of context is a similar device for changing the meaning of a statement simply by removing it from the context in which the statement was made. These pitfalls are seldom committed accidentally.

## LIFTING STATEMENTS OUT OF CONTEXT

A-12. Lifting statements out of context is another pitfall demonstrating the improper use of language.

### Example

An analyst argues the position that key military figures of a certain South American country are about to take over the government. He cites a returning State Department official who recently visited the country. The man stated that “conditions are ripe for a coup d’etat in South America.” (The exact quotation was: “Conditions are always ripe for a coup d’etat in South America, but there is nothing to suggest that the situation today is any more critical than it was five years ago.”)

## BIASES

A-13. All perception is shaped by bias, which is part of the human experience. Every person perceives information differently through a prism of their own life’s experience. Bias is quick to form but is resistant to change. Bias also manipulates new information to suit preconceptions held by the person reviewing the data. The four main types of biases are cultural and social, organizational, personal, and cognitive.

## CULTURAL BIAS

A-14. As Americans, Army intelligence analysts see the world in a certain way. In reaching a decision they employ the values and standards analysts have been taught through childhood and into the military service. The analysts’ views, judgments, and decisions are all products of how and where that particular Soldier was reared and educated. This in turn implies a certain level of cultural bias on how things are evaluated and accomplished.

A-15. Analysts must be aware of and try to avoid the natural tendency to make assumptions and draw conclusions based on cultural and social biases. In a foreign land analysts often find that their own cultural bias interferes with their ability to think the way a threat commander might think or to give informed advice to policymakers on the reaction of foreign governments to American policy.

A-16. At the turn of the 20th century, Russia, the United States, and Great Britain demonstrated cultural bias in their dealings with Japan. For their part, the Japanese did the same with the Chinese and Koreans.

**Example**

Prior to the Russo-Japanese War (1904–1905) the Russians consistently stated that the Japanese not only were unable to fight (because of physical limitations) but also lacked the willpower to fight one of the great powers. To the surprise of the world, the Japanese quickly and easily defeated Russia.

Less than 40 years later the United States and Great Britain said much the same thing about Japan. A short time later both suffered operational defeat by the supposedly inferior Japanese at Pearl Harbor, Wake Island, the Philippines, Singapore, and Hong Kong.

**ORGANIZATIONAL BIAS**

A-17. Organizational bias is being less than objective in analysis due to direct or indirect pressure from the organization. There is often a tendency within an organization to be less than objective with analysis and assessments. Problems that may result from a subjective internal analysis include—

- The unconscious altering of judgment because of exposure to selective information and common viewpoints held among individuals.
- Deliberately altering a judgment to provide what the commander wants to hear.

**Example**

The American government exhibited organizational bias in its 1968 analysis of the Vietcong's ability to sustain combat operations in Vietnam. While the fact was that the Vietcong had been defeated on the battlefield and was no longer a cohesive fighting force, the U.S. military and government officials still thought they were a serious threat to U.S. objectives in Vietnam.

**PERSONAL BIAS**

A-18. Personal bias is closely related to organizational bias. Organizations consist of individuals and the ideas and attitudes of one leader who can profoundly influence organizations. Inserting a personal bias contrary to fact is often called “poisoning the well.”

**Example**

Despite the fact of a growing number of reports stating otherwise, General Douglas MacArthur told President Harry Truman that the Chinese would never cross the Yalu River and risk war with the United Nations.

**COGNITIVE BIASES**

A-19. Three major cognitive biases continue to plague intelligence analysts:

- Absence of evidence.
- Persistence of impressions based upon discredited evidence.
- Hindsight.

**Absence of Evidence**

A-20. Lack of information is by far the most common problem, especially in a tactical environment. This does not mean that analysts should be content with the information on hand. The intelligence mission is

designed to be a continuous process and focus should remain on priority targets. Analysts should not hold back information because it is not conclusive; it rarely is. The analyst should—

- Realize that often information is missing (an information gap).
- Identify areas where information is lacking and consider alternative hypotheses.
- Consider whether an information gap is normal in those areas or whether the absence of information is itself an indicator.

### **Persistence of Impressions Based on Discredited Evidence**

A-21. Another related problem reveals itself when analysts reason away information contrary to their favorite hypothesis. This does the commander a disservice. Analysts must be professional and capable of saying, “I was wrong.” The most glaring example of this type of thinking was probably shown during the failed Allied operations in Holland in 1944 when, in the face of information showing the presence of German armored formations, Operation Market-Garden was allowed to proceed.

### **Hindsight**

A-22. Three types of hindsight bias have been identified:

- Overseers of intelligence production tend to overestimate the degree to which events might have been foreseen.
- Analysts tend to overestimate the accuracy of their own past judgments.
- Intelligence consumers tend to underestimate the true value of intelligence analysis.

## **AVOID THE RUSH TO DECIDE**

A-23. The need for a quick answer often causes the analyst to be pressured to make an unsupported analytical judgment. To preclude such a situation, the analyst must rely on experience and maturity. Additionally, by adhering to the milestones, or battle rhythm associated with the section’s standing operating procedures, analysts will be able to follow a well-defined process that addresses all critical elements of analytical effort, a process which is not susceptible to the rush to decide.

A-24. Finally, the G-2/S-2 and the analyst should not be afraid to point out when there is insufficient data to make a judgment, or that the data does not support the expected hypothesis. On the other hand, analysts should not be afraid to make a determination when they have sufficient data supporting their conclusions. Commanders will refer to this decision as having a significant amount of firm facts with some solid assumptions that point to an analytical conclusion.

A-25. Upon completion of analysis, and prior to briefing the commander, the analyst must be prepared to answer the following questions:

- Who is the unit fighting?
- When will the engagement occur?
- Where will friendly forces most likely encounter the threat’s forces?
- What assets is the threat bringing to the fight (personnel and equipment)?
- How lethal are threat forces (strengths and limitations)?
- What is the threat’s center of gravity (prime assets)?
- How will the threat fight friendly forces (tactics and techniques)?

A-26. A hasty decision may result in mission failure or unnecessary injuries and loss of lives. A late decision may also carry the same results; therefore, analysts must train and practice to achieve a level of proficiency that enables them to find balance. Information is only considered intelligence if it is timely, relevant, accurate, predictive, precise, usable, reliable, and complete. If analysts make a hasty decision without determining that the information meets all of the above requirements, their decision may be more detrimental than useful to the mission.



## Appendix B

# The Intelligence Running Estimate

This appendix provides the analyst information about the intelligence running estimate. Intelligence analysts must be familiar with these reports since they are used for analysis, either as input to the analytical process or as an output or product of analysis. For a detailed explanation of the orders process, see FM 5-0 and FM 6-0.

B-1. The intelligence running estimate is a logical and orderly examination of the intelligence factors affecting mission accomplishment. It provides commanders with a basis for planning operations and for disseminating intelligence to their staffs and to other headquarters. It consists of five paragraphs, which outline an analysis of the AO, enemy strength, and enemy capabilities that can influence the mission. It may be presented to the commander formally or informally and may be written or oral, detailed or summarized. However, when possible, a written estimate is preferred.

B-2. The intelligence staff officer prepares the intelligence running estimate of the enemy situation. An estimate is prepared at the commander's direction or on the intelligence staff officer's initiative. It is updated as required upon changes in the enemy situation, terrain, weather, and civil considerations. The intelligence running estimate includes—

- Mission.
- AO.
- Enemy situation.
- Enemy capabilities.
- Conclusions.

B-3. Figure B-1 (page B-2) provides an annotated intelligence running estimate. G-2/S-2 staff officers, noncommissioned officers, and analysts must consider the time available to complete the estimate. Most estimates are written during the MDMP, but estimates must be prepared for each new mission the command undertakes. The estimate may not include each element shown in the sample, but should be as complete as time permits. As new information is developed or received, the estimate must be updated in order to incorporate that information. Intelligence update reports or briefings can be used for a short time, but eventually those update reports must be included in the intelligence running estimate.

INTELLIGENCE RUNNING ESTIMATE (CLASSIFICATION)	
<b>Headquarters</b>	
<b>Place</b>	
<b>Date, time, and zone</b>	
INTELLIGENCE RUNNING ESTIMATE NO. ____	
<b>References:</b> Maps, charts, or other documents.	
<b>1. MISSION.</b>	
The unit's mission determined by the commander.	
<b>2. AREA OF OPERATIONS (IPB step 1).</b>	
State the unit's area of operation (AO) and established area of interest. Both physical and human geography must be taken into account. Consider tribal lines, family lines, cultural lines, economic lines, as well as physical lines such as roads and bodies of water. Cross-border ties may allow insurgents safe haven outside their country and aid in smuggling across the border. Information in this paragraph is based upon the facts and conclusions of intelligence preparation of the battlefield (IPB) and the analysis of the AO.	
<b>a. Terrain (IPB step 2).</b>	
(1) <b>Existing situation.</b> Terrain analysis observation and fields of fire, avenue of approach, key terrain, obstacles, concealment and cover [OAKOC]), analyzing the physical geography (natural and manmade features). In counterinsurgency (COIN) operations, emphasize complex terrain, suburban and urban terrain, key infrastructures, and lines of communication (LOCs). Complex terrain is multifaceted, with physical, social (human), and informational dimensions. Include as much information as necessary for an understanding of OAKOC. Geospatial engineer elements conduct a major portion of the terrain analysis. Geospatial overlay products include vegetation (tree spacing and trunk diameter), surface drainage (stream width, depth, velocity, bank slope, and height), surface materials (soil types and conditions that affect mobility), surface configuration (slopes that affect mobility), obstacles (natural and manmade—consider obstacles to flight as well as ground mobility), transportation systems (bridge classifications and road characteristics such as curve radius, slopes, and width), and effects of actual or projected weather such as heavy precipitation or snow cover.	
Analyze the military aspects of terrain (OAKOC). <b>Observation and fields of fire:</b> Evaluating observation and fields of fire allow you to identify fire sacks and kill zones, ambush sites, engagement areas, battle positions, and defensible terrain. Identify specific system or equipment positions and areas where maneuvering forces are most vulnerable to observation and fires. Include both visual or with the use of surveillance devices, include electronic and optical line of sight. Include friendly and enemy systems such as weapon sights, laser range finders, radars, radios, and jammers. Identify observation posts and listening posts, areas of visual dead space. <b>Avenues of approach:</b> An air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. Include air and ground routes (and mobility corridors), to assist in development of named areas of interest and target areas of interest (TAIs), infiltration routes, and exfiltration routes; <b>Key terrain:</b> For enemy and friendly units—tall structures, choke points, intersections, bridges, industrial complexes.	

Figure B-1. Annotated intelligence running estimate format

In COIN, the people of the area are always key terrain. **Obstacles:** Manmade or natural terrain that stops, impedes, or diverts military movement. Examples include cant and slope, intervening crests, rivers, lakes, forests, deserts, swamps, jungles, built-up areas, densely populated areas, buildings, road craters, minefields, and trenches. Obstacles to air mobility include features that exceed the aircraft's service ceiling restrict nap-of-the-earth flight or that force the aircraft to employ a particular flight profile, and obstacles that affect the aircraft landing zone and drop zone. Examples are tall trees, towers, power lines, buildings, rapidly rising terrain features, mountains, and smoke or other obscurants. **Cover and Concealment:** Cover examples from direct and indirect fires include ditches, caves, river banks, folds in the ground, ridges, fingers, forested and built-up areas, shell craters, buildings, walls, and embankments. Concealment examples include woods, underbrush, snowdrifts, tall grass, and cultivated vegetation. The evaluation of cover and concealment aids in identifying defensible terrain, possible approach routes, assembly areas, deployment and dispersal areas, ambush sites or positions, specific system or equipment locations, and battle positions.

Use graphic representations and overlays. Use annexes for detailed material. Include effects of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) and enhanced conventional weapons fires, and any other pertinent considerations on each of these factors as appropriate.

(2) **Effect on enemy operations and broad COAs.** Describe the effects of terrain on enemy operations and broad COAs. State how it favors or disfavors enemy operations. Include how the terrain affects the threat's use of CBRNE weapons, and any special methods, techniques, equipment, procedures, or forces the threat may have.

(3) **Effect on own operations and broad COAs.** Describe in the same manner as for (2) above, except exclude the friendly use of biological agents.

#### **b. Civil Considerations.**

(1) **Existing situation.** Civil Considerations (ASCOPE) are analyzed for all types of military operations. Civil considerations of the environment can either help or hinder friendly personnel and mission, as well as the threat's personnel and mission. Understanding the impact on military operations better prepares the commander and staff, and enhances situational awareness and situational understanding. Analyze civil considerations using the acronym ASCOPE: Areas, Structures, Capabilities, Organizations, People, Events. Use templates and overlays to graphically depict civil considerations areas analyzed.

(a) **Areas.** Analyze the localities and aspects of the terrain that are not normally militarily significant to determine key civilian areas. Analyze the key civilian areas to determine how military operations affect these areas, and how these areas affect military operations. Examples of key civilian areas are (1) Boundaries, (for example, political precincts and districts, districts within a city, or municipalities within a region; boundaries for social, religious, or criminal enclaves; (2) Government centers; (3) Commercial zones (for example, agricultural regions, mining regions, trade routes; (4) LOCs (for example, street patterns, urban patterns, subterranean passages and underlying terrain; and (5) Possible sites for military applications (for example, temporary settlement of displaced civilian camps or other civil functions).

(b) **Structures.** Structures include (1) high-value targets (HVTs) or HPTs (for example, bridges, communication towers, power plants, dams; (2) cultural sites protected by international law or other agreement (for example, churches, temples, mosques, national libraries, and hospitals; (3) Structures that have practical applications which can support military operations (for example, jails, warehouses, television and radio stations, and print plants).

**Figure B-1. Annotated intelligence running estimate format (continued)**

(c) **Capabilities.** Host nation (HN), aggressor nation or some other body's ability to provide key functions or services to save, sustain, or enhance life (in that priority). Examples include emergency services, fire and rescue, food, water supply, fuel, electric power stations, communication facilities, health services, public works and utilities, public safety, public health, public administration, economics, commerce, and technology. Also include resources and services that can be contracted to support the military. Examples include interpreters, laundry services, construction materials, and equipment.

(d) **Organizations.** Nonmilitary groups or institutions in the AO that interact with and influence the populace and the force. Indigenous examples include church groups, fraternal organizations, patriotic or service organizations, labor unions, criminal organizations, and community watch groups. Groups from outside the area include corporations, United Nations agencies, U.S. governmental agencies, and NGOs, such as the International Red Cross/Red Crescent. Include information on their activities, capabilities, and limitations, how their activities affect military operations, and vice versa.

(e) **People.** Civilians within or outside the AO whose actions, opinions, or influence can affect the mission, either positively, negatively, or neutrally. Analyze and identify by their capabilities, needs, and intentions. Consider historical, cultural, ethnic, political, economic, humanitarian factors, key communicators, formal and informal influences. Examples to include are history of the area and how it influences the insurgency, events leading or contributing to the insurgency; tribal, clan, or familial groups and their geographic location and their influences; religious groups, their geographic location, and their influences; ethnic groups, their geographic location and their influences; languages spoken; key people who influence the society, their affiliations and loyalties, and their interrelations with other people; public perceptions of the insurgency; points of agreement or disagreement with insurgent ideology or ideologies; major industries and sources of employment; communication links to other regions; and media influence on local populace.

(f) **Events.** Events are routine, cyclical, planned, or spontaneous activities that significantly affect people, organizations, or military operations. Examples include national and religious holidays, agricultural crop or livestock and market cycles, elections, civil disturbances, and celebrations. Examples of spontaneous events include disasters from natural, manmade, or technological sources. These events create civil hardship and require emergency responses. Also include events precipitated by military forces. Examples include combat operations, deployments, redeployments, and paydays. Once significant events are determined, template and analyze the events for their political, economic, psychological, environmental, and legal implications.

(2) **Effect on enemy operations and broad COAs.** Describe the civil considerations effects on enemy operations and broad COAs. State how it favors or disfavors enemy operations. Also include how the threat's use of CBRNE weapons, any special methods, techniques, equipment, procedures, or forces affects civil considerations and vice versa. Use templates and overlays.

(3) **Effect on own operations and broad COAs.** Describe in the same manner as for (2) above, except exclude the friendly use of biological agents.

**c. Weather.**

(1) **Existing situation.** The main portion of weather analysis is conducted by the Air Force staff weather officer. Using geospatial intelligence (GEOINT) principles and techniques, the engineer detachment works closely with the staff weather officer to ensure the terrain analysis incorporates the effects of current and projected weather, thus enhancing automated support of the terrain analysis process.

Figure B-1. Annotated intelligence running estimate format (continued)

Include climate, current weather report, and weather forecasts on the overall environment. Evaluation of the military aspect of weather includes visibility, winds, precipitation, cloud cover, temperature, and humidity. The analysis focus is on the effects of weather on military operations rather than on the factors that make up the analysis. Include thermal crossover, a natural phenomenon which normally occurs twice daily when temperature conditions are such that there is a loss of thermal contrast between two adjacent objects. Include light data for the period of time of military operations. Use appendixes for detailed information.

(2) **Effects on the mission variables (METT-TC).** Describe how the weather favors or disfavors mission, enemy, terrain and weather, troops and support available, time available, and civil considerations.

**d. Other Characteristics.** When applicable, include other characteristics not covered above. Analyze using the same subheadings (existing situation, effect on enemy operations, effect on own operations and COA). Examples of other characteristics may include wildlife or diseases.

### 3. ENEMY SITUATION.

This paragraph gives information on the enemy, which will permit later development of their capabilities and vulnerabilities, and refinement of these capabilities into specific COAs and their relative probability of adoption.

#### a. Composition.

**In conventional operations:** Summary of threat characteristics that can influence accomplishment of the mission. Include state and unit organization. Special mention is made of electronic warfare (EW), special operations forces (SOF), and CBRNE, as appropriate. **In COIN operations:** Key influential people; political cadre, cells, organization; command and control staff (internal and external), intelligence cells, attack teams and operation cells, finance (internal and external), logistic and support cells, external ties; and, as required, religious organization; ethnic organization; tribal organization; and family organization. Special mention is made of EW, SOF, and chemical, biological, radiological, nuclear, as appropriate. Reference other documents, as required.

#### b. Disposition.

**In conventional operations:** Geographic location of threat elements and how they are deployed or employed. Include recent, current, and projected movements. Reference overlays, situation maps (SITMAPs), previously published documents. **In COIN operations:** Areas of control (religious, ethnic, tribal, political, or familial demographics and neighborhoods), command and control locations, safe houses, front organizations, training camps, and sustainment and support locations.

#### c. Strength.

**In conventional operations:** Committed forces, reinforcements, air, and CBRNE weapons. The preponderance of strength or lack thereof affects the raising or lowering of the analyst's estimate of the enemy capabilities and vulnerabilities in paragraph 5. Information concerning strength provides an indication of threat capabilities and helps determine the enemy probable COAs or options open or closed.

(1) **Committed forces.** Include ground maneuver units currently in contact and those ground maneuver units with which imminent contact can be expected, regardless of the specific friendly COA, location, controlling headquarters, and doctrine. The intelligence officer usually accounts for committed forces based upon the size of unit doctrinally used to oppose the friendly unit. Generally, enemy units are

Figure B-1. Annotated intelligence running estimate format (continued)

counted in terms of units two echelons below the friendly unit's size. (For example, a brigade S-2 normally considers committed forces in terms of companies, a division G-2 in terms of battalions, and a corps G-2 in terms of regiments or brigades.) If there is doubt whether a unit is a committed force or a reinforcement, it is considered a reinforcement. This attributes to the enemy the maximum capability to reinforce forces to oppose a given friendly COA.

(2) **Reinforcements.** Include designation and location. Reinforcements are those enemy maneuver units that may or may not be employed against friendly forces, depending upon our specific choice of a COA and upon enemy plans. Reinforcements are enemy units not committed in or out of the friendly sector, but which can react to the friendly COA, subject to time and distance considerations, in time to influence the accomplishment of the mission. Imminent contact is not expected. Disposition, location, level of control, or other factors at the time of the estimate are considered in determining which enemy forces are reinforcements.

(3) **Air.** List the number of enemy aircraft by type within operational radius; if known, include the number of possible sorties per day by type of aircraft.

(4) **CBRNE weapons and agents.** Estimate, as appropriate, the number, type, yield, and the delivery means of enemy CBRNE weapons or agents available to the enemy.

**In COIN operations:** Generating popular support is the center of gravity of the insurgency. Insurgent strength is measured largely by how much popular support the insurgency has. As the insurgent group gains in support, its capabilities grow, which in turn enable it to gain more support. Popular support results in safe havens, freedom of movement, logistic support, financial support, intelligence, and new personnel for the insurgency. A gain in support for the insurgents is a loss for the government, and a loss of support for the government is a gain for the insurgents. Evaluate and list the following:

(a) Level of popular support to the insurgency relative to the government includes regional, national, international support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving sustainment, or just withholding information. Include information on the areas they control (religious, ethnic, tribal, political organization, demographics, and neighborhoods).

(b) Forms of popular support the insurgents receive may include safe havens, freedom of movement, logistic support, financial support (internal and external), intelligence, and recruitment for the threat.

(c) Sources of popular support by type (active, passive, internal, external).

(d) Segments of populace supporting the insurgency.

(e) Foreign government support may come from a variety of venues; for example, influential figures pronouncing support; training facilities or safe houses; recruitment, financial support; and providing safe passage across national or international borders. The insurgency may also receive sustainment from national and international countries.

(f) NGO support.

(g) Criminal network support.

(h) Other sources of support.

(i) Methods used to generate popular support and their effectiveness.

(j) Grievance (real or perceived) exploited by insurgents.

(k) Capabilities and vulnerabilities in generating popular support.

Figure B-1. Annotated intelligence running estimate format (continued)

(l) Attack teams and operation cells.

(m) Recruitment.

**d. Tactics and Training.** In conventional and COIN operations list strategy, methods of operations, and doctrine, tactics, and training or other information of interest that provide a basis for analysis to determine relative probability of adoption of specific COAs and to determine enemy vulnerabilities. Enemy failure to take expected action is listed, as well as positive information. In COIN operations, tactics also involve political, military, psychological, and economic considerations. Tactics may include assassinations, arson, bombings, hostage taking, kidnapping, hijacking, seizure, raids, sabotage, denial and deception, hoaxes; use technology to destroy key elements of the national infrastructure—transportation, telecommunications, energy, banking, public health, and water supply; and use CBRNE.

**e. Sustainment.** Analysts can more accurately evaluate the enemy capabilities, strengths, and combat effectiveness with knowledge of the enemy’s sustainment and support structure. The enemy’s adoption of a COA depends on the logistic system to support the action. In conventional operations include procurement, maintenance, distribution, and replacement of all types of material including transport of personnel. In COIN operations, sustainment may include weapons and ammunition, IED and bomb-making components, food, water, propaganda equipment and materials, medical, transportation, and finance. Finance is who is providing the threat with financial support, how the money is transferred, and which financial institutions the enemy uses.

**f. Operational Effectiveness.** Operational effectiveness studies the threat morale, weapons effectiveness, equipment readiness, leadership, and personnel. Strength must be tied to the operational effectiveness, but is important enough to have its own mention earlier in the estimate. Conventional weapons, such as artillery ranges, should be addressed here.

**g. Intelligence.** Estimate the enemy’s intelligence collection capability. Include how threat picks and evaluates a target; method of ISR; ISR success, ISR vulnerabilities, or ISR susceptibility to deception and detection. HUMINT, IMINT (including threat use of commercial software) and EW capabilities must be addressed if known. How the threat passes intelligence information—radio, cell phone, electronic message—and how it can be interdicted.

**h. Communications.** Evaluate and list enemy’s communication modes may include high-frequency short wave, cell phone, Internet, mail, courier, face-to-face, citizen band, or amateur radio sets or the drop system.

**i. Other.** Use the threat characteristics listed in chapter 3 and include any other factors necessary for creating as thorough a picture of the threat as possible.

**4. ENEMY CAPABILITIES.**

Based upon all the previous information and analyses, develop and list enemy capabilities and limitations. A capabilities listing provides a basis for analyzing the available information. It shows those capabilities the enemy can adopt as specific COAs and their relative probability of adoption.

**In COIN operations:** The listing should show the task and purpose.

**In conventional operations:**

**a. State enemy’s capabilities.** State what, where, when, and in what strength for each capability.

**b. State enemy’s limitations.** Discuss each limitation, the cause and effect.

Figure B-1. Annotated intelligence running estimate format (continued)

**c. Analysis and Discussion.** Discuss each capability (or appropriate combination of capabilities) in a separate subparagraph, and any effects of the terrain, civil considerations, and weather may have on each capability. This will provide a basis for conclusions of enemy capabilities and their relative probability of adoption. Include consideration of enemy deception measures. All the previous pertinent information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious, or if there is no evidence that the enemy will adopt the capability, unless the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

**In COIN operations.** Evaluation of the threat in COIN operations must begin early and cover a wide range of factors in building an accurate threat model. Based upon all the information and analysis, develop and list enemy capabilities. First, evaluate the following characteristics of the insurgency as a basis for evaluating the enemy COA.

**a. Insurgent goals.** Does the threat desire a different social or political organization than that which exists under current conditions? How will they conduct operations towards that goal?

**b. Insurgent motivations.** Are they motivated by ideological, religious, or monetary?

**c. Popular support.** Include regional, national, and international.

**d. Key leaders and personalities.** Key influential people (political, ideological, religious, military) and key members who bring expertise (demolition special weapons, assassinations, specialized trainers) staff members, family members, and informal leaders.

**e. Organization.**

**f. Morale of the leaders and members.**

g. Then, evaluate the enemy's capability to conduct operations. This should tie in with operational effectiveness (paragraph 3f above). State each capability as a task and purpose. State what, where, when, and in what strength for each task. State enemy's limitations and vulnerabilities. Include the cause and effect of the limitation. Evaluate the following capabilities of the insurgency as a basis for evaluating the threat COA:

(1) Conduct violent activities (for example, murder, assassination, arson, bombing, hostage taking, kidnapping, hijacking, seizure, and raids).

(2) Conduct other operations (for example, sabotage, denial and deception, hoaxes, and use of technology).

(3) Conduct intelligence operations.

(4) Conduct training.

(5) Conduct sustainment and supply activities.

(6) Conduct information activities.

(7) Conduct political activities.

(8) Conduct recruitment.

h. Analysis and Discussion. Discuss each capability (or appropriate combination of capabilities). In a separate subparagraph, include any effects of the terrain, civil considerations, and weather may have on

**Figure B-1. Annotated intelligence running estimate format (continued)**



each capability. This will provide a basis for conclusions of enemy capabilities and their relative probability of adoption. Include consideration of enemy deception measures. All the previous pertinent information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious, or if there is no evidence that the enemy will adopt the capability, unless the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

**5. CONCLUSIONS.**

Based upon all the previous information and analysis, state conclusions concerning the total effects of the AO on threat operations. List all possible enemy COAs in the order of probability of adoption. Include enemy vulnerabilities that can be exploited. State which COAs are considered most likely and those that are the most dangerous COAs. This will assist the commander and staff in selecting friendly COA during wargaming.

a. Probable enemy COAs. List COAs in order of relative probability of adoption. A listed COA may include several subordinate COAs that can be executed concurrently. Usually, no more than two or three COAs, in order of probability of adoption, can be justified by the available evidence. The G-2/S-2 should identify which COA is most likely and which is most dangerous at a minimum.

b. Enemy vulnerabilities. List the enemy peculiarities and weaknesses that result in vulnerabilities which are exploitable at own, higher, or lower levels of command.

c. Intelligence consideration on operations. Indicate whether the mission set forth in paragraph 1 above can be supported from the intelligence standpoint. Indicate which COAs can best be supported.

ACKNOWLEDGE: [Designated staff officer's last name]

[Designation of staff officer]

OFFICIAL:

[Authenticator's Name]

[Authenticator's Position]

(CLASSIFICATION)

Figure B-1. Annotated intelligence running estimate format (continued)

**This page intentionally left blank.**

## Appendix C

# Indicators

This appendix provides intelligence analysts information concerning the indications of certain enemy actions. The events and their possible meaning described will assist in developing the ISR synchronization plan during collection planning. As ISR assets identify certain activities analysts can refer to the tables herein to understand their possible meaning. As with all intelligence operations and this circular, these lists are not all-inclusive.

C-1. An indicator is positive or negative evidence of a specific threat activity or evidence of measurable characteristics of the operational environment that denote actions of the civilian populace. Indicators may be envisioned through logical deduction or from previous actions from the threat or populace.

C-2. Indicators are discernable physical, operational, or technical features. Indicators may also include discernable ideological and rhetorical trends and beliefs, especially in the measurement of perceptions and attitudes and the support of information operations. This appendix is not meant to be an all-inclusive listing on possible indicators; it merely gives examples of some possible indicators. Based upon the supported unit's AO, analysts will have to specify what indicators are most or least important and probably have to specify their own. These examples should give the analyst a starting point to begin development of specific indicators applicable to their particular operation or environment.

C-3. Given the wide range of stability operations and civil support operations, the possible indicators of various activities can be enormous. However, most stability operation and civil support operation evolutions still involve the requirement to identify risks to friendly forces.

C-4. Asymmetric indicators are difficult to acquire because many threat forces rely on low-tech capabilities, covert methods, standoff attacks, and close-combat avoidance. Asymmetric indicators derive from incidents such as—

- Bombings, ambushes, or other attacks.
- Kidnappings.
- Capture or killing of militants.
- Seizure of arms.
- Other incidents.

C-5. By their nature, these operations generally concern indigenous populations, regardless of the nature of the mission. The following indicators focus on those events associated with possible threats emerging from indigenous populations. Tables C-1 (page C-2), C-2 (page C-4), C-3 (page C-5), and C-4 (page C-5) provide starting points for analysts when developing case-specific indicators for both conventional and irregular warfare.

Table C-1. Sample offensive indicators

<b>Activity</b>	<b>Explanation</b>
Massing of maneuver elements, armor, artillery, and logistic support.	May indicate the main effort by weakening areas of secondary importance.
Deployment of combat elements on a relatively narrow frontage (not forced by terrain).	May provide maximum combat power at the point of attack by reducing frontages. Likely enemy decisive effort.
Massing of indirect fire support assets.	May indicate initiation of main effort.
Extensive artillery preparation of up to 50 minutes in duration or longer.	Initiates preparation preceding an attack.
Dispersal of tanks and self-propelled artillery to forward units.	Can indicate formation of combined arms assault formations with tanks accompanying the leading maneuver elements and artillery following in bounds.
Surface-to-surface missile units located forward.	Provides depth to threat offensive operations; places friendly support and unassigned areas in range. May also indicate, when employed alone, harassing or special weapons (chemical) delivery.
Antiaircraft artillery and mobile surface-to-surface missiles located well forward with maneuver elements.	Provides increased protection to massed forces prior to attack; extends air defense umbrella forward as units advance.
Demonstrations and feints.	May precede an attack; may deceive actual point of attack.
Establishment and strengthening of counter-reconnaissance screen.	Protects assembly areas and forces as they prepare for attack. May be effort to prevent friendly forces from seeing attack preparations.
Concentration of mass toward one or both flanks within the forward area.	May indicate intent for single or double envelopment, particularly if massing units are armor heavy.
Increased patrolling or ground reconnaissance.	May indicate efforts to gather detailed intelligence regarding friendly dispositions prior to attack.
CPs located well forward; mobile CP identified.	Indicates preparation to command and control an offensive operation from as far forward as possible.
Movement of noncombatants from the combat zone.	Indicates preparation for rapid forward advance of troops and follow-on forces.
Extensive conduct of drills and rehearsals in unassigned areas.	Often indicates major attacks, particularly against fortified positions or strongly defended natural or man-made barriers, which require rehearsal of specialized tactics and skills.
Cessation of drills and rehearsals.	Rehearsals are completed and the unit is preparing for offensive operations.

Table C-1. Sample offensive indicators (continued)

<b>Activity</b>	<b>Explanation</b>
Increased activity in supply, maintenance, and motor transport areas.	May indicate movement of additional forces to the front to sustain a major attack. Stocking of sustainment items, such as ammunition and medical supplies, prior to an attack.
Increased aerial reconnaissance (including UAS).	Threat effort to collect further intelligence on friendly dispositions or defensive positions.
Establishment of forward arming and refueling points, auxiliary airfields, or activation of inactive airfields.	Preparation for increased sorties for aircraft and faster turnaround time and aviation sustainment. Indicates preparation to support offensive operations with aircraft as far forward as possible.
Clearing lanes through own obstacles.	Facilitates forward movement and grouping of assault units, particularly at night, and usually immediately precedes and attack.
Reconnaissance, marking, and destruction of defending force's obstacles.	Indicates where assaults will occur.
Gap-crossing equipment (swimming vehicles, bridging, ferries, assault boats) located in forward areas (provided large water obstacle or gap).	Expect a substantial effort to cross a water obstacle during a main attack.
Staging of airborne, air assault, or special forces with transportation assets, such as transport aircraft or helicopters.	Airborne or air assault operations will likely indicate efforts to attack friendly command and control, communications, or sustainment nodes. May indicate a main effort in which airborne forces will link with ground maneuver forces.
Increased signals traffic or radio silence.	May indicate intent to conduct offensive operations; however, increased traffic may be an attempt to deceive. Radio silence denies information derived from signals intelligence (SIGINT).
SIGINT and EW assets located forward.	Provides electronic attack and surveillance support for the attack.

Table C-2. Sample defensive indicators

<i>Activity</i>	<i>Explanation</i>
Preparation of battalion and company defensive areas consisting of company and platoon strong points.	Indicates intent for holding terrain with defense in- depth, normally supported by armored counterattack forces.
Extensive preparation of field fortifications, obstacles, and minefields.	Indicates strong positional defense.
Attachment of additional antitank assets to frontline defensive positions.	Indicates intent to contest friendly armor in forward positions, and attempts to attrite and channel friendly armor into engagement areas for armor counterattack forces.
Formation of antitank strong points in depth along avenues of approach.	May allow penetration of friendly armor into engagement areas. Will engage armor in depth.
Preparation of alternate artillery positions.	Increases survivability of artillery in the defense. Indicates great effort to support main defensive area with artillery—no withdrawal of maneuver forces from main defense unless defeated.
Concentration of armor units in assembly areas in the rear of the main defensive area.	Indicates holding armor units in reserve for possible counterattack or counteroffensive operations.
Presence of concentrated antitank reserves.	Provides quick reaction capability against armor penetrations of the main defense.
Displacement of sustainment and medical units toward the rear area.	Facilitates defensive repositioning, maneuver, and counterattacks (support units are not “in the way”).
Prestocking of ammunition, supplies, and engineer or pioneer equipment in forward positions.	Reduces the burden on sustainment support during the battle, reduces vulnerability of interdiction of supplies, and ensures strong points can survive for reasonable periods if bypassed or cut off by advancing forces.
Increased depth from the forward line of troops of artillery and surface-to-surface missile units.	Allows continued employment of artillery during maneuver defense without significant rearward displacement.
Increased use of land-line communications—often with corresponding decrease in radio traffic.	Implies intent to remain in position because landlines are less vulnerable to EW and provide more secure communications.
Presence of dummy positions, CPs, and weapons.	Complicates friendly targeting and analysis. Deceives attacking force of actual defensive positions and strength.
Air defense more concentrated in one particular area.	Indicates location of numerous HVTs, such as armor, sustainment, artillery, or CPs.

**Table C-3. Sample delaying indicators**

<b>Activity</b>	<b>Explanation</b>
Withdrawal from defensive positions before becoming heavily engaged.	Indicates delaying action to avoid decisive engagements.
Numerous local counterattacks with limited objectives; counterattacks broken off before position is restored.	Assists disengaging units in contact, rather than an attack to restore position.
Units bounding rearward to new defensive positions, while another force begins or continues to engage.	Indicates units conducting local withdrawals to new positions. Usually an effort to preserve the defending force and trade space for time.
Maximum firepower located forward, firing initiated at long ranges.	Intent to inflict casualties thus slowing advance of attacking force and provide sufficient volume of fire to avoid decisive engagements. Allows for time to disengage and reposition defending forces.
Extremely large unit frontages compared to usual defensive positions.	Indicates delaying action to economize force, allowing larger formations to withdraw.
Chemical or biological weapons in forward areas. Reports of enemy in chemical protective clothing while handling munitions.	Indicates possible chemical munitions use. Chemically contaminated areas cause significant delays to attacking forces.
Identification of dummy positions and minefields.	Indicates defending force using economy of force. Causes advancing force to determine if mines are live or inert.

**Table C-4. Sample withdrawal indicators**

<b>Activity</b>	<b>Explanation</b>
Systematic destruction of bridges, communication facilities, and other assets.	Denies advancing force the use of infrastructure and installations in withdrawal areas.
Establishment of a covering force or rear guard.	Covers withdrawal of main body; usually consists of a subelement of the main force; usually only the rear guard element engages attacking forces.
Increased rearward movement at night, particularly during inclement weather.	Attempt to avoid contact with the attacking unit in order to preserve the force and its combat power.
Minimal presence of sustainment and medical units.	Withdrawal of nonessential sustainment and medical assets. It may also indicate the inability to move depots and dumps.
Establishing and marking withdrawal routes and traffic control points.	Facilitates rapid movement of forces to the rear. Indicates attempt to preserve force by conducting an organized and rapid withdrawal.
Preparation of new defensive positions beyond supporting range of present positions.	Indicates an attempt to establish new positions along suitable terrain prior to the arrival of deliberately withdrawn forces.
Increased engineer activity and stockpiling of explosives in threat rear area near bridges, tunnels, or built-up areas.	Mobility operations facilitate a withdrawal by maintaining LOCs for own forces. Demolition preparation indicates likely destruction of infrastructure in front of attacking force.
Rearward movement of long-range artillery.	Positions long-range artillery in subsequent defensive positions in order to support withdrawal with indirect fire.
Activation of CPs well removed (beyond usual norms) from the present battle area. Positioning of CPs along route of withdrawal.	Establishes command and control nodes in the new position and along route of march in order to control movement and arrival of forces.

C-6. The activities listed in the following tables may indicate insurgent, criminal, or other activity that may cause instability or violence within a population: C-5, C-6 (page C-8), C-7 (page C-9), C-8 (page C-10), C-9 (page C-11), C-10 (page C-11), and C-11 (page C-12).

**Table C-5. Sample population indicators**

<b>General Activity Within the Population</b>
Identification of agitators, insurgents, and militias or criminal organizations, their supporters and sympathizers, who suddenly appear in, or move from, an area.
New faces or unknown people in a rural community.
Unusual gatherings among the population.
Disruption of normal social patterns.
Mass migration from urban to rural locations, or from rural to urban locations.
Massing of combatants of competing power groups.
Increase in the size of embassy or consulate staffs from a country or countries that support indigenous disaffected groups, particularly those hostile to the United States or the current intervention.
Increase in neighboring countries of staff and activities at embassies or consulates of countries associated with supporting indigenous disaffected groups.
Lack of children playing outside in neighborhoods.
Increased travel by suspected subversives or leaders of competing power bases to countries hostile to the United States or opposed to the current intervention.
Influx of opposition, resident, and expatriate leaders into the AO.
Reports of opposition or disaffected indigenous population receiving military training in foreign countries.
Increase of visitors such as tourists, technicians, businesspersons, religious leaders, officials, from groups or countries hostile to the United States or opposed to the current intervention.
Close connections between diplomatic personnel of hostile countries and local opposition groups.
Communications between opposition groups and external supporters.
Increase of disaffected youth gatherings such as student protests or demonstrations.
Establishment of organizations of unexplained origin and with unclear or nebulous aims.
Establishment of new organizations that replace an existing organizational structure with identical aims.
Appearance of many new members in existing organizations, such as labor unions.
Infiltration of student organizations by known agitators.
Appearance of new organizations stressing grievances or interests of repressed or minority groups.
Reports of large donations to new or revamped organizations.
Reports of payment to locals for engaging in subversive or hostile activities.
Reports of the formation of opposition paramilitary or militia organizations.
Reports of lists of targets for planned opposition attacks.
Appearance of "professional" agitators in gatherings or demonstrations that result in violence.
Evidence of paid and armed demonstrators' participation in riots or violent protests.
Significant increase in thefts, armed robberies, and violent crime in rural areas; increase in bank robberies in urban areas.



Table C-5. Sample population indicators (continued)

<b><i>Opposition Directed Activities</i></b>
Refusal of population to pay, or unusual difficulty in collecting, rent, taxes, or loan payments.
Trends of demonstrated hostility toward government forces or the mission force.
Unexplained disappearance of the population or avoidance of certain areas.
Unexplained disappearance or relocation of children and adolescents.
Reported incidents of attempted recruitment to join new movements or underground organizations.
Criminals and disaffected youth who appear to be acting with and for the opposition.
Reports of extortion and other coercion by opposition elements to obtain financial support.
Use of fear tactics to coerce, control, or influence the local population.
Surveillance of HN government or mission force facilities and personnel.
<b><i>Activities Directed Against the Government or Mission Force</i></b>
Failure of police and informer nets to report accurate information, which may indicate sources are actively supporting opposition elements or the sources are intimidated.
Decreasing success of government law enforcement or military infiltration of opposition or disaffected organizations.
Assassination or disappearance of government intelligence sources.
Reports of attempts to bribe or blackmail government officials, law enforcement employees, or mission personnel.
Classified information leaked to the media.
Sudden affluence of certain government and law enforcement personnel.
Recurring failure of government or mission force raids on suspected opposition organizations or illegal activities apparently due to forewarning.
Increased hostile or illegal activity against the government, its law enforcement and military organizations, foreigners, minority groups, or competing political, ethnic, linguistic, or religious groups.
Demonstrations against government forces, minority groups, or foreigners designed to instigate violent confrontations with government or mission forces.
Increased antigovernment or mission force rhetoric in local media.
Occurrence of strikes or work force walkouts in critical industries or geographic areas intended to cast doubt on the government's ability to maintain order and provide security and services to the people.
Unexplained loss, destruction, or forgery of government identification cards and passports.
Recurring unexplained disruption of public utilities.
Reports of terrorist acts or extortion attempts against local government leaders and businesspersons.
Murder or kidnapping of government, military, and law enforcement officials or mission force personnel.
Closing of schools.
Reports of attempts to obtain classified information from government officials, government offices, or mission personnel.

Table C-6. Sample propaganda indicators

<b>General Propaganda Activities</b>
Dissident propaganda from unidentified sources.
Increase in the number of entertainers with a political message.
Increase of political themes in religious services.
Increase in appeals directed at intensifying general ethnic or religious unrest in countries where ethnic or religious competition exists.
Increase of agitation on issues for which there is no identified movement or organization.
Renewed activity by dissident or opposition organizations thought to be defunct or dormant.
Circulation of petitions advocating opposition or dissident demands.
Appearance of opposition slogans and pronouncements by word-of-mouth, graffiti, posters, leaflets, and other means.
Propaganda linking local ethnic groups with those in neighboring countries or regions.
Clandestine radio broadcasts intended to appeal to those with special grievances or to underprivileged ethnic groups.
Use of bullhorns, truck-mounted loudspeakers, and other public address equipment in "spontaneous" demonstrations.
Presence of nonmedia photographers among demonstrators.
Rallies to honor "martyred" opposition personnel. Mass demonstrations honoring local dissident heroes or dates significant to the opposition.
Nationwide strikes called to demonstrate the strength of the opposition movements.
<b>Propaganda Activities Directed Against the Established Government</b>
Attempts to discredit or ridicule national or public officials.
Attempts to discredit the judicial and law enforcement system.
Characterization of government projects and plans.
Radio propaganda from foreign countries that is aimed at the target country's population and accuses the target country's government of failure to meet the people's needs.
<b>Propaganda Activities Directed Against the Mission Force and HN Military and Law Enforcement</b>
Spreading accusations that the HN military and police are corrupt and out of touch with the people.
Spreading accusations that mission force personnel will introduce customs or attitudes that are in opposition to local cultural or religious beliefs.
Character assassinations of mission, military, and law enforcement officials.
Demands to remove strong antiopposition or anticrime military and law enforcement leaders from office.
Calls for the population to cease cooperating with the mission force or HN military and law enforcement.
Deliberate incidents to provoke mission, military, or police reprisals during demonstrations or strikes.
Widespread hostile media coverage of even minor criminal violations or incidents involving mission force personnel.
Accusations of brutality or ineffectiveness, or claims that mission or government forces initiated violence following confrontations.
Publication of photographs portraying repressive and violent acts by mission force or government forces.
Refusal of businesspersons and shop owners to conduct business with mission force personnel.
<b>Propaganda Activities Directed Against the Education System</b>
Appearance of questionable doctrine and teachings in the educational system.
Creation of ethnic, tribal, religious, or other interest group schools outside the government educational system, which propagate opposition themes and teachings.
Charges that the educational system is only training youth to do the government's bidding.
Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

Table C-7. Sample commodities indicators

<b><i>Food-Related Activities</i></b>
Diversion of crops or meat from markets.
Unexplained shortages of food supplies when there are no reports of natural causes.
Increased reports of foodstuffs pilfering.
Sudden increase in food prices, possibly indicating an opposition-levied tax.
Unwillingness of farmers to transport food to populations centers, indicating a fear of traveling highways.
Spot shortages of foodstuffs in regions or neighborhoods associated with a minority group or weaker competing interest group, while food supplies are generally plentiful in other areas. Conversely, sudden local shortages of foodstuffs in rural areas may indicate the existence of an armed opposition group in that region.
Sudden increase of meat in markets, possibly indicating slaughtered livestock because of a lack of fodder to sustain them.
Appearance of emergency relief supplies for sale in black markets possibly indicating diversion from starving population.
Appearance of relief supplies for sale in normal markets in a country or region recently suffering from large-scale hunger, which may indicate the severity of the food crisis is diminishing.
<b><i>Arms and Ammunition-Related Activities</i></b>
Increased loss or theft of weapons from military and police forces.
Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.
Attacks on patrols resulting in the loss of weapons and ammunition.
Increased purchase of surplus military goods.
Sudden increase in prices for arms and ammunitions on the open market.
Reports of large arms shipments destined for neighboring countries, but not intended for that government.
Reports of known arms traffickers establishing contacts with opposition elements.
Increase in armed robberies.
Reports of thefts or sudden shortages of chemicals, which could be used in the clandestine manufacture of explosives.
Reports of large open-market purchases of explosives-related chemicals without an identifiable industrial user.
Appearance of manufactured or smuggled arms from noncontiguous foreign countries.
<b><i>Clothing-Related Activities</i></b>
Unusual, systematic purchase or theft of clothing materials that could be used for the manufacture of uniforms or footwear.
Unusual scarcity of clothing or material used in the manufacture of clothing or footwear.
Distribution of clothing to underprivileged or minority classes by organizations of recent or suspect origin.
Discovery of caches of uniforms and footwear or materials that could be used to manufacture uniforms and footwear.
Increase of males in the streets wearing military style clothing or distinctive markings.
<b><i>Medicine-Related Activities</i></b>
Large-scale purchasing or theft of drugs and medicines or the herbs used to manufacture local remedies.
Scarcity of drugs and medicinal supplies on the open or black markets.
Diversion of medical aid donations.
Discovery of caches or medical supplies.
<b><i>Communications-Related Activities</i></b>
Increase in the purchase and use of radios.
Discovery of caches of communication equipment.
Unusual increase in amateur radio or cellular telephone communications traffic.

Table C-8. Environment-related indicators

<b><i>Rural Activities</i></b>
Evidence of increased foot traffic in the area.
Increased travel within and into remote or isolated areas.
Unexplained trails and cold campsites.
Establishment of new, unexplained agricultural areas or recently cleared fields.
Unusual smoke, possibly indicating the presence of a campsite or a form of communication.
Concentration of dead foliage in an area, possibly indicating use of camouflage.
Presence of foot traps, spikes, booby traps, or improvised mines along routes and trails.
<b><i>Urban Activities</i></b>
Apartments, houses, or buildings being rented, but not lived in as homes.
Slogans written on walls, bridges, and streets.
Defacement of government and mission force information signs.
Sabotage of electrical power network, pollution of urban area's water supply.
Terrorist acts against physical targets such as bridges, dams, airfields, or buildings.
Change of residence of suspected agitators or opposition leaders.
Discovery of message dead drops.
Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.
Appearance of abnormal amounts of counterfeit currency.
Increase in bank robberies.
Work stoppages or slowdowns in essential industries.
<b><i>Urban Activities</i></b>
Marked decline in product quality in essential industries.
Marked increase in equipment failures in essential industries.
Unexplained explosions in essential utilities and industries.
Establishment of roadblocks or barricades around neighborhoods associated with opposition elements.
Attempts to disrupt public transport through sabotage.
Malicious damage to industrial products or factory machinery.

**Table C-9. Improvised explosive device indicators**

<b>Basic IED Indicators</b>
Vehicles following convoys for a long distance and then pulling off the side of the road.
Dead animals along the roadways.
Freshly dug holes along the roadway (possible future IED report).
New dirt or gravel piles.
Obstacles in roadway used to channel the convoy.
Personnel on overpasses.
Signal with flares or city lights (turned off or on) as convoy approaches.
Absence of the ordinary children in the area, merchants at a market.
<b>Key Indicators That Should Indicate that Something is About to Happen</b>
Dramatic changes in population from one block to the next.
Dramatic changes in illumination (lights) from one area to the next during hour of limited visibility.
Absence of children when normally present.
Identification of markings indicated in intelligence reports of an IED site.

**Table C-10. Sample threat environment indicators**

<b>Indicator</b>	<b>Information Objective</b>
<b>Local Conflict / Casualty</b>	What groups (tribes, clans) are local rivals?
	How intense is the rivalry?
	What are the relative strengths or external alliances of rival groups?
	U.S. presence or host government?
	Do locals normally carry arms?
	Does group rivalry parallel rivalry within the host government?

**Table C-11. Recurrence of same clan indicators**

<i>Indicator</i>	<i>Information Objective</i>
<b>Recurrence of Same Clan Name Among Detainees</b>	Is clan native to the area? If so, where does clan reside, in which villages?
	How big is the clan, how many male adults?
	Who is the acknowledged chief?
	Do or did any members of clan have positions in former regime? Who are they? Do any of them have access to arms or ammunition? Where is their cache or source?
	Do any of them provide training to other relatives?
	What are the usual economics of the clan?
	Can the clan exploit these activities to gain arms or facilitate or conceal their operations?
	Has any relative been killed by U.S. or multinational forces? If so, is there a current mood of blood vengeance within the clan?
	Which mosques do clan members attend? Do the imams follow a particular doctrine? Is that doctrine radical or moderate? If radical, do the imams encourage hostility to the U.S. presence?
	Has the clan offered "protection" to any strangers or foreigners? Are these people recent arrivals or long-term residents? What is the identity and agenda or business of such people?

## **Appendix D**

# **Other Analytical Approaches**

This appendix provides the analyst with other approaches for analysis. For specific details and methodology discussion of special operations forces (SOF) targeting operations see JP 3-05.1. SOF select targets for exploitation with careful and deliberate consideration. Effective integration of SOF into an operational plan is possible only through synchronized targeting and mission planning. Detailed evaluation of an adversary's vulnerabilities and application of SOF capabilities at critical nodes are the foundation of SOF employment. SOF targeting considerations include the political, military, economic, and psychological impact on the enemy force's capabilities, morale, and its support base.

### **CARVER TARGET ANALYSIS METHOD**

D-1. The criticality, accessibility, recuperability, vulnerability, effect, recognizability (CARVER) targeting technique assists in selecting the appropriate components when targeting. The CARVER method is used mainly by SOF units to assess, validate, and define requirements planning. The CARVER targeting process may be used in addition to vulnerability assessments. Its use is not required but is highly recommended to complete force protection plans.

D-2. The CARVER selection factors assist in selecting the best targets or components to meet the commander's desired outcome. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a CARVER matrix as shown in figure D-1 (page D-2). After values for each target or component are assigned, the sum of the values indicates the highest value target or component to be attacked within the limits of the requirements and commander's intent.

### **STRATEGIC CARVER EVALUATION CRITERIA**

D-3. The purpose of strategic target analysis is to determine the critical systems or subsystems that must be attacked for progressive destruction or degradation of an adversary's warfighting capacity and will to fight. Strategic operations have long-range, rather than immediate, effects on an adversary and its military forces. Strategic target analysis identifies adversary's systems or subsystems; for example, electric power and rail facilities. The results of the strategic target analysis, as well as any additional guidance received from the President and the Secretary of Defense, determine priorities of systems or subsystems to be targeted.

### **OPERATIONAL CARVER EVALUATION MATRIX**

D-4. The purpose of operational target analysis is to determine the critical subsystem or target complex within the strategically critical system for interdiction. This analysis is done by Army special operations forces units at the battalion level and below.

### **TACTICAL CARVER EVALUATION MATRIX**

D-5. The purpose of tactical target analysis is to determine the military importance of target components, the priority of attack, and the weapons required to obtain a desired effect on a target or set of targets within

a target system. Tactical-level analysis lists the complexes or the components of subsystems or complexes selected for attack.

CARVER VALUE RATING SCALE (NOTIONAL)							
VALUE	C	A	R	V	E	R	VALUE
5	Loss would be mission stopper	Easily accessible; away from security	Extremely difficult to replace; long down time (1 year)	Special operations forces definitely have the means and expertise to attack	Favorable sociological impact; neutral impact on civilians	Easily recognized by all with no confusion	5
4	Loss would reduce mission performance considerably	Easily accessible outside	Difficult to replace with long down time (<1 year)	Special operations forces probably have the means and expertise	Favorable impact; no adverse impact on civilians	Easily recognized by most, with little confusion	4
3	Loss would reduce mission performance	Accessible	Can be replaced in a relatively short time (months)	Special operations forces may have the means and expertise to attack	Favorable impact; some adverse impact on civilians	Recognized with some training	3
2	Loss may reduce mission performance	Difficult to gain access	Easily replaced in a short time (weeks)	Special operations forces probably have no impact	No impact; adverse impact on civilians	Hard to recognize confusion probable	2
1	Loss would not affect mission performance	Very difficult to gain access	Easily replaced in short time (days)	Special operations forces do not have much capability to attack	Unfavorable impact; assured adverse impact on civilians	Extremely difficult to recognize without extensive orientation	1

*Note: For specific targets, more precise target-related data can be developed for each element in the matrix.*

**Figure D-1. CARVER value rating scale (notional)**

D-6. As each potential target is evaluated for each CARVER factor, the analyst enters the numerical rating into the matrix. When all the potential targets have been evaluated, the analyst adds the scores for each target. The totals represent the relative desirability of each potential target and constitute a prioritized list of targets. The targets with the highest totals are considered first for attack.

D-7. For more information on CARVER analysis, see JP 3-05.1.

**Criticality**

D-8. Criticality or target value is the primary consideration in targeting. Criticality is related to how much a target’s destruction, denial, disruption, and damage will impair the adversary’s political, economic, or military operations, or how much a target component will disrupt the function of a target complex. In determining criticality, individual targets within a target system must be analyzed with relation to the other elements critical to the function of the target system or complex. Critical targets may also be selected for surveillance and reconnaissance missions.

**Accessibility**

D-9. A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access.

**Recuperability**

D-10. A target’s recuperability is measured in time; that is, how long will it take to replace, repair, or bypass the destruction of or damage to the target? Recuperability varies with the sources and types of targeted components and the availability of spare parts availability. Recuperability may not be as important



in terrorist targeting as the considerations of publicity, the symbolism of the target, and the desire to successfully accomplish an attack.

### **Vulnerability**

D-11. A target is vulnerable if there are the means and expertise to successfully attack it. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. At the strategic level, a much broader range of resources and technology is available to conduct the target attack. At the tactical level, resources may be limited to organic personnel, weapons, and munitions or assets that can be attached, borrowed, or improvised.

### **Effect**

D-12. The target should be attacked only if the desired military effects can be achieved. These effects may be of a military, political, economic, informational, or psychological nature. The effect on the populace is viewed in terms of alienating the local inhabitants, strengthening the resistance movement, or triggering reprisals against the indigenous people in the immediate target area. Collateral damage must also be calculated and weighed against the expected military benefit to determine if an attack would be advisable under the concept of proportionality. Collateral damage includes but is not limited to civilian injuries, deaths, and adverse economic impacts of the proposed attack.

### **Recognizability**

D-13. A target's recognizability is the degree to which it can be recognized by the threat, and his ISR assets, under varying conditions. Weather has an obvious and significant impact on visibility. Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must also be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the threat.

## **DSHARPP FORCE PROTECTION TARGET VALUE ANALYSIS**

D-14. SOF use the traditional SOF target analysis method of CARVER and combine it with the demography, symbolism, history, accessibility, recognizability, population, and proximity (DSHARPP) force protection target value analysis method to create an approach to evaluate the environment for the asymmetric threat. The SOF intelligence Soldier's training is designed to foster creative thinking to identify potential threats (HVTs and HPTs) or targets of opportunity and to develop or refine operational recommendations.

D-15. This process applies from the Special Forces Operational Detachment Alpha to the Theater Special Operations Command level. It can be applied from the perspective of the asymmetric threat or the friendly force perspective. Results will drive development of operational recommendations, operations, or intelligence fusion production and collections focus. The end state is development of actionable intelligence: human targets (hostile or friendly), asymmetric threat activities, or HN OPSEC security weaknesses or vulnerabilities. Some of the categories for consideration in the asymmetrical threat environment are—

- Foreign influences.
- HN military and security forces (population control measures).
- Socio-economic factors enabling the terrorist elements.
- Socio-economic factors enabling SOF operations.
- Asymmetric threat forces use of black market and illicit economy.
- Nonstate or state actors potentially enabling terrorists.

- Nonstate or state actors potentially enabling SOF operations.
- Telecommunication infrastructure.
- Border security.
- OPSEC environment enabling or hindering asymmetric threat forces or SOF operations.
- HN grievances.
- LOCs.

D-16. The DSHARPP force protection target value analysis method is used to determine the value of the high-risk target (HRT) to the terrorist attacker. Figure D-2 is an example of how this information is compiled using the following:

- **Demography.** Type of personnel immediately affected by the attack (government service, military, family members, mixture of local nationals and military).
- **Symbolism.** Symbolic significance of target to attacker and population attacker is terrorizing (Marines – Hezbollah; Statue of Liberty – Americans).
- **History.** History of attacks against this type of target (abortion clinics – right to life groups; federal buildings – militia groups; Jewish centers – neo-Nazi or Palestinian or Arab groups).
- **Accessibility.** How accessible the target is to the public (open posts, building with multiple entrances, no guards or detectors, close to the road).
- **Recognizability.** How well known the target is to the public at large. How easy the value is to recognize without specialized or inside information or explanation of the attack.
- **Population.** How many people are directly affected by the attack. Casualties are a factor for some; embarrassing government drives for others.
- **Proximity.** Whether the target is located near other personnel, facilities, or resources that, because of their intrinsic value or “protected” status and a fear of collateral damage, afford it some form of protection (for example, near national monuments, protected or religious symbols that the enemy holds in high regard).

<i>HRT</i>	<i>D</i>	<i>S</i>	<i>H</i>	<i>A</i>	<i>R</i>	<i>P</i>	<i>P</i>	<i>TOTAL</i>
#1	10	10	1	3	10	8	8	50
#2	2	4	1	4	9	10	10	40
#3	1	1	1	9	5	3	1	21

Figure D-2. Example of DSHARPP matrix tool

D-17. The DSHARPP tool also assists analysts in identifying targets that need additional protection to repel an attack. Each factor is analyzed and given a numerical value that represents the desirability of attack. The sum of the values is determined, thereby indicating the highest value target or component vulnerable to attack. The DSHARPP tool is used to assess criticality and is linked more closely to assessing personnel vulnerabilities.

## TARGET INFORMATION FOLDERS

D-18. Target folders contain target intelligence and related materials and information prepared for planning and executing action against a specific target. Additional data may be added to the basic target folder, such as—

- Imagery.
- Building blueprints.
- Maps or area asketches.
- Photographs of relevant individuals, vehicles, other.

- Biographical data on known associates.
- Demographical information of the targeted area.

D-19. The types and amount of additional data is dependent upon the type of target operation being conducted, phase of the targeting process the unit is in, and the information requirements of the commander and staff. Figures D-3, D-4 (page D-6), and D-5 (page D-8) and tables D-1 (page D-6) D-2 (page D-7), D-3 (page D-8) and D-4 (page D-10) are examples of additional information that may be included in a target folder. For additional information on intelligence support to targeting, see FM 2-0.

D-20. Highly detailed information is required during the planning stages of a raid or assault on an individual building. The degree of detail needed in such missions is reflected in the following list of intelligence requirements. The design and construction of buildings vary within a functional (industrial area as opposed to residential) and cultural development of the region. For additional information on building analysis, see FM 3-06.11. Critical factors to be considered in evaluating the construction of a building for attack, defense, or destruction include—

- Protective value offered by walls, roofs, ceilings, and doors, as well as the types of obstructions found on rooftops that may impede heliborne operations.
- Ease with which a building, wall, or roof may be demolished.
- Availability of internal LOCs and the effort required to breach exterior walls.
- Time, effort, and material required to use the building.
- Potential fire hazard.

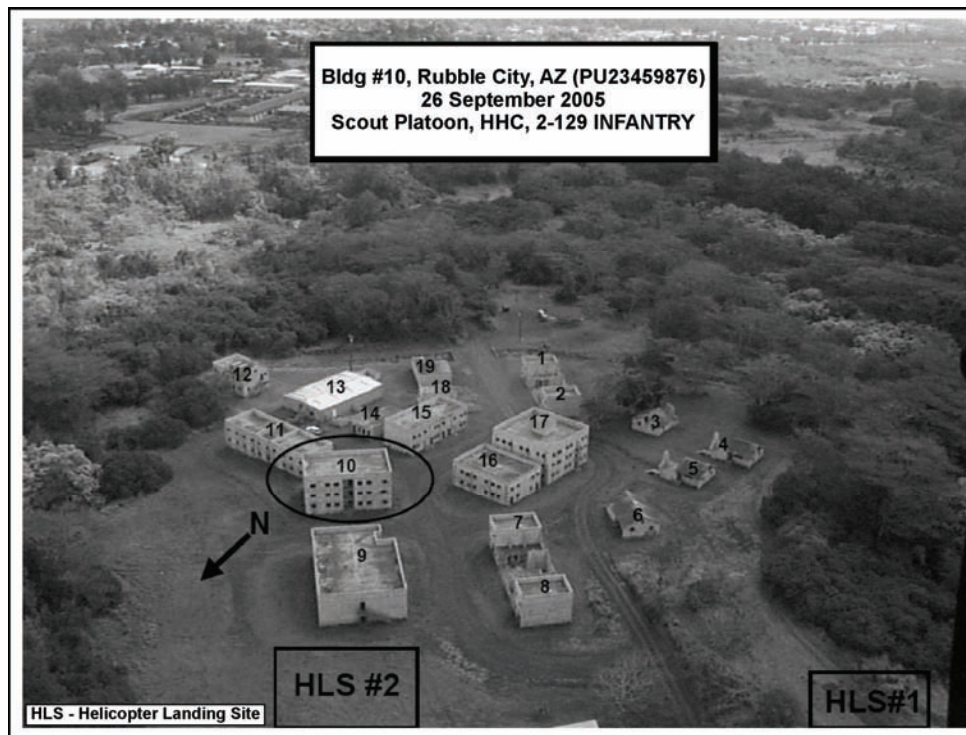


Figure D-3. Sample imagery of target area

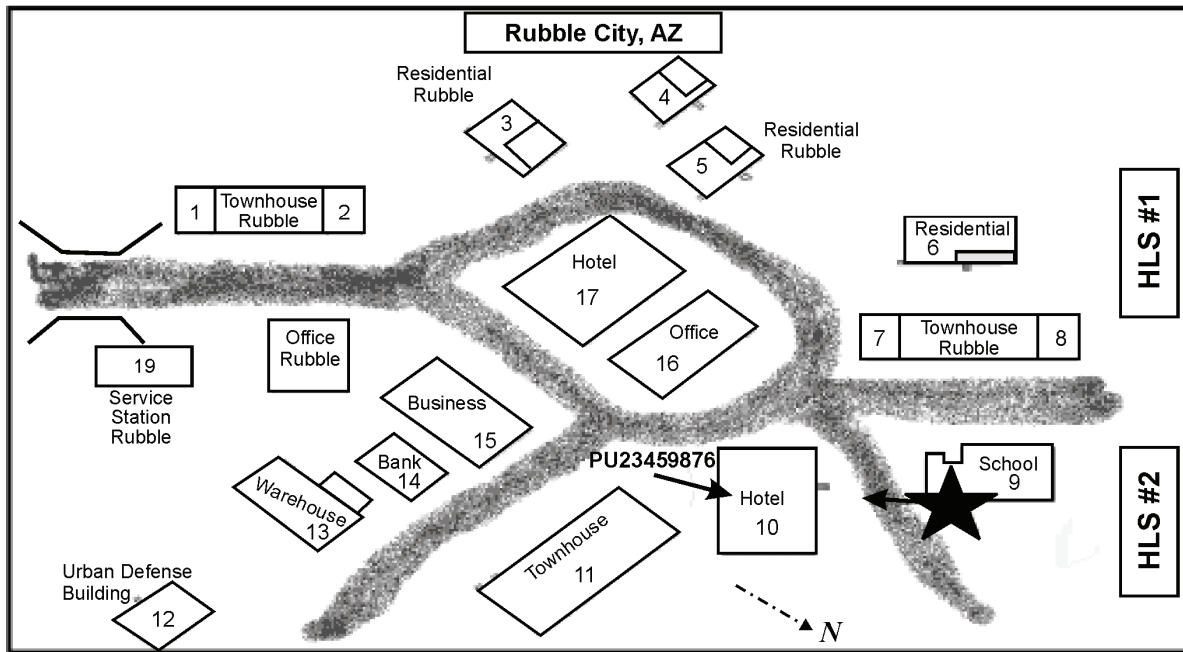


Figure D-4. Sample sketch of target area

Table D-1. Structure analysis matrix

Step	Concern	Details
1	Structural Shape	Structural shapes will be identified as square, rectangular, T-shaped, L-shaped, U-shaped, H-shaped, X-shaped, and irregular.
	Square	Designed so that all four sides are of equal size. Such designs are normally found in inner-city construction, smaller family dwellings, and in utility company maintenance buildings.
	Rectangular	Designed so that opposite sides are of equal size. The most commonly used shape in building construction.
	T-Shaped	A modification of a square or rectangle with a wing extending from the center of the front or back of the building.
	L-Shaped	A modification of a square or rectangle with a wing extending from one end or the other of the front or back of the building. A common design for family dwellings.
	U-Shaped	A modification of a rectangle with a wing extending from each end of the front or back of the building. A modification of a U-shape is the multiple U, with more than two wings extending from the front or back. The U-shape is common to larger official buildings and hospitals.
	H-Shaped	A modification of a rectangle with a wing extending from each end to the front and back. A modification of the H-shaped is the multiple H. The multiple H has more than two wings extending to the front and back.
	X-Shaped	A center common area with T-shaped wings extending from the center of each side. X-shaped designs are found in some apartment complexes.
	Irregular	Buildings that do not fit traditional designs, such as the Pentagon, religious structures, sports arenas, and permanent fortifications.

**Table D-1. Structure analysis matrix (continued)**

2	Structural Face Designation	Once the shape has been determined, the structure's main entrance is located and designated "white." If none of the building faces are identifiable as the main one, the commander will designate a face as white. Once done, the other faces will be color-coded in a clockwise manner with the white face serving as the base. While facing the white face, progressive faces will be designated as red, black (rear face), and green. For irregularly shaped structures, the white face will be designated and the remaining faces color-coded. Any report addressing this structure will include the direction the sides take relative to each other. An example of color coding and shape follows. <b>EXAMPLE:</b> "irregular, white face one, white face two right, red face, black face, green face." This describes a pentagon-shaped irregular design.
3	Measurement of Side Lengths	Once the structural faces have been color-coded, the shape, face color, and dimensions of the respective sides will be given. For irregularly shaped structures, the same procedure is used with the addition of direction the sides take relative to each other. Send measurements as feet, length first followed by height. <b>EXAMPLE:</b> "Rectangle, red face 20 by 30."
4	Numbering of Floors	Floors will be numbered from "1" beginning with the ground floor. (Basements and other subterranean areas are addressed later.) Roofs, floors, attics, porches, balconies, chimneys, stairs, fire escapes, and other substructures will not be numbered but designated as what they are. Once the structural shape, face, and measurements are reported, then report using face, floor, and any additional information. <b>EXAMPLE:</b> "Black face, three, patio and fire escape."
5	Numbering of Windows or Openings	Windows will be designated "window," doors as "door," and all other openings as "opening." Designated from left to right as "Alpha, Bravo, Charlie, etc." <b>EXAMPLE:</b> "Window Alpha"; "opening Delta."
6	Numbering of Basements and Other Subterranean Levels	Subbasements, tunnels, or vaults may be dug deep into the earth and provided multiple subterranean levels. Such structures will be designated one at a time and given an alpha designation (first level = Alpha, second level = Bravo, third level = Charlie). Additionally, the type of structure or equipment on a given level must be identified. <b>EXAMPLE:</b> A basement will be designated basement. "Subbasement 'Alpha' parking garage." Tunnel 'Charlie' gas pipeline." "Vault 'Delta' with electrical conduit tunnel." (Reflects a vault on the 4th level below the street level and that it has electrical conduits or lines running through it.)

**Table D-2. Sample building analysis matrix**

<i>Bldg #</i>	<i>Type Construction</i>	<i>Floors</i>	<i>Rooms</i>	<i>Stairwells</i>	<i>Basement Y/N/U</i>	<i>Attic Y/N/U</i>	<i>Apertures N/S/E/W</i>	<i>Entry or Exit Locations</i>	<i>Additional Information</i>
10	Framed Block	3	14	3 Inside	N	N	3 x W	N/S/E/W	None
<b>KEY:</b> <b>Y/N/U – Yes / No / Unknown</b> <b>N/S/E/W – North / South / East / West</b>									

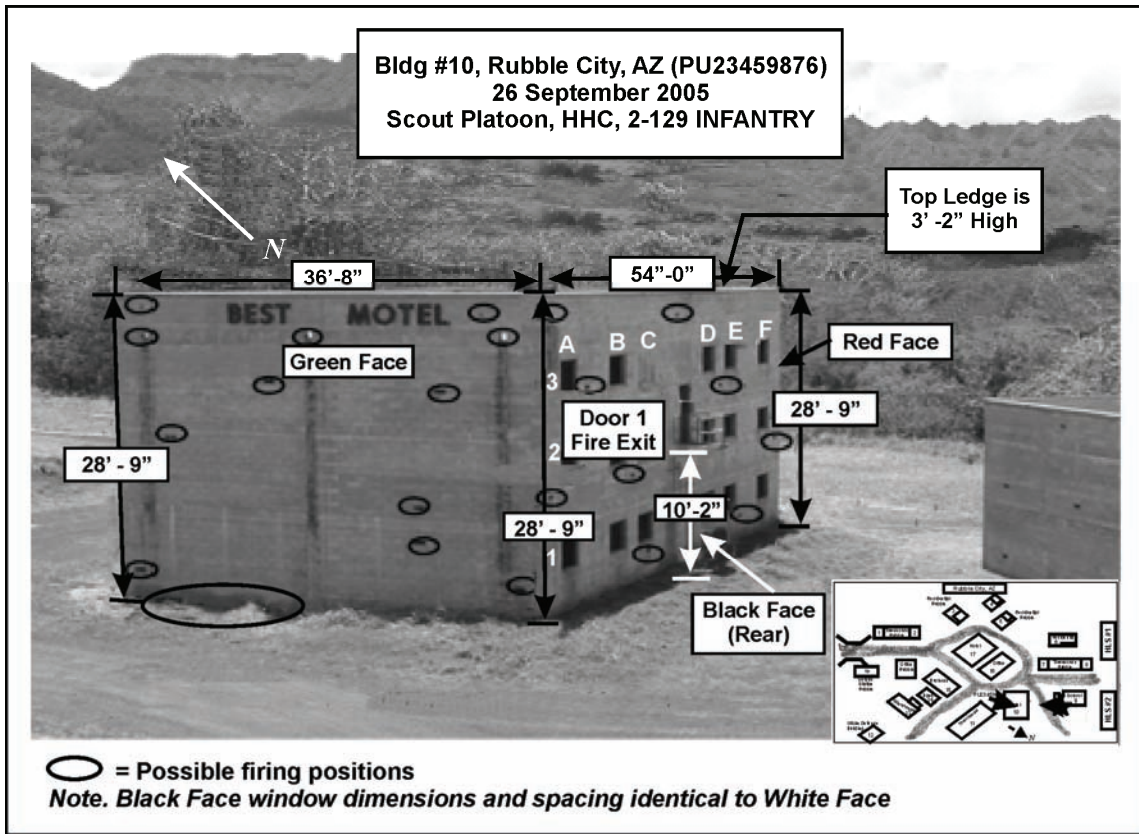


Figure D-5. Sample of labeled target building (rear)

Table D-3. Example intelligence requirements for individual buildings

<b>General Building Information</b>	
Provide general building information: <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Type.</li> <li>■ Number of stories.</li> <li>■ Date of construction.</li> <li>■ Ownership.</li> <li>■ Occupants.</li> </ul>	Obtain building blueprints or documents: <ul style="list-style-type: none"> <li>■ Obtain photographs or other imagery of the outside of the building and surrounding area.</li> <li>■ Identify individuals with knowledge of the building interior (building engineer and maintenance personnel).</li> <li>■ Note the general proximity to other structures.</li> </ul>
<b>Identify Building Specifications</b>	
Identify building dimensions. Identify the external and internal doors: <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Dimension.</li> <li>■ Type of material.</li> <li>■ Composition.</li> <li>■ Windows.</li> <li>■ Location of hinges.</li> <li>■ Method of opening. (Do the doors open outwards or inwards?)</li> <li>■ Locks.</li> </ul>	Identify crawl spaces: <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Dimensions.</li> <li>■ Openings.</li> <li>■ Descriptions.</li> <li>■ Identify basements or cellars:                             <ul style="list-style-type: none"> <li>■ Location of entrance.</li> <li>■ Staircase location.</li> <li>■ Dimensions.</li> <li>■ Use.</li> </ul> </li> </ul>

**Table D-3. Example intelligence requirements for individual buildings (continued)**

<b>Identify Building Specifications (continued)</b>	
<p>Identify windows:</p> <ul style="list-style-type: none"> <li>■ Locations.</li> <li>■ Type of construction materials.</li> <li>■ Dimensions.</li> <li>■ Method of locking.</li> <li>■ Do the windows open in, out to the side, or up and down?</li> <li>■ Mouse holes:                             <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Dimensions.</li> </ul> </li> </ul> <p>Identify hallways.</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Width.</li> <li>■ Length.</li> <li>■ Number of doors.</li> <li>■ Overhead openings.                             <ul style="list-style-type: none"> <li>■ Areas the hallway connects</li> </ul> </li> </ul> <p>Identify closet spaces.</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Dimensions.</li> </ul> <p>Method of opening.</p>	<p>Identify attic spaces:</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Location of staircase.</li> <li>■ Dimensions.</li> <li>■ Use.</li> <li>■ Field of view from the attic.</li> </ul> <p>Identify ventilation system.</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Exhaust fans.</li> <li>■ Pipes.</li> <li>■ Chimney:                             <ul style="list-style-type: none"> <li>- Location.</li> <li>- Dimension.</li> <li>- Composition.</li> <li>- Opening inside.</li> </ul> </li> </ul> <p>Identify stairwells:</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Type.</li> </ul> <p>Identify roof:</p> <ul style="list-style-type: none"> <li>■ Size</li> <li>■ Material.</li> <li>■ Access to interior.</li> </ul> <p>Obstructions.</p>
<p>Identify elevators:</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Dimensions.</li> <li>■ Location of control box.</li> <li>■ Mechanism for opening elevator inside shaft.</li> </ul> <p>Describe the subterranean spaces:</p> <ul style="list-style-type: none"> <li>■ Sewers.</li> <li>■ Subways.</li> <li>■ Basements or cellars.</li> <li>■ Other utility tunnels.</li> </ul> <p>Examine the building's utility and communication systems.</p> <p>Determine types of utilities used in the building.</p> <p>Determine whether utilities can be regulated from outside the building.</p> <p>Locate the utility control box or switches.</p> <p>Identify the buildings telephones:</p> <ul style="list-style-type: none"> <li>■ Location.</li> <li>■ Number.</li> <li>■ Type.</li> </ul>	<p>Describe other means of communication:</p> <ul style="list-style-type: none"> <li>■ Radios.</li> <li>■ Internet.</li> <li>■ Cell phones.</li> </ul> <p>Examine building construction:</p> <ul style="list-style-type: none"> <li>■ Pattern of construction.</li> <li>■ Composition of the outer wall (whether small arms will penetrate).</li> <li>■ Composition of inner walls:                             <ul style="list-style-type: none"> <li>- Whether small arms will penetrate.</li> <li>- Whether walls are reinforced.</li> </ul> </li> <li>■ Support structure.</li> <li>■ Insulation used in the walls (whether it is flammable).</li> </ul>

Table D-4. Example intelligence requirements for an individual person

<b>Name of HVT (Individual).</b>
<b>Suspected location of HVT (Individual).</b>
<b>Collection overview.</b> Map with objective locations (grid coordinate) of target, target's known pattern of activity, intelligence sources (HUMINT detainee, SIGINT report, IMINT such as national imagery or UAS).
<b>Photograph of HVT (Individual).</b>
<b>Intelligence gaps—positively identified.</b>
<b>Physical description:</b>
– <b>Age.</b> Unless known accurately, should be bracketed.
– <b>Build.</b> Thin, medium, well built.
– <b>Clothes.</b> Middle Eastern- or Western-style trousers and shirt.
– <b>Distinguishing features.</b> Scars, tattoos, missing limbs, small head, other.
– <b>Height/Weight.</b> ___ inches and ___ pounds.
– <b>Eyes.</b> Blue, green, other.
– <b>Face.</b> Round, slim, gaunt, fat, jowls, double chin, big nose, other.
– <b>Gait.</b> The walk, upright, slouched, any limp.
– <b>Hair.</b> Color, length, and style. Does the individual wear a hat?
– <b>License plate number for all vehicles known to be used by HVT (Individual).</b>
– <b>Vehicles.</b> All vehicles known to be used by HVT (Individual).
– <b>Aliases.</b> All known aliases for primary target.
<b>Background.</b> Key bullets on the individual's background—family, education, past events, or experiences that the reviewer should know to determine the individual's character, leadership potential, or past roles.
– <b>Category.</b> To which major category does the individual belong (for example, Jihadist)?
– <b>Affiliation.</b> With which groups is the individual affiliated (for example, 1920 Revolutionary Group)?
– <b>Connections with government, military, police.</b>
– <b>Role.</b> List the functions that the individual provides (for example, leader, facilitator, enabler, financier).
– <b>Area of operations.</b> Where does the individual operate (for example, Baghdad, Iraq, transnational, other)?
– <b>Religious affiliation.</b> Sunni, Shia?
– <b>Province from.</b> Self-explanatory.
– <b>Civilian education.</b> AS, MBA, Ph.D.
– <b>Military education.</b> Military Intelligence, Infantry, War College.
– <b>Known disabilities.</b> Uses a cane.
– <b>Health status.</b> Heart disease.
– <b>Travel.</b> Locations outside country to which the HVT (Individual) travels.
– <b>Previously Detained.</b> Where, When, Why, By Whom?
– <b>Military/Insurgency experience.</b> IED maker, sniper, VBIED maker, combatant in Afghanistan.
– <b>Expected actions.</b> Will surrender. Will fight until captured or killed.
<b>Responsible for.</b> List key events or actions for which the individual is responsible or involved. Summary of few specific key events that depict what the individual has done to support the insurgency.



Table D-4. Example intelligence requirements for an individual person (continued)

HVT (Individual) Associates: List the top five associates (secondary targets) that might be on objective. Associates' attitude and capabilities. Insert pictures and description if available.
– <i>Photo of HVT (Individual) associates.</i>
– <i>Associate's description.</i>
– <i>Connections with government, military, police.</i>
– <i>Previously Detained. Where, When, Why, by Whom.</i>
– <i>Military/Insurgency experience. IED maker, Sniper VBIED maker, Combatant in Afghanistan.</i>
– <i>Expected actions. Will surrender. Will fight until captured or killed.</i>
– <i>Aliases. List all known aliases for secondary targets.</i>
HVT (Individual) Family. List all family members that might be on objective with HVT (Individual). Family's attitude and capabilities. Insert pictures and description.
– <i>Photo of HVT (Individual) Family.</i>
– <i>Family Background and Descriptions.</i>
– <i>Family Members' Locations. List location with grid for all possible locations of family members.</i>
– <i>Connections with government, military, police.</i>
– <i>Previously Detained. Where, When, Why, By Whom.</i>
– <i>Military/Insurgency experience. IED maker, Sniper, VBIED maker, Combatant in Afghanistan.</i>
– <b>Expected Actions:</b> <i>Will surrender. Will fight until captured or killed.</i>
– <b>Aliases.</b> <i>List all known aliases for family members.</i>
<b>INTELLIGENCE PRODUCTS:</b>
– <b>Assessment of HUMINT Source.</b> <i>Assess the source as it applies to the suspected location of the target. (Report Type and Number) Source description, rating. Who vetted the source? Develop this information for each objective. Important to keep information at the NOFORN (not releasable to foreign nationals) level.</i>
– <b>Summary of HUMINT Reports.</b> <i>Gist of report and how it ties the target to the objective.</i>
– <b>HUMINT requests for information for source handler:</b> <i>Grid of HVT, family, meeting location.  Map with location of HVT (Individual).  Map to HVT (Individual) with routes.  Sketch of HVT (Individual) location.  Pictures of HVT (Individual) location.  Pictures of HVT (Individual) and family.</i>
– <b>HUMINT: Is source available to perform these tasks?</b> <i>GPS - use waypoint to develop route to site or pattern of life.  Drive by HVT (Individual) location and give signal to UAS.  Drive by HVT (Individual) family location and give signal to UAS.  Go to HVT (Individual) location and leave a marker—Infrared or Beacon.  Go to HVT (Individual) family location and leave a marker—Infrared or Beacon.  Drive by meeting place and give signal to UAS.  Drive by meeting place and leave a marker—Infrared or Beacon.  Pinpoint spider holes and weapons storage sites at HVT (Individual) location.  Pinpoint security positions and vehicles.  Details of security forces weapons and emplacements.  Ride to site with unit taking action.</i>

Table D-4. Example intelligence requirements for an individual person (continued)

<b>IMINT.</b> <i>A picture is worth a thousand words.</i>
<i>– Imagery products pertaining to the objective. With a view from the cardinal directions, security positions, vehicles, roads, trails, and activity on objective or activity around objective (national level imagery, UAS).</i>
<b>– IMINT PIR Example:</b> <i>Shows trails around structure—to spider holes and weapons storage sites. Roads, alleys, trails. Terrain, ditches, walls, fences, abandoned vehicles, makeshift barriers, other obstacles that will stop or slow a vehicle. Utility access points—sewer utility covers, any ingress and egress points. Obstacles around structure—vegetation, antenna towers, power lines, or any other obstacles that restrict the use of aircraft on objective. Structures that can be used as observation points next to site. All smaller structures on site—tool sheds, garages, boat houses, dog houses, other. Security positions. Fighting positions to include trails to fighting positions. Vehicles on objective; patterns of life.</i>
<b>SIGINT Products/PIRs.</b> <i>Assessment of the objective, to include communication devices, scanners, and jammers at objective.</i>
<b>MASINT Products/Requests for information.</b> <i>Trails, spider holes, fighting positions' directions, security positions, vehicles, roads, trails, activity on objective, activity around objective.</i>
<b>OBJECTIVE SUMMARY.</b>
<i>– Collective assessment of the intelligence.</i>
<i>– Pattern of activity. Dates and times at locations, lights on or off, meeting times, vehicle traffic at site.</i>
<i>– Include details from collections. Security element signature, posture, attitude, number and type of special weapons or equipment on site, enemy situation in area, possible booby traps.</i>
<i>– Attitude and capabilities of surrounding population. (Surrounding population's support of insurgency. Surrounding population's support for individual. Is this a heavily populated area?)</i>
<i>– Potential triggers. Identify any recommended or available triggers for the operations, source trigger, SIGINT trigger, other intelligence trigger.</i>
<i>– History of objective. Previous missions conducted against objective, has objective been previously prosecuted or not?</i>
<i>– Alternate locations. Alternate locations, in vicinity of primary objective to which target may flee or be occupying as an alternate site.</i>
<i>– All known persons that are part of security. Neighbors acting as lookouts or other security forces.</i>

Table D-4. Example intelligence requirements for an individual person (continued)

OBJECTIVE DETAILS
<p><b>– Provide tactical information on structure:</b></p> <p>Construction type.</p> <p>New or old structure.</p> <p>Floor plan.</p> <p>Number of stories.</p> <p>Number of exits from building.</p> <p>Structure configuration.</p> <p>Walls and fences.</p> <p>Vegetation around structure.</p> <p>Details of roads alleyways surrounding the structure.</p> <p>Condition and width.</p> <p>Openings in walls, fences.</p> <p>Window locations in structure.</p> <p>Type and direction of opening.</p> <p>Hardware.</p> <p>Door locations in structure.</p> <p>Type and direction of opening.</p> <p>Hardware.</p> <p>Possible routes of ingress and egress.</p> <p>External lights on and around structure.</p> <p>What utilities are connected?</p> <p>Electronic burglar alarm.</p> <p>Animals.</p> <p>Blind spots, dead spaces, tallest building providing view of structure in area.</p> <p>Details of electronic equipment at site.</p> <p>Special terrain features—roads (name or # for all major roads in area), rivers, major power lines, tunnels, mines, other.</p> <p>Overall lighting in area.</p> <p>Checkpoints, bottlenecks, bridges on roads to objective.</p> <p>Overall assessment of the surrounding terrain for trafficability.</p>
<p><b>– Personnel at objective.</b> Details of personnel at structure, such as groundskeepers, housekeepers, other.</p> <p>Gender.</p> <p>Age.</p> <p>Willingness to fight or surrender.</p>
<p><b>– Route to objective.</b> Map with detailed annotations for best route to objective, the objective with grid.</p>
<p><b>– Alternate objective summaries:</b></p> <p>All known alternate locations with grids.</p> <p>Safe houses.</p> <p>Houses, offices, meeting places.</p> <p>Primary residence.</p> <p>Secondary residence.</p> <p><b>Note. Develop HUMINT, IMINT, OBJECTIVE folders for each location.</b></p>
<p><b>Provide intelligence to support the information operations strategy as required.</b></p>

**This page intentionally left blank.**

## Appendix E

# Threat Characteristics and Intelligence Analysis in Counterinsurgency Operations

This appendix provides intelligence analysts specific information to consider when studying threat characteristics during counterinsurgency (COIN) operations. This material is by no means a comprehensive study for COIN. See FM 3-24 for additional information on COIN. See also the U.S. Army and U.S. Marine Corps COIN center web page at <http://usacac.army.mil/cac2/coin/index.asp>.

## THREAT CHARACTERISTICS IN COUNTERINSURGENCY

E-1. Chapter 3 discussed the process analysts use when categorizing and analyzing an enemy force. Most of the same threat characteristics are present in an insurgent force; those applicable characteristics are discussed in this appendix. Additionally, this appendix discusses other insurgency factors which require analysis.

### COMPOSITION

E-2. Insurgents use wings, cells, branches, and their personnel and combine other people having common characteristics that support insurgent goals. Many characteristics exploited by the insurgent include common religion, ethnicity, economic and social status, politics, tribe, and labor or job organizations. Specific cells, fronts, wings, teams, and elements of an insurgency may still have a specific name or number, type, relative size or strength, and subordination.

E-3. Composition in an insurgent force can include—

- Wings (guerrilla, political, underground, and shadow leadership).
- Fronts. Task force type units whose size depends on their mission or a short- or long-term objective. These fronts, like a task force, include the operational combat, combat support, and service support (and possible SOF) elements.
- Cells. Operational and support cells similar to sections in a military unit. Cells or teams based (with or without intermediaries) to include—
  - Guerrilla cells (sniper, ambush, raid, intimidation, kidnapping).
  - Support or sustainment cells (sustainment, intelligence, counterintelligence, information operations, population control, recruiting).
  - Underground cells (covert and clandestine operations to include or support sabotage; assassination; maintain safe houses; capture, interrogate, and move hostages; move highly valued weapons and documents or communications; and cache equipment for covert operations and sleeper cells; infiltrate the security forces, contractors, and government).
  - Internal and external command and control that may be locally, regionally, or internationally based.
  - Internal and external support structure. (This may include smugglers, transportation assets, advisors specially sent from an external actor or assigned from the higher leadership of the insurgency.)
  - Assassination and kidnapping squads specially assigned for a mission or objective.

- Bomb and demolition squads designed to build and plant explosives (car bombs) or conduct ambushes against convoys (IEDs and small arms fire). These also include the use of suicide bombers and their support elements. At times the suicide bomber driving a vehicle may not know or trigger the device but instead trigger the support element.
- Sniper teams (can be one lone sniper but usually moves in teams of two to three to provide spotting, transportation, security). Generally terrain that does not provide 300 meters or more of standoff does not require a sniper spotter due to reduced effect of the wind at closer ranges.

E-4. It is important to understand that underground cells likely include shadow leadership as a part of the underground or that leadership could be a separate element. Underground cells are both guerrilla and support based and are designed primarily for covert and clandestine operations. These include underground intelligence cells, logistic cells, and guerrilla cells. External elements, such as drug smugglers who are not interested in the insurgency or elements of a nearby country's border patrol, may provide support from remote areas or borders when insurgents need reserves or cover while crossing a border.

## DISPOSITION

E-5. Geographic location of insurgent elements and how they are deployed, employed, or located. Additionally, disposition includes the recent, current, and projected movements or locations of the following elements:

- Training camps.
- Base camps.
- Logistic camps.
- Headquarters.
- Safe houses.
- Front organizations or businesses, to include farms, factories, universities, markets, trading posts.
- Populated areas under the control of the insurgency (urban and rural). In these cases insurgents may be using homes still occupied with civilians to mask their presence and for the use of human shields.
- Cultural sites insurgents use such as shrines, religious structures, cemeteries, ruins, schools, and other protected sites as protection from counterinsurgent forces and for the psychological impact of counterinsurgents entering or firing on such a site.

## TACTICS

E-6. Tactics and operations include strategy, methods, techniques, procedures, and doctrine. Each refers to the insurgent's accepted principles of organization and employment of forces. Tactics also involve political, military, psychological, and economic considerations. Insurgent tactics and operations vary in sophistication according to the level of training, indoctrination, leadership, level of organization, and popular support.

E-7. The possible tactics used by insurgents are nearly impossible to list completely. The more popular tactics are discussed below.

## Arson

E-8. Less dramatic than most tactics, arson has the advantage of low risk to the perpetrator and requires only a low level of technical knowledge.

### **Attacking First Responders**

E-9. Sometimes insurgents plan on focusing their effort on first responders of medical, media, explosive ordnance disposal, police, onlookers, helicopters that are landing (and most exposed). Use clearing techniques and principles of patrolling, even when responding to emergencies.

### **Assassination**

E-10. Assassinations are either political or tactical. Political assassination generally refers to killing a government or community leader to eliminate his ability to provide leadership to the people or government. Tactical assassination usually refers to eliminating an obstacle to the insurgency's progress in infiltration. For assassination to be a terrorist-type attack the purpose must primarily be to incite fear and intimidation within the population, not eliminating key personnel because of their abilities.

### **Bombing**

E-11. The IED is the insurgent's or terrorist's weapon of choice. IEDs can be inexpensive to produce and, because of the various detonation techniques available, may be a low risk to the perpetrator. However, suicidal bombing cannot be overlooked as an employment method. Other IED advantages include their ability to gain publicity, as well as the ability to control casualties through timed detonation and careful placement of the device. It is also easily deniable should the action produce undesirable results. IEDs are also used as a mechanical ambush to disrupt and destroy vehicles and convoys which can be command detonated or tripped by some device like a pressure plate. Understanding the purpose of the attacks (to destroy, disrupt, harass, propagandize, kill personnel) is another important insight to insurgents and will dictate tactics used by them.

### **Far Ambush**

E-12. Harassment and disruption, especially in open areas or terrain that allows for stand-off weapons, usually means a far ambush (outside hand grenade range). Guerrillas tend to use indirect, crew-served, and sniper-type weapons to accompany ambushes initiated by subservice or roadside explosives as the most casualty-producing weapon. Far ambushes are designed to disable a vehicle to stop the convoy and draw protected forces outside their vehicles; they are also for the psychological impact against counterinsurgent forces, newer HN military and police, and less offensively trained and equipped sustainment and support units, as well as the local HN and U.S. citizens and the political leadership.

### **Near Ambush**

E-13. This tactic is used to kill personnel and destroy vehicles; so the insurgent can conduct battlefield recovery of weapons/equipment, gather intelligence on COIN patrols' equipment, frequencies, documents or maps, and overall capabilities; capture prisoners and hostages; and for the psychological impact on counterinsurgent troops and to impact local HN and U.S. citizen for public opinion to effect political leadership.

### **Mines and Booby Trap-Type Systems**

E-14. Usually used against vehicles, helicopters, dismounted troops on patrol, in homes, while searching enemy equipment and personnel, and first responders. There are many methods to trigger mines and booby traps, but the most common are types of systems ranging from metallic trip wires, infrared light beams, pressure plates, or command detonation. Some are cleverly tripped by a miniparachute that opens and deploys when helicopter downwash catches the parachute. The types of explosives (artillery shells, plastic, gelatinized gasoline, phosphorous, glycerin-based dynamite and TNT, black powder both processed and homemade or enhanced; the packaging, detonators, fuses, and triggering devices, and employment techniques are as vast as the materials available, and the skill, experience, and imagination of the insurgent.

### **Field Craft and Improvising**

E-15. Insurgents commonly use field craft (the art of improvising, repairing, or modifying what is available for weapons and tools). This skill can be taught by skilled guerrillas, hunters, farmers, Soldiers, and other individuals with similar skills. Most commonly these skills are learned through necessity and the austere conditions common in guerrilla warfare. Therefore, the longer the insurgency the better their ability of field craft.

### **Information Operations and Propaganda**

E-16. Information operations like propaganda are used to inform and influence the target audience with the main difference being the level of truth. An information operation publicizes insurgent actions, delegitimizes acts of the government and security forces, promotes the insurgents goals, and provides moral support. Insurgents tend to use a method of delivery to which the people are accustomed. At times they may use local leaders at the normal time and place where the people gather. Propaganda is used by those very skilled or very unskilled. Since the art of propaganda (truth spun with lies) is tricky and can backfire if deemed disingenuous, it can be a strength or a weakness to insurgent forces. Skilled insurgents use this to their advantage but do not push it to the point of being not credible, whereas less-skilled insurgents get sloppy and overly aggressive and lose credibility.

### **Hoaxes**

E-17. These are threats or actions that confuse, disorient, and demoralize counterinsurgents and the people while making security forces waste their resources. It also causes friendly forces to demonstrate their response time, routes, equipment, and techniques. These include threats of assassination, bombings; chemical, biological, and radiological attacks; attacks on commercial airports; poisoning of water and food supplies; or the threat of arson on key structures. Additionally, false alarms dull the analytical and operational efficiency of key security personnel, thus degrading readiness.

### **Infiltration**

E-18. This is the ability of the enemy to infiltrate the military, police, civil defense forces, and local government. This ability is usually tasked to an underground for the use of assassination, sabotage, kidnapping, intimidation, and intelligence or counterintelligence.

### **Intimidation or Blackmail**

E-19. Insurgents may attempt to gain coerced political, fiscal, or logistic support from local government officials, local businesspersons, or other influential community leaders through intimidation or blackmail. This could be in the form of threats on the individual's life, kidnapping of people close to the individual, or threats to disrupt or destroy (for example, bombing or arson) infrastructure that is important to the individual (like their business).

### **Kidnapping or Hostage Taking**

E-20. Although not identical, kidnapping or hostage taking are used to gain revenue, leverage, and publicity. This is risky and must be conducted by well-trained and disciplined insurgent members because the operation may entail eliminating local security while avoid killing the hostage. It takes well-trained personnel to plan and execute moving, and secretly storing detaining the hostage for long periods. Additional danger and coordination comes in planning for any exchanges or releases. Hostage's deaths through disease, injury, mistreatment, or natural causes can turn public opinion away from the insurgents.

### **Raids or Attacks on Facilities**

E-21. Armed attacks on facilities are usually undertaken for one of three purposes: Insurgents want to gain access to radio or television facilities to prevent government usage or to broadcast propaganda;



demonstrate the government's inability to secure critical facilities or national symbols; or to acquire resources (for example, robbery of a bank or armory).

### **Sabotage**

E-22. The objective in most sabotage incidents is to demonstrate how vulnerable a particular society or government is to insurgent actions. Industrialized areas are more vulnerable to sabotage than less highly developed societies. Utilities, communications, and transportation systems are so interdependent that a serious disruption of any one affects all of them and gains immediate public attention. Sabotage of industrial or commercial facilities is one means of identifying the target while making a statement of future intent. Military facilities and installations, information systems, and information infrastructures may become targets of insurgent sabotage.

### **Seizure**

E-23. Seizure usually involves a building or object that has political and cultural significance. Although security forces have time and flexibility to react as the insurgents are fixed, the insurgents may be using hostages or the value of the site to dissuade physical attack until psychological or extortion goals are met. Insurgents may want to draw aggression to blame counterinsurgents for the destruction of a valued site and the heavy-handed nature of the friendly force attack.

### ***Sniper Operations***

E-24. Skilled snipers will mask their shots by use of camouflage and concealment, light and sound distortion from suppressors, firing several meters from the edge of buildings or windowsills, by staging downwind, or utilizing sound distortion of buildings, cliffs, and valleys. Snipers may fire starting at the rear of a movement or up from the rear of the formation to maximize number of Soldiers killed or wounded and to disorient the patrol. Snipers may attempt to wound instead of kill Soldiers if the sniper has the skill and range; they do this because it normally takes 2 to 3 or more Soldiers to recover a wounded Soldier versus the loss of one, and medical evacuation is a priority for wounded versus killed which can take the pressure of countersniper operations off the shooter. This also causes the patrol to change the focus from countersniper and continued movement-to-contact versus defending wounded Soldiers and preparing for air or ground medical evacuation.

### **Use of Technology**

E-25. Never underestimate the insurgent's use of technology for weapons, communications, to deliver their information operations through mass media, precision indirect fires, use of the Internet, or counterfeiting money and identification documents. Some insurgent force are sophisticated enough to use helicopters or small planes for reconnaissance and resupply. Since infrastructure systems are becoming more dependent upon computers, insurgents can hack, disrupt, and disable computer systems with their own personnel or with the assistance of external state actors. Targets of hacking can include military and governmental sustainment, command and control, and intelligence systems, as well as other systems such as power plants, government records, and mass transit systems.

### **Infrastructure Attacks**

E-26. Insurgents often desire the ability to conduct sabotage against key infrastructure components that disable or destroy entire systems such as power plant and substations, dams and bridges, transportation, banking, public health, reconstruction projects, telecommunication, water and food supplies, and mass media. Insurgents, especially those who use more advanced strategies, may patiently infiltrate personnel who work at the facilities in order to gather information about the systems and conduct precision sabotage as dictated by the insurgent's objectives.

E-27. While those listed previously are the most common tactics used by insurgents, some of these tactics require more study.

E-28. Bombings can also be used against civilians, police stations, dismounted patrols (military, police, and civil defense forces), markets, sometimes against specific individuals, and for the psychological effect to delegitimize the government or draw a disproportionate response by the government against the people (this will depend on the objective and the insurgent strategy).

E-29. Vehicle-borne improvised explosive devices (VBIEDs) can be used as a mobile device against checkpoints, voting stations, cultural sites, ports and ships, combat outposts, traffic control points, or other targets usually defended making placing the explosive difficult. This in many cases the bombing is conducted by a sapper or suicide bomber. VBIEDs include explosives on vehicles, bicycles, boats, animals, or strapped to the person or in a pack to include men, women, and children.

E-30. Insurgent information operations and propaganda uses include communicating insurgent overall goals, often by publishing caliphates and manifestos; manipulating atrocities by government forces (whether real or fake); informing the people of insurgent operations to prevent their injury, supporting insurgent operations, demoralizing and intimidating pro-government civilians, local police, government officials, and civil defense forces. PSYOP, like those detailed above, are designed to gain support of the people and separate the populace from the government. The physical aspect of guerrilla warfare is in most cases to support the main psychological effects desired by the insurgent leadership. All lethal operations are intended to support nonlethal propaganda purposes.

E-31. Snipers have a great psychological effect against dismounted Soldiers. Their ability to disrupt operations by killing officers and patrol leaders, and to causing Soldiers (especially less-trained HN forces) to fire in a suppressive manner instead of at point target killing, often causes the wounding and terrorizing of civilians. Snipers historically heighten their effectiveness through the use of propaganda on their skill, bravery, and the inability of the enemy to find them. Care must be taken once a sniper is killed to discredit and publicize the sniper's death to ensure the sniper does not become immortalized. This immortality will exist even after the sniper's capture or death as others take the sniper's place under the same name if friendly forces do not use the death of a sniper or sniper team in the information operations realm.

## TRAINING

E-32. Training will be based on how advanced the insurgency is and their specific strategy. Indoctrination is a part of training which is critical to maintaining allegiance and focusing cells to conduct continuous operations without frequent communication and direction from insurgent leadership. The level of indoctrination helps analysts identify the skill and strategy of the insurgency and includes more than just the overall objective of the insurgency. Subordinate leaders within an insurgency are indoctrinated because they must function as the commander's intern and guide operations until redirected. The better the indoctrination of a commander's intent the more decentralized, self-sufficient, and focused the insurgent cells are.

E-33. Higher education also plays a role in insurgent training. Many insurgent leaders are well educated and understand how to use things such as the Internet and mass media to communicate their messages. Guerrillas, however, who are the "trigger pullers" of the insurgency, might not be as well educated. Some insurgent leaders will mobilize college students in order to create mass protests and other events which, when the proper instigators are involved, can become violent riots. The government reaction to these events is often used by insurgents to show the harsh tactics of the government forces.

E-34. Training also includes individual and collective training depending on the role of the insurgent and the insurgent's specialty or assigned cell (guerrilla, support, underground) and the specific skills of the insurgent (sniper, IO, HUMINT, raid or ambush, communications, sustainment and caches, ISR, bomb maker). Training includes how to conduct themselves if captured, including resistance to interrogation and operations within detention facilities (recruiting, clandestine communications, and maintaining control of other insurgents).

## **SUSTAINMENT**

E-35. The effectiveness of insurgent operations depends heavily on sustainment. The support cells and active supporters within the population accumulate, move, store, and disseminate supplies for the other cells. Specialty underground cells tend to have their own covert sustainment elements in order to ensure secrecy and security. Insurgents obtain sustainment from active supporters, smugglers, black markets, extortion, theft, and external actors.

E-36. Insurgents can purchase items such as food, water, medicine, bomb-making materials, propaganda products, transportation, and places to store or cache supplies. Cells obtain certain supplies to gain support of the local farmers, merchants, and smugglers while maintaining a sustainable flow of materials. Sometimes an insurgent's location and disposition is dictated in part on where the sustainment or supplies exist. This indicator can be used to find insurgents through their sustainment and supply line analysis. These indicators include outposts and bases near rivers, farms, smuggling routes, markets and black markets, hospitals, drug fields and laboratories, near borders.

## **OPERATIONAL EFFECTIVENESS**

E-37. Operational effectiveness for insurgent forces is not measured the same way as operational effectiveness for conventional forces. Analysis of operational effectiveness generally includes the insurgent's ability to coordinate and sustain operations designed to draw counterinsurgent forces to a time and place to accomplish their goals (space, time, and will). This includes the ability of the different guerrilla, support, and underground cells, together with shadow leadership, to work towards their common goals, using a common strategy, and common phases.

E-38. Insurgencies commonly use different strategies and phases in different areas but not within the same tactical area. Such differences can be exploited by friendly forces by identifying which element is in an earlier phase and exploiting their inability to support those in the more advanced phase (for example, sustainment, operations, coordination, IO).

E-39. Operational effectiveness also includes the morale and condition of cells and their support bases. Analysts must look at level of support (locally and externally), morale, living conditions, food, shelter, illness, desertion level, lack of leadership, need for medicine and hygiene, disease, and the effectiveness of HN internal defense and development projects. The study of insurgent IO and their ability to meet with local leaders from which they historically could intimidate or enjoy loyalty from and other related factors must be considered.

## **COMMUNICATIONS**

E-40. Insurgents may compensate for the lack of daily communications by masking their communication in radio, television, or Internet messages. They may also maintain information in cameras, high frequency, short-wave, and amateur (ham radio) sets, cellular phones, the mail, computers, or memory storage devices transported by couriers. Identifying how the insurgents communicate can be used to track movements, gather information, or jam their communications.

## **PERSONALITIES**

E-41. Personality is a critical factor when conducting analyzing an insurgency. Attention must be focused on individuals and leaders. Insurgent organizational diagrams can be built through multidimensional link analysis (determining relationships between critical personalities and then their group associations, discussed in detail in chapter 5). This applies to virtually any threat represented in an insurgency. Once relationships and the level of contact or knowledge the personalities have are known, many of their activities can be determined.

E-42. Build link diagram for cells, leadership (political, ideological, religious, military), staff members and planners, spokespersons, and those skilled at PSYOP and media manipulation, insurgent family members

(immediate and extended), possible skilled personnel the insurgents may seek out (medical, engineers, chemistry, business owners, those owning transportation), trainers, recruiters, intelligence and HUMINT, those conducting population control and their code names and nicknames.

E-43. Some of the questions analysts must answer are—

- Who are the leaders? Is there a single, dominant, charismatic leader?
- Is the leadership highly dedicated to an ideology?
- Are the leaders committed to a specific organizational and operational pattern?
- Are there differences of opinion among leaders as to purpose and methods? Will a schism or other event occur as a result?
- What is the relationship between the leadership and the operational and support elements?
- What is the decisionmaking process of the insurgent leadership? Is decisionmaking centralized or decentralized?

## **OTHER INSURGENCY FACTORS FOR ANALYSIS**

E-44. Within all insurgencies there are many other factors analysts must study to gain a more complete understanding of the enemy force. These include, but are not limited to, strengths and weaknesses of insurgent forces, organizational flexibility, how the insurgent will use terrain and weather, and the culture in which the insurgency is going on.

### **STRENGTHS**

E-45. Insurgents typically have many strengths that must be examined. Their ability to collect intelligence, knowledge of the operational environment, and population and resource control are just some. Each insurgency is different, and this list provides guidelines of the things to look for when analyzing insurgent forces.

E-46. Intelligence networks as part of the insurgent's infrastructure (in the support and the underground cells). These networks usually provide continuous and current information on government force dispositions, strengths, weaknesses, and abilities. Compartmentalized cells, cutaways, dead drops, screening recruits, population control, and intimidation make it more difficult for the government to penetrate and disrupt insurgent forces.

E-47. Early intelligence collection and analysis must be aggressive to build an effective database. Pattern analysis and other techniques can result in friendly force operations to remove key personnel and communications thereby taking the intelligence collection advantage from the insurgent. Analysts do this by conducting link analysis between cells (see chapter 5). They study the ability of the insurgents to conduct and gather intelligence, and their ability to conduct counterintelligence against friendly intelligent nets. Friendly forces can also overcome this intelligence advantage through the use of deception, OPSEC, and communications security.

E-48. Insurgents have a great knowledge of the operational environment. This knowledge includes things like the indigenous characteristics of the people, which provide them the ability to blend in with the local population enhancing their ability to operate with secrecy. The basis of this is usually the insurgent's ethnicity and physical characteristics. Insurgents also have the ability to blend in with the locals in their culture, daily schedules, accents, and local slangs. They will wear similar clothing, have like postures, mannerisms, and hand gestures, body movements, walking speed, greetings, body motions, eye contact (or lack of), social norms of food and drink, and sleeping schedules. Usually insurgents are operating in their own country and own ethnic group, making it extremely difficult for friendly forces to identify people in the community as somebody connected with the insurgency.

E-49. Populace and resource control is key to the insurgent's success. Together with the knowledge of the local populace is the knowledge of the terrain, local businesses, as well as social, economic, religious, and political characteristics. The ability to understand these aspects of the population assists in controlling the

population through intimidation and indoctrination; this ability allows the insurgent to provide leadership and provide basic needs to the population. Population and resource control is best accomplished through interaction with the population and leadership in their normal surrounding where the people and leaders gather, communicate, conduct day-to-day business.

E-50. Insurgents can be identified if they do not know the local trade, business, and the skills and connections that accompany them. The insurgent's knowledge of the population and terrain also provides them with an additional psychological hold over the people since the insurgents are one of them, seemingly entrenched and completely integrated into the local culture. Threats of retaliation from within can intimidate the population to support the local cause rather than the government.

E-51. Friendly forces must identify the insurgents and remove or isolate them from the civilian populace. This is best accomplished through the use of population and resource controls. Civilians must not be injured or mistreated due to COIN operations. The friendly force must overcome this advantage by fostering a strong relationship between the government forces and the populace. The insurgent's advantage can be overcome by continuous presence of a COIN force stationed and constantly present within the population. These security forces must support the government and address the grievances and underlying issues through local community and government leadership.

E-52. Insurgent leaders are trained, disciplined, and motivated. They reinforce motivation within the insurgent force by applying discipline. Usually, the insurgent is strongly devoted to a cause.

E-53. Insurgents are not usually responsible for maintaining normal governmental obligations toward society. This frees all of their efforts to conduct operations in support of the insurgency goals. However, insurgents may be tasked to perform certain political services to back up the shadow leadership's initiatives. It is when the insurgents conduct political services in support of insurgent goals that they become vulnerable to detection by COIN forces.

E-54. Many insurgents are in outstanding physical condition. One of the major advantages an insurgent has is the ability to endure hardship. Due to the situation, insurgents must survive with less, forcing them to adapt and be innovative. Conditioning may also include adaptability in varying weather, difficult terrain, moving great distances, with little food and water. Insurgents who also live in jungles or mountain ranges have a particular advantage over other forces.

E-55. Weapons and equipment (arms, ammunitions, demolitions—types, number, and effectiveness) will vary from insurgency to insurgency and location to location within an area. Generally, combat equipment falls into two categories:

- **Regular.** Small arms, basic load, crew served, sniper systems, mortars, rocket-propelled or rifle-launched grenades, heavier explosive and antitank style weapons. Analysts must know each one's capabilities and ranges. Note that guerrilla tactics use multiple systems together. Study the use of specific weapons to determine which are used in close quarters or open areas and various terrains (woods, jungle, desert, mountain, urban).
- **Special.** These are exceptional weapons used by guerrillas that can cause drastic physical and psychological effects and require counterinsurgents to change basic tactics and responses. These include handheld surface-to-air missiles, antitank guided missiles, platter charges (concave metal plates propelled by an explosive charge designed to penetrate armor), weaponized chemical and biological weapons, radiological based explosives (dirty bombs), heavy mortars, small and mobile rockets.

E-56. Analysts must determine if the insurgents have a reserve capability or way of calling for reinforcements of people or fires. Consider how long an insurgent force and of what size can operate in the area. Know what their ability is to counterattack, defend, and conduct deception operations.

E-57. External support can come in many forms. Most often seen is the use of foreign fighters, advisors, resources, guides, and access to sanctuary. Insurgents will make deals with anybody who can assist them in achieving their objectives even if it goes against previously stated moral stands. The use of poppy growing and the heroin trade by the Taliban in Afghanistan is a classic example.

E-58. Popular support comes in two forms:

- **Active.** This support ranges from those assisting the insurgent cells at times but not regular insurgents, active sympathizers, criminals and groups that the insurgents can “hire out” for sectarian violence, kidnapping, riots or demonstrations, assassinations, smuggling, and sabotage.
- **Passive.** This support is essential for an insurgency. Passive support allows the enemy freedom of movement among the people and denial of assistance to the government for information.

E-59. Information operations and propaganda provide the insurgent with the ability to utilize local leadership, effective themes, become credible, and use credible delivery methods to—

- Propagate the insurgent agenda.
- Exaggerate the effects of military operations.
- Conduct international recruiting campaign.
- Garner national and international support resulting in—
  - Gaining sympathy from adjacent regions, external states, and international organizations to obtain political, moral, resources, and sanctuary support.
  - Leveraging the media as a combat multiplier.
  - Gaining legitimacy locally and abroad.
  - Exploiting the causes of dissatisfaction among the population.
  - Creating political pressure and doubt in the minds of HN government and security forces as well those in the U.S.

## WEAKNESSES

E-60. Insurgents have some weaknesses that can be exploited. Analysts must look for these in order to provide their commander and staff information on vulnerable points in the insurgent force.

E-61. Most insurgencies have limited personnel and resources. Long periods without resupply can affect the enemy’s ability to sustain the effort. If identified as a weakness, it can be exploited by applying pressure to the insurgent force by conducting raids on cell members, recovering enemy caches, interdicting supply routes, searching cars, homes, and personnel entering the AO, separating the insurgents from access to markets, smugglers, black-market goods, and by offensive operations that diminish guerrilla numbers.

E-62. Analysts should study the effectiveness of psychological factors against individual insurgents, sympathizers, and passive supporters. Friendly forces can conduct COIN IO, especially through local leaders and credible members of the HN government and security forces. When done correctly this can encourage insurgent desertions and exasperate the differences between insurgent ideology and that of the government. Properly conducted IO will stress the insurgents’ use of criminal terrorist tactics and external forces. However, friendly forces must address the grievances of the people to deny popular support to the insurgent.

E-63. There are also individual factors which can be analyzed and exploited. Insurgent movements are vulnerable to friendly force IO that show the danger, futility, privation, and numerical inferiority to government forces. In some cases the fear of being treated as a criminal if captured, and fear of violence to them and their family can cause desertions and defections. In some societies, good treatment, pardon, protection, food, shelter, and participation in the government may be stronger incentives than the fear of criminal punishment to induce desertions. Other stress factors include sustained combat and a hostile environment that weakens insurgent resolve.

E-64. Operational weaknesses may include security which requires many resources and slows responsiveness. The insurgent’s dependence on popular support is also a weakness. If support waivers or is withdrawn, the insurgent cannot operate effectively. Another potential operational weakness is the lack of sophisticated communications. This requires the insurgent to spend much time in preparing an operation. Political, religious, and ethnic differences among insurgent groups can be major exploitable weaknesses.

E-65. The decentralized nature of the cells that provide the insurgent OPSEC can also be a weakness because the information moves very slowly. The ability for the insurgent to receive encouragement by superiors and members of the political wing, direction in the face of counterinsurgent pressures, and lack of ability to openly call for reinforcements and sustainment due to their OPSEC plan can make the insurgents feel isolated, alone, confused, and unsupported. Analysts need to look for these points and recommend operations directed at the insurgents to demoralize and promote their defection.

### **ORGANIZATIONAL FLEXIBILITY**

E-66. Flexibility is important to an insurgent's ability to adapt to friendly force tactics, employment, operations, and initiatives. The insurgent must be flexible to be effective and have unity of command. Analysts must look for indicators that tell if the insurgent can strike at will with sufficient combat power.

E-67. The more rigid the insurgent is to loss of key personnel, changing attitudes among the population, counterinsurgent tactics, the introduction of additional security forces, reconstruction and reforms efforts by government agencies, and diminished support among the population the harder it is to maintain the insurgency. This can also become a weakness if the insurgents are prone to jealousy of other elements when they gain notoriety.

E-68. Analysts should study how organizations replace leader and cadre casualties and what the primary factors are which determine how these replacements are selected. Analysts should study the methods the insurgents use to reward and punish their members and whether the methods are consistently applied. Some insurgent groups will have internal rivalries that supersede organizational discipline. Analysts should scrutinize the basic motivation of the members of the insurgency (from leaders to recruits to civilian sympathizers) in line with the insurgent's stated goal, revenge, family, greed, fear, duty, or personal. These factors may be either strengths or weaknesses in an insurgent organization.

### **TERRAIN AND WEATHER**

E-69. Insurgents generally utilize terrain and weather for their operations, resupply, movement, and training to a greater extent than counterinsurgent forces due to their need for secrecy, adaptability and rapid movement, exposure to the elements, desire to blend in, need to conduct their own resupply or live off the land, the need for preplanned escape routes, and the need for detection and early warning of advancing counterinsurgent forces.

E-70. Skilled insurgents will use complex terrain like mountains, woods, swamps, and jungles to diminish the ability of friendly forces to use their technology of close air support, indirect fire, optics, reconnaissance platforms, and armored vehicles. The art of using terrain in guerrilla warfare also includes drawing counterinsurgent forces into terrain that gives the guerrilla force the advantage, like heavily populated and dense urban areas, which provide the insurgent with early warning of the arrival of counterinsurgent elements.

E-71. Urban terrain provides the insurgent the ability to locate and neutralize informants, use gangs for violent actions, and incite angered civilians to attack police or cause riots. Complex terrain also can be used to gain recruits, pass information, plan and prepare for operations, and consolidate and reorganize. Insurgents use the psychological impacts of friendly force operations that result in the injuring, arresting, or mistreatment of civilians in the attempt to reach insurgents.

E-72. Weather may include seasons to fight due to the weather or harvest seasons utilized to move into areas. Certain seasons may mask movement of insurgents with migrating civilians, and provide opportunities to recruit. Daily weather can be used to the advantage of the insurgent and counterinsurgent based on their capabilities and skill. The side with the greater skill will more than likely use weather and terrain to attack their opponent. Operations conducted in the heat, cold, darkness, and inclement weather will generally be used by the more skilled force. The less skilled will be less prepared offensive operations and often less alert to attack.

## CULTURE

E-73. Culture is defined by the ideologies, values, ethics, morals, and what a people define as good and evil. It includes daily structure, directs daily life, and provides a pattern of thinking and behavior. Cultural issues that must be analyzed include—

- Religion (beliefs, customs, and protocols).
- Ideology (political and economic beliefs and work ethic).
- Family (tribe, clan, and family; hierarchies, allegiances, and loyalties; family economic interests; matriarchies versus patriarchies).
- Ethnicity (race, nationality, and minority status—both real and perceived).
- Regional affiliations (internal to a nation and determine those that extend past national borders).
- Law and justice (local rules, laws, and crimes; human, civil, and property rights; types of punishments, and who the police, judge, jury, and enforcers of punishment are).

E-74. The more insurgents understand and practice local culture and the customs, the better their ability to blend in, gain support, and maintain situational awareness.



## Glossary

<b>AA</b>	avenue of approach
<b>ACH</b>	analysis of competing hypotheses
<b>AO</b>	area of operations
<b>ASCOPE</b>	areas, structures, capabilities, organizations, people, events
<b>CARVER</b>	criticality, accessibility, recuperability, vulnerability, effect, recognizability (used in target analysis)
<b>CBRNE</b>	chemical, biological, radiological, nuclear, high-yield explosives
<b>CCIR</b>	commander's critical information requirement
<b>COA</b>	course of action
<b>COIN</b>	counterinsurgency
<b>COP</b>	common operational picture
<b>CP</b>	command post
<b>DCGS-A</b>	Distributed Common Ground System-Army
<b>DSHARPP</b>	demography, symbolism, history, accessibility, recognizability, population, and proximity
<b>DTG</b>	date-time group
<b>EW</b>	electronic warfare
<b>G-2</b>	assistant chief of staff (intelligence)
<b>HN</b>	host nation
<b>HRT</b>	high-risk target
<b>HPT</b>	high-payoff target
<b>HUMINT</b>	human intelligence
<b>HVT</b>	high-value target
<b>IED</b>	improvised explosive device
<b>IO</b>	information operations
<b>IPB</b>	intelligence preparation of the battlefield
<b>ISR</b>	intelligence, surveillance, and reconnaissance
<b>LEA</b>	law enforcement agency
<b>LOC</b>	line of communication
<b>MDMP</b>	military decisionmaking process
<b>METT-TC</b>	memory aid for the mission variables: mission, enemy, terrain and weather, troops and support available, time available, civil considerations
<b>MI</b>	military intelligence
<b>MIL-STD</b>	Department of Defense Military Standard
<b>MTI</b>	moving target indicator

<b>NGO</b>	nongovernmental organization
<b>OAKOC</b>	memory aid for military aspects of terrain: observation and fields of fire, avenue of approach, key terrain, obstacles, concealment and cover
<b>OPSEC</b>	operations security
<b>PIR</b>	priority intelligence requirement
<b>PSYOP</b>	psychological operations
<b>SIGINT</b>	signals intelligence
<b>SITMAP</b>	situation map
<b>SOF</b>	special operations forces
<b>TTP</b>	tactics, techniques, and procedures
<b>UAS</b>	unmanned aircraft system
<b>VBIED</b>	vehicle-borne improvised explosive device
<b>WMD</b>	weapon of mass destruction

## References

### REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

FM 1-02. *Operational Terms and Graphics*. 21 September 2004.

### RELATED PUBLICATIONS

These sources contain relevant supplemental information.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

FM 2-0. *Intelligence*. 17 May 2004.

FM 3-0. *Operations*. 27 February 2008.

FM 3-06.11. *Combined Arms Operations in Urban Terrain*. 28 February 2002.

FM 3-24. *Counterinsurgency*. 15 December 2006.

FM 3-34.230. *Topographic Operations*. 3 August 2000.

FM 3-90. *Tactics*. 4 July 2001.

FM 5-0. *Army Planning and Orders Production*. 20 January 2005.

FM 5-33. *Terrain Analysis*. 11 July 1990.

FM 6-0. *Mission Command: Command and Control of Army Forces*. 11 August 2003.

FMI 2-01.301. *Specific Tactics, Techniques, and Procedures and Applications for Intelligence Preparation of the Battlefield*. 31 March 2009.

JP 2-03. *Geospatial Intelligence Support to Joint Operations*. 22 March 2007.

JP 3-0. *Joint Operations*. 17 September 2006.

JP 3-05.1. *Joint Special Operations Task Force Operations*. 26 April 2007.

MIL-STD-2525C. *Common Warfighting Symbolology*. 17 November 2008. (Contains symbols created after FM 1-02 was published.)

### READINGS RECOMMENDED

Elder, Linda and Richard Paul. *25 Days to Better Thinking and Better Living*. Upper Saddle River, NJ: Pearson Prentice Hall. 2006. [www.criticalthinking.org](http://www.criticalthinking.org).

Elder, Linda and Richard Paul. *The Thinker's Guide to Analytic Thinking*. Dillon Beach: Foundation for Critical Thinking Press. 2007. [www.criticalthinking.org](http://www.criticalthinking.org).

Elder, Linda and Richard Paul. *The Miniature Guide to the Human Mind*. Dillon Beach: Foundation for Critical Thinking Press. 2007. [www.criticalthinking.org](http://www.criticalthinking.org).

Elder, Linda and Richard Paul. *The Thinker's Guide to Intellectual Standards*. Dillon Beach: Foundation for Critical Thinking Press. Paul, Richard and Linda Elder [www.criticalthinking.org](http://www.criticalthinking.org).

Elder, Linda and Richard Paul. *The Thinker's Guide: A Glossary of Critical Thinking Terms and Concepts*. Dillon Beach: Foundation for Critical Thinking Press. 2009. [www.criticalthinking.org](http://www.criticalthinking.org).

## References

---

- Paul, Richard and Linda Elder. *Critical Thinking: Tools for Taking Charge of Your Professional and Personal Life*. Upper Saddle River, NJ: Pearson Prentice Hall. 2002.  
www.criticalthinking.org.
- Paul, Richard and Linda Elder. *The Miniature Guide to Understanding the Foundations of Ethical Reasoning*. Dillon Beach: Foundation for Critical Thinking Press. 2006.  
www.criticalthinking.org.
- Paul, Richard and Linda Elder. *The Thinkers Guide to Fallacies: The Art of Mental Trickery and Manipulation*. Dillon Beach: Foundation for Critical Thinking Press. 2006.  
www.criticalthinking.org.
- Paul, Richard and Linda Elder. *The Miniature Guide to the Art of Asking Essential Questions*. Dillon Beach: Foundation for Critical Thinking Press. 2006. www.criticalthinking.org.
- Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking Concepts and Tools*. Dillon Beach: Foundation for Critical Thinking Press. 2009. www.criticalthinking.org .

## SOURCES USED

These are the sources quoted or paraphrased in this publication.

- Elder, Linda and Richard Paul. *The Thinker's Guide to Analytic Thinking*. 2007.
- Elder, Linda and Richard Paul. *The Miniature Guide to Critical Thinking: Concepts and Tools*. 2008.
- Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Central Intelligence Agency: Center for the Study of Intelligence, 1999. <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/index.html>.

## PRESCRIBED FORMS

None.

## REFERENCED FORMS

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

# Index

Entries are by page number.

## A

activities matrix, 2-20, 5-11, 5-12  
analysis of  
  area of operations, 1-3, B-1, B-2  
  enemy intent, 1-1  
  environment, 3-17  
  indicators, 4-13  
  information, 4-1, 5-1  
  operational effectiveness, E-7  
  situation, 4-2  
  situation map, 4-4  
  weather, 3-17  
  weather conditions, 4-11  
analysis of competing hypotheses, 2-1, 2-10  
  matrix, 2-13  
  procedures, 2-11  
  steps, 2-11  
  tests, 2-16  
analytical pitfalls, viii, 2-10, A-4  
analytical process, 5-1, B-1  
areas, structures, capabilities, organizations, people, events, 3-20, 3-21  
  civil considerations, B-3  
  elements, 3-21  
  variables, 3-21  
association matrix, 2-20, 5-11, 5-12, 5-13, 5-17  
automated analysis tools, 5-18

## C

civil considerations, 1-3, 3-1, 3-20, 3-21, 5-20, B-1, B-3  
combined obstacle overlay, 3-16  
conceptual modeling, 2-19  
course of action, v, 1-3, 1-4, 2-13, 2-20, 3-1, 3-6, 3-14, 3-17, 4-1, 4-4, 4-9, 4-11, 4-12, 5-1  
  development, 1-5

wargaming, 1-5, B-9

critical thinking, 2-1  
criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER), D-1

## D

databases, 1-2, 2-21, 3-13  
  all-source, 4-11  
  cultural, 3-24  
  geospatial, 3-17  
  intelligence, 5-19  
  multiple, 5-19  
  terrain, 3-17  
  types of, 5-19  
  web-based, 5-19  
deductive reasoning, 2-8  
demography, symbolism, history, accessibility, recognizability, population, and proximity (DSHARPP), D-3, D-4  
diagram  
  iconic, 5-8  
  link, 2-21, 4-3, 4-4, 5-11, 5-14, 5-15, E-7  
  network, 2-21  
  network nodal, 5-9  
  organizational, E-7

## E

enemy course of action, 4-3, 4-4, 4-11, 4-13, B-8, B-9

## F

force generation, 1-1, 1-2, 4-11  
friendly course of action, 4-4, B-5, B-6, B-9  
full spectrum operations, vii, 1-3, 2-20  
  threat characteristics, 3-1  
functional analysis, 2-20, 2-21, 4-1, 4-6, 4-9, 5-4

## I

incident overlay, 4-4, 5-4  
indicators, E-7, E-11  
  analyzing, 4-14  
  asymmetric, C-1  
  clan, C-12  
  commodities, C-9  
  deceptive, 4-12  
  defensive, C-4  
  delaying, C-5  
  developing, 4-11, 4-14, 4-15  
  environment-related, C-10  
  examples of, 4-15  
  false, 4-12  
  improvised explosive device, C-11  
  intelligence, 4-4  
  multiple, 4-11  
  offensive, C-3  
  population, C-6  
  propaganda, C-8  
  sample, 4-12  
  tactical, 2-20  
  threat environment, C-11  
  weighting, 4-12  
  withdrawal, C-5  
inductive reasoning, 2-8  
  stages, 2-8  
information superiority, 1-1  
insurgency factors, E-8  
  organizational flexibility, E-11  
  strengths, E-8  
  terrain and weather, E-11  
  weaknesses, E-10  
insurgent tactics, 3-4  
intelligence analysis  
  art of, 2-13, 2-15, 4-4  
  automation, 5-18  
  fundamentals, v  
  in counterinsurgency operations, viii, E-1  
  methodology, 2-18, 2-20  
  process, 1-1, 2-20  
    functional, 2-20  
    link, 2-20

nodal component, 2-21  
 pattern, 2-21  
 predictive, 2-20

intelligence characteristics, 1-2  
 accurate, 1-2  
 predictive, 1-2  
 relevant, 1-2  
 timely, 1-2

intelligence preparation of the  
 battlefield  
 process, 1-3, 2-20, 3-5, 4-1,  
 4-3, 4-4, 5-1  
 products, 4-11

intelligence process, 1-2

intelligence running estimate, v,  
 1-3, 2-16, 4-1, 4-3, 4-4, B-1,  
 B-2

intelligence warfighting  
 function, viii, 1-2

intelligence, surveillance, and  
 reconnaissance, 1-1  
 assets, 2-17  
 operations, 1-1, 1-4  
 overlay, 1-5  
 plan, 1-5  
 synchronization, 1-2, 1-5

**L**

link analysis, 2-9, 2-20, 3-11, 5-  
 1, 5-11, 5-14, 5-18, 5-20, E-  
 7, E-8

**M**

military aspects of terrain, 3-14,  
 4-11, B-2

military aspects of weather, 3-  
 17  
 cloud cover, 3-19  
 humidity, 3-20  
 precipitation, 3-19  
 temperature, 3-20  
 visibility, 3-17

military decisionmaking  
 process, 1-2, 1-3, 1-4, 4-1,  
 4-4, B-1

mission analysis, 1-4, 1-5

**N**

nodal component analysis, 2-  
 21, 5-1, 5-4, 5-8

**O**

operational effectiveness, 3-7

operational environment, vii, 1-  
 2, 3-5, 5-2, 5-18, E-8  
 analysis, 3-5  
 and the threat, 4-1  
 ASCOPE, 3-20  
 characteristics, 4-10  
 cultural aspects, 3-13  
 cultural information, 3-24  
 definition, 1-1  
 indicators, C-1  
 overlays, 3-16  
 process, v  
 terrain effects, 3-17  
 threat characteristics, 3-12,  
 4-14  
 understanding, 1-1

operational themes, vii, viii

**P**

pattern analysis, 2-9, 2-21, 4-3,  
 4-4, 5-1, 5-2, 5-4, E-8

predictive analysis, 2-20, 5-1

**R**

reasoning, 2-2  
 analogy, A-3  
 in a circle, A-2, A-3  
 process, A-1  
 tests, 2-16

**S**

scientific method  
 communicate results, 2-10  
 define the program, 2-9  
 draw conclusion, 2-10  
 form hypothesis, 2-9  
 gather data, 2-9  
 steps, 2-9  
 test hypothesis, 2-9

situation development, 4-1, 4-2,  
 4-11, 5-1

situation map, 4-2, 4-4  
 purpose, 4-3

situation template, 4-3, 4-11

situational awareness, 4-3, 4-4,  
 5-20, B-3, E-12

situational logic, 2-1, 2-19

situational understanding, 1-1,  
 1-4, 3-1, 4-1, 4-14

staff weather officer, B-4

support operations categories,  
 3-9

sustainment categories, 3-6

**T**

targeting operations, viii, 1-1, 1-  
 2, 5-18, 5-20, D-1, D-2

terrain analysis, 3-14, 3-17, 4-  
 3, B-2, B-4  
 and weather, 5-18

threat  
 analysis, 3-1, 4-6  
 capabilities, 3-1, 4-8, 4-9, 4-  
 10, 4-11, B-5  
 characteristics, 1-1, 3-1, 3-  
 12, 4-3, 4-4, 4-10, 4-11,  
 4-14, B-5, B-7, E-1  
 environment, vii, D-3  
 functions, 4-6  
 objectives, 4-6

threat characteristics  
 in counterinsurgency  
 operations, E-1

threat characteristics for full  
 spectrum operations, 3-1  
 composition, viii, 3-1, 3-4, 3-  
 12, 4-2, 4-11, 4-14  
 database, 3-12  
 disposition, 1-1, 2-8, 3-1, 3-  
 3, 3-12, 4-1, 4-2, 4-10, 4-  
 11, 4-14  
 in irregular warfare, vii, viii,  
 3-13, 4-11  
 recordkeeping, 3-12  
 recruitment, 3-8  
 tactics, 1-3, 3-1, 3-4, 3-5, 3-  
 8, 4-14, E-2, E-5, E-9  
 training, 3-4, 3-8, 4-14

threat course of action, 2-20, 4-  
 1, 4-10, 4-12, B-8

time event analysis, 5-1

**W**

weather  
 analysis, 3-17, 3-19, B-4  
 and terrain, 1-1  
 data, 3-17  
 effects, 1-1, 3-14, 3-17, 3-  
 19  
 team, 3-17

**TC 2-33.4**  
**1 July 2009**

By order of the Secretary of the Army:

**GEORGE W. CASEY, JR.**  
*General, United States Army*  
*Chief of Staff*

Official:



**JOYCE E. MORROW**  
*Administrative Assistant to the*  
*Secretary of the Army*  
0916303

**DISTRIBUTION:**

*Active Army, Army National Guard, and U.S. Army Reserve:* Not to be distributed; electronic media only.

PIN: 085562-000

**FOR OFFICIAL USE ONLY**