ATP 2-01.3
MCRP 2-10B.1
(Formerly MCRP 2-3A)

Intelligence Preparation of the Battlefield/*Battlespace*

November 2014

Headquarters, Department of the Army
Headquarters, United States Marine Corps

ERRATUM

to

MCRP 2-3A

INTELLIGENCE PREPARATION OF THE BATTLEFIELD/BATTLESPACE

1. Change all instances of MCRP 2-3A, *Intelligence Preparation of the Battlefield/Battlespace*, to MCRP 2-10B.1, *Intelligence Preparation of the Battlefield/Battlespace.*

2. File this transmittal sheet in the front of this publication.

This publication is available at Army Knowledge Online
(https://armypubs.us.army.mil/doctrine/index.html).
To receive publishing updates, please subscribe at
http://www.apd.army.mil/AdminPubs/new_subscribe.asp.

+*This publication is available at the U.S. Marine Corps
Doctrine Web site (https://doctrine.usmc.mil)*

ATP 2-01.3, C1
MCRP 2-3A, C1

Army Techniques Publication	*Headquarters*
No. 2-01.3	*Department of the Army*
Marine Corps Reference Publication	*Washington, DC*
No. 2-3A	

Headquarters
United States Marine Corps
Deputy Commandant
Combat Development & Integration
Quantico, Virginia

26 March 2015

Intelligence Preparation of the Battlefield/*Battlespace*

1. This change changes the distribution restriction on this manual, adds the uniform resource locator for the U.S. Marine Corps Doctrine Web Site to the inside cover, and corrects the U.S. Marine Corps address on the title page.

2. A plus sign (+) indicates changed material.

3. ATP 2-01.3/MCRP 2-3A, 10 November 2014, is changed as follows:

Remove Old Pages	**Insert New Pages**
front cover	front cover
pages i through ii	pages i through ii

4. File this transmittal sheet in the front of the publication for reference purposes.

Marine Corps PCN: 144 000141 00

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1506206

By Direction of the Commandant of the Marine Corps:

K. J. GLUECK, JR.
Lieutenant General, U.S.
Marine Corps
Deputy Commandant
Combat Development and
Integration

DISTRIBUTION:

Active Army, the Army National Guard, and the United States Army Reserve. Not to be distributed; electronic media only.

Intelligence Preparation of the Battlefield/*Battlespace*

Contents

PART TWO   FUNDAMENTAL TASK TECHNIQUES

Figures

Tables

Preface

ATP 2-01.3/*MCRP 2-3A* is a dual-designated Army and Marine Corps manual that constitutes current doctrine on how to systematically evaluate the effects of significant characteristics of the operational environment for specific missions. It describes how the commander and staff examine mission variables to understand how these variables may affect operations. It discusses intelligence preparation of the battlefield/*intelligence preparation of the battlespace* (IPB) as a critical component of the military decisionmaking process (MDMP)/*Marine Corps Planning Process (MCPP)* and how IPB supports decisionmaking, as well as integrating processes and continuing activities.

This publication supersedes FM 2-01.3/*MCRP 2-3A* and FMI 2-01.301 and expedites delivery of doctrine that the proponent has approved for immediate use in IPB support to operations. It facilitates a common understanding, foundational concepts, and methods of the IPB process.

The principal audience for ATP 2-01.3/*MCRP 2-3A* is Army/*Marine Corps* commanders and staffs. Commanders and staffs of Army/*Marine Corps* headquarters serving as a joint task force or a multinational headquarters also refer to applicable joint or multinational doctrine related to IPB. Trainers and educators throughout the Army/*Marine Corps* also use this publication.

ATP 2-01.3/*MCRP 2-3A* uses joint terms where applicable. Selected joint, Army, and *Marine Corps* terms, and definitions appear in both the glossary and the text. In doctrinal publications, the normal convention for identifying terms is through the use of italics. Since this is a dual-designated Army and *Marine Corps* manual, the following protocol is used to distinguish proponency (authority) for information and terms:

- Terms and phrasing in italics—Marine Corps.
- Terms and definitions in bold—Terms for which ATP 2-01.3/*MCRP 2-3A* is the proponent publication.
- Terms in bold and definitions in plain text—Joint terms and Army terms with proponent publication other than ATP 2-01.3, with the proponency publication in parentheses.

All references to "staffs" in this manual refer to the operations, intelligence, and other coordinating and special staff sections unless indicated otherwise.

This manual applies to intelligence activities conducted outside the United States. Intelligence activities conducted inside the United States, as well as those that target U.S. persons and groups outside the United States, invoke additional requirements and intelligence oversight rules. To the extent any of the activities described in this publication are conducted inside the United States, or target U.S. persons or groups outside the United States, consult your judge advocate for assistance.

ATP 2-01.3/*MCRP 2-3A* applies to the Active Army and Marine Corps, the Army National Guard/Army National Guard of the United States, United States Army Reserve, and the United States Marine Corps Reserve unless otherwise stated.

The proponent of ATP 2-01.3/*MCRP 2-3A* is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Capabilities Development and Integration Division, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-CDI-D (ATP 2-01.3), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017, by e-mail to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

United States Marine Corps readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in MCO 3900.15B, which can be obtained from the Marine Corps Publications Electronic Library Online.

The UNS recommendation should include the following information:
- *Location of change.*
  - *Publication number and title.*
  - *Current page number.*
  - *Paragraph number (if applicable).*
  - *Line number.*
  - *Figure or table number (if applicable).*
- *Nature of change.*
  - *Addition or deletion of text.*
  - *Proposed new text.*

Introduction

ATP 2-01.3/*MCRP 2-3A* updates and describes the fundamentals of IPB. The following paragraphs summarize the most important updates and changes.

ATP 2-01.3/*MCRP 2-3A* contains 10 chapters and two appendixes.

Chapter 1 makes the following change: Redefines the Army's definition of IPB as "Intelligence Preparation of the Battlefield (IPB) is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations."

Chapter 3 replaces the sub-steps of step 1 with the following:

- Identify the limits of the commander's area of operations (AO).
- Identify the limits of the commander's area of interest.
- Identify significant characteristics within the AO and area of interest for further analysis.
- Evaluate current operations and intelligence holdings to determine additional information needed to complete IPB.
- Initiate processes necessary to acquire information necessary to complete IPB.

Chapter 4 replaces the sub-steps of step 2 with the following:

- Describe how the threat/*adversary* can affect friendly operations.
- Describe how terrain can affect friendly and threat/*adversary* operations.
- Describe how weather can affect friendly and threat/*adversary* operations.
- Describe how civil considerations can affect friendly and threat/*adversary* operations.

Chapter 5 replaces the sub-steps of step 3 with the following:

- Identify threat characteristics/*adversary order of battle*.
- Create or refine threat/*adversary* models.

Chapter 6 replaces the sub-steps of step 4 with the following:

- Develop threat/*adversary* courses of action (COAs).
- Develop the event template and matrix.

G-2/S-2 is used in cases when actions are conducted by both U.S. Army and the Marine Corps.

This publication uses "holdings" to annotate many different feeds (for example, biometrics). "Holdings" is used in this publication to refer to information or data, such as data files and/or databases that the command or its higher headquarters has, or information that the command can access. This publication avoids discussing specific disciplines and complementary intelligence capabilities. It describes the IPB process which occurs after this information is collected, processed, and stored.

Based on current doctrinal changes, certain terms for which ATP 2-01.3/*MCRP 2-3A* is proponent have been added, rescinded, or modified for purposes of this manual. The glossary contains acronyms and defined terms. See introductory table 1 and introductory table 2 on the next page for specific term changes.

Introductory table 1. Rescinded Army terms

Term	Remarks
event template	Rescinded Army definition. Adopts the joint definition.

Introductory table 2. Modified Army terms

Term	Remarks
intelligence preparation of the battlefield/*battlespace*	Modifies the definition.
latest time information is of value	Proponent publication changed to ATP 2-01.

Fundamental Principles, Process Activities, and Relationships

---

Chapter 1

Fundamentals of Intelligence Preparation of the Battlefield/*Battlespace*

INTELLIGENCE PREPARATION OF THE BATTLEFIELD/ *BATTLESPACE* (IPB)

1-1.   **Intelligence Preparation of the Battlefield (IPB) is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations.** *Intelligence Preparation of the Battlespace (IPB) is the systematic, continuous process of analyzing the threat and environment in a specific geographic area.*

1-2.   The G-2/S-2 begins preparing for IPB during the generate intelligence knowledge task/*problem framing step*. (For U.S. Army, see FM 7-15, chapter 2, for the complete list of tasks and their measures of performance. *For the Marine Corps, see MCWP 5-1 for information on problem framing.*) The intelligence staff creates data files and/or databases based on the operational environment. Given the limited time available to collect and evaluate information, this information may not be specific enough to support the military decisionmaking process (MDMP)/*Marine Corps Planning Process (MCPP)*. However, this information helps create the operational environment frame during the design methodology.

1-3.   IPB results in the creation of intelligence products that are used during the MDMP/*MCPP* to aid in developing friendly courses of action (COAs) and decision points for the commander. Additionally, the conclusions reached and the products created during IPB are critical to planning information collection/*intelligence collection* and targeting operations. (*See MCWP 5-1 for a discussion on the MCPP.*)

1-4.   The G-2/S-2 leads this staff effort and begins preparing for IPB during the generate intelligence knowledge process associated with force generation and is incorporated into the Army design methodology. During generate intelligence knowledge, the intelligence staff creates data files on specific operational environments based on an evaluation of the information and intelligence related to the operational variables identified in the memory aid PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, time)/*PMESII (political, military, economic, social, information, and infrastructure)*. (*For the Marine Corps, see MCWP 5-1 for more information on intelligence support to planning and problem framing.*)

1-5.   Given the limited time available to collect and evaluate information and intelligence on the operational variables, this information may not be specific enough to support the MDMP/*MCPP*. However, it can be used by the commander and the entire staff to aid the Army design methodology. Throughout the operations process, the commander and staff continue to collect information and analyze the operational variables in order to provide increased situational understanding. Upon receipt of a warning order or

mission, they draw relevant information that was categorized by the operational variables and filter it into the mission variables used during mission analysis/*problem framing*. During IPB, the staff focuses on the relevant aspects of the operational environment as it pertains to their warfighting function and the mission variables. The intelligence staff is primarily focused on the mission variables of enemy, terrain, weather, and civil considerations.

1-6.   To be effective, IPB must—

- Accurately define the commander's area of interest in order to focus collection and analysis on the relevant aspects of the mission variables of enemy, terrain, weather, and civil considerations. Relevant is defined as having significant effect on friendly operations and threat/*adversary* operations, and population in a unit's area of operations (AO).
- Describe how each of these four mission variables will affect friendly operations and how terrain, weather, and civil considerations will affect the enemy.
- Provide the IPB products necessary to aid each step of the MDMP/*MCPP* in accordance with the planning timelines and guidance provided by the commander.
- Determine how the interactions of friendly forces, enemy forces, and indigenous populations affect each other to continually create outcomes that affect friendly operations. This aspect of IPB is not the sole responsibility of the intelligence staff. This complex analysis involves the commander and the entire staff working together to determine these effects.

1-7.   IPB is most effective and best aids the commander's decisionmaking when the intelligence staff integrates the expertise of the other staff and supporting elements, such as civil affairs teams and military information support personnel, into its analysis. This is especially true when operating in environments where the effects of the enemy, terrain, weather, and civil considerations are complex and not easily determined.

1-8.   IPB aids commanders in reducing uncertainty by evaluating how the enemy, terrain, weather, and civil considerations may affect operations and decisionmaking. Most intelligence requirements are generated as a result of IPB and its interrelationship with decisionmaking.

1-9.   A key aspect of IPB is refinement. The conclusions made and the products developed during IPB are continually refined throughout the operation. This information is incorporated into the running estimate as new information is obtained and further analysis is conducted during situation development. This refinement ensures that the commander's decisions are based on the most current information and intelligence available.

PROCESS ACTIVITIES

1-10.   The IPB process consists of the following four steps:

- Define the operational environment.
- Describe environmental effects on operations/d*escribe the effects on operations*.
- Evaluate the threat/*adversary*.
- Determine threat/*adversary* COAs.

STEP 1—DEFINE THE OPERATIONAL ENVIRONMENT

1-11.   Defining the operational environment results in the identification of significant characteristics of the operational environment that can affect friendly and enemy operations. This step also results in the identification of gaps in current intelligence holdings. (Step 1 is discussed fully in chapter 3.)

1-12.   Step 1 is important because it assists the commander in defining relative aspects of the operational environment in time and space. During step 1, the intelligence staff must identify those significant characteristics related to the mission variables of enemy, terrain, weather, and civil considerations that are relevant to the mission and justify that analysis to the commander. Failure to identify or misidentify the effect these variables may have on operations can hinder decisionmaking and result in the development of an ineffective information collection strategy/*intelligence collection strategy* and targeting effort.

1-13. Understanding friendly and enemy forces is not enough; other factors, such as culture, languages, tribal affiliations, and operational and mission variables, can be equally important. Defining the significant characteristics of the operational environment is essential in identifying the additional information needed to complete IPB. Once approved by the commander, this information becomes the command's initial intelligence requirements. This focuses the command's initial information collection efforts/*intelligence collection efforts* and the remaining steps of the IPB process.

1-14. *For the Marine Corps, the term "operational environment" is consistent with the need to study and learn as much as possible about a situation. Essentially, commanders analyze the operational environment in order to determine the physical dimensions of their battlespace in the form of areas of interest, influence, and operations. (See MCDP 1-0.)*

STEP 2—DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS/*DESCRIBE THE EFFECTS ON OPERATIONS*

1-15. Once the intelligence staff has identified in step 1 of IPB the significant characteristics related to enemy, terrain, weather, and civil considerations of the operational environment, step 2 describes how these characteristics affect friendly operations. The intelligence staff also describes how terrain, weather, civil considerations, and friendly forces affect enemy forces. This evaluation focuses on the general capabilities of each force until threat/*adversary* COAs are developed in step 4 of IPB and friendly COAs are developed later in the MDMP/*MCPP*. Finally, the entire staff determines the impact and effects to the population of friendly and enemy force actions.

1-16. If the intelligence staff does not have the information it needs to form conclusions, it uses assumptions to fill information gaps—always careful to ensure the commander understands when assumptions are used in place of fact to form conclusions. (Step 2 is discussed fully in chapter 4.)

STEP 3—EVALUATE THE THREAT/*ADVERSARY*

1-17. The purpose of evaluating the threat/*adversary* is to understand how a threat/*adversary* can affect friendly operations. Although threat/*adversary* forces may conform to some of the fundamental principles of warfare that guide Army/*Marine Corps* operations, these forces will have obvious, as well as subtle, differences in how they approach situations and problem solving. Understanding these differences is essential in understanding how a threat/*adversary* force will react in a given situation. Threat/*adversary* evaluation does not begin with IPB. The intelligence staff conducts threat/*adversary* evaluation and develops threat/*adversary* models as part of the generate intelligence knowledge task of support to force generation. Using this information, the intelligence staff refines threat/*adversary* models, as necessary, to support IPB. When analyzing a well-known threat/*adversary*, the intelligence staff may be able to rely on previously developed threat/*adversary* models. When analyzing a new or less well-known threat/*adversary*, the intelligence staff may need to evaluate the threat/*adversary* and develop models during the mission analysis step of the MDMP/*problem framing step of MCPP*. When this occurs, the intelligence staff relies heavily on the threat/*adversary* evaluation conducted by higher headquarters and other intelligence agencies.

1-18. In situations where there is no threat/*adversary* force, the intelligence analysis conducted and the products developed relating to terrain, weather, and civil considerations may be sufficient to support planning. An example of this type of situation is a natural disaster. (Step 3 is discussed fully in chapter 5.)

STEP 4—DETERMINE THREAT/*ADVERSARY* COURSES OF ACTION

1-19. During step 4 the intelligence staff identifies and develops possible threat/*adversary* COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat/*adversary* COAs to aid in developing friendly COAs during the COA development and selecting a friendly COA during COA steps of the MDMP/*MCPP*. The identification and development of all valid threat/*adversary* COAs minimize the potential of the commander being surprised by an unanticipated enemy action.

1-20. Failure to fully identify and develop all valid threat/*adversary* COAs may lead to the development of an information collection strategy/*intelligence collection strategy* that does not provide the information necessary to confirm what COA the enemy has taken and may result in the commander being surprised. When needed, the staff should identify all significant civil considerations (this refers to those civil considerations identified as significant characteristics of the operational environment) so that the interrelationship of threat/*adversary*, friendly forces, and population activities is portrayed.

1-21. The staff develops threat/*adversary* COAs in the same manner friendly COAs are developed. Although written specifically as a guide to develop friendly COAs, the COA development discussion in ADRP 5-0/*MCWP 5-1* is an excellent model to use in developing valid threat/*adversary* COAs that are suitable, feasible, acceptable, unique, and consistent with threat/*adversary* doctrine. Although the intelligence staff has the primary responsibility for developing threat/*adversary* COAs, it needs assistance from the rest of the staff to ensure the most accurate and complete analysis is presented to the commander. (Step 4 is discussed fully in chapter 6.)

INTELLIGENCE ESTIMATE

1-22. The intelligence estimate includes all the IPB products necessary to support planning and operations, such as—

- Enemy situation overlays with associated COA statements and high-value target lists (HVTLs).
- Event templates and associated event matrices.
- Modified combined obstacle overlays (MCOOs), terrain effects matrices, and terrain assessments.
- Weather forecast charts, weather effects matrices/*operational impacts charts*, light and illumination tables, and weather estimates.
- Civil considerations overlays and assessments.

STAFF INTEGRATION INTO IPB

1-23. Staff sections bring their own areas of expertise to IPB. Collaborative analysis among the staff facilitates a greater degree of situational understanding for the commander.

Collaboration Examples

The intelligence staff can provide the personnel staff with information on how the threat/*adversary* may affect personnel replacement or casualty evacuation.

The intelligence staff can provide the sustainment staff with threat/*adversary* information that may have an impact on friendly logistic efforts.

Conversely, the intelligence staff needs to utilize the expertise of the other staff sections.

Collaborating with the staff engineers can provide valuable information on terrain mobility, where the threat/*adversary* is likely to emplace obstacles, and where the threat/*adversary* could employ engineer assets.

Coordinating with the surgeon concerning the health status of threat/*adversary* forces can indicate the willingness of threat/*adversary* forces to engage in long-term operations.

1-24. Staff sections bring their expertise to IPB as follows:

- The chief of staff, or executive officer—
    - Synchronizes staff activities during IPB.
    - Using tools, such as the one-third to two-thirds planning rule as a guide, determines—
        - How long each step of the MDMP/*MCPP* will take.
        - How much time is allocated to mission analysis/*problem framing.*
- How much time within mission analysis/*problem framing* can be sub-allocated to IPB. The G-2/S-2 has staff responsibility for the analysis of enemy, terrain, weather, and civil considerations. The G-2/S-2 aids the commander in improving the understanding of how these mission variables can affect operations through the production of an intelligence assessment that supports the MDMP/*MCPP*; the integrating processes of targeting and risk management; and the continuing activities of information collection/*intelligence collection* and security operations. The rest of the staff aids the G-2/S-2 in this effort.
- The G-3/S-3 is the staff subject matter expert (SME) on the art and science of military operations and aids the G-2/S-2 by—
    - Evaluating threat/*adversary* COAs to ensure they are valid from an operational perspective.
    - Evaluating enemy situation overlays, COA statements, HVTLs, and civil considerations overlays and assessments to ensure they contain the information necessary to support friendly COA development and analysis.
    - Evaluating the event template and matrix to ensure they contain the information necessary to support friendly COA analysis and the development of the decision support template.
- The G-4/S-4 is the staff SME on sustainment operations and aids the G-2/S-2 by—
    - Assisting in identifying and evaluating threat/*adversary* and host-nation logistic capabilities.
    - Assisting in identifying potential supply routes and resupply points.
- The G-6/S-6 is the staff SME on friendly communications systems and aids the G-2/S-2 by assisting in identifying and evaluating friendly communications systems' vulnerabilities to cyber and electronic attack.
- For U.S. Army, the Information Operations Office is responsible for integrating information-related capabilities and aids the G-2/S-2 by assisting in identifying and evaluating threat/*adversary* information capabilities and deception and denial capabilities, as well as the means to influence the population. *For the Marine Corps, the G-3/S-3 is responsible for information operations.*
- For U.S. Army, the G-9/S-9 is the staff SME on civil affairs operations. *For the Marine Corps, the G-3/S-3 is responsible for civil affairs.* This section aids the G-2/S-2 by—
    - Assisting in identifying and evaluating civil considerations on military operations and evaluating the effect of military operations on civilian populations in conjunction with the G-3/S-3.
    - Assisting, along with the chief of fires or fire support officer/*fire support coordinator or force fires coordinator,* in identifying protected targets.
    - Creating and maintaining civil considerations assessments, files, and data files and/or databases.
- For U.S. Army, the chief of fires at division and above and the fire support officer at brigade and below is the staff SME on fires. *For the Marine Corps, the fire support coordinator at battalion, the Marine expeditionary unit, regiment, and division and the force fires coordinator at the Marine expeditionary brigade and the Marine expeditionary force is the SME on fires.* The SME on fires (artillery and air defense) aids the G-2/S-2 by—
    - Assisting in developing threat/*adversary* high-value targets (HVTs).
    - Assisting in evaluating threat/*adversary* fire support operations, including identifying potential friendly high-payoff targets (HPTs) from the threat/*adversary* perspective.

- Assisting in positioning threat/*adversary* fire support assets on the situation template.
- Assisting the staff on protection from threat/*adversary* air and aids the G-2/S-2 by assisting in identifying enemy air avenues of approach (AAs) and in assessing threat/*adversary* fixed-wing, rotary-wing, and air defense capabilities.

- The engineer coordinator is the staff SME on mobility and countermobility and aids the G-2/S-2 by assisting in developing enemy obstacle plans for the threat/*adversary* situation overlay.
- The chemical, biological, radiological, and nuclear (CBRN) officer is the staff SME on CBRN and aids the G-2/S-2 by assisting in determining the locations of CBRN assets and potential areas of employment.
- The surgeon is the staff SME for the analysis and disposition of captured enemy medical materiel and for the analysis of any medications carried by captured or detained threat/*adversary* personnel.

1-25. Deployed units will have additional subject matter expertise that will have input to the IPB process, such as the following groups:

- For U.S. Army, human terrain teams (HTTs), when available, can provide sociocultural research and analysis of the population that supports the intelligence staff's analysis of civil considerations. Units that support corps, divisions, and brigade combat teams without a HTT get this support from the supported headquarters. *For the Marine Corps, when available, foreign area officers, regional affairs officers, other cultural enablers, State Department officers, and other knowledgeable sources can provide sociocultural information, research, and analysis of the population.*
- Red Teams.

RELATIONSHIPS

1-26. As one of the integrating processes, IPB is integral to targeting, risk management, information collection/*intelligence collection*, planning, and decisionmaking. IPB is also related to generate intelligence knowledge and situation development.

TARGETING

1-27. Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. During steps 3 and 4 of IPB, the intelligence staff identifies HVTs associated with each threat/*adversary* capability or COA. This aids the fires cell in conducting target-value analysis (TVA). The following techniques may be useful in identifying and evaluating HVTs:

- Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and size, activity, location, unit, time, and equipment (SALUTE) reports. A review of threat/*adversary* tactics, techniques, and procedures (TTP) and previous threat/*adversary* operations as well as understanding threat/*adversary* objectives, tasks, purpose, and intent will be useful.
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat/*adversary* might react to the loss of each identified HVT. Consider the threat's/*adversary's* ability to substitute other assets as well as to adopt branches or sequels.

1-28. After identifying the set of HVTs, place them in order of their relative worth to the threat's/*adversary's* operation and record them as part of the threat/*adversary* model. A HVT's value will vary throughout an operation.

1-29. The high-payoff target list (HPTL) is a prioritized list of HPTs. A **high-payoff target** is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60). HPTs are those HVTs that must be acquired and successfully attacked for the success of the friendly commander's mission. HPTs are developed by the staff, and can include various threat/*adversary* considerations that can be detrimental to the success of friendly missions.

1-30. The intelligence staff, aided by other warfighting staffs, also identifies the indicators associated with these targets that assist in determining their location and activities. Chapter 6 discusses the development of HVTs and indicators. Developing HVTs during IPB is essential to developing HPTs during the COA development step of MDMP/*MCPP*, and refining those targets throughout the operations process, particularly during targeting boards and meetings. During targeting meetings, the intelligence officer, along with other staff elements, assesses friendly capabilities, friendly missions, and the effects of friendly actions on the civilian populace. As HPTs are identified, the analysis of enemy, terrain, weather, and civil considerations conducted during IPB aids in developing intelligence target packages on these targets. (See FM 3-60 for more information on targeting.)

RISK MANAGEMENT

1-31. Risk management is a process for identifying hazards and controlling risks. Throughout the operations process commanders and staffs use risk management to mitigate risks associated with all hazards that have the potential to injure or kill friendly and civilian personnel, damage or destroy equipment, or otherwise impact mission effectiveness. (See ATP 5-19 for additional information on risk management.)

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE AND INFORMATION COLLECTION/*INTELLIGENCE COLLECTION*

1-32. Information collection/*intelligence collection* relies on the results of IPB. The staff's completion of IPB provides an analysis of the operational environment and the options it presents to friendly and threat/*adversary* forces. It also provides information required to plan information collection/*intelligence collection* activities, such as—

- Characteristics of the area of interest that will influence friendly and threat/*adversary* operations (including civil considerations).
- Enemy event templates, including decision points and matrices critical to information collection planning.
- Information collection assets' sensitivities to weather and the effects of weather on planned or potential operations.
- Threat characteristics/*adversary order of battle*, doctrine, tactics, techniques, and behavior.
- Possible and likely threat/*adversary* COAs.
- HVTs.

1-33. The Army/*Marine Corps* executes intelligence, surveillance, and reconnaissance through the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging the larger intelligence enterprise) and information collection/*intelligence collection*. The intelligence staff identifies and taps into ongoing or existing information collection activities or joint intelligence, surveillance, and reconnaissance collection that may offer relevant information to fill gaps. These requirements identify the critical pieces of information that the commander must know to successfully plan, prepare, execute, and assess operations.

1-34. There is a relationship between IPB and information collection/*intelligence collection*. All of the IPB products feeding intelligence drive information collection/*intelligence collection* requirements; this means that the IPB process identifies intelligence gaps that are translated into information requirements and priority intelligence requirements (PIRs), which are then answered through collection.

1-35. The staff collaborates on information/*intelligence* considerations and works to integrate available resources into an integrated information collection plan. Developing requirements also supports the commander's decisionmaking regarding targeting. Well-stated information requirements help the commander to accomplish the mission by illustrating those key knowledge gaps and earmarking them for collection.

1-36. To effectively target the threat/*adversary*, the staff develops named areas of interest (NAIs) and target areas of interest. (The staff also develops an HVTL that can include geographic NAIs and TAIs as well as enemy/*adversary* organizations, networks, and individuals identified as key or critical to the

operational environment and are taken into account in branches and sequels.) NAIs should not be tied to a specific terrain; rather, they should be based upon the enemy locations or suspected locations.

NAI Example

Rather than looking at an area surrounding a hilltop named 1631 to see if the enemy has placed an air defense unit there, NAIs should be focused on an enemy unit or functional capability; for example, the suspected locations where the enemy may place his combined arms reserve. In order to refine the locations, analysts should study the enemy's doctrinal or historical use of the combined arms reserve, coupled with the capabilities of the critical combat systems associated with the combined arms reserve, and the known rates of march for the terrain in which the combined arms reserve will be operating.

1-37. Units need to consistently and continuously conduct information collection/*intelligence collection*. In order to be effective, information collection/*intelligence collection* must be based on the results of IPB and adjusted as the results of IPB are refined through the situation development process. Conversely, the results of reconnaissance, surveillance, security operations, and intelligence operations drive the refinement of IPB as appropriate. The staff must understand the roles and relationships of reconnaissance, surveillance, security operations, and intelligence operations and how the commander assesses ongoing operations as the unit develops the situation through action.

1-38. Commanders plan for and the staff controls the execution of all information collection/*intelligence collection* means throughout the operation. The unit must carefully plan for and synchronize reconnaissance, surveillance, security operations, and intelligence operations because the threat/*adversary* will try to use deception and other means to evade friendly collection efforts. Commanders need to know detailed information/*intelligence* about the threat/*adversary* disposition, capabilities, and intentions. Often it is necessary to designate a combined arms unit to develop the situation through close contact with the threat/*adversary* or civilian population.

GENERATE INTELLIGENCE KNOWLEDGE

1-39. Generate intelligence knowledge begins before mission receipt and provides the relevant knowledge required regarding the operational environment for the conduct of operations. As soon as the intelligence officer and other staff sections begin to collect data on the operational environment, they organize the data into databases. The information and intelligence obtained are refined into knowledge for use in mission analysis/*problem framing* through functional analysis. Information is obtained through intelligence reach; research; data-mining; database access; academic studies, products, or materials; intelligence archives; open-source intelligence; reconnaissance and security operations; and other information sources. Generate intelligence knowledge is the foundation for performing IPB and mission analysis/*problem framing*. The primary product of the generate intelligence knowledge task is the creation of initial data files based on the analysis of the operational variables of PMESII-PT/*PMESII* and the intelligence survey. (See ADRP 2-0 for more information on generate intelligence knowledge.)

1-40. *First published in 1995, the* Marine Corps Generic Intelligence Requirements Handbook (GIRH) *promulgates frequently used PIRs and information requirements to facilitate crisis planning for Marine expeditionary forces (MEFs). The GIRH details baseline intelligence requirements to allow Marines to efficiently request updated, accurate, and complete information. Intelligence Marines can use a GIRH as a checklist to identify information gaps, a reference when requesting information, or a baseline support tool when providing intelligence to operational units. In addition to the original GIRH, the Marine Corps Intelligence Activity (MCIA) has produced the following specific GIRHs:*

- *Police forces.*
- *Cultural.*
- *Jungle.*

- *Riverine.*
- *Urban.*
- *Information operations.*

1-41. *All GIRHs are available on MCIA's Joint Worldwide Intelligence Communications System and SECRET Internet Protocol Router Network (SIPRNET) Web sites.*

SITUATION DEVELOPMENT

1-42. Situation development is a process for analyzing information and producing current intelligence concerning the portions of the mission variables of enemy, terrain, weather, and civil considerations within the AO before and during operations. The process helps the intelligence staff recognize and interpret indicators of threat/*adversary* intentions and objectives. Situation development confirms or denies threat/*adversary* COAs, provides threat/*adversary* locations, explains what the threat/*adversary* is doing in relation to the friendly force commander's intent, and provides an estimate of threat/*adversary* combat effectiveness.

1-43. The locations and actions of noncombatant elements and nongovernmental organizations (NGOs) in the AO that may impact operations are also considered. Through situation development, the intelligence officer—

- Quickly identifies information gaps.
- Recommends new information requirements.
- Explains threat/*adversary* activities in relation to the unit's operations.
- Assists the commander in gaining and maintaining situational understanding.

1-44. Situation development helps commanders make decisions, including when to execute branches and sequels. The intelligence staff uses the products developed during IPB as a baseline to begin situation development.

This page intentionally left blank.

Chapter 2

IPB Support to Decisionmaking During Planning

IPB AND DECISIONMAKING

2-1. Decisionmaking refers to selecting a COA as the one most favorable to accomplish the mission. Decisionmaking includes knowing whether to decide or not, then when and what to decide, and finally understanding the consequences. (See ADRP 3-0 for further discussion on decisionmaking.) Commanders make decisions in part based on the intelligence developed during initial IPB and on the refinement of that intelligence throughout the operations process. (See ADRP 5-0 for further discussion on the operations process. *See MCWP 5-1 for further discussion on MCPP.*)

2-2. Commanders require accurate and timely intelligence about the operational environment in order to make informed and good decisions. Through IPB, the staff aids the commander's understanding of how the enemy, terrain, weather, and civil considerations influence the operational environment and affect operations. IPB also helps the commander understand how to influence, use, or employ these variables to achieve desired conditions and end state. IPB is essential in helping the commander to understand, visualize, and describe the operational environment, make and articulate decisions, and assess military operations.

- Understand operations. Understanding involves analyzing the mission variables in a given operational environment. IPB defines and describes the mission variables of enemy, terrain, weather, and civil considerations but, more importantly, concludes how the interrelationships, dynamics, and interactions of these variables cause changes in the operational environment.
- Visualize operations. Visualization involves developing situational understanding, determining an end state, and envisioning the sequence of events the force must ensure to achieve the end state. Every product developed during IPB is essential in aiding the commander in visualizing the situation. These products must be produced on time and in accordance with unit standard operating procedures.
- Describe operations. After commanders visualize an operation, they communicate their vision to their staffs and subordinate commands using the staff products developed during IPB.

IPB AND PLANNING

2-3. Commanders conduct planning in order to understand a problem or situation; envision a desired future, and, with the assistance of their staffs, develop COAs that can bring about that future. During planning commanders focus their activities on understanding, visualizing, and describing, while directing and assessing. IPB is one of the processes commanders use to aid in planning. IPB supports the MDMP/*MCPP* and troop leading procedures (TLP).

MILITARY DECISIONMAKING PROCESS/*MARINE CORPS PLANNING PROCESS*

2-4. The MDMP/*MCPP* methodology integrates the activities of the commander, staff, subordinate headquarters, and other partners to—

- Understand the situation and mission.
- Develop and compare COAs.
- Decide on a COA that best accomplishes the mission.
- Produce an operation plan (OPLAN) or operation order (OPORD) for execution.

2-5.   For the Army, the MDMP is a seven-step planning methodology comprising—

- Receipt of mission.
- Mission analysis.
- COA development.
- COA analysis (wargaming).

- COA comparison.
- COA approval.
- Orders production, dissemination, and transition.

2-6.   *For the Marine Corps, the MCPP is a six-step process comprising—*

- *Problem framing.*
- *COA development.*
- *COA wargaming.*

- *COA comparison and decision.*
- *Orders development.*
- *Transition.*

2-7.   Figure 2-1 shows the relationship between IPB and the steps of MDMP/*MCPP*. (See ADRP 5-0 for more information on the MDMP.) *Appendix A and MCWP 5-1 provide more information on MCPP.*
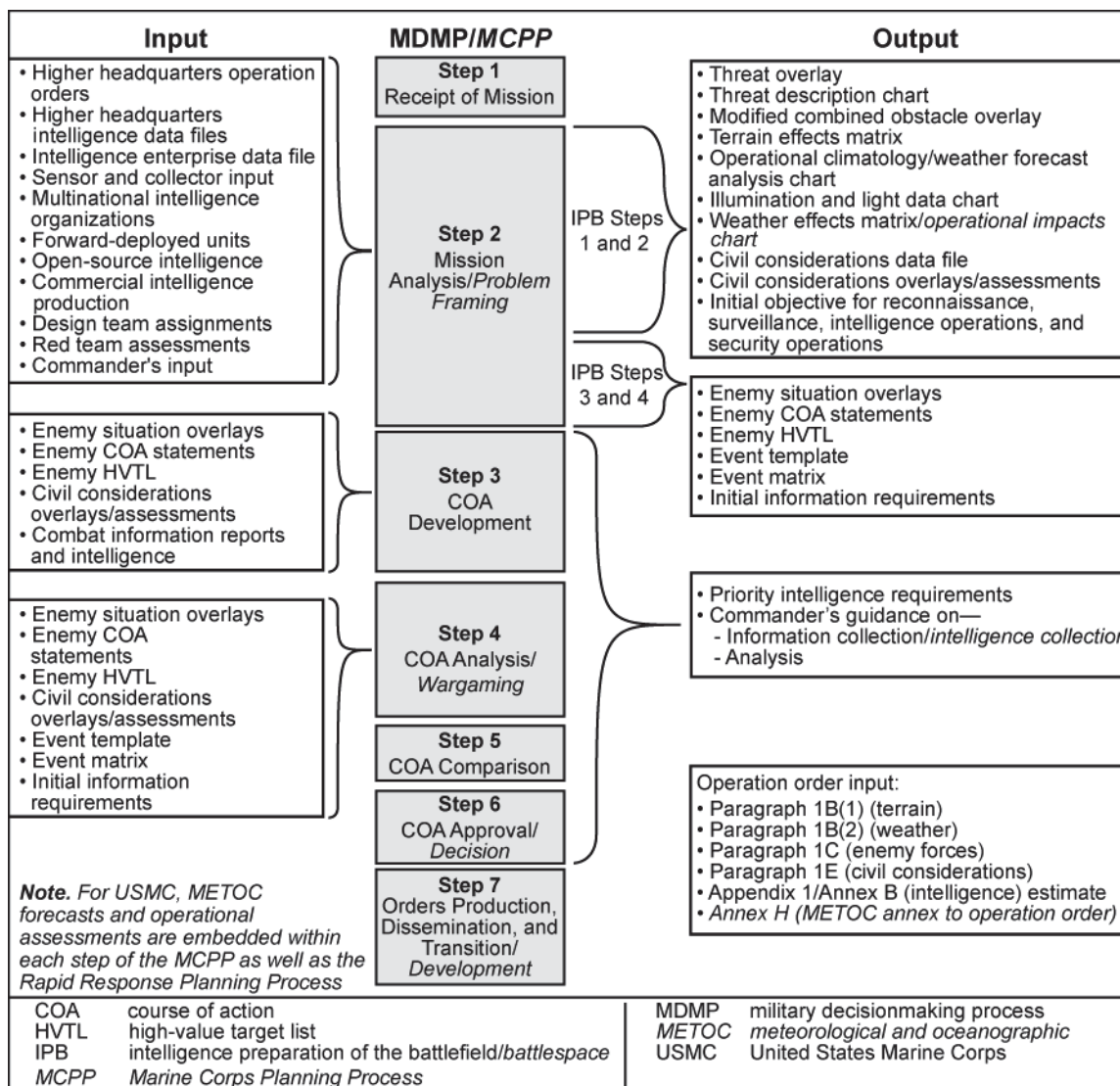
Figure 2-1. IPB and the MDMP/*MCPP* steps

Troop Leading Procedures

2-8. The TLP extend the MDMP to the small-unit level. The MDMP and TLP are similar but not identical. **Troop leading procedures** are a dynamic process used by small-unit leaders to analyze a mission, develop a plan, and prepare for an operation (ADP 5-0). These procedures enable leaders to maximize available planning time while developing effective plans and preparing their units for an operation.

2-9. The sequence of actions assists leaders to effectively and efficiently use available time to issue orders and execute tactical operations. TLP consist of eight steps. The sequence of the steps is not rigid. Leaders modify the sequence to meet the mission, situation, and available time. The following steps are done concurrently while others may go on continuously throughout the operation.

- Step 1 – Receive the mission.
- Step 2 – Issue a warning order.
- Step 3 – Make a tentative plan.
- Step 4 – Initiate movement.
- Step 5 – Conduct reconnaissance.
- Step 6 – Complete the plan.
- Step 7 – Issue the order.
- Step 8 – Supervise and refine.

2-10. The intelligence staff at the battalion develops and provides all the IPB products the company commander needs to do TLP. The commanders should not need to do any other refinement of these products.

2-11. The standard IPB products the battalion provides to assist the commander for TLP includes—

- Enemy situation overlays and COA statements.
- Terrain and weather products.
- Tactical decision aids (such as the MCOO and the evaluation of terrain effects, weather forecast weather effects, and light data tables).
- Civil considerations tools and products.

Note. Company commanders coordinate with the battalion intelligence staff for any IPB products or tools they think they will need.

2-12. However, due to the lack of a staff, resources, and time constraints, the small-unit leader depends on the timely delivery of IPB products developed by higher headquarters tailored to support small-unit planning. Specifically, the components of IPB inform steps 2 through 5 and actions within TLP, as discussed below.

Step 2—Issue a Warning Order

2-13. The battalion intelligence staff provides IPB products to the company commander on what to include in warning orders for areas such as but not limited to—

- Terrain analysis.
- Enemy forces.
- AOs and areas of interest.
- Commander's critical information requirements (CCIRs) and essential elements of friendly information (EEFIs).
- Risk guidance.
- Surveillance and reconnaissance to initiate.
- Security measures.

- Deception guidance.
- Mobility and countermobility.
- Guidance on rehearsals.

Step 3—Make a Tentative Plan

2-14. When developing a tentative plan, the company commander relies on the battalion intelligence staff to provide IPB tools as the leader conducts the mission analysis, COA development, COA analysis, and COA comparison and selection (PIRs, friendly force information requirement, and EEFIs).

2-15. The battalion intelligence staff provides IPB tools and products for the leader on mission analysis by evaluating enemy, terrain, weather, and civil considerations. This includes providing information and analysis on the terrain, enemy, and friendly forces that most affect tactical operations.

2-16. In COA development, the battalion intelligence staff provides IPB products to assist the leader in the construct of a solid COA. The purpose of COA development is to determine one or more ways to accomplish the mission that is consistent with the immediate higher commander's intent. A COA describes how the unit might generate the effects of overwhelming combat power against the enemy at the decisive point with the least friendly casualties.

2-17. The battalion intelligence staff provides tools from IPB to leaders during COA analysis. COA analysis begins with both friendly and enemy COAs and, using a method of action-reaction-counteraction wargame, results in a synchronized friendly plan, identified strengths and weaknesses, and updated risk assessment. After developing the COA, the leader analyzes it to determine its strengths and weaknesses and gains insights into actions at the decisive point of the mission. COA analysis (wargaming) brings together friendly and enemy forces on the actual terrain to visualize how the operation will unfold. Wargaming helps the leader synchronize friendly actions while considering the likely reactions of the enemy. The battalion intelligence staff provides IPB tools the leader can use to determine how the enemy will likely react during wargaming.

2-18. During COA comparison and selection, the battalion intelligence staff provides products from IPB to leaders to determine PIRs, friendly force information requirement, and EEFIs. Even though EEFIs are not part of the CCIRs, they still become priorities, and this information must be protected from identification by the enemy.

Step 4—Initiate Movement

2-19. The battalion intelligence staff provides IPB products to leaders on any movement necessary to continue mission preparation or to posture the unit for the start of the mission.

Step 5—Conduct Reconnaissance

2-20. If time permits, leaders verify intelligence from higher headquarters by reconnoitering visually to seek to confirm PIRs that support their tentative plans. These PIRs usually consist of assumptions or critical facts about the enemy (to include strength and location). The PIRs can also include information on the terrain (to verify that a tentative support-by-fire position can suppress the enemy or an AA is useable).

Understand the Situation and Mission

2-21. During the mission analysis step of the MDMP/*problem framing step of MCPP*, the staff conducts IPB in order to understand the situation and mission. The IPB products developed during this step are discussed fully in chapters 3 through 6. The products listed below are critical to developing and comparing COAs, deciding on a COA, and producing an OPORD:

- Intelligence gaps.
- Information requirements.
- Enemy situation templates with an associated threat/*adversary* COA statement and HVTL.
- Event template with associated event matrix.
- Relative combat power matrix for enemy forces.

- Geospatial intelligence tactical decision aids required to support continued planning (terrain effects).
- Weather tactical decision aids required to support continued planning (operational climatology or weather forecast analysis chart and weather effects matrix).
- Civil considerations tactical decision aids required to support continued planning (civil considerations effects).
- Estimates on how other significant variables may affect the mission.
- Reconnaissance objectives.
- The tempo and focus of reconnaissance, surveillance, security operations, and intelligence operations to answer PIRs and meet other requirements.

Develop and Compare COAs

2-22. In the COA development step of the MDMP/*MCPP*, friendly COAs are broad potential solutions to an identified problem. These solutions are based on the conclusions reached during initial IPB and any refinement of those conclusions that occurs between the conclusion of mission analysis/*problem framing* and the beginning of COA development. The primary IPB product required for COA development is the enemy situation template with an associated enemy COA statement.

Decide on a COA that Best Accomplishes the Mission

2-23. In the COA analysis/*wargaming* step of the MDMP/*MCPP,* deciding on a COA enables commanders and staffs to identify difficulties or coordination problems as well as probable consequences of planned actions for each COA being considered. The primary IPB products required for deciding a COA are—

- The enemy situation template with an associated enemy COA statement.
- The event template with the associated event matrix.
- The relative combat power matrix for enemy forces.

2-24. During counterinsurgency operations and stability tasks, additional products may be required such as civil considerations overlays and assessments. Information collection/*intelligence collection* operations undertaken at the mission analysis/*problem framing* step of the MDMP/*MCPP* will provide pertinent combat information that will inform COA development. This information confirms or denies the enemy situation template and associated enemy COA statement.

Produce an OPLAN or OPORD for Execution

2-25. At the conclusion of the MDMP/*MCPP*, the staff prepares the OPLAN or OPORD by turning the selected COA into a clear, concise concept of operations and required supporting material. The results of IPB are included within the base order and appropriate annexes.

RAPID DECISIONMAKING AND SYNCHRONIZATION PROCESS/*RAPID RESPONSE PLANNING PROCESS*

2-26. The rapid decisionmaking and synchronization process (RDSP)/*rapid response planning process (R2P2)* is a technique that commanders and staff commonly use during execution. Throughout mission execution, continuous information collection is conducted to answer information requirements and to close intelligence gaps. The RDSP/*R2P2* is usually conducted based on an existing OPORD that includes the IPB products and estimates produced during MDMP/*MCPP*. (See ADRP 5-0 for more information on the RDSP. *See MCWP 5-1 for more information on R2P2.*)

2-27. For the U.S. Army, RDSP includes five steps:

- **Compare the current situation to the order.** During execution, the staff is continually refining the running estimates based on new information. Part of this process is to compare the current situation to the situation expressed in the OPORD to determine whether adjustments need to be made to the OPLAN and identify any decisions the commander may need to make. During execution, the staff looks for indicators of change variances that may affect the overall operation.

These change variances must be identified in order for the commander to make necessary modifications to the OPLAN. The event template and event matrix and the decision support template developed during step 4 of IPB are the primary IPB tools the staff uses to identify variances and alert the commander to situations that require a decision. These products are updated as changes occur.

- **Determine that a decision, and what type, is required.** When a variance is identified, the staff describes the variance and determines if it provides a significant opportunity to either friendly forces or the threat/*adversary*.

- **Develop a COA.** If the situation warrants the development of a new friendly COA, it may result in the creation of new or modified PIRs and HVTs. It may also require the creation of a new or modified event template and event matrix.

- **Refine and validate the COA.** During this step, the commander and staff conduct a mental wargame of the new COA. At a minimum the enemy situation template and COA statement, along with friendly operations graphics and COA statement, are required to focus the mental wargame.

- **Implement.** The commander normally implements the new COA by issuing a fragmentary order. The following IPB products are issued as part of that fragmentary order:
    - IPB products including enemy situation template with COA statement and HPTL, terrain, weather, and civil considerations products.
    - Updated PIRs.

2-28. *The Marine Corps R2P2, as defined in MCWP 5-1, is a time-constrained six-step process that includes—*

- *Problem framing.*
- *COA development.*
- *COA wargame.*
- *COA comparison and decision.*
- *Orders development.*
- *Transition.*

PART TWO

Fundamental Task Techniques

Chapter 3

Step 1 of the IPB Process—Define the Operational Environment

WHAT IS IT?

3-1. Step 1 of the IPB process identifies for further analysis the significant characteristics of the operational environment that may influence friendly COAs and command decisions. Within an operational environment, an Army leader may be faced with major combat, military engagements, and humanitarian assistance simultaneously in the same AO. The following examples portray planning scenarios.

Example 1

During planning for a foreign humanitarian task, a brigade/*unit* S-2 identifies five ethnic groups that have armed militias that have attacked each other, as well as indigenous governmental security forces over the past 12 months. In the last month, a helicopter from the nation's Army was shot down by a rocket-propelled grenade. Although these militias have not attacked any of the nongovernmental aid organizations in the area, they have demonstrated the willingness to use violence. Because of this, the S-2 determines each of these groups is a potential threat/*adversary*. There is no information about these groups in the command's intelligence data files or in the data files of their higher headquarters to aid the S-2 in developing valid potential COAs these groups may adopt when U.S. forces enter their AOs.

The S-2 staff conducts a search of various organizations' data files within the intelligence enterprise. The staff determines that while little is known about the threat characteristics/*adversary order of battle* of these militias, there is some information available. Each of these militias is a company-sized element with various types of small-arms and crew-served weapons, mortars, demolitions, and anti-armor rockets. It is not known whether these militias have any air defense artillery.

The S-2 initiates a request for collection on the current location, disposition, strength, and capabilities of each of these militias. Realizing that he will not have this information during IPB, the S-2 determines possible threat/*adversary* COAs based on what he knows and what he assumes, ensuring that the commander and the rest of the staff understand what is known and what is assumed about the threat/*adversary*. As intelligence related to the request for collection arrives, the S-2 updates the threat/*adversary* COAs and informs the commander and the rest of the staff.

Example 2
During planning for an attack, a brigade/*unit* S-2 identifies the enemy has an attack helicopter squadron that could threaten the friendly mission. When developing the enemy situation overlay, the S-2 includes the reported location of the attack helicopter battalion, air attack corridors that could be used to support the enemy defense, and forward arming and refueling points. The S-2 also generates collection requests to locate and track these assets in support of the command's targeting operations.

DESIRED END STATE

3-2.   Step 1 of the IPB process focuses the IPB effort on the characteristics of the operational environment that can influence friendly and threat/*adversary* operations. The intelligence staff acquires the intelligence needed to complete IPB in the degree of detail required to support the decisionmaking process. The primary outputs associated with step 1 of the IPB process may include developing the—

- Determination of the AO and area of interest.
- Determination of the area of intelligence responsibility.
- Identification of general characteristics of the AO that could influence the unit's mission.
- Identification of gaps in current intelligence holdings, translating them into requirements for collection (requests for information, requests for collection) in order to complete IPB.

SO WHAT?

3-3.   The "so what" in this step is clearly defining for the commanders what the relevant characteristics of their areas of interest are.

- Success results in saving time and effort by focusing only on those characteristics that will influence friendly COAs and command decisions.
- Consequences of failure:
  - Failure to focus on only the significant characteristics leads to wasted time and effort collecting and evaluating intelligence on characteristics of the operational environment that will not influence the operation.
  - Failure to identify all the significant characteristics may lead to the command's surprise and unpreparedness when some overlooked feature of the operational environment has an effect on the operation for which the commander did not plan.

HOW TO DO IT: (THE PROCESS)

3-4. Defining the operational environment consists of the sub-steps shown in figure 3-1.
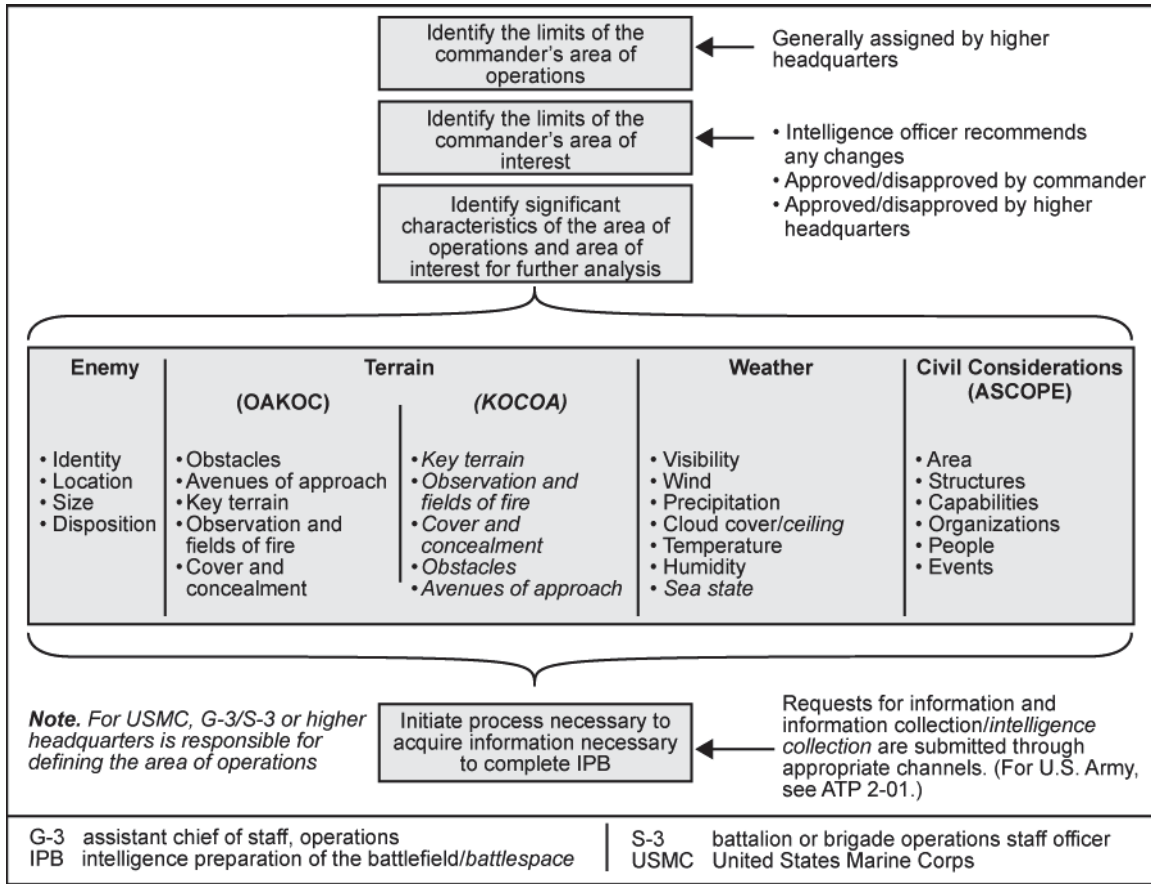
Figure 3-1. Sub-steps of step 1 of the IPB process

IDENTIFY THE LIMITS OF THE COMMANDER'S AREA OF OPERATIONS

3-5. The **area of operations** is defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces (JP 3-0). The AO is comprised of an external boundary that delineates the AOs of adjacent units and includes subordinate unit AOs. Subordinate unit AOs may be contiguous or noncontiguous. Parts of an AO not assigned to subordinate units are called deep areas. The AO may be impacted due to political boundaries and/or other civil considerations. Once assigned, an AO can be subdivided by that command, as necessary, to support mission requirements. Figure 3-2 on page 3-4 illustrates various AOs.
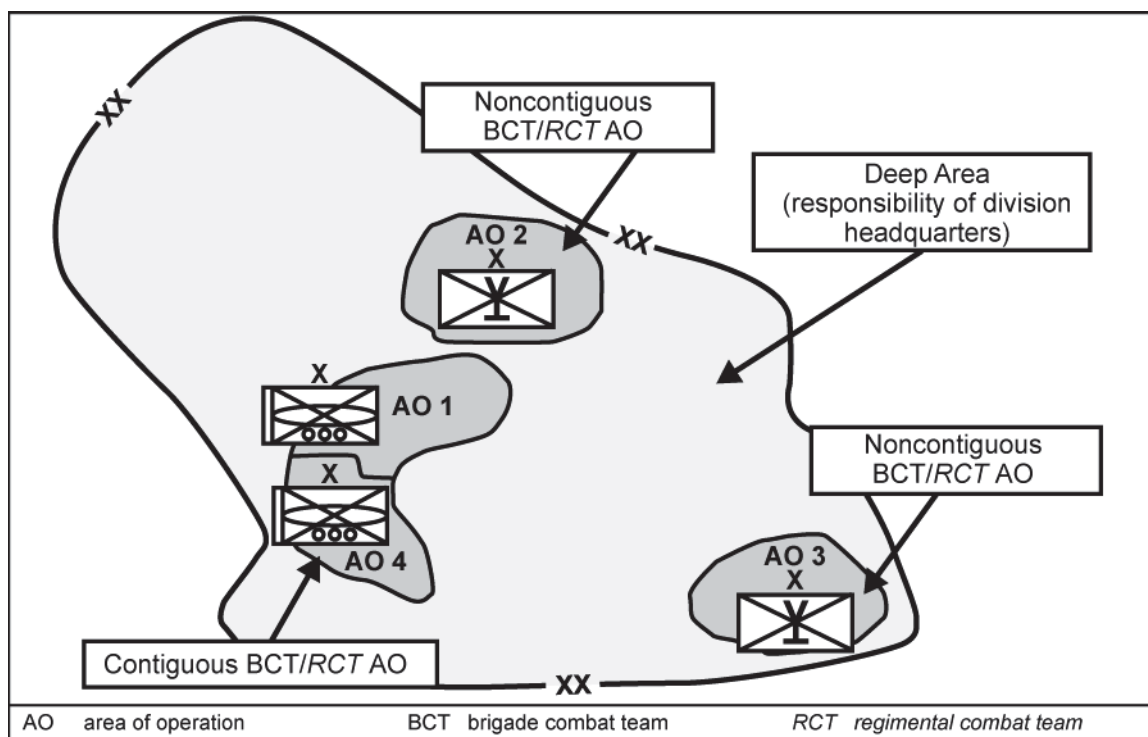
Figure 3-2. Example areas of operations

3-6.   An **area of influence** is a geographical area where a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control (JP 3-0). The area of influence is—

- An area that includes terrain inside and outside the AO.
- An area determined by both the G-2/S-2 and the G-3/S-3.

IDENTIFY THE LIMITS OF THE COMMANDER'S AREA OF INTEREST

3-7.   An **area of interest** is that area of concern to the commander, including the area of influence, areas adjacent thereto and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission (JP 3-0). The area of interest is—

- Established by the commander with input from the G-2/S-2 or G-3/S-3. The mission, enemy, terrain and weather, troops and support available, time available, civil considerations (METT-TC)/*mission, enemy, terrain and weather, troops and support available, time available (METT-T)* factors must be considered.
- An area normally larger than the area of influence and may require more intelligence assets to monitor. It may include staging areas.

3-8.   The area of interest is a geographical area from which information and intelligence are required to execute successful tactical operations and to plan for future operations. It includes any threat/*adversary* forces or characteristics that will significantly influence accomplishing the command's mission. In combat operations/*major operations*, the area of interest extends into enemy territory to the objectives of current or planned friendly operations if those objectives are located outside the assigned AO. In stability operations or defense support of civil authorities operations, the area of interest is typically much larger than that defined for combat operations/*major operations*.

3-9.   An additional consideration would be to divide the area of interest into several components; for example, ground area of interest and air area of interest. Such a division accommodates the types of information relevant to each area of interest as well as their usually different geographical limits. At some

point, it will likely become necessary to integrate the various areas of interest into a whole in order to present the commander with a complete, integrated picture.

3-10. An area of interest may be irregular in shape and overlap the areas of adjacent and subordinate unit AOs. The area will change as the situation changes and as commanders determine new information requirements. It is the geographical area from which information is required to facilitate planning and the successful conduct of the command's operation.

> **Analyzing the Area of Operations**
> By analyzing a commander's AO in terms of the area of influence and area of interest, a commander determines whether the assigned AO is appropriate. This analysis may include the forces' capabilities to conduct actions across the warfighting functions. Commanders consider the extent of subordinates' areas of influence when defining subordinates' AOs. In identifying an AO, the staff should avoid making it substantially larger than the unit's area of influence. Ideally, the entire AO is encompassed by the area of influence. The area of influence is useful to the commander in focusing information collection operations to shape the battlefield/*battlespace* to facilitate future operations.

3-11. *For the Marine Corps, battlespace includes the area of interest, area of influence, and operational areas. Operational areas for Marine air-ground task forces (MAGTFs) are usually an AO. The staff may recommend battlespace refinements based on the analysis of the terrain and tasks as well as friendly and adversary centers of gravity, capabilities, and limitations. The size of the area of interest may change based on the commander's understanding of the situation. The **area of influence** is a geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control (JP 3-0). The extent of the area of influence may change if forces are added or deleted, equipment capability (for example, the range of lethal and nonlethal weapon systems) and availability change, or rules of engagement change. The commander's AO may need to change based on the scope of the mission, the results of operations, operational reach, or to ensure sufficient battlespace to maneuver and protect his force.*

IDENTIFY SIGNIFICANT CHARACTERISTICS WITHIN THE AREA OF OPERATIONS AND AREA OF INTEREST FOR FURTHER ANALYSIS

3-12. In order to focus IPB and what is important to the commander, the staff identifies and defines the aspects of the enemy, terrain, weather, and civil considerations of the operational environment to determine the significance of each in relation to the mission; essentially building an environmental model as the framework to conduct and then present analysis to the commander. This prevents unnecessary analysis and allows the staff to maximize resources on critical areas. The initial analysis that occurs in this sub-step determines the amount of time and resources the intelligence staff commits to the detailed analysis that occurs in step 2 of the IPB process.

ENEMY

3-13. An **enemy** is a party identified as hostile against which the use of force is authorized (ADRP 3-0). Analysis of the enemy includes not only the known enemy but also other threats/*adversaries* to mission success. Such threats/*adversaries* might include multiple adversaries posing with a wide array of political, economic, religious, and personal motivations. Additionally, threats/*adversaries* may wear uniforms and easily be identifiable. Or, they may not wear uniforms and blend into the population. To understand threat/*adversary* capabilities and vulnerabilities, commanders and staffs require detailed, timely, and accurate intelligence produced as a result of IPB.

TERRAIN AND WEATHER

3-14. Terrain and weather are natural conditions that profoundly influence operations. Terrain and weather favor neither friendly nor enemy forces unless one is more familiar with—or better prepared to operate in—the physical environment. Terrain includes natural features (such as rivers and mountains) and manmade features (such as cities, airfields, and bridges). Terrain directly affects how commanders select objectives and locate, move, and control forces. Terrain also influences protective measures and the effectiveness of weapons and other systems.

3-15. Effective use of terrain reduces the effects of enemy fires, increases the effects of friendly fires, and facilitates surprise. Terrain appreciation—the ability to predict its impact on operations—is an important skill for every leader. For tactical operations, commanders analyze terrain using the five military aspects of terrain, expressed in the Army memory aid OAKOC (obstacles, avenues of approach, key terrain, observation and fields of fire, and cover and concealment) and the Marine Corps memory aid *KOCOA (key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach).*

3-16. The discussion of terrain in chapter 4 covers the broad aspects of terrain analysis essential to all-source intelligence analysts conducting terrain analysis in support of threat/*adversary* analysis. (See ATP 3-34.80 and JP 2-03 for more information on analyzing the military aspects of terrain.)

3-17. Climate refers to the average weather conditions for a location, area, or region for a specific time of the year as recorded for a period of years. Operational climatology is used to assess effects on weapon systems, collection systems, ground forces, tactics and procedures, enemy TTP, and other capabilities based on specific weather sensitivity thresholds when operational planning occurs more than 10 days prior to the execution. Climatological data is important at both the operational and tactical levels. Actual weather forecasts and/or predictions, using weather models and other tools, are used to assess weather effects on weapon systems, collection systems, ground forces, TTP, and other capabilities when operations occur within 10 days of operational planning.

CIVIL CONSIDERATIONS

3-18. Civil considerations reflect the influence of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within the operational environment on the conduct of military operations. Commanders and staffs analyze civil considerations in terms of the categories expressed in the memory aid ASCOPE (areas, structures, capabilities, organizations, people, and events).

3-19. Civil considerations help commanders understand the social, political, and cultural variables within the AO and their effect on the mission. Understanding the relationship between military operations and civilians, culture, and society is critical to conducting operations and is essential in developing effective plans. Operations often involve stabilizing the situation securing the peace, building host-nation capacity, and transitioning authority to civilian control. Combat operations/m*ajor operations* directly affect the populace, infrastructure, and the force's ability to transition to host-nation authority. The degree to which the populace is expected to support or resist U.S. and friendly forces also affects offensive and defensive operational design.

3-20. Commanders and staffs use personal knowledge and running estimates to assess social, economic, and political factors. Commanders consider how these factors may relate to potential lawlessness, subversion, or insurgency. Their goal is to develop their understanding to the level of cultural awareness. At this level, they can estimate the effects of friendly actions and direct their subordinates with confidence. Cultural awareness improves how Soldiers/*Marines* interact with the populace and deters their false or unrealistic expectations. They have more knowledge of the society's common practices, perceptions, assumptions, customs, and values, giving better insight into the intent of individuals and groups.

> *Note.* FM 4-02 has extensive information on the medical aspects of IPB that relate mainly to civil considerations in the AO.

3-21. To improve the commander's sociocultural understanding, intelligence staffs can use sociocultural databases and repositories as well as HTTs/*foreign area officers, regional affairs officers, and other cultural enablers,* when available, to aid the intelligence analysis conducted as part of assessing civil considerations. Additionally, commanders and staffs continually seek to improve cultural understanding to improve their roles in IPB.

EVALUATE CURRENT OPERATIONS AND INTELLIGENCE HOLDINGS TO DETERMINE ADDITIONAL INFORMATION NEEDED TO COMPLETE IPB

3-22. Not all the information needed to complete IPB will be in the data files and databases of the commands or their higher headquarters. Information gaps should be identified early and prioritized based on the commander's initial guidance and intent for intelligence and information collection/*intelligence collection*. The staff should ensure the commander is aware of any information gaps that cannot be answered within the time allotted for IPB. The staff develops reasonable assumptions to use in place of these answers and explains to the commander how they arrived at these assumptions.

INITIATE PROCESSES NECESSARY TO ACQUIRE THE INFORMATION NEEDED TO COMPLETE IPB

3-23. After determining that information necessary to complete IPB is not contained within local and searchable external data files and databases, staff elements submit requests for information or requests for collection to obtain the information necessary to complete IPB. As information is received, IPB products are updated and intelligence gaps are eliminated. New intelligence gaps and information requirements may be developed as IPB continues. (See FM 3-55/*MCWP 2-2* for more information on information collection/ *intelligence collection*. See ATP 2-01/*MCWP 2-2* for more information on planning requirements and assessing collection.)

This page intentionally left blank.

Chapter 4

Step 2 of the IPB Process—Describe Environmental Effects on Operations/*Describe the Effects on Operations*

WHAT IS IT?

4-1. Step 2 of the IPB process determines how significant characteristics of the operational environment can affect friendly and threat/*adversary* operations. The following example shows how the significant characteristic of the operational environment (specifically the terrain) impacts friendly operations.

> **Example**
>
> A brigade/*unit* S-2 tells his commander that the terrain the brigade/*unit* must attack through will canalize friendly forces into platoon-sized mobility corridors that will prevent our forces from supporting each other. The S-2 also tells the commander the terrain favors enemy use of obstacles, small antitank ambushes, and indirect fire throughout its security zone.

DESIRED END STATE

4-2. Identify how the operational environment influences friendly and threat/*adversary* COAs. The primary outputs associated with step 2 of the IPB process may include ensuring—

- Terrain analysis for the AO and area of interest are completed, in particular:
  - Ground and air avenues of approach (AAs).
  - Key terrain.
  - Potential objectives, decision points, NAIs, and TAIs are identified.
- The effects of weather and light data are integrated.
- Any request for information on requests for collection are refined and updated.

SO WHAT?

4-3. The "so what" in this step is identifying how relevant characteristics of the area of interest will affect friendly and threat/*adversary* operations:

- Success results in allowing the commander to quickly choose and exploit terrain, weather, and civil considerations to best support the mission.
- Consequences of failure:
  - The commander may not have the information needed to exploit the opportunities the operational environment provides.
  - The enemy commander may have the information needed to exploit the opportunities the operational environment provides in a way the friendly commander did not anticipate.

HOW TO DO IT: (THE PROCESS)

4-4.   Describing environmental effects on operations consists of the actions illustrated in figure 4-1.
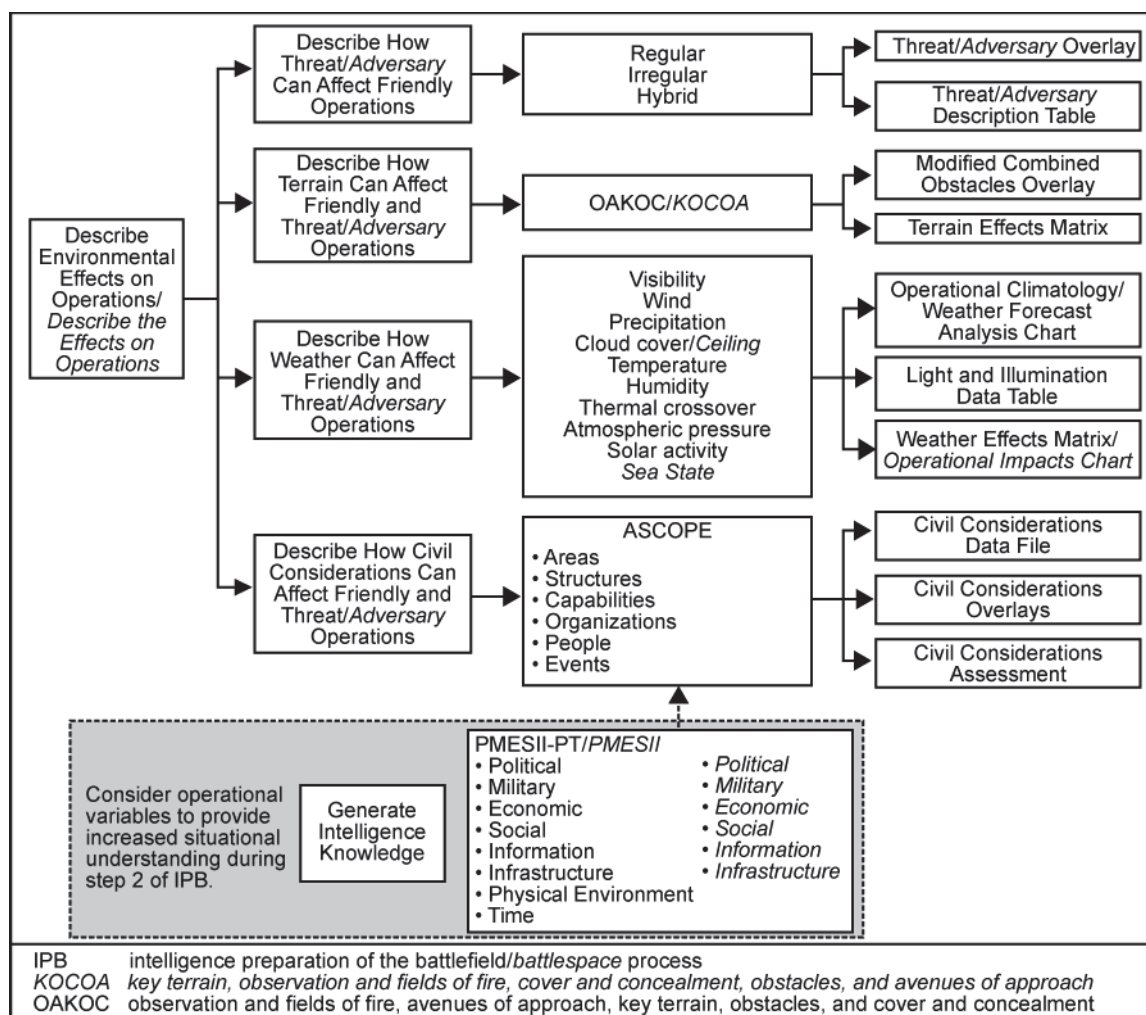
Figure 4-1. Step 2 of the IPB process

DESCRIBE HOW THE THREAT/*ADVERSARY* CAN AFFECT FRIENDLY OPERATIONS

4-5.   Threats/*adversaries* are part of the operational environment. Commanders need to understand all the threats/*adversaries* to the operations within the AO and the area of interest. They may face one unified threat/*adversary* force or several disparate threat/*adversary* forces that must be engaged in order to accomplish the mission. Although detailed analysis of enemy forces occurs during steps 3 and 4 of the IPB process, the type of enemy forces and their general capabilities must be defined during step 2. This is done to place the existence of these forces in context with other variables to understand their relative importance as a characteristic of the operational environment. For example:

- When facing a regular force in major operations regardless of where the engagement occurs, that force is most likely the most important characteristic in that operational environment.
- When facing an irregular force conducting operations as part of an insurgency in a failing nation-state, the state of governance and other civil considerations may be more significant than the threat/*adversary* posed by these irregular forces.

4-6.   The threat/*adversary* overlay and threat/*adversary* description table focus the analysis of threat/*adversary* at this point and aid in communicating that analysis to the commander.

THREAT/*ADVERSARY* OVERLAY

4-7.   The threat/*adversary* overlay is a depiction of the current physical location of all potential threats/*adversaries* in the AO and the area of interest. This graphic includes the identity, size, location, strength, and AO for each potential threat/*adversary*. Figure 4-2 is an example of a threat/*adversary* overlay for irregular forces.
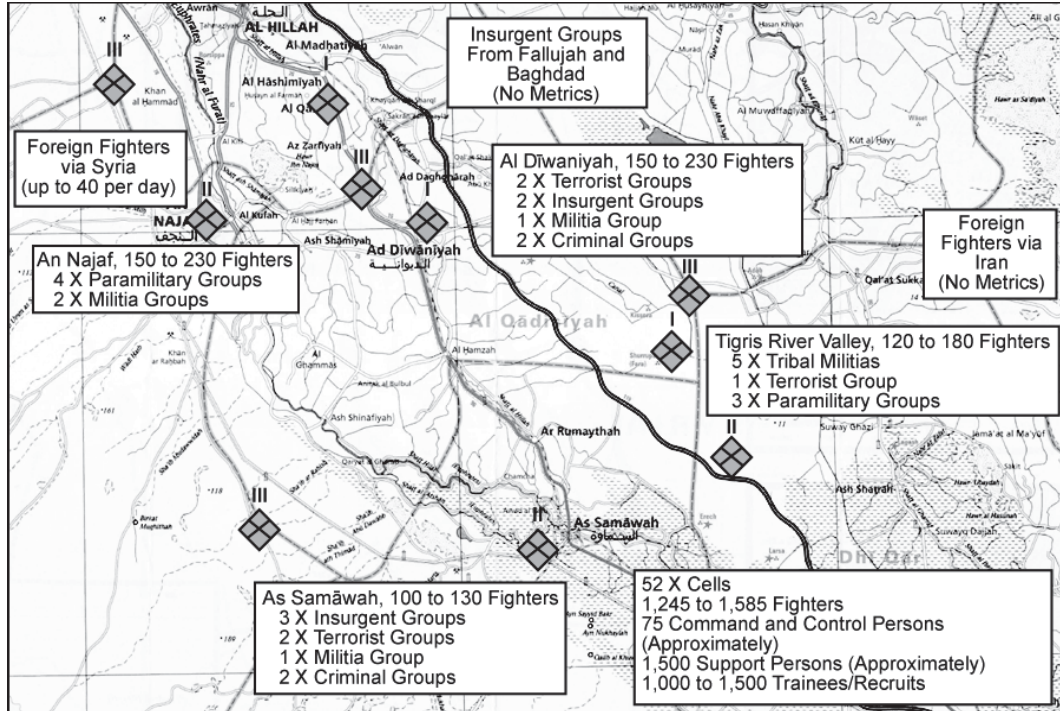
Figure 4-2. Example threat/*adversary* overlay (irregular forces)

THREAT/*ADVERSARY* DESCRIPTION TABLE

4-8.   The threat/*adversary* description table supports the threat/*adversary* overlay by classifying the type of threats/*adversaries* identified on the overlay and describing the broad capabilities of each threat/*adversary*. Table 4-1 is an example of a threat/*adversary* description for irregular forces.

Table 4-1. Example threat/*adversary* description table (irregular forces)

Identity	*Location*	*Disposition*	*Description*
26 x separate threat/*adversary* groups	Mosul	Unknown—groups operate from sanctuary locations among the population	Threat/*adversary* groups in Mosul operate independently to disrupt multinational stability tasks
9 x separate threat/*adversary* groups	Tigris River Valley	Unknown—groups operate from sanctuary locations among the population	Facilitate movement of foreign fighters from Syria into Mosul
6 x separate threat/*adversary* groups	Tal Afar	Unknown—groups operate from sanctuary locations among the population	Facilitate movement of foreign fighters from Syria into Mosul
8 x separate threat/*adversary* groups	Sinjar/Biaj	Unknown—groups operate from sanctuary locations among the population	Facilitate movement of foreign fighters from Syria into Mosul

DESCRIBE HOW TERRAIN CAN AFFECT FRIENDLY AND THREAT/*ADVERSARY* OPERATIONS

4-9.   Terrain analysis is the evaluation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on friendly and enemy operations. It involves 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 as changes in the operational environment may alter the analysis of its effect on operations.

4-10. There are two types of terrain in which a command may operate—natural and urban. Both of these terrain types are analyzed based on military aspects using the OAKOC/*KOCOA* considerations. Analysis of natural terrain focuses on surface area, airspace, and subsurface areas. Analysis of urban terrain also focuses on surface area and airspace, but must also consider subsurface as well as internal and external supersurface areas.

ANALYZE THE MILITARY ASPECTS OF TERRAIN

4-11. Generally in the Army, detailed terrain analysis is conducted by geospatial intelligence cells assigned to brigade combat teams, division headquarters, corps headquarters, and theater headquarters based on priorities established by the intelligence officer. These cells have state-of-the-art digital mapping tools and access to national-level support from agencies like the National Geospatial Intelligence Agency. *Generally in the Marine Corps, geospatial intelligence capability resides within the intelligence battalion and the Marine aircraft wing (MAW). During the conduct of operations, this capability can be deployed down to the regimental combat team or Marine aircraft group level.* The result of terrain analysis is the evaluation of the military aspects of terrain on operations.

4-12. Analyzing the military aspects of terrain involves the collection, processing, evaluation, and interpretation of geographic information on natural and manmade features of the terrain, combined with other relevant factors, to determine potential effects of the terrain on military operations. It involves the study and interpretation of natural and manmade features of an area, effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continuous process as changes in the operational environment may change the analysis of its effect on the operation or threat/*adversary* COAs.

Obstacles

4-13. An **obstacle** is any natural or man-made obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force (JP 3-15). 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.
- Wire obstacles (concertina wire. barbed wire, and overhead wire).

4-14.   Obstacles affect certain types of movement differently. Obstacles such as rivers, lakes, swamps, dense forested areas, road craters, rubble in the street, or densely populated urban areas may have a greater effect on mounted movement than on dismounted movement. Minefields, concertina wire, or steep slopes may be more effective against dismounted movement.

4-15. Obstacles to air mobility include terrain features that exceed the aircraft's service ceiling; affect nap-of-the-earth flight; impact aircraft lift capabilities; or that force the aircraft to employ a particular flight profile. Examples are tall buildings, cellular telephone towers, power lines, rapidly rising terrain features, mountains, smoke, geologic features, high mountains, and other obscurants. High mountainous regions can impact rotary- and fixed-wing aircraft lift capabilities.

4-16. Obstacles may also decrease the effectiveness of information-related capabilities to influence adversary or enemy operations and activities, friendly populations, and neutral populations. For example, mountains may block terrestrial-based signals used to broadcast surrender appeals and morale-lowering messages to enemy-held territory or messages to populations explaining the intent of U.S. operations. Use of other message delivery platforms may be necessary to compensate for the effects of local terrain.

4-17. Figure 4-3 illustrates examples of obstacles in natural terrain.
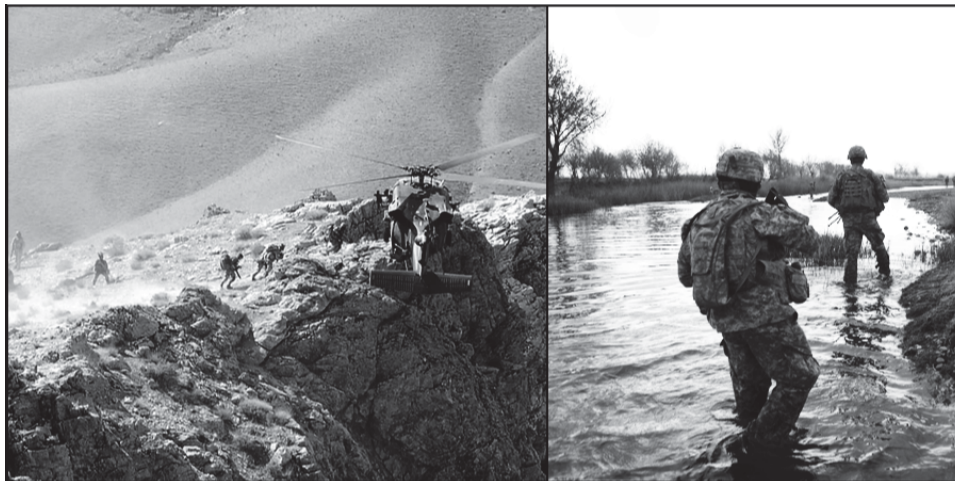
Figure 4-3. Example of obstacles in natural terrain

4-18. Figure 4-4 illustrates examples of obstacles in urban terrain.

Figure 4-4. Example of obstacles in urban terrain

Avenues of Approach

4-19. AAs are air or ground routes used by an attacking force leading to its objective or to key terrain in its path. The identification of AAs is important because all COAs that involve maneuver depend on available AAs. During offensive tasks, the evaluation of AAs leads to a recommendation on the best AAs 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, it is important to identify AAs that support enemy offensive capabilities and avenues that support the movement and commitment of friendly reserves. AAs are developed by identifying, categorizing, and grouping mobility corridors and evaluating AAs.

4-20. **Mobility corridors** are that are relatively free of obstacles where a force will be canalized due to terrain restrictions allowing military forces to capitalize on the principles of mass and speed (JP 2-01.3).

4-21. Identifying mobility corridors requires some knowledge of friendly and enemy forces and their preferred tactics. The best mobility corridors use unrestricted terrain that provided enough space for a force to move in its preferred doctrinal formations while avoiding major obstacles. Mobility corridors can follow, for example, the direction of roads, trails, rivers, streams, ridgelines, subway lines, foot paths, tunnels, and human-sized drainage ditches. Factors other than obstacles and mobility may have to be evaluated when identifying mobility corridors.

4-22. Mobility corridors, like obstacles, are a function of the type and mobility of the force being evaluated. Military forces, such as mechanized infantry or armored units, require large open areas in which to move and maneuver. Irregular forces are less impacted by the presence of obstacles and terrain that would hinder movement of a large formation. The size of a mobility corridor can be determined based on terrain constrictions.

4-23. Mobility corridors are categorized by the size or type of force they can accommodate. Mobility corridors can also be categorized by likely use. For example, a mechanized force requires logistical sustainment; a mobility corridor through unrestricted terrain supported by a road network is generally more desirable. A dismounted force might be able to use more restrictive corridors associated with the arctic tundra, swamps or marshes, jungles, or mountains that may or may not have a road network. Due to their rate of march and lack of fire power, dismounted forces require a more covered and concealed route for survivability to reach their objective.

4-24. AAs consist of a series of mobility corridors through which a maneuvering force must pass to reach its objective. An AA must provide ease of movement and enough width for dispersion of a force large enough to significantly affect the outcome of the operation. Mobility corridors are classed based on the distance between the terrain features that form the corridor. Mobility corridor ranges are not absolute but reflect the relative and approximate distance between terrain features. Table 4-2 identifies these classifications.

Table 4-2. Mobility corridor ranges

Avenue of approach	Cross-country mobility corridor classification	Approximate distance between terrain features (in kilometers)
Division	Brigade/Regiment	10
Brigade/Regiment	Brigade/Regiment	6
Battalion	Company	2

4-25. Evaluating AAs is a combined effort of the entire staff. Evaluating AAs identifies those that best support threat/*adversary* or friendly capabilities. The AAs should be prioritized based on how well each supports the ability to meet the desired result in a timely and efficient manner. AAs are evaluated for suitability in terms of—

- Access to key terrain and adjacent avenues.
- Degree of canalization and ease of movement.
- Sustainability (line of communications [LOC] support).
- Access to the objective.

4-26. Once evaluated, AAs are prioritized on how well each supports maneuver. Figure 4-5 is an example of the identification of AAs with mobility corridors.
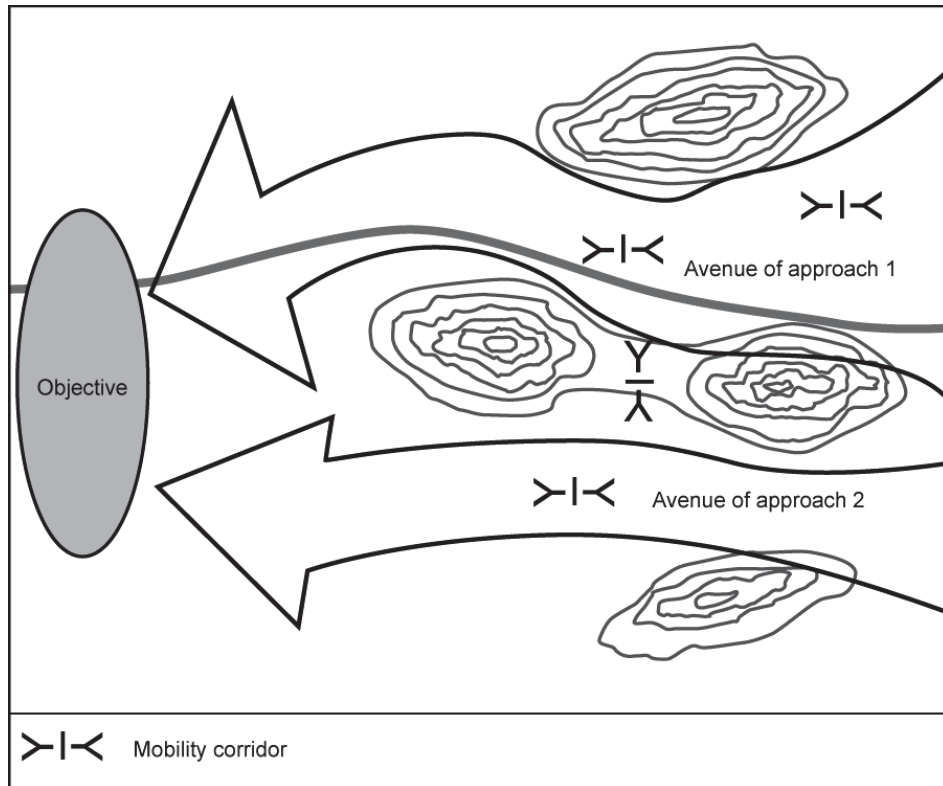
Figure 4-5. Avenues of approach with mobility corridors

4-27. Figure 4-6 is an example of the identification mobility corridors in urban terrain.
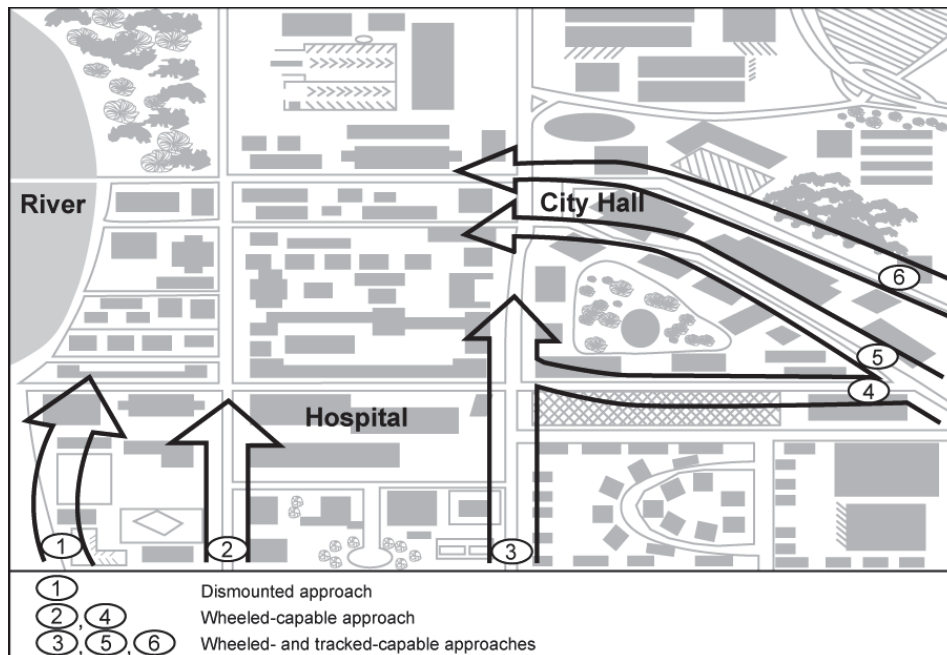
Figure 4-6. Mobility corridors (urban terrain)

Key Terrain

4-28. **Key terrain** is any locality, or area, the seizure or retention of which affords a marked advantage to either combatant (JP 2-01.3). In natural terrain dominated by restrictive terrain features, 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 can be key terrain because it offers good cover and concealment.

4-29. In urban environments, infrastructure (such as bridges, medical facilities, choke points, intersections, industrial complexes, and economic, social, and government institutions) can be considered key terrain. *For the Marine Corps, this includes the local population and certain local groups or individuals.* For example, control of a bridge may equate to control over an AA. However, the command needs to consider the operational and strategic impact on the civil dimension when deciding to control a bridge.

Key Terrain Considerations

Control of a bridge may negatively impact commerce, LOC support, military load class of supporting LOCs, and access to the objective. An example of economic or social institution as key terrain is the main bazaar in a town because whoever controls the bazaar or market controls the town. Economic health of the market will be key to the economic health of the area. If the enemy can maneuver through and control the key terrain of the market, the enemy can shut down the town and the economy.

An example for a government institution being key terrain is the local police, who may exert a great deal of influence on the local population (elections, law enforcement, tribal politics, other). Tactical use of terrain is often directed at increasing the capability for applying combat power and at the same time forcing the threat/*adversary* into areas to reduce their ability to apply combat power.

4-30. Key terrain is evaluated by assessing the impact of its control by either force. A technique that aids this assessment is to use the evaluation of the other four aspects of military terrain to assist in determining key terrain.

4-31. In the offense, key terrain features are usually forward of friendly dispositions and are often assigned as objectives. Adjacent terrain features may be key terrain if their control is necessary for the continuation of the attack or the accomplishment of the mission.

4-32. In the defense, key terrain is usually within and/or behind the defensive area, such as terrain that gives good observation over AAs to and through the defensive position; terrain that permits the defender to cover an obstacle by fire; or areas along an LOC that affect the use of reserves or sustainment operations. In counterinsurgency operations, key terrain may include portions of the population, such as political, tribal, and religious groups or leaders; a localized population; infrastructure; or governmental organizations.

4-33. Decisive terrain is key terrain whose seizure and retention is mandatory for successful mission accomplishment. Key terrain is not necessarily decisive terrain. Decisive terrain has an extraordinary impact on the mission. The successful accomplishment of the mission depends on seizing, retaining, or denying the use of the terrain to an enemy force.

4-34. Commanders designate decisive terrain to communicate to the staff and subordinate commanders how important the terrain is to the concept of operations.

4-35. Figure 4-7 illustrates the concept of key terrain in a natural environment.
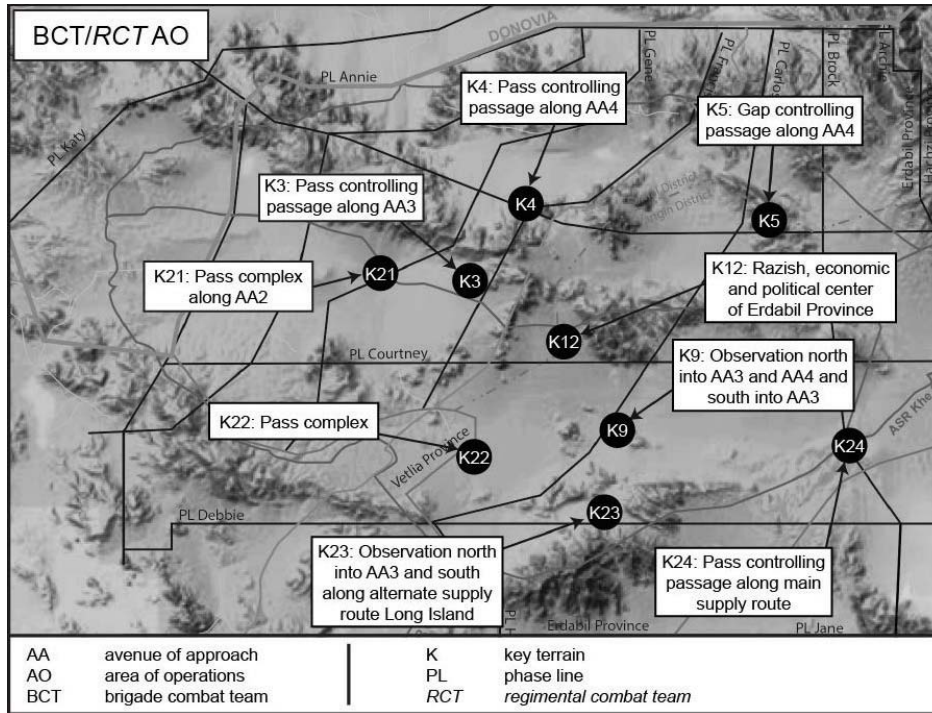
Figure 4-7. Key terrain (natural terrain)

4-36. Figure 4-8 illustrates the concept of key terrain in an urban environment.
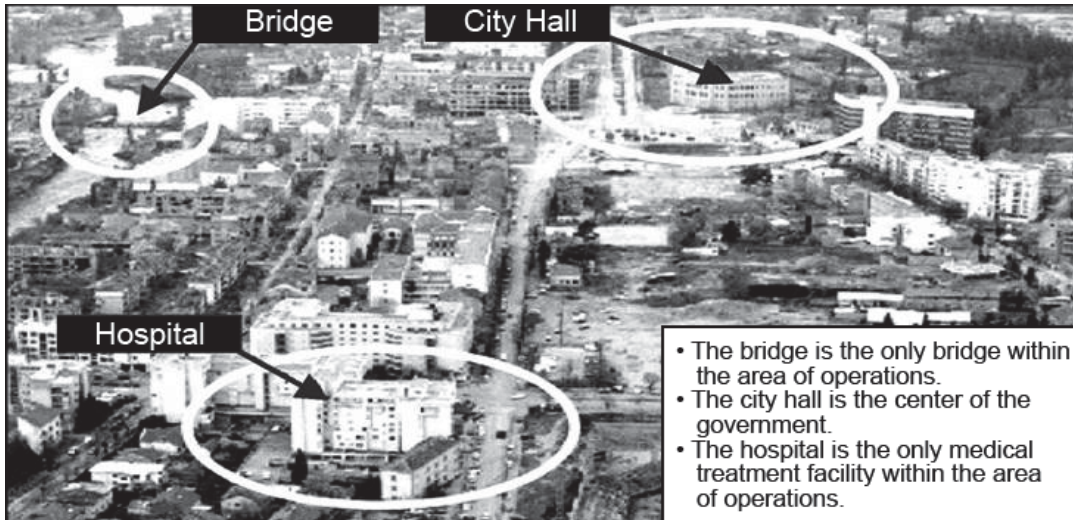
Figure 4-8. Key terrain (urban terrain)

Observation and Fields of Fire

4-37. Observation is the condition of weather and terrain that permits a force to see friendly, enemy, and neutral personnel, systems, and key aspects of the operational 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.

4-38. In natural terrain, there are limitations on observation caused by relative, localized, and often subtle variations in terrain elevations. These limitations are known as intervisibility lines (IVLs). Intervisibility is the condition of being able to see one point from the other. Figure 4-9 illustrates IVLs.
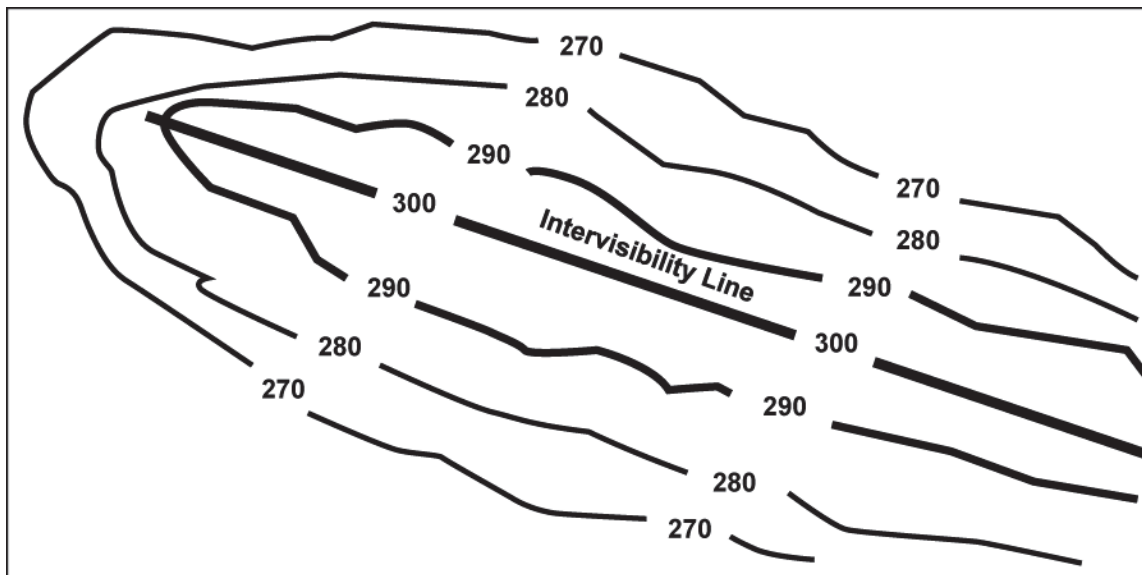
Figure 4-9. Example of intervisibility lines

4-39. Observation can also be limited by adverse weather, dusk, and smoke. In urban terrain, observation is primarily limited by manmade structures, as well as the activity and debris associated with human activity. Analyzing observation and fields of fire in urban terrain is more complicated than it is for natural terrain.

4-40. When evaluating observation and fields of fire for urban terrain, analysts must consider surface, supersurface, subsurface, external, and internal surface areas.

4-41. Fields of fire is observation limited to a specific linear distance based on weapons systems capabilities. 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.
- Specific equipment or equipment positions.
- Areas where forces are most vulnerable to observation and fires.
- Identification of visual dead space.

4-42. Analysis of fields of fire includes an evaluation of all direct and indirect fire weapons systems in a command's inventory. An ideal field of fire for a direct fire weapon is an open area in which the threat/*adversary* can be seen and on which the threat/*adversary* has no protection out to the maximum effective range of that weapon. An ideal field of fire for an indirect fire weapons system is a target area that has no protection from the system's munitions. Terrain that offers good observation and fields of fire generally favors defensive COAs.

4-43. Both observation and fields of fire are based on lines of sight. **Line of sight is the unobstructed path from a Soldier's/*Marine's* weapon, weapon site, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another.** In other words, a line of sight is a straight line from one point to another. There are two types of lines of sight normally evaluated during terrain analysis—horizontal and oblique.

- Horizontal line of sight is an unobstructed path from a Soldier's/*Marine's* weapon, weapon sight, laser designator, and electronic sending and receiving antennas.
- Oblique or vertical lines of sight aid in planning air defense artillery systems locations, selecting landing zones and drop zones, and selecting forward arming and refueling points.

4-44. Identifying areas vulnerable to threat/*adversary* aerial intelligence collection systems aids in selecting friendly battle positions. Establishing lines of sight and identifying IVLs are critical parts of analyzing observation and fields of fires because they have a bearing on line-of-sight direct fire weapons, antennas, reconnaissance, and some electro-optical systems.

4-45. An effective technique for analyzing observation and fields of fire is to produce a graphic that displays observation and fields of fire. The use of computer-generated terrain applications can assist in producing observation and fields of fire graphics. An ideal field of fire for direct fire weapons is an open field in which the threat/*adversary* can be seen and has no protection from fires. Analysts identify features of terrain that allow good observation for indirect fire weapons and determine if the terrain has any effect on fire support missions.

4-46. Figure 4-10 shows line-of-sight analysis used to determine observation and fields of fire in natural terrain.

1:250,000 - Afghanistan - Digital Terrain Elevation Data Level 2 - Shaded Relief

Fair   Good   Poor   Unsuited
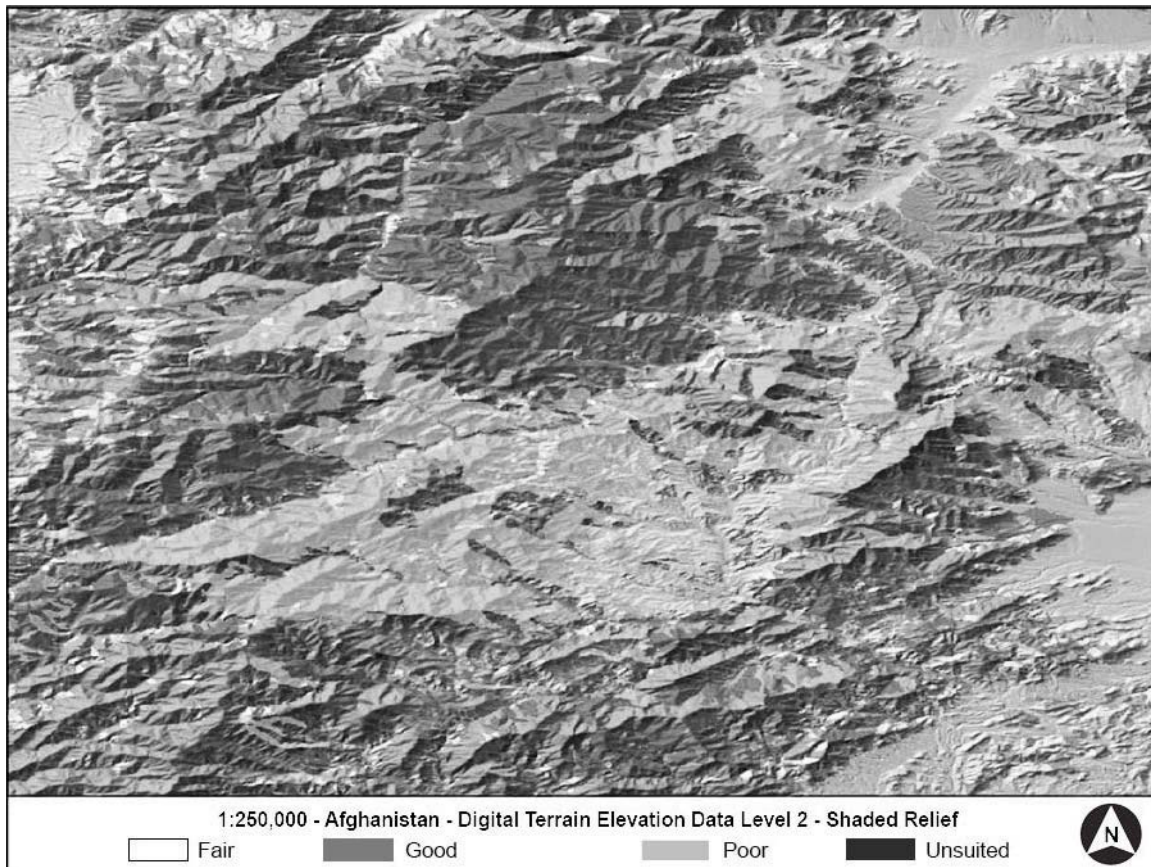
Figure 4-10. Observation and fields of fire (natural terrain)

4-47. Figure 4-11 shows line-of-sight analysis used to determine observation and fields of fire in urban terrain.
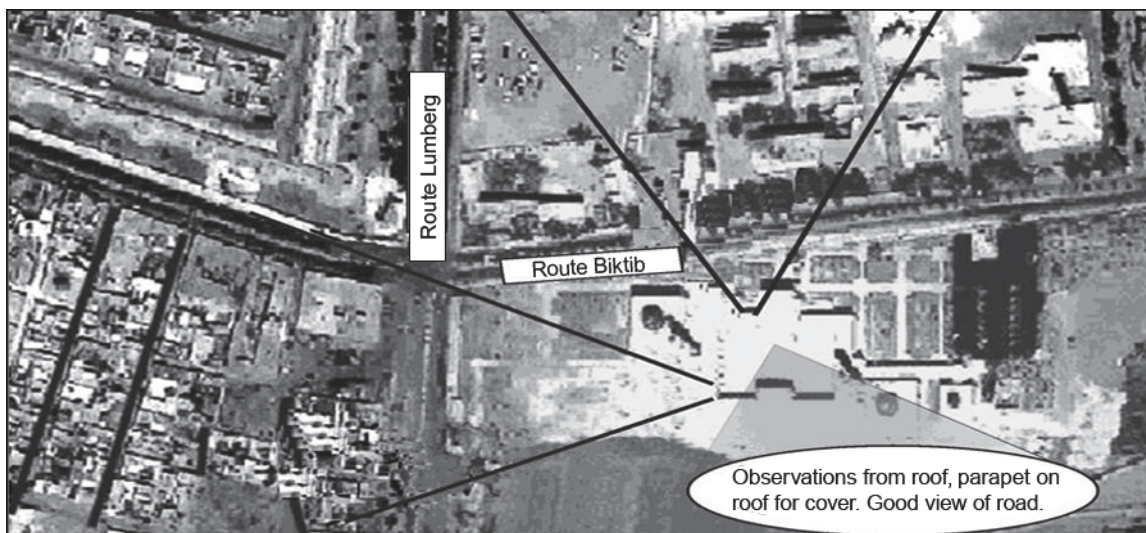
Figure 4-11. Observation and fields of fire (urban terrain)

Cover and Concealment

4-48. In intelligence usage, **cover** pertains to those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information (JP 2-01.2). Cover is the 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. 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.

4-49. **Concealment** is protection from observation or surveillance (ADRP 1-02). It degrades the threat's/ *adversary's* ability to observe forces, equipment, or position. Concealment can be provided by trees, underbrush, tall grass, cultivated vegetation, weather conditions (such as snow, fog, or rain), as well as manmade camouflage. Concealment does not necessarily provide cover.

4-50. Line-of-sight analysis determines the observation, fields of fire, and cover and concealment that the terrain provides to both the friendly and enemy/*adversary* forces. The following example and figure 4-12 illustrate the concept of cover and concealment in natural terrain and line-of-sight analysis.

Line-of-Sight Example
The masked area all lies behind terrain that is level with or higher than the defensive position. One cannot see into the masked area or fire direct weapons into it. One does not have observation or fields of fire behind the masking terrain. The masked area provides the attacker cover from the defender's direct fire and concealment from the defender's observations. If the enemy/*adversary* has done proper analysis, then they would select one or more of the approach routes.

Cover and concealment example

Suspected Threat/*Adversary* Position

Line-of-sight analysis example

Range

3,000

Masked Area

Masked Area

2,000

Masked Area

The arrows show covered and concealed approach routes to the unit's defense

1,000

Vantage Line
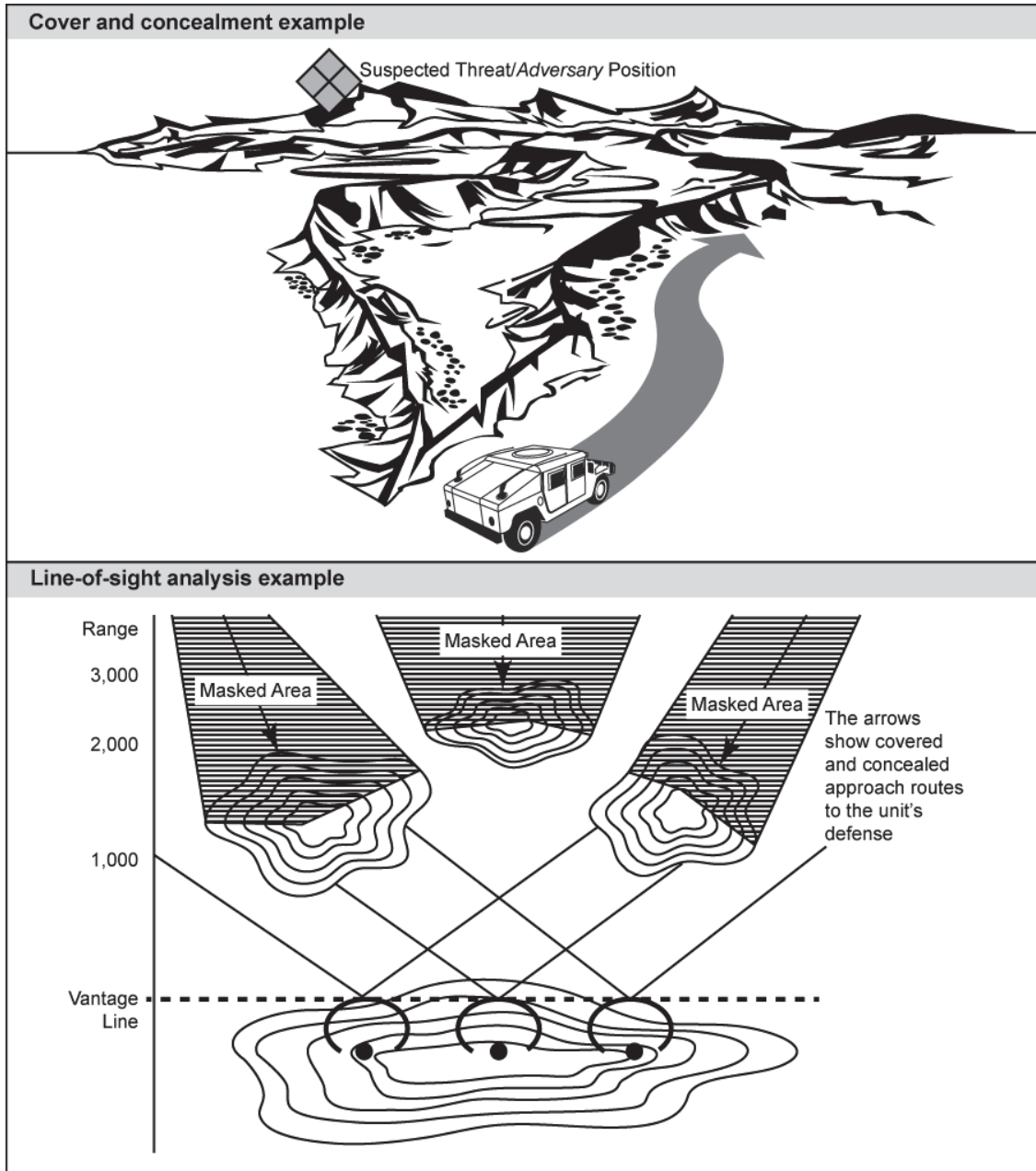
Figure 4-12. Cover and concealment (natural terrain) and line-of-sight analysis

4-51. Figure 4-13 illustrates the concept of cover and concealment in urban terrain.

Figure 4-13. Example of cover and concealment in urban terrain

TERRAIN EFFECTS

4-52. After determining terrain characteristics, the staff must determine the effect that the terrain will have on friendly and threat/*adversary* operations. The primary analytic tools used to aid in determining this effect are the MCOO and the terrain effects matrix.

Modified Combined Obstacle Overlay

4-53. The MCOO is a graphic product that portrays the effects of natural and urban terrain on military operations. The MCOO normally depicts military significant aspects of the terrain and other aspects of the terrain that can affect mobility. Though not all inclusive, some of these aspects are—

- AAs.
- Mobility corridors.
- Natural and manmade obstacles.
- Terrain mobility classifications.
- Key terrain.

4-54. The combined obstacle overlay provides a basis for identifying ground AAs and mobility corridors. Unlike the cross-country mobility, the combined obstacle overlay integrates all obstacles to vehicular movement, such as built-up areas, slope, soils, vegetation, and hydrology into one overlay. The overlay depicts areas that impede movement (severely restricted and restricted areas) and areas where friendly and enemy forces can move unimpeded (unrestricted areas).

4-55. The MCOO is tailored to the mission and is a collaborative effort involving input from the entire staff. The MCOO depicts the terrain according to mobility classification. These classifications are severely restricted, restricted, and unrestricted:

- Severely restricted terrain severely hinders or slows movement in combat formations unless some effort is made to enhance mobility. This could take the form of committing engineer assets to improving mobility or deviating from doctrinal tactics, such as moving in columns instead of line formations, or at speeds much lower than those preferred. For example, severely restricted terrain for armored and mechanized forces is typically characterized by steep slopes and large or densely spaced obstacles with little or no supporting roads. A common technique is to depict this type of severely restricted terrain on overlays and sketches by marking the areas with cross-hatched diagonal lines. Another technique is to color code the areas in red.

- Restricted terrain hinders movement to some degree. Little effort is needed to enhance mobility, but units may have difficulty maintaining preferred speeds, moving in combat formations, or transitioning from one formation to another. Restricted terrain slows movement by requiring zigzagging or frequent detours. Restricted terrain for armored or mechanized forces typically consists of moderate-to-steep slopes or moderate-to-densely spaced obstacles, such as trees, rocks, or buildings. Swamps or rugged terrain are examples of restricted terrain for dismounted infantry forces. Logistical or sustainment area movement may be supported by poorly developed road systems. A common and useful technique is to depict restricted terrain on overlays and sketches by marking the areas with diagonal lines. Another technique is to color code the areas in yellow.
- Unrestricted terrain is free of any restriction to movement. Nothing needs to be done to enhance mobility. Unrestricted terrain for armored or mechanized forces is typically flat to moderately sloping terrain with scattered or widely spaced obstacles such as trees or rocks. Unrestricted terrain allows wide maneuver by the forces under consideration and unlimited travel supported by well-developed road networks. No symbology is needed to show unrestricted terrain on overlays and sketches.

4-56. Terrain mobility classifications are not absolute but reflect the relative effect of terrain on the different types and sizes of movement formations. They are based on the ability of a force to maneuver in combat formations or to transition from one type of formation to another. The staff should consider the following:

- Obstacles are only effective if they are covered by observation and fire. However, even undefended obstacles may canalize an attacker into concentrations, which are easier to detect and target or defend against.
- When evaluating the terrain's effect on more than one type of organization (for example, mounted or dismounted), the obstacle overlays reflect the mobility of the particular force.
- The cumulative effects of individual obstacles in the final evaluation. For example, individually a gentle slope or a moderately dense forest may prove to be an unrestrictive obstacle to vehicular traffic. Taken together, the combination may prove to be restrictive.
- Account for the weather's effects on factors that affect mobility.
- The classification of terrain into various obstacle types reflects only its relative impact on force mobility. There are many examples of a force achieving surprise by negotiating supposedly "impassable" terrain.

4-57. Figure 4-14 is an example of a MCOO developed for natural terrain.
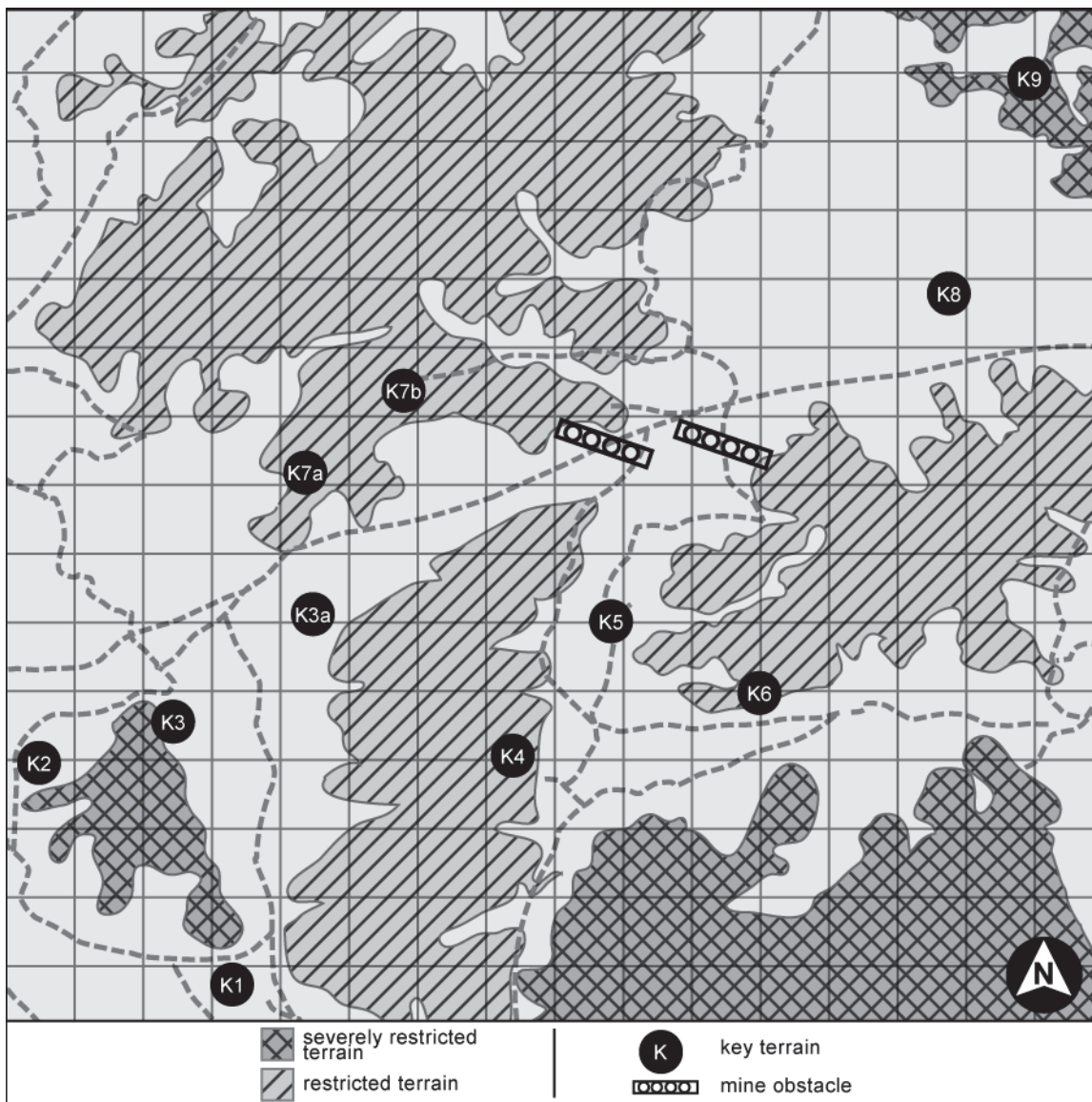
Figure 4-14. Example modified combined obstacle overlay (natural terrain)

4-58. For urban terrain, graphics typically depict population status overlays (population centers, urban areas, political boundaries); logistics sustainability overlays; LOCs; route overlays (street names, patterns, and widths); bridges, underpass and overpass information; potential sniper and ambush locations (likely this data will be a separate overlay); and key navigational landmarks. In developing urban terrain overlays, the following should be depicted:

- Natural terrain—the underlying natural terrain on which manmade terrain is superimposed, such as rivers, streams, hills, valleys, forests, desert, bogs, swamps.
- Manmade terrain—streets, bridges, buildings, railways, canals, traffic control points; building density, construct, dimensions; functional zone disposition; and street construct, materials, disposition, dimensions.
- Key facilities, targets and/or terrain—banks, bridges, airports, electric power grids, oil facilities, military facilities, key residences and places of employment, waterways; tall structures (skyscrapers); choke points; intersections; bridges; industrial complexes; other facilities; density of construction or population; street patterns.

- Obstacles—rubble and vehicles in the road; fixed barriers; masking of fires; burning of buildings and other fire hazards; rivers and lakes; power lines; cell phone towers; population; trenches; minefields; certain religious or cultural sites; wire obstacles (concertina wire, barb wire).

Note. In urban terrain, depict storm and drainage systems as well as public transportation routes, which may present themselves as obstacles to future friendly operations.

- In addition to the above factors, also consider—
    - The street level necessary to support the smallest enemy or friendly unit size, and the local street names whenever possible (official and unofficial).
    - Surface structure composition (cobblestone, concrete, dirt), along with elevation and slope.
    - Construction status (building or destroying) if development is underway.
    - Time pattern plots as necessary to show local population use in terms of movement.
    - Parking areas with weight restrictions, electrification of public transport, local airports, heliports and runways, inland-ports, and any known pipelines (along with their status: active, inactive, dimensions).

Evaluate Terrain Effects on Operations

4-59. Using the MCOO as a guide, the terrain effects matrix describes the effect each aspect of OAKOC/*KOCOA* has on friendly and threat/*adversary* operations. Table 4-3 is an example of a terrain effects matrix using a table format.

Table 4-3. Example terrain effects matrix

OAKOC aspects	*Terrain effects*
Obstacles	Wadis throughout the area of operations with an average depth of 5 to 10 feet and an average width of 20 feet that runs 6 to 10 kilometers long. Above-ground oil and transport pipeline that runs through the central width of the area of operations.
Avenues of approach	Primary and secondary road systems for high avenues of approach. Generally flat terrain with brigade-sized mobility corridors between small villages. Railroad in the north running east to west.
Key terrain	Airfield used as resupply and troop movements. Dam control waterflow on the river and is the primary objective of the threat/*adversary*.
Observation and fields of fire	Sparse vegetation on generally flat desert terrain with observation of 3 to 5 kilometers. There are 10 kilometers between intervisibility lines. Air support observation is unlimited due to sparse terrain and curve of the earth. Fields of fire for direct fire is 300 to 500 meters for small arms.
Cover and concealment	Cover is provided by intervisibility lines. Concealment is limited by the open terrain and sparse vegetation.

Note. For table 4-3, the Marine Corps uses *KOCOA (key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach) aspects.*

DESCRIBE HOW WEATHER CAN AFFECT FRIENDLY AND THREAT/*ADVERSARY* OPERATIONS

4-60. Weather analysis is the collection, processing, evaluation, and interpretation of relevant military aspects of weather. There are two sub-steps in weather analysis: analyze the military aspects (characteristics) of weather; and evaluate the weather's effects on military operations.

ANALYZE THE MILITARY ASPECTS OF WEATHER

4-61. The following are military aspects of weather:
- Visibility.
- Wind.
- Precipitation.
- Cloud cover/*ceiling*.
- Temperature.
- Humidity.
- Atmospheric pressure (as required).
- *Sea state.*

Visibility

4-62. Visibility is defined as the greatest distance that prominent objects can be seen and identified by the unaided, normal eye. A major factor in evaluating visibility is the amount of available light based on weather conditions and illumination as determined by the factors discussed below:
- **Begin morning nautical twilight** (also called BMNT) is start of that period where, in good conditions and in the absence of other illumination, the sun is 12 degrees below the eastern horizon and enough light is available to identify the general outlines of ground objects and conduct limited military operations (JP 2-01.3). Light intensification devices are still effective and may have enhanced capabilities.
- **Begin morning civil twilight** (also called BMCT) is the period of time at which the sun is halfway between beginning morning and nautical twilight and sunrise, when there is enough light to see objects clearly with the unaided eye (JP 2-01.3). At this time, light intensification devices are no longer effective, and the sun is six degrees below the eastern horizon.
- **Sunrise** is the apparent rising of the sun above the horizon. The rising times are dependent on latitude.
- **Sunset** is the apparent descent of the sun below the horizon. The setting times are dependent on latitude.
- **End evening civil twilight** (also called EECT) is the point in time when the sun has dropped 6 degrees beneath the western horizon, and is the instant at which there is no longer sufficient light to see objects with the unaided eye (JP 2-01.3). Light intensification devices are recommended from this time until begin morning civil twilight.
- **End of evening nautical twilight** (also called EENT) is the point in time when the sun has dropped 12 degrees below the western horizon, and is the instant of last available daylight for the visual control of limited military operations (JP 2-01.3). At end of evening nautical twilight there is no further sunlight available.
- **Moonrise** is the time at which the moon first rises above the horizon. The rising times are dependent on latitude.
- **Moonset** is the time at which the moon sets below the horizon. The setting times are dependent on latitude.

4-63. Other weather conditions can affect visibility as well. Temperature can affect the use of thermal sights. Cloud cover can negate illumination provided by the moon. Additionally, precipitation and other obscurants can have varying effects as well. Low visibility is beneficial to offensive and retrograde operations because it conceals concentration of maneuver forces, thus enhancing the possibility of surprise.

Low visibility hinders the defense because cohesion and control become difficult to maintain, reconnaissance operations are impeded, and target acquisition is degraded.

Wind

4-64. Wind of sufficient speed from any direction can reduce the combat effectiveness of a force as a result of blowing dust, smoke, sand, or precipitation. Strong winds and wind turbulence limit airborne, air assault, and aviation operations. High winds near the ground can lower visibility due to blowing dust; they also can affect movement or stability of some vehicles. Blowing sand, dust, rain, or snow can reduce the effectiveness or stability of radars, antennas, communications, and other electronic devices. High winds can also affect persistent threat/*adversary* detection systems like an aerostat. Evaluation of weather in support of operations requires information on the wind at the surface as well as at varying altitudes and elevations.

Precipitation

4-65. Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types. 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.

Cloud Cover/*Ceiling*

4-66. Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many intelligence sensors and target acquisition systems and general aviation operations. Conversely, low cloud cover may increase the available level of light when there is ground-based light, such as what is available in urban areas. Excessive low cloud cover may restrict visibility and limit safe aviation operations.

4-67. A *ceiling* means the height above the Earth's surface of the lowest layer of clouds or obscuring phenomena that is reported as broken, overcast, or obscuration, and not classified as thin or partial. A ceiling listed as "unlimited" means that the sky is clear or is free of any substantial cloud cover. Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many intelligence sensors and target acquisition systems and general aviation operations. Conversely, low cloud cover may increase the available level of light when there is ground-based light, such as what is available in urban areas. Excessive low cloud cover may restrict visibility and limit safe aviation operations.

Temperature

4-68. Temperature extremes can reduce effectiveness of troops and equipment capabilities. They may affect the timing of combat operations/*major operations*. For example, extremely high temperatures in a desert environment may require dismounted troops to operate at night. High temperatures can also affect the lift capability of medium-rotary-lift assets in high altitudes and elevations. For example, during Operation Enduring Freedom, during the summer months in Afghanistan, the UH 60 could not carry its full complement of passengers.

4-69. Thermal crossover is the condition in which the temperature of a ground-based vehicle is close to, if not the same as, the surrounding land. As a result of this condition, thermal optics are unable to detect enemy vehicles until a temperature disparity exists between the land and the vehicles. *Using Target Acquisition Weapons Software, meteorological and oceanographic (METOC) personnel can forecast for thermal crossover and determine specific times that the phenomenon will occur.*

4-70. High temperatures also can increase fuel consumption in vehicles, cause overheating, and affect the muzzle velocity of both direct and indirect fire weapons (155 millimeter howitzers, sniper rifles, tanks, other).

Humidity

4-71. Humidity is the state of the atmosphere with respect to water vapor content. 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 either relative humidity or absolute humidity.

Atmospheric Pressure (As Required)

4-72. Atmospheric pressure has a significant impact on aviation operations. Based on the elevation of the operational area, atmospheric pressure affects the lift capacity of aircraft, especially rotary-wing and tiltrotor aircraft in mountainous terrain. When combined with extreme temperatures, atmospheric pressure increases the amount of runway an aircraft requires for takeoff. (See JP 3-04 for more information on tiltrotor aircraft operations.)

Sea State

4-73. A *sea state* is the general condition of the surface on a large body of water—with respect to wind waves and swell—at a certain location and moment. A sea state is characterized by statistics, including the wave height, period, and power spectrum. The sea state varies with time, as the wind conditions or swell conditions change. The sea state can either be assessed by an experienced observer, like a trained mariner, or through instruments like weather buoys, wave radar, or remote sensing satellites.

EVALUATE THE WEATHER'S EFFECTS ON MILITARY OPERATIONS

4-74. Weather has both direct and indirect effects on military operations. The following are examples of direct and indirect effects on military operations:

- Temperature inversions might cause some battle positions to be more at risk to the effects of chemical agents as a result of atmospheric ducting, a process that occurs when strong high pressure influences an area and prevents particulates from dispersing into the upper atmosphere.
- Local visibility restrictions, such as fog, can have an effect on observation for both friendly and threat/*adversary* forces. Severe restrictions to visibility often restrict aviation operations.
- Hot, dry weather might force friendly and threat/*adversary* forces to consider water sources as key terrain.
- Dense, humid air limits the range of loudspeaker broadcasts affecting sonic deception, surrender appeals to enemy forces, and the ability to provide instruction to friendly or neutral audiences.
- Sandstorms with high silica content may decrease the strength and clarity of radio and television signals.

4-75. Weather and climate effects have an impact on seasonal outlooks, which have utility for seasonal decisionmaking; for example, giving crop selection and rotation advice in a particular area that boosts plant growth. Knowing that a particular area may be susceptible to locust swarms may enable pesticide application to prevent such a swarm. If a drought is expected, civil affairs personnel may advise planting another crop that raises the benefit to the farmer.

4-76. The following work aids assist in analyzing and describing weather effects on operations. (See *MCWP 3-35.7,* NWP 3-59M*/MCWP 3-35.10*, and JP 3-59 for additional weather-related operational and tactical decision aids.)

4-77. Figure 4-15 is an example of a weather forecast chart. This work aid provides a guide for determining the weather information needed for planning and operations.

Figure 4-15. Example weather forecast chart

4-78. Figure 4-16 is an example of a light and illumination table. This work aid provides a guide for determining the light and illumination data needed for planning and operations.
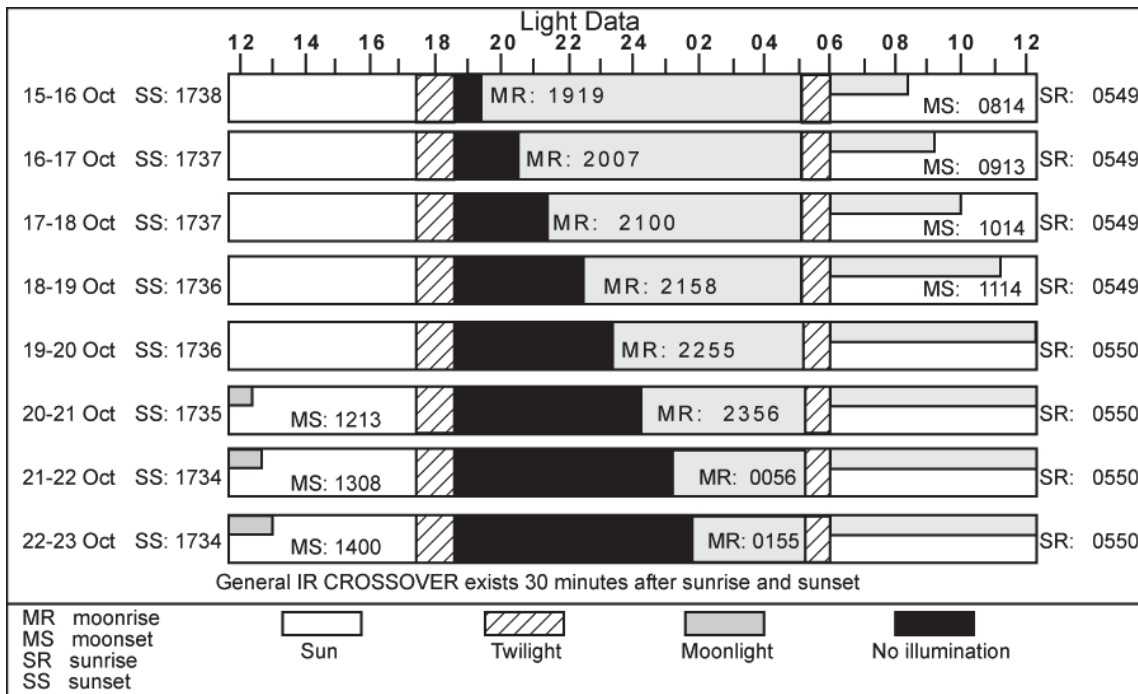
Figure 4-16. Example light and illumination table

4-79. Figure 4-17 is an example of a weather effects matrix/*operational impacts chart* in a table format. This work aid provides a guide for determining the weather effects on personnel, weapons, and equipment needed for planning and operations.

Figure 4-17. Weather effects matrix/*operational impacts chart*

4-80. *In the Marine Corps, METOC Marines are tasked with rendering tactical METOC support to every element of the MAGTF. Throughout the IPB process, METOC considerations are embedded within each step of the planning to ensure a full understanding of environmental impacts across the full range of military operations. As a Service component, the Marine Corps specializes in amphibious landing—forcible entry from the sea. A core competency unique to the Marine Corps, amphibious landings have specific METOC support requirements that must be exercised to ensure mission accomplishment. Current and forecast environmental conditions are applied to the array of vehicles used during amphibious insertions; sea states and surf zone conditions impact all amphibious landing craft in different ways, and a solid forecast is crucial when determining if an amphibious landing is a viable option.*

4-81. *The main amphibious platforms used by the Marine Corps personnel are the amphibious assault vehicle, landing craft/air cushioned, combat rubber reconnaissance craft, landing craft/utility, and rigid-hull inflatable boat. Forecasting for amphibious landings requires an in-depth knowledge of the platforms used in the operation, as well as environmental parameters that establish Go/No-Go criteria. Each of these platforms has specific operational thresholds while operating over the open ocean as well as within the surf zone at the landing site. Prior to launching any amphibious assets, METOC personnel analyze sea and surf zone conditions, and in concert with topographic and imagery Marines, conduct environmental and geographical analysis on proposed beach landing sites. Key beach landing sites analysis points include but are not limited to—*

- *Hydrographic surveys (usually accomplished by force reconnaissance Marines or embedded Navy sea, air, and land teams).*
- *Beach slope (>1/30 favorable, 1/30 to 1/50 marginal, >1/50 unfavorable).*
- *Soil composition.*
- *Breaker type (surf observations).*
- *Sea state.*
- *Modified surf index at the proposed landing time.*
- *Bioluminescence.*
- *Underwater hazards.*
- *Littoral current speed and direction.*
- *Immersion survivability time/water temperature.*

4-82. *Marine METOC personnel work with their Navy METOC counterparts to provide a unified forecast; this coordination usually takes place aboard navy amphibious ships, but also takes place among Marine Corps METOC sections attached to intelligence units.*

> ### Example
> *During the D-Day invasion at Normandy, surf zone conditions were extremely choppy; however, the date of 6 June 1944 was specifically chosen because that date offered a slight break in sea conditions that were otherwise impassable. Allied forces were able to execute a successful landing, and the German stronghold in France was finally broken.*

4-83. *METOC conditions have historically played a crucial role in operational planning, and are no less important today than they have been in the history of amphibious warfare.*

4-84. *Figures 4-18 through 4-26 on pages 4-24 through 4-28 are samples of METOC products used during Navy/Marine Corp METOC collaboration while at sea to illustrate Marine Corps METOC support to amphibious operations. (See 3-35.7, NWP 3-59M/MCWP 3-35.10, and JP 3-59 for additional information on Navy/Marine Corp METOC while at sea and during the execution of METOC support.)*

Amphibious Landing Brief

Sky Condition:
Mostly clear, becoming mostly cloudy by the late afternoon.

Visibility:
Unrestricted/occasionally 2 to 3 miles with mist in the late evening.

Maximum/Minimum Temperature:
67°F/51°F

Winds:
Winds will be out of the north from 9 to 11 knots overnight.

48- to 72-Hours Extended Outlook:
Another period of rain will affect the Camp Pendleton area on 27 January.

Tidal Data for Jan 24:		Surf Zone		Flight Level Winds	
Time	Depth			Feet	Knots
0408	4.9 feet	Modified Surf Index:	2.0	1,000	06005
1212	0.3 feet	Breaker Height:	1.5 feet	2,000	07005
1856	2.8 feet	Breaker Angle:	10 degrees	3,000	08005
2218	2.5 feet	Period:	13 seconds	4,000	08007
		Winds:	01005 knots	5,000	09008

Figure 4-18. *Amphibious landing weather example*

Amphibious Landing Brief VT: 110623 / 1200Z

Underwater Hazards: None
Average Swell: 1.5 KT
Littoral Current: N/NW 0.3 KT
Breaker Type: Spilling

Average Beach Slope: 1:33
Sea Surface Temperature (June): 63°F
Bioluminescence: N/A
Survival Times:
    With Immersion Suit: 6.3 hours
    Without Immersion Suit: 1.9 hours

Swell Direction

TIDES
(Type/Height/Time)

High	15.51 FT	17/2042Z
Low	-8.87 FT	18/0248Z
High	18.48 FT	18/0924Z
Low	-6.34 FT	18/1524Z

Blue Beach
Left Flank   **Right Flank**

	MSI Values	12Z-18Z	18Z-00Z	00Z-06Z	06Z-12Z	No forecast impacts to amphibious operations.
LCAC						
LCU						

F	Fahrenheit	KT	knots	LCU	landing craft, utility	N/A	not applicable	VT	valid time
FT	feet	LCAC	landing craft, air cushion	MSI	modified surf index	N/NW	north/northwest	Z	Zulu

Figure 4-19. *Beach landing site weather example*
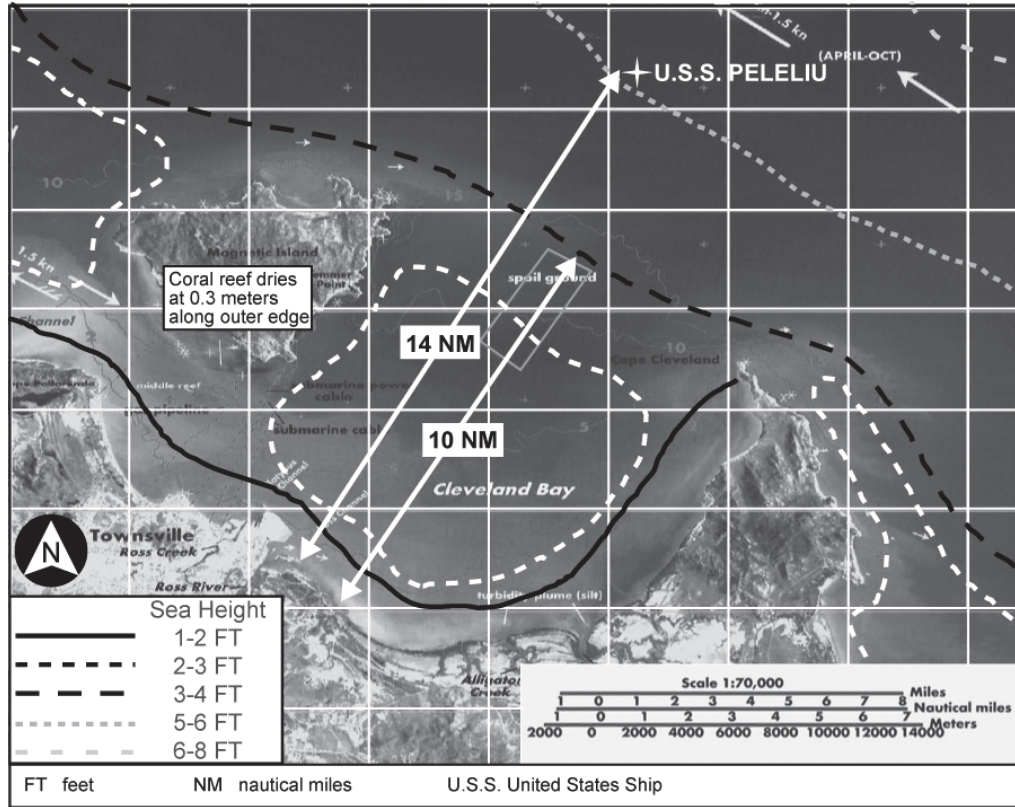
Figure 4-20. *Littoral weather example*
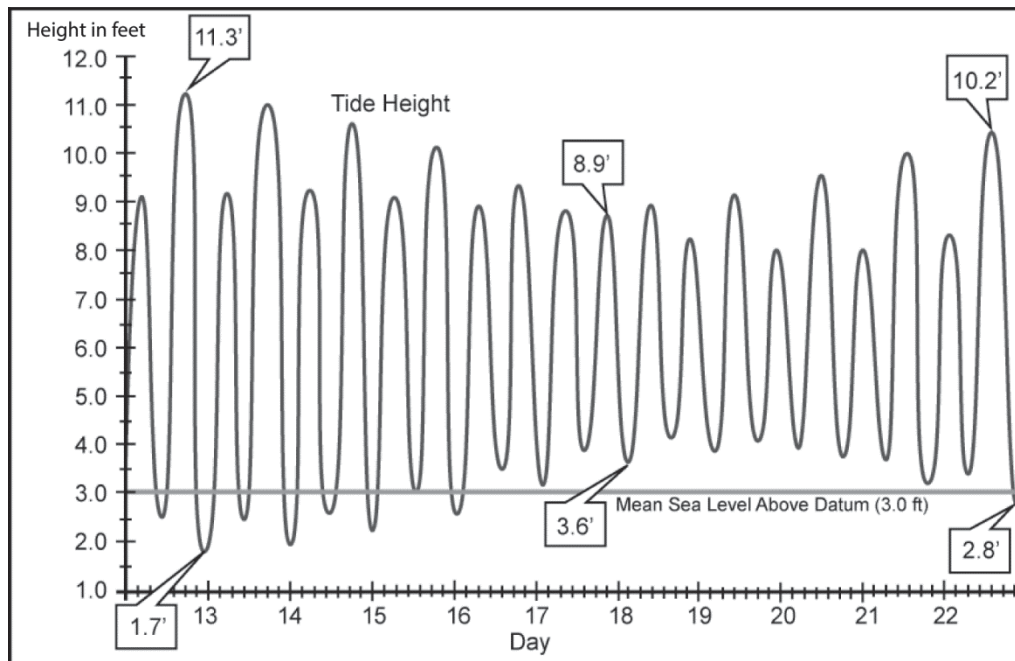
Figure 4-21. *Tidal weather example*

96-HOUR FORECAST

U.S.S. Peleliu

A cold front will move over the southern California region today, bringing rain showers and thunderstorms late this afternoon and evening. The system will move through the area tonight and tomorrow morning, with precipitation expected to end by the early afternoon on Sunday.

Flight Level Winds

1,000 FT - 20,018 KT   10,000 FT - 26,035 KT
2,000 FT - 20,020 KT   15,000 FT - 24,050 KT
3,000 FT - 21,016 KT   20,000 FT - 23,060 KT
4,000 FT - 25,020 KT   30,000 FT - 23,085 KT
5,000 FT - 25,020 KT

Day	Conditions	
SAT JAN 4 Rain Showers	**SKY CON:** Mostly cloudy **VIS:** Unrestricted, 1 to 3 miles in moderate rain showers **WINDS:** SW 10 to 12 KT becoming W/NW 18 to 20 KT by early evening **MAX/MIN TEMP:** 62°F/49°F **RELATIVE HUMIDITY:** 75% **PRECIP:** Afternoon rain showers and evening thunderstorms	**TURB:** LT/MOD SFC-150 **FRZ LVL:** 5,000 FT **ICING:** MOD, MXD 080-160 In the Evening **SEAS:** W/NW 3 to 5 FT
SUN JAN 5 Morning Rain	**SKY CON:** Mostly cloudy **VIS:** Unrestricted, 1 to 3 miles In rain showers and thunderstorms **WINDS:** W/NW 15 to 17 G27 KT **MAX/MIN TEMP:** 54°F/42°F **RELATIVE HUMIDITY:** 85% **PRECIP:** Rain showers/ thunderstorms tampering off by early afternoon	**TURB:** MOD SFC-200 **FRZ LVL:** 5,000 FT **ICING:** MOD, MXD 050-110 **SEAS:** W/NW 3 to 5 FT
MON JAN 6 Mostly Clear	**SKY CON:** Mostly cloudy **VIS:** Unrestricted **WINDS:** W/NW 12 to 14 KT **MAX/MIN TEMP:** 57°F/47°F **RELATIVE HUMIDITY:** 55% **PRECIP:** None	**TURB:** None **FRZ LVL:** 7,500 FT **ICING:** None **SEAS:** W/NW 4 to 7 FT
TUE JAN 7 Mostly Clear	**SKY CON:** Mostly cloudy **VIS:** Unrestricted **WINDS:** W/NW 12 to 14 KT **MAX/MIN TEMP:** 57°F/47°F **RELATIVE HUMIDITY:** 55% **PRECIP:** None	**TURB:** None **FRZ LVL:** 9,000 FT **ICING:** None **SEAS:** W/NW 4 to 7 FT

CON	conditions	MAX/MIN	maximum/minimum	TEMP	temperature
F	fahrenheit	MOD	moderate	TURB	turbulence
FRZ LVL	freezing level	MXD	mixed	U.S.S.	United States Ship
KT	knots	PRECIP	precipitation	VIS	visibility
L	low pressure	SEAS	sea conditions	W/NW	west/northwest
LT	light	SW	southwest		

Figure 4-22. 96-hour forecast weather example

ASTRONOMICAL DATA GRAPHIC — 24-Hour Timeline

Sunrise: 0517
Sunset: 1827
Hours of Daylight: 13:10
Moonrise: 2029
Moonset: 0834
% Illumination: 89
Begin Civil Twilight: 0451
End Civil Twilight: 1853
Begin morning nautical light: 0421
End evening nautical light: 1923

SOLAR TIME	ANGLE	LUNAR TIME	ANGLE	LUX
0600	7.7°	2200	11.3°	.006
0700	20.2°	2300	23.6°	.017
0800	32.7°	2400	35.9°	.028
0900	44.6°	0000	47.8°	.039
1000	55.8°	0100	59.4°	.047
1100	64.5°	0200	68.3°	.051
1200	67.5°	0300	71.4°	.052
1300	62.7°	0400	65.8°	.042
1400	53.2°	0500	55.8°	.032
1500	41.7°	0600	31.3°	.016
1600	29.4°			
1700	16.9°			
1800	4.5°			

Rising
Falling

Figure 4-23. *Astronomical data weather example*

LIGHT LEVEL PLANNING CALENDAR

Sun Above Horizon
Moon Below Horizon
Nautical Twilight
Civil Twilight
High Moonlight Level (≥0.0022 lux)
Low Moonlight Level (<0.0022 lux)

MEAN ASTRONOMICAL TIMES:

Date	SR	SS	% ILLUM	BMNT	EENT
11-20 Oct	0655	1814	57%-99%-89%	0600	1908

BMNT begin morning nautical light
EENT end evening nautical twilight
ILLUM illumination
Lux luminous
SR sunrise
SS sunset

Figure 4-24. *Light level weather example*

Operational Impacts Graphic									
	0800	1200	1600	2000	0000	0400	48 HR	72 HR	96 HR
Fixed Wing		Occasionally severe due			C,V,TS	C,V,TS	C,V	C	
Rotary Wing		to ceiling and visibility			C,V,TS	C,V,TS	C,V	C	
Personnel	C	C	C	C,V	C,V,TS	C,V,TS	C,V	C	
UAS Operations	C	C	C	C,V	C,V	C,V	C,V	C	
Collections			C	C	C	C	C,V	C,V	C
NVGs				C	C	C	C		
Communications				C	C	C	C		
Trafficability				P	P	P	P	P	
LCAC (Inner area)							S	S	S
LCU (Inner area)							S	S	S
AAV	S	S	S	S	S	S	S	S	S
CRRC/RHIB	S	S	S	S	S	S	S	S	S

☐ No Impacts ☐ Marginal Impacts ■ Severe Impacts ▨ Nonapplicable	• Marginal-to-severe impacts to FW/RW assets, UAS operations, and collections due to extensive cloud cover, rain, low visibilities, and area of thunderstorms. • Marginal-to-severe impacts to surface craft due to high seas during the 48- to 96-hour period. • Severe impacts to personnel due to freezing temperatures on land.

AAV	amphibious assault vehicle		P	precipitation
C	ceiling		RHIB	rigid hull inflatable boat
CRRC	combat rubber reconnaissance craft		RW	rotary wing
FW	fixed wing		S	seas
NVG	night vision goggles		TS	thunderstorms
LCAC	landing craft, air cushioned		UAS	unmanned aircraft system
LCU	landing craft, utility		V	visibility

Figure 4-25. *Operational impacts weather example*
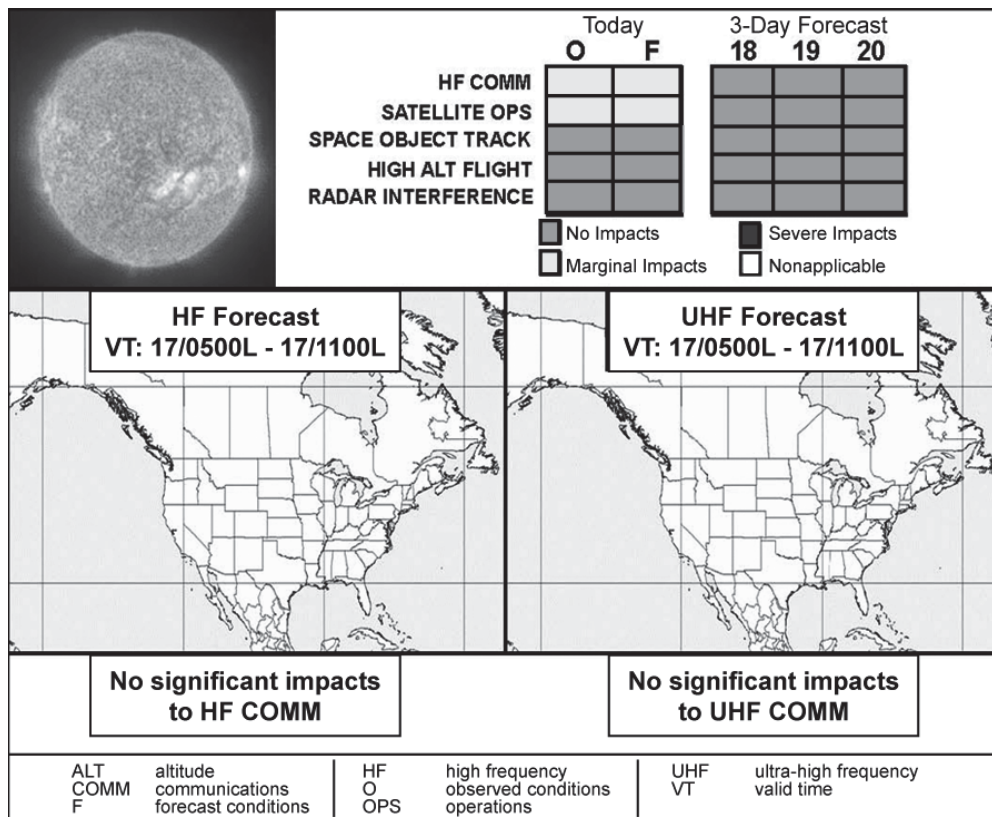
Figure 4-26. *Space weather example*

DESCRIBE HOW CIVIL CONSIDERATIONS CAN AFFECT FRIENDLY AND THREAT/*ADVERSARY* OPERATIONS

4-85. An understanding 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. The intelligence staff should leverage the rest of the staff, as well as outside agencies, who have expertise in civil considerations to aid the intelligence analysis in this area. Building knowledge during Army force generation is an opportunity to leverage agencies which are not deploying with the unit, but which have relevant regional knowledge.

4-86. Civil considerations comprise six characteristics, expressed in the memory aid ASCOPE. Civil considerations encompass the manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an AO and how these elements influence military operations. Tactical Army/*Marine Corps* staffs use ASCOPE to analyze civil considerations that are essential to support the development of effective plans for operations. Table 4-4 lists one method of cross-walking the operational variables PMESII and some examples for each ASCOPE characteristic.

4-87. ***Sociocultural factors*** *are the social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment (JP 2-01.3) must be closely analyzed during irregular warfare and hybrid conflicts. This cultural information incorporated into the IPB process provides the backdrop against which an analysis of social and political factors will allow for successful operations. The MCIA produced a cultural GIRH and Cultural Intelligence Indicator Guide that will assist Marine forces in understanding foreign cultures. Both documents are available on MCIA's SIPRNET Web site. Used in conjunction with ASCOPE analysis, an appreciation of cultural intelligence enables Marines to understand the environment in which they operate and ultimately lead to mission accomplishment.*

Table 4-4. PMESII and ASCOPE examples

	AREAS	STRUCTURES	CAPABILITIES	ORGANIZATIONS	PEOPLE	EVENTS

POLITICAL	• Enclaves
	• Municipalities
	• Provinces
	• Districts
	• Political districts
	• Voting
	• National boundaries
	• Party affiliation areas
	• Shadow government influence areas
		• Courts (court houses, mobile courts)
		• Government centers
		• Provincial/district centers
		• Meeting halls
		• Polling sites
			• Public administration:
			  ◦ Civil authority, practices, and rights
			  ◦ Political system
			  ◦ Political stability
			  ◦ Political traditions
			  ◦ Standards and effectiveness
			• Executive:
			  ◦ Administration
			  ◦ Policies
			  ◦ Powers
			  ◦ Organization
			• Legislative:
			  ◦ Administration
			  ◦ Policies
			  ◦ Powers
			  ◦ Organization
			• Judicial/legal:
			  ◦ Administration
			  ◦ Capacity
			  ◦ Policies
			  ◦ Civil and criminal codes
			  ◦ Powers
			  ◦ Organization
			  ◦ Law enforcement
			• Dispute resolution, grievances
			• Local leadership
			• Degrees of legitimacy
				• Major political parties:
				  ◦ Formal
				  ◦ Informal
				• Nongovernment organizations
				• Host government
				• Insurgent group affiliations
				• Court system
				• Covert political power
				• Partnerships: foreign
					• United Nations representatives
					• Political leaders
					• Governors
					• Councils
					• Elders
					• Community leaders
					• Paramilitary members
					• Judges
					• Prosecutors
						• Elections
						• Council meetings
						• Speeches (significant)
						• Security and military training sessions
						• Significant trials
						• Distribution of power
						• Political motivation
						• Treaties
						• Will

MILITARY	• Area of influence • Area of interest • Area of operation • Safe havens or sanctuary • Multinational/local nation bases • Historic ambush/improvised explosive device sites/insurgent bases	• Bases • Headquarters (police) • Known leader houses/businesses	• Doctrine • Organization • Training • Materiel • Leadership • Personnel manpower • Facilities • History • Nature of civil-military relationships • Resource constraints • Local security forces • Quick reaction force • Insurgent strength • Enemy recruiting	• Host-nation forces present • Insurgent groups present and networks • Multinational forces • Paramilitary organizations • Terrorists • Multinational forces present • Fraternal organizations • Civic organizations	• Key leaders • Multinational, insurgent, military	• Combat • Historical • Noncombat • Kinetic events • Unit reliefs • Loss of leadership

Table 4-4. PMESII and ASCOPE examples (continued)

	AREAS	STRUCTURES	CAPABILITIES	ORGANIZATIONS	PEOPLE	EVENTS

ECONOMIC	• Commercial
	• Fishery
	• Forestry
	• Industrial
	• Livestock dealers
	• Markets
	• Mining
	• Movement of goods/ services
	• Smuggling routes
	• Trade routes
	• Black market areas
		• Banking
		• Fuel:
		  ◦ Distribution
		  ◦ Refining
		  ◦ Source
		• Industrial plants
		• Manufacturing
		• Mining
		• Warehousing
		• Markets
		• Silos, granaries, warehouses
		• Farms/ranches
		• Auto repair shops
			• Fiscal:
			  ◦ Access to banks
			  ◦ Currency
			  ◦ Monetary policy
			• Ability to withstand drought
			• Black market
			• Energy
			• Imports/exports
			• External support/aid
			• Food:
			  ◦ Distributing
			  ◦ Marketing
			  ◦ Production
			  ◦ Processing
			  ◦ Rationing
			  ◦ Security
			  ◦ Storing
			  ◦ Transporting
			• Inflation
			• Market prices
			• Raw materials
			• Tariffs
				• Banks
				• Business organizations
				• Cooperatives
				• Economic nongovernment organizations
				• Guilds
				• Labor unions
				• Major illicit industries
				• Large landholders
				• Volunteer groups
					• Bankers
					• Employers/employees
					• Labor occupations
					• Consumption patterns
					• Unemployment rate
					• Underemployment rate (if this exists)
					• Job lines
					• Landholders
					• Merchants
					• Money lenders
					• Black marketers
					• Gang members
					• Smuggling chain
						• Drought, harvest, yield, domestic animals, livestock (cattle, sheep) and market cycles
						• Labor migration events
						• Market days
						• Payday
						• Business openings
						• Loss of business

SOCIAL	• Refugee camps
	• Enclaves:
	  ◦ Ethnic
	  ◦ Religious
	  ◦ Social
	  ◦ Tribal
	  ◦ Families or clans
	• Neighborhoods
	• Boundaries of influence
	• School districts
	• Parks
	• Traditional picnic areas
	• Markets
	• Outdoor religious sites
		• Clubs
		• Jails
		• Historical buildings/ houses
		• Libraries
		• Religious
		• Schools/universities
		• Stadiums
		• Cemeteries
		• Bars and tea shops
		• Social gathering places (meeting places)
		• Restaurants
			• Medical:
			  ◦ Traditional
			  ◦ Modern
			• Social networks
			• Academic
			• Strength of tribal/village traditional structures
			• Judicial
				• Clan
				• Community councils and organizations
				• School councils
				• Criminal organizations
				• Familial
				• Patriotic/service organizations
				• Religious groups
				• Tribes
					• Community leaders, councils and their members
					• Education
					• Ethnicity/racial:
					  ◦ Biases
					  ◦ Dominant group
					  ◦ Percentages
					  ◦ Role in conflict
					• Key figures:
					  ◦ Criminals
					  ◦ Entertainment
					  ◦ Religious leaders
					  ◦ Chiefs/elders
					• Language/dialects
					• Vulnerable populations
					• Displaced persons
					• Sports
					• Influential families
					• Migration patterns
					• Culture:
					  ◦ Artifacts
					  ◦ Behaviors
					  ◦ Customs
					  ◦ Shared beliefs/values
						• Celebrations
						• Civil disturbances
						• National holidays
						• Religious holidays and observance days
						• Food line
						• Weddings
						• Birthdays
						• Funerals
						• Sports events
						• Market days
						• Family gatherings
						• History: Major wars/ conflicts

INFORMATION	• Broadcast coverage area (newspaper, radio, television)
	• Word of mouth
	• Gathering points
	• Graffiti
	• Posters
		• Communications:
		  ◦ Lines
		  ◦ Towers (cell, radio, television)
		• Internet service:
		  ◦ Satellite
		  ◦ Hard wire
		  ◦ Cafes
		• Cellular phone
		• Postal service
		• Print shops
		• Telephone
		• TV stations
		• Radio stations
			• Availability of electronic media
			• Indigenous communications networks
			• Internet access
			• Intelligence services
			• Printed material:
			  ◦ Journals
			  ◦ Newspapers
			  ◦ Flyers
			• Propaganda mechanisms
			• Radio
			• Television
			• Social media
			• Literacy rate
			• Word of mouth
				• Media groups and news organizations
				• Religious groups
				• Insurgent inform and influence activities groups
				• Government groups
				• Public relations and advertising agencies
					• Decisionmakers
					• Media personalities
					• Media groups and news organizations
					• Community leaders
					• Elders
					• Heads of families
						• Disruption of services
						• Censorship
						• Religious observance days
						• Publishing dates
						• Inform and influence activities campaigns
						• Project openings

INFRASTRUCTURE	• Commercial
	• Industrial
	• Residential
	• Rural
	• Urban
	• Road systems
	• Power grids
	• Irrigation networks
	• Water tables
		• Emergency shelters
		• Energy:
		  ◦ Distribution system
		  ◦ Electrical lines
		  ◦ Natural gas
		  ◦ Power plants
		• Medical:
		  ◦ Hospitals
		  ◦ Veterinary
		• Public buildings
		• Transportation:
		  ◦ Airfields
		  ◦ Bridges
		  ◦ Bus stations
		  ◦ Ports and harbors
		  ◦ Railroads
		  ◦ Roadways
		  ◦ Subways
		• Waste distribution, storage, and treatment:
		  ◦ Dams
		  ◦ Sewage
		  ◦ Solid
		• Construction sites
			• Construction
			• Clean water
			• Communications systems
			• Law enforcement
			• Fire fighting
			• Medical:
			  ◦ Basic
			  ◦ Intensive
			  ◦ Urgent
			• Sanitation
			• Maintain roads, dams, irrigation, sewage systems
			• Environmental management
				• Construction companies:
				  ◦ Government
				  ◦ Contract
					• Builders
					• Road contractors
					• Local development councils
						• Scheduled maintenance (road/bridge construction)
						• Natural/manmade disasters
						• Well digging
						• Community center construction
						• School construction

4-88. Due to the complexity and volume of data involving civil considerations, there is no simple model for presenting civil considerations analysis. Rather, it comprises a series of intelligence products composed of overlays and assessments. The six characteristics of ASCOPE are discussed in paragraphs 4-89 through 4-116.

AREAS

4-89. Key civilian areas are localities or aspects of the terrain within an AO that often are not militarily significant. This characteristic approaches terrain analysis (OAKOC/*KOCOA*) from a civilian perspective. The intelligence staff analyzes key civilian areas in terms of how they may affect the missions of friendly forces as well as how friendly military operations may affect these areas. Examples of key civilian areas are—

- Areas defined by political boundaries, such as districts within a city or municipalities within a region.
- Locations of government centers.
- Social, political, religious, or criminal enclaves.
- Ethnic/Sectarian fault lines.
- Agricultural and mining regions.
- Trade routes.
- Possible sites for the temporary settlement of displaced civilians or other civil functions.

4-90. The intelligence staff maintains this information in the civil considerations data file and constructs an areas overlay to aid in planning. The civil considerations data file and the areas overlay are discussed beginning at paragraph 4-117.

STRUCTURES

4-91. Existing structures can have various degrees of significance. Analyzing structures involves determining how the location, functions, capabilities, and consequences of its use can support or hinder the operation. Using a structure for military purposes often competes with civilian requirements. Commanders must carefully weigh the expected military benefits against costs to the community that have to be addressed in the future. Commanders also need to consider the significance of the structure in providing stability to the AO. Certain structures are critical in providing a state of normalcy back to the community and need to be maintained or restored quickly. The possibility of repaying locals for the use of shared facilities or building more of the same facilities, time and cost permitting, should also be considered. The following are examples of structures:

- Military bases.
- Police stations.
- Jails.
- Courtrooms.
- Political offices.
- Electrical power plants and substations.
- Petroleum, oils, and lubricants refineries.
- Dams.
- Water and sewage treatment and distribution facilities.
- Communications stations and networks.
- Bridges and tunnels.
- Warehouses.
- Airports and bus terminals.
- Universities and schools.

4-92. Other structures are cultural sites that international law or other agreements generally protect, for example:

- Religious structures.
- National libraries and archives.
- Hospitals and medical clinics.
- Monuments.
- Works of art.
- Archaeological sites.
- Scientific buildings.
- Museums.
- Crops, livestock, and irrigation works.
- United Nations Educational, Scientific and Cultural Organizations-designated World Heritage Sites.

4-93. The intelligence staff maintains this information in the civil considerations data file and, due to the amount of information in these categories, constructs multiple overlays for structures to aid in planning.

CAPABILITIES

4-94. Commanders and staffs analyze capabilities from different levels. They view capabilities in terms of those required to save, sustain, or enhance life, in that priority. Capabilities can refer to the ability of local authorities—those of the host nation, aggressor nation, or some other body—to provide a populace with key functions or services, such as—

- Public administration.
- Public safety.
- Emergency services.
- Technology.
- Basic necessities (food, water, medical availability).

4-95. Capabilities include those areas in which the populace may need help after combat operations/*major operations*, such as public works and utilities, public health, economics, and commerce. Capabilities also refer to resources and services that can be contracted to support the military mission, such as interpreters, laundry services, construction materials, and equipment.

4-96. The intelligence staff maintains this information in the civil considerations data file and constructs a structures overlay to aid in planning.

ORGANIZATION

4-97. IPB considers the organization dimension (such as the nonmilitary groups or institutions) and political influence and their impacts in the AO. Organizations influence and interact with the populace, friendly forces, the threat/*adversary*, and each other. An important aspect of civil considerations is the political dimension of the local population and their expectations relative to threat/*adversary* and friendly operations.

4-98. Political structures and processes enjoy varying degrees of legitimacy with populations from local through international levels. Formally constituted authorities and informal or covert political powers strongly influence events. Political leaders can use ideas, beliefs, violence, and other actions to enhance their power and control over people, territory, and resources. There are many sources of political interest. These may include charismatic leadership; indigenous security institutions; and religious, ethnic, or economic factors. Political opposition groups or parties also affect the situation. Each may cooperate differently with U.S. or multinational forces.

4-99. Understanding the political circumstances helps commanders and staffs recognize key organizations and determine their aims and capabilities. Understanding political implications requires analyzing all relevant partnerships—political, economic, military, religious, and cultural. This analysis captures the presence and significance of external organizations and other groups, including groups united by a common cause. Examples include private security organizations, transnational corporations, and NGOs that provide humanitarian assistance.

4-100. Political analysis must include an assessment of varying political interests and the threat's/*adversaries'* political decisive point/*center of gravity* and will. Will is the primary intangible factor; it motivates participants to sacrifice to persevere against obstacles. Understanding what motivates key groups (for example, political, military, and insurgent) helps commanders understand the groups' goals and willingness to sacrifice to achieve their ends.

4-101. Organizations are nonmilitary groups or institutions in the AO. They influence and interact with the populace, the force, and each other. They generally have a hierarchical structure, defined goals, established operations, fixed facilities or meeting places, and a means of financial or logistic support. Some organizations may be indigenous to the area. These organizations may include—

- Religious organizations.
- Fraternal organizations.
- Patriotic or service organizations.
- Labor unions.
- Criminal organizations.
- Community watch groups.

- Political groups.
- Agencies, boards, committees, commissions (local and regional, councils).
- Multinational corporations.
- Intergovernmental organizations (IGOs), such as United Nations agencies.
- Other host-nation government agencies (foreign version of Department of Education, United States Agency for International Development).
- NGOs, such as the International Committee of the Red Cross.

> *Note.* The other host-nation government agencies designated above are separate from organizations within the threat/*adversary* capability (military, intelligence, police, paramilitary), such as the Central Intelligence Agency.

4-102. To enhance their situational awareness, commanders must remain familiar with organizations operating in their AOs, such as local organizations which understand the political dimension of the population. Situational awareness includes having knowledge of how the activities of different organizations may affect military operations and how military operations may affect these organizations' activities. From this, commanders can determine how organizations and military forces can work together toward common goals when necessary.

4-103. In almost every case, military forces have more resources than civilian organizations. However, civilian organizations may possess specialized capabilities that they may be willing to share with military forces. Commanders do not command civilian organizations in their AOs. However, some operations require achieving unity of effort between them and the force. These situations require commanders to influence the leaders of these organizations through persuasion. They produce constructive results by the force of argument and the example of their actions.

4-104. The intelligence staff maintains this information in the civil considerations data file and, due to the amount of information in these categories, constructs multiple overlays for organizations to aid in planning.

PEOPLE

4-105. The use of the general term "people" describes nonmilitary personnel encountered by military forces. The term includes all civilians within an AO as well as those outside the AO whose actions, opinions, or political influence can affect the mission. Individually or collectively, people can affect a military operation positively, negatively, or neutrally. In stability tasks, Army/*Marine Corps* forces work closely with civilians of all types. Understanding the sociocultural factors of the people in the AO is a critical component of understanding the operational environment.

4-106. There can be many different kinds of people living and operating in and around an AO. As with organizations, people may be indigenous or introduced from outside the AO. An analysis of people will identify them by their various capabilities, needs, and intentions. It is useful to separate people into distinct categories such as demographically, social and political groups, and target audiences. (A target audience list can be obtained from the military information support operations element or information operations officer/G-3.) When analyzing people, commanders consider historical, cultural, ethnic, political, economic, religious, and humanitarian factors. They also identify the key communicators and the formal and informal processes used to influence people.

4-107. The languages used in the region will have a huge impact on operations. The staff identifies the languages and dialects used within the AO so language training, communication aids (such as phrase cards and requisitioning of translators) can begin. Translators will be crucial for collecting intelligence, interacting with local citizens and community leaders, and developing products.

4-108. Another aspect of language involves the transliteration guide not written using the English alphabet. This will have an impact on all intelligence operations to include collection, analysis, dissemination, and targeting. In countries that do not use the English alphabet, a theater-wide standard should be set for spelling names. Without a spelling standard, it can be difficult to conduct effective analysis. In addition, insurgents and/or criminals may be released from custody if their names are

misidentified. To overcome these problems, there must be one spelling standard for a theater. Because of the interagency nature of counterinsurgency operations, the standard must be agreed upon by non-Defense agencies. Intelligence staffs should also be aware of family naming conventions in places like the Middle East where various cultures do not use an individual's surname and family name.

4-109. Another major consideration when analyzing people is religion. Religion has shaped almost every conflict of the past, and there are indicators that its influence will only grow. The staff considers the following when incorporating religion in planning. They—

- Know when religious traditions will be affected by the mission and try to determine how religion will affect the mission.
- Know when religious figures have influenced social transformations in a negative or positive way.
- Attempt to understand all parties, no matter how violent or exclusive.

4-110. Religion has the ability to shape the operational environment. Religion can add a higher intensity, severity, brutality, and lethality to conflicts than almost any other factor. Religion can motivate the masses quickly and inexpensively.

4-111. Part of the analysis of people is identifying cultural terms and conditions. Cultural terms and conditions describe both American and foreign ways of thought and behavior. Understanding culture gives insight into motives and intent of nearly every person or group in the operational environment: friend, enemy, or other. This insight in turn allows commanders and staffs to allocate resources, outmaneuver opponents, alleviate friction, and reduce the fog of war. The study of culture for military operations is not an academic exercise and therefore requires specific military guidelines and definition. The analyst sets aside personal bias and judgment and examines the cultural group dispassionately, basing the analysis purely on facts. The military studies broad categories of cultural factors, such as—

- Social structure.
- Behavioral patterns.
- Perceptions.
- Religious beliefs.
- Tribal relationships.
- Behavioral taboos.
- Centers of authority.
- Lifestyles.
- Social history.
- Gender norms and roles.

4-112. Culture is studied in order to give insights into the way people think, the reasons for their beliefs and perceptions, and what kind of behavior they can be expected to display in given situations. Because cultures are constantly shifting, the study of culture is an enduring task that requires historical perspective as well as the collection and analysis of current information.

4-113. The intelligence staff maintains this information in the civil considerations data file and, due to the amount of information in these categories, constructs multiple overlays for people to aid in planning.

EVENTS

4-114. Events are routine, cyclical, planned, or spontaneous activities that significantly affect organizations, people, and military operations. Examples include—

- National and religious holidays.
- Agricultural crop or livestock and market cycles.
- Elections.
- Civil disturbances.
- Celebrations.

●   Natural phenomenon (such as monsoon, seasonal floods and droughts, volcanic and seismic activity, natural disasters).
●   Manmade disasters.

4-115.   Examples of events precipitated by military forces include combat operations/*major operations*, congested road networks, security restrictions, and economic infrastructure disruption or stimulus. Once significant events are determined, it is important to template the events and to analyze them for their political, economic, psychological, environmental, and legal implications.

4-116.   The intelligence staff maintains this information in the civil considerations data file and constructs an events overlay to aid in planning. The civil considerations data file and overlays are discussed below.

CIVIL CONSIDERATIONS DATA FILES, OVERLAYS, AND ASSESSMENTS

4-117.   As stated previously, the intelligence staff maintains a civil considerations data file that organizes all the information it has collected and analyzed based on the ASCOPE characteristics. This data file organizes the raw data the intelligence staff uses to assess civil considerations during IPB, as well as to support targeting and civil affairs operations. The data file includes all the information related in the ASCOPE characteristics.

Example

Under the "capabilities" characteristic there may be a section for the sub-characteristic of "oil." This section includes information on the location of all the infrastructure components associated with "oil." It would also include the biographical, contact, and location information for the personnel associated with this capability. Finally, this section includes any intelligence assessments and recommendations associated with "oil."

4-118.   One way of maintaining civil considerations data is in a data file and/or database; this contributes to the continuous evaluation of civil considerations as part of the running estimate by organizing the vast amount of information necessary to analyze civil considerations.

4-119.   Civil considerations overlays are graphic depictions of the data file and aids planning throughout the MDMP/*MCPP*, as well as aiding situation development during operations. These overlays aid the intelligence staff in describing civil considerations effects, as assessed in the data file, to the commander and rest of the staff.

4-120.   The civil considerations data file and associated overlays aids the commander and staff in identifying information and intelligence requirements not normally identified through the event templating process associated with determining threat/*adversary* COAs. In contingency operations, or when conducting stability tasks, these work aids are critical in assisting the intelligence staff in determining and assessing threat/*adversary* COAs.

4-121.   The civil consideration assessment is used throughout the MDMP/*MCPP*. Civil consideration assessments utilize both the civil considerations data files and overlays in order to provide the supported commander with a detailed analysis of the civil component of the area of interest in accordance with ASCOPE characteristics. Potential areas of investigation in the civilian consideration assessment could include, but are not limited to, mapping of social and political patterns, including formal and informal leadership as well as identifying key societal friction points. As stated previously, civil considerations help commanders understand the social, political, and cultural variables within the AO and their effect on the mission.

4-122.   Understanding the relationship between military operations and civilians, culture, and society is critical to operations and is essential in developing effective plans. The development of civil considerations data files, overlays, and assessments can be augmented by regional civil considerations data repositories maintained at the national and theater levels.

4-123. During predeployment, unit intelligence staffs should become familiar with the information available on assigned or contingency regions in military and other data repositories, Web sites, and portals. During operations, units utilize, update, and add to the body of information available to them and others. During relief in place and/or transfer of authority, it is critical that outgoing units educate incoming units on the information sources available for their areas of operation.

4-124. HTTs/*foreign area officers, regional affairs, and other cultural enablers* can also provide detailed information and analysis pertaining to sociocultural factors as an aspect of civil considerations.

4-125. There is no standard set of sub-characteristics and overlays the intelligence staff produces under this task. The determination of what is needed is based on the intelligence staff's assessment of the situation and complexity of the AO.

4-126. The civil considerations data file is a spreadsheet set up in a workbook format that is tabbed using the categories identified in the ASCOPE characteristics. Figures 4-27 through 4-32 on pages 4-37 through 4-39 are examples of how to construct data files and overlays.

Figure 4-27. Example of civil considerations data file
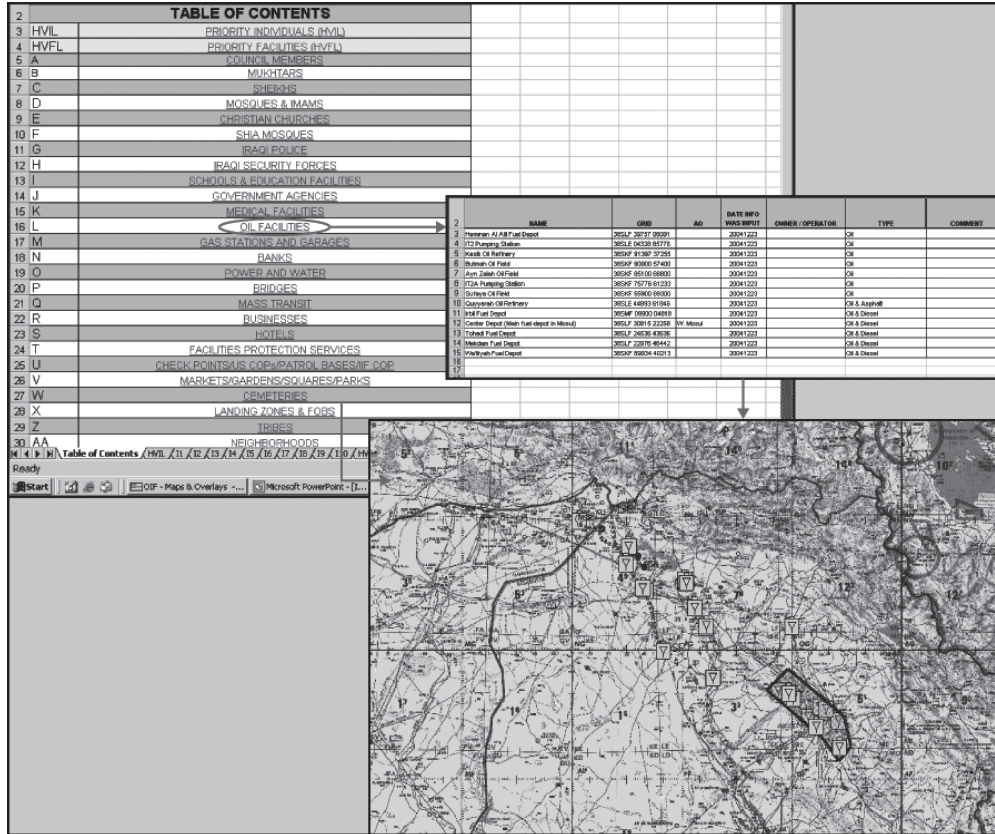
Figure 4-28. Civil considerations data file example (inside view with overlay)
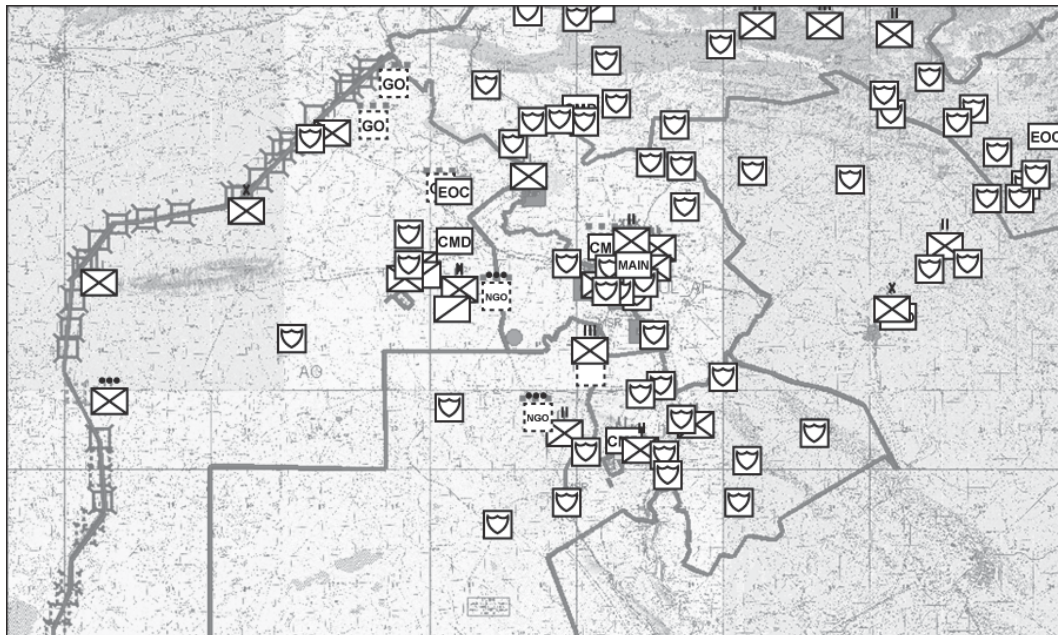
Figure 4-29. Security organizations and bases example
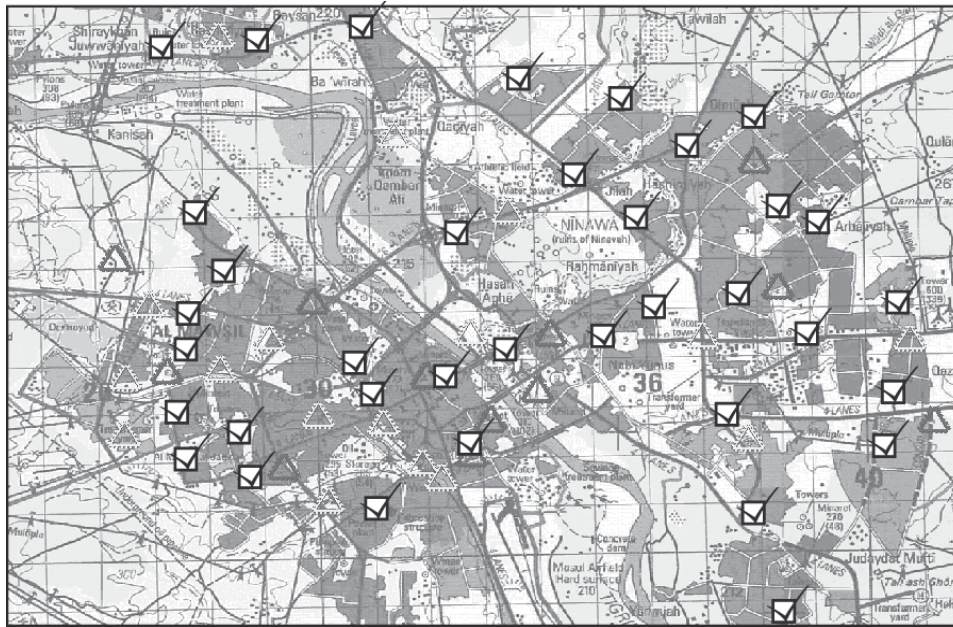
Figure 4-30. Voting locations example
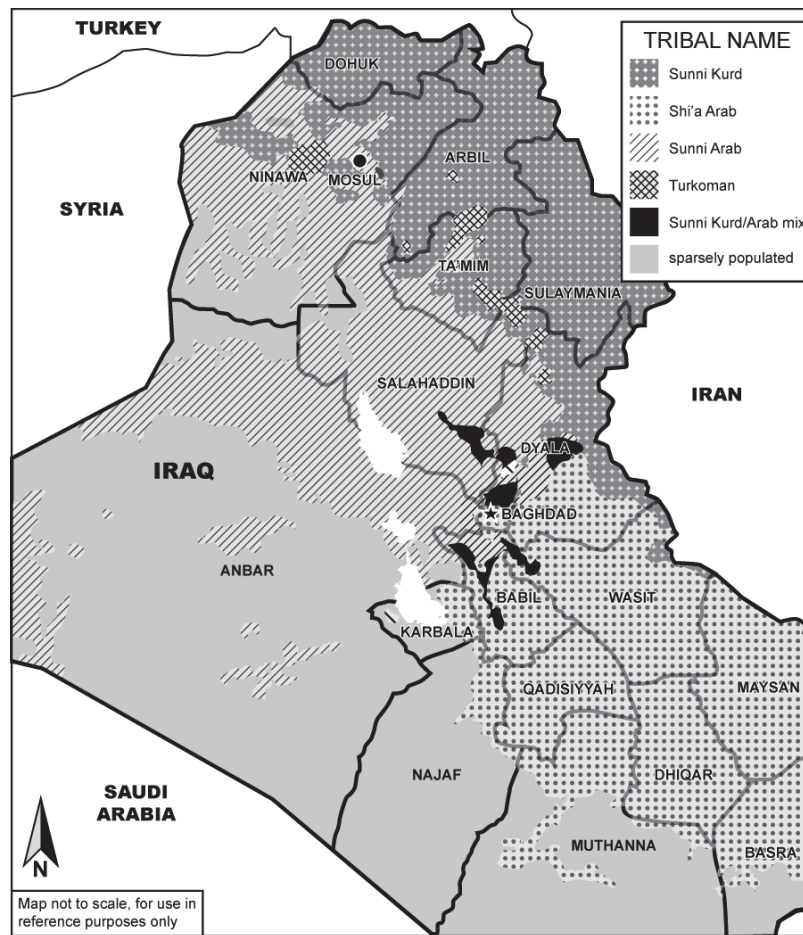
Figure 4-31. Population status example
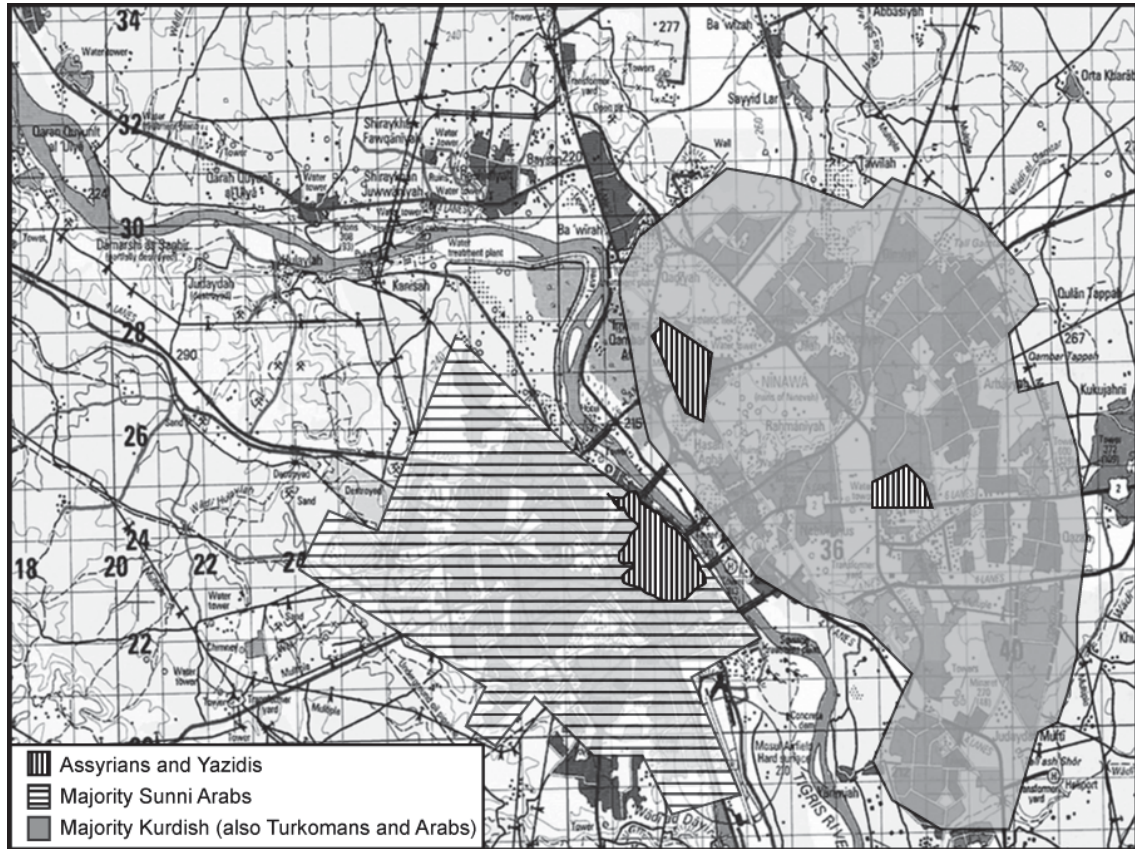
Figure 4-32. Ethnic overlay example

This page intentionally left blank.

Chapter 5

Step 3 of the IPB Process—Evaluate the Threat/*Adversary*

WHAT IS IT?

5-1.   Step 3 of the IPB process determines threat/*adversary* force capabilities and the doctrinal principles and TTP threat/*adversary* forces prefer to employ. This may include threats/*adversaries* that create multiple dilemmas for our maneuver forces by simultaneous employment of regular, irregular, terrorist forces, and criminal elements, using an ever-changing variety of traditional and nontraditional tactics.

Example

While planning a contingency show-of-force operation, a G-2 directs the Joint Intelligence Center to study the decisions on record of the targeted country's dictator. As a result of this research, the intelligence center produces a model of how the dictator makes decisions, with special emphasis on the dictator's tendencies during political crises. Meanwhile, the S-2 of the brigade/*unit* that will conduct the operation does an individual evaluation of the threat/*adversary* that includes the S-2's contingency area threat characteristics/*adversary order of battle* files and determines that the two threat/*adversary* brigades within the target area are equipped, organized, and trained well enough to be capable of offensive as well as defensive tasks against the friendly brigade/*unit*. The S-2 prepares threat/*adversary* models depicting the threat/*adversary* normal offensive and defensive tasks in built-up areas (the setting for the show-of-force operation).

DESIRED END STATE

5-2.   The G-2/S-2 develops threat/*adversary* models which accurately portray how threat/*adversary* forces normally execute operations and how they have reacted to similar situations in the past for the threats/*adversar*ies specific to the mission and environment. The primary output associated with step 3 of the IPB process is a compilation of threat/*adversary* models for each identified threat/*adversary* in the AO that the intelligence staff uses to guide the development of threat/*adversary* COA. This may include—

- Creating and updating threat characteristics/*adversary order of battle* files.
- Developing the situation template.
- Creating threat/*adversary* capabilities statement.
- Determining the HVTL.
- Updating the intelligence estimate.
- Any request for information on requests for collection, which are refined and updated.

SO WHAT?

5-3.   The "so what" in this step is enhancing the commander's understanding of the regular, irregular, catastrophic, or disruptive threat/*adversary* force within the commander's area of interest:

- Success results in threat/*adversary* COAs developed in the next step of IPB to reflect what the threat/*adversary* is capable of and trained to do in similar situations.
- Consequences of failure:
  - The staff will lack the intelligence needed for planning.

- ▪ The threat/*adversary* will surprise the friendly force with capabilities that the G-2/S-2 failed to account for.
- ▪ The staff may waste time and effort planning against threat/*adversary* capabilities that do not exist.

HOW TO DO IT: (THE PROCESS)

5-4.   Step 3 of the IPB process consists of the following actions, which are shown in figure 5-1.
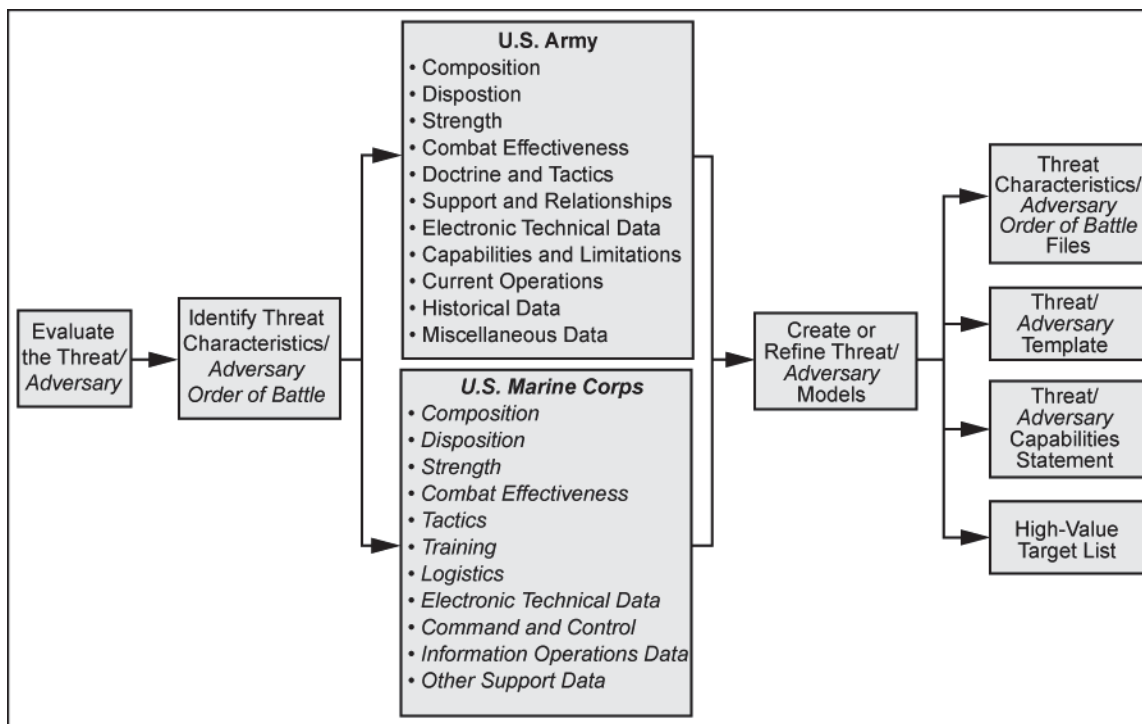
Figure 5-1. Evaluate the threat/*adversary*

5-5.   Threats/*adversaries* are a fundamental part of an overall operational environment for any operation but are discussed separately here simply for emphasis. A **threat** is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADRP 3-0). Threats/*adversaries* may include individuals, groups of individuals (organized or not organized), paramilitary or military forces, nation-states, or national alliances.

5-6.   Threats/*adversaries* are generally nation-states, organizations, people, groups, or conditions that can damage or destroy life, vital resources, or institutions. Army/*Marine Corps* doctrine divides these threats/*adversaries* into the following categories: regular, irregular, hybrid, disruptive, catastrophic, and hazards. This publication only discusses the evaluation of regular, irregular, and hybrid threat/*adversary* forces. Evaluating the threat/*adversary* should begin with identifying there is a threat/*adversary*, followed by the analysis of the threat's characteristics/*adversary*'s *order of battle*, and ultimately leading to the identification of the threat/*adversary* model (regular, irregular, or hybrid structure).

- ● **Regular threats/*adversary* forces** are part of nation-states employing recognized military capabilities and forces in understood forms of military competition and conflict. The Islamic Republic of Iran Army and the Peoples Liberation Army of China are examples of regular forces.
- ● **Irregular threat/*adversary* forces** are an opponent employing unconventional, asymmetric methods and means to counter U.S. advantages. A weaker enemy often uses unconventional methods to exhaust the U.S. collective will through protracted conflict. Unconventional methods include such means as terrorism, insurgency, and guerrilla warfare. Economic, political,

informational, and cultural initiatives usually accompany and may even be the chief means of irregular attacks on U.S. influence. The Revolutionary Army Forces of Columbia-People's Army and Al Qaeda are examples of irregular forces.

● **Hybrid threats/*adversary* forces** are the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects.

5-7. The analysis of any enemy force involves understanding that enemy through the de-aggregation of its component parts (threat characteristics/*adversary order of battle*).

5-8. A commander's understanding of the threat/*adversary* is based in part on the intelligence staff's research and analysis on threat/*adversary* characteristics. To ensure this understanding is as complete as possible, the intelligence staff considers the following when assessing these factors:

● Threat characteristics/*adversary order of battle* form a framework for the consistent evaluation of any force.

● The threat characteristics/*adversary order of battle* evaluation framework should be adapted to the mission and a unit's needs.

● Properly maintained files are sources of information on the threat's/*adversary*'s operations, capabilities, and weaknesses.

● Threat characteristics/*adversary order of battle* are analyzed as a whole.

5-9. Although threat/*adversary* forces may conform to some of the fundamental principles of warfare that guide Army/*Marine Corps* operations, these forces all have obvious and subtle differences in how they approach situations and problem solving. Understanding these differences is essential in understanding how a threat/*adversary* force will react in a given situation. (See ADRP 2-0 for additional information on threat capabilities. *See MCWP 2-3 for a discussion on adversary capabilities.*)

IDENTIFY THREAT CHARACTERISTICS/*ADVERSARY ORDER OF BATTLE*

5-10. There are 11 broad areas the intelligence staff considers when analyzing threat characteristics/*adversary order of battle*: composition, disposition, strength, combat effectiveness, doctrine and tactics, support and relationships, electronic technical data, capabilities and limitations, current operations, historical data, and miscellaneous data. (*See MCWP 2-3 for a discussion on adversary order of battle factors such as composition, disposition, strength, tactics, training, logistics, combat effectiveness, electronic technical data, information operations data, and other support data.*)

5-11. During steps 1 and 2 of the IPB process, the intelligence staff identified and defined each individual threat/*adversary* within the commander's area of interest. During step 3, the intelligence staff analyzes the characteristics associated with each of these threats/*adversaries*. The intelligence staff also develops threat/*adversary* models for each of these threats/*adversaries*.

5-12. When operating against a new or emerging threat/*adversary* that is not identified and described in the unit's enemy data files, the intelligence staff has to develop new data files for each of these threats/*adversaries*.

COMPOSITION

5-13. Composition is the identification and organization of a threat/*adversary*. It applies to specific units or commands as opposed to types of units. Regular forces are normally self-identified and organized similar to friendly forces. Irregular forces may follow similar rules but most often are organized based on a cellular structure. Understanding an enemy's composition is—

● Essential in determining its capabilities and limitations.

● Aids in constructing the threat/*adversary* models that help in the development of valid enemy COAs and friendly counteractions.

● Aids in determining an enemy's/*adversary*'s combat effectiveness and in conducting combat assessment.

5-14. Composition describes how an entity is organized and equipped—essentially the number and types of personnel, weapons, and equipment. The staff uses line-and-block chart products to visually see the enemy's composition.

5-15. Composition also refers to how an entity is commanded and controlled. Military forces have distinct and well-defined organizational structures generally built around a linear chain of command. These forces include air and ground forces that, regardless of national origin, generally follow a modern or contemporary military organizational model. Irregular forces also have distinct and well-defined organizational structures generally cellular in nature and directed through a decentralized chain of command usually unique to the area and/or conflict. Regardless of the type of threat/*adversary*, knowing its structure aids in understanding its capabilities and limitations. Figure 5-2 is an example of the organization of a regular threat/*adversary* force. Figure 5-3 is an example of the organization of an irregular threat/*adversary* force.
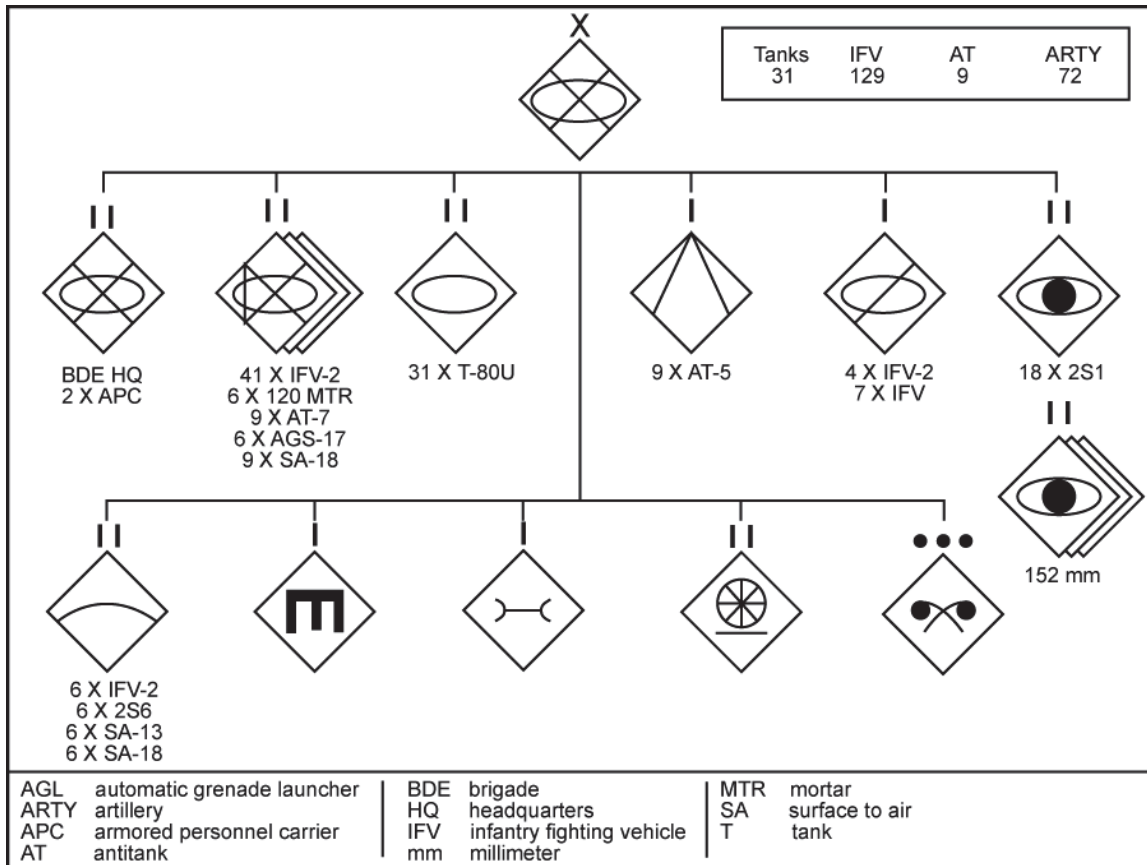
Figure 5-2. Example organizational chart for a regular threat/*adversary* force
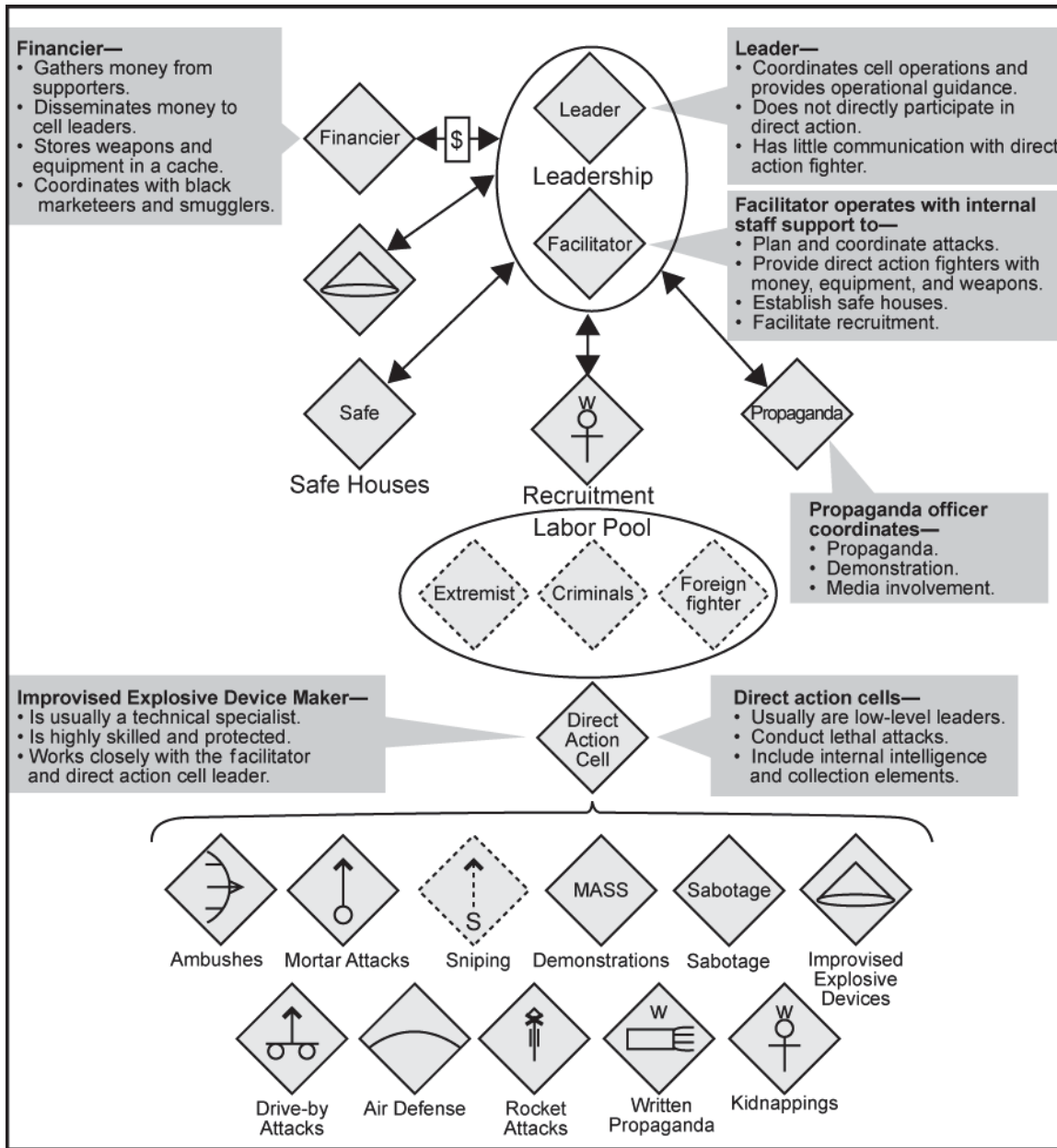
Figure 5-3. Example organizational chart for an irregular threat/*adversary* force

Regular Threat/*Adversary* Forces

5-16. The identity and organization of the regular forces belonging to the world's various nation-states are generally known by the U.S. intelligence community and maintained by the National Ground Intelligence Center. U.S. forces intelligence staffs can access this data as needed to support respective commands. The composition of regular forces is organized around a central command structure. The composition of a regular force is easily communicated though the use of organizational charts that depict the number and types of units in the force as well as the number and types of personnel, weapons systems, and equipment associated with these units.

Irregular Threat/*Adversary* Forces

5-17. Determining composition for irregular threat/*adversary* forces involves the identification of military, political, religious, ethnic, criminal, or terrorist organizations. Unit identification consists of the complete designation of a specific entity by name or number, type, relative size or strength, and subordination. Composition includes—

- Operational and support cells (similar to sections in a military unit).
- Echelons.
- Staff elements.
- Political, religious, ideological, and military aims.
- Internal and external command and control.
- Operational organizations.
- Internal and external support structure.
- External ties.
- Assassination squads.
- Bomb and demolition squads.
- Attack or hit squads.

5-18. The identity and organization of irregular threat/*adversary* forces is not always known. Irregular threat/*adversary* forces are generally part of an insurgency and are often relatively new organizations. Broadly speaking, there are two kinds of insurgencies: national insurgencies and resistance movements.

- In a national insurgency, the conflict is between the government and one or more segments of the population. In this type of insurgency, insurgents seek to change the political system, take control of the government, or secede from the country. A national insurgency polarizes the population and is generally a struggle between the government and insurgents for legitimacy and popular support.
- In contrast, a resistance movement (sometimes called a liberation insurgency) exists when insurgents seek to expel or overthrow what they consider a foreign or occupation government. The grievance is foreign rule or foreign intervention. Resistance movements tend to unite insurgents with different objectives and motivations. However, such an insurgency can split into competing factions when foreign forces leave and the focus of resistance is gone. That situation may result in a civil war.

5-19. Irregular forces generally have political objectives and are motivated by an ideology or grievances. These grievances may be real or perceived. Identifying these objectives and motivations can be difficult for a number of reasons:

- There may be multiple insurgent groups with differing goals and motivations.
- Insurgent leaders may change and the movement's goals change with them.
- Movement leaders may have different motivations from their followers.
- Insurgents may hide their true motivations and make false claims.
- The goals of an insurgency may change due to changes in the operational environment.

5-20. Irregular forces are usually armed military organizations or terrorist groups that have bypassed legitimate political authority and have taken up arms to pursue a common cause. The list at table 5-1, although not all-inclusive, is a description of potential irregular forces.

Table 5-1. Description of potential irregular forces

Type	Description
Revolutionary	Organizations involved in a revolution. These forces almost always have a political component that established its goals and objectives.
Guerrilla	Organizations that use unconventional tactics to combat regular forces that have an advantage in size, capability, and support.
Militia	Generally composed of ordinary citizens who have been organized for a specific purpose.
Partisan	General unconventional forces that oppose control of an area by a foreign power or by an Army of occupation by some kind of insurgent activity.
Paramilitary	Usually elements of a regular force using unconventional tactics to combat an occupying regular Army.
Terrorist groups	Organizations that target civilians in order to gain political leverage.
Insurgent organizations	Have no regular table of organization and equipment structure. The mission, environment, geographic factors, and many other variables determine the configuration and composition of each insurgent organization and its subordinate cells. A higher insurgent organization can include organizations at regional, provincial, district, national, or transnational levels. Higher insurgent organizations can contain a mix of local insurgent and guerrilla organizations. Each of these organizations provides differing capabilities.
Mercenaries	Armed individuals who use conflict as a professional trade and service for private gain. Depending on the circumstances, a mercenary may not be a lawful combatant. The term "mercenary" applies to those acting individually and in formed units. Ground forces serving officially in foreign armed forces are not mercenaries. Loan service personnel sent to help train ground forces of other countries as part of an official training agreement between sovereign governments are not mercenaries even if they take a direct part in hostilities.
Criminal organizations	Normally independent of nation-state control. Large-scale criminal organizations often extend beyond national boundaries to operate regionally or worldwide and include a political influence component. Individual criminals or small gangs do not normally have the capability to adversely affect legitimate political, military, and judicial organizations. Large-scale criminal organizations can challenge governmental authority with capabilities and characteristics similar to a paramilitary force. By mutual agreement or when their interests coincide, criminal organizations may become affiliated with other actors, such as insurgents or individuals. They may provide capabilities similar to a primitive Army for hire. Insurgents or guerrillas controlling or operating in the same area as a criminal organization can provide security and protection to the criminal organization's activities in exchange for financial assistance, intelligence, arms and materiel, or general logistical support.

Hybrid Threat/*Adversary* Forces

5-21. A hybrid threat/*adversary* force is comprised of two or more of the following entities that combine, associate, or affiliate in order to achieve mutually beneficial goals and objectives:

- A nation-state regular force.
- A nation-state irregular force.
- Insurgent groups.
- Guerilla units.
- Criminal organizations.

5-22. There is no standard organizational structure for a hybrid threat/*adversary* force.

DISPOSITION

5-23. Disposition refers to how threat/*adversary* forces are arrayed on the battlefield/*battlespace*. It includes the recent, current, and projected movements or locations of tactical forces. Regular threat/*adversary* forces are generally conducting some form of offensive or defensive maneuver. Irregular threat/*adversary* forces are generally in some part of the plan, prepare, execute, and assess phases for an operation such as a raid or ambush. Understanding how the threat/*adversary* doctrinally arrays itself on the battlefield/*battlespace* is essential in developing threat/*adversary* models in step 3 of the IPB process and threat/*adversary* situation overlays in step 4 of the IPB process. The intelligence staff familiarizes themselves with graphic training aids that visually depict range fans with weapons' fire limits and direct and indirect weapons capabilities to better understand enemy weapon systems.

Regular Threat/*Adversary* Forces

5-24. When evaluating a regular threat/*adversary* force, disposition refers to geographical location, tactical deployment, and movement of formations. Disposition consists of the location of threat/*adversary* units and the manner in which these units are tactically (or administratively in times of peace) deployed. In addition, disposition includes the recent, current, and proposed (or probable) movements of enemy units.

5-25. Location refers to a geographical area or position occupied by a unit or units. Knowledge of the strength and location of an enemy assists the intelligence staff in determining the capabilities of the force and its effect upon the accomplishment of the friendly mission. Data of this type is collected during peacetime and forms the basis for accessing capabilities during the initial period of hostilities.

5-26. Tactical deployment is the relative position of units with respect to one another or to the terrain. Tactical formations are designed for executing the various tactical maneuvers. If this deployment can be predetermined, it leads to an accurate appraisal of intentions. The knowledge of how enemy units are echeloned may indicate (if the enemy assumes the offensive) which units will be used in the main attack and which units will be used in supporting reserve roles. Tactical deployment with respect to terrain is also important. A study of dispositions and an analysis of the terrain aid the development of conclusions concerning enemy capabilities, vulnerabilities, and intentions.

5-27. Movement of enemy units is also part of disposition. Movement is the physical relocation of a unit from one geographical point to another. Patrol activity may be an indication of planned movement. Movement is significant because it automatically changes the tactical deployment of the enemy forces. When an enemy unit has moved, is moving, or will be moving, there are a number of actions which may affect the situation; for example, a unit may be moving into an attack position, or moving to reinforce or replace a unit, or perform other missions unknown to friendly forces. In view of these possibilities, movement of an enemy unit becomes important and units are monitored at all times in order for the analyst to provide correct and detailed data on enemy dispositions.

5-28. When evaluating a regular enemy force at any point prior to receipt of mission, intelligence staffs will not know the terrain on which either the enemy or friendly force will be operating. Therefore, arraying the enemy on the battlefield/*battlespace* as commonly seen on an enemy situation overlay is not possible. However, it is possible to doctrinally portray how the enemy will array itself on the battlefield/*battlespace* to conduct specific operations. This process is called threat/*adversary* templating, and is part of the threat/*adversary* modeling process. This is an ongoing process that is part of garrison intelligence operations. The threat/*adversary* templates developed here are reexamined and refined during IPB. The development of threat/*adversary* templates is the responsibility of intelligence staffs at any echelon. *(See figure A-2 on page A-4 for an example of an adversary doctrinal template.)*

Irregular Threat/*Adversary* Forces

5-29. For irregular threat/*adversary* forces, disposition consists of the geographic location of the following elements:

- Safe houses.
- Movement routes.
- Training camps.
- Base camps.
- Logistic bases and resupply points.

5-30. Additionally, disposition includes the recent, current, and projected movements or locations of tactical forces.

5-31. For the U.S. Army, figure 5-4 on page 5-10 shows an example of a complex battle position for a task-organized guerilla platoon threat model followed by an example scenario. Paragraphs 5-32 through 5-36 apply only to the U.S. Army. *(For the Marine Corps, see paragraph 5-37 and figure 5-5 on page 5-11.)*

5-32. Complex battle positions typically have the following characteristics that distinguish them from simple battle positions:

- Limited AAs. (Complex battle positions are not necessarily tied to an AA.)
- Any existing AAs are easily observable by the defender.
- A 360-degree fire coverage and protection from attack. (This may be due to the nature of surrounding terrain or engineer activity such as tunneling.)
- Engineer effort prioritizing camouflage, concealment, cover, and deception measures; limited countermobility effort that might reveal the complex battle position location.
- Large logistics caches.
- Sanctuary from which to launch local attacks.

5-33. Leaders of a unit, cell, or organization occupying complex battle positions intend to preserve their combat power until conditions permit offensive action. The threat defending in complex battle positions will use restrictive terrain and engineer countermobility efforts to deny the enemy the ability to approach, seize, and occupy the position. They will also make maximum use of camouflage, concealment, cover, and deception and cultural standoff to deny the enemy the ability to detect and attack the position.

5-34. Complex battle position defenders typically engage only as long as they perceive an ability to defeat the enemy. Should the defending complex battle position leaders evaluate that their forces are about to be decisively engaged, they will attempt a withdrawal or a withdrawal under pressure in order to preserve combat power.

5-35. Depending on the size and capabilities of an irregular force, functions can be allocated to disruption, main defense, support, and a reserve. Reconnaissance and other security measures are a constant activity to observe AAs near a complex battle position in order to provide early warning to the threat leader.

5-36. Information warfare elements of the complex battle position maintain situational awareness and understanding of local conditions with relevant populations as integral to threat reconnaissance, intelligence, surveillance, and target acquisition tasks. Generally, the complex battle position will not have easily detectable information warfare activities.

Figure 5-4. U.S. Army example of a complex battle position for a task-organized guerilla platoon threat model

Example

The guerilla platoon occupies a complex battle position as a defensive location designed to employ a combination of complex terrain; camouflage, concealment, cover, and deception; and engineer effort to protect the unit from detection and attack while denying their seizure and occupation by the enemy. A simple battle position differs from a complex battle position in that a simple battle position is a defensive location oriented on the most likely enemy AA and is not necessarily tied to complex terrain. (See TC 7-100.2, paragraphs 4-106, 4-108, and 4-145 to 4-171, for more information on battle positions.)

5-37. *For the Marine Corps, figure 5-5 shows an example of a Marine Corps doctrinal template for an irregular adversary.*
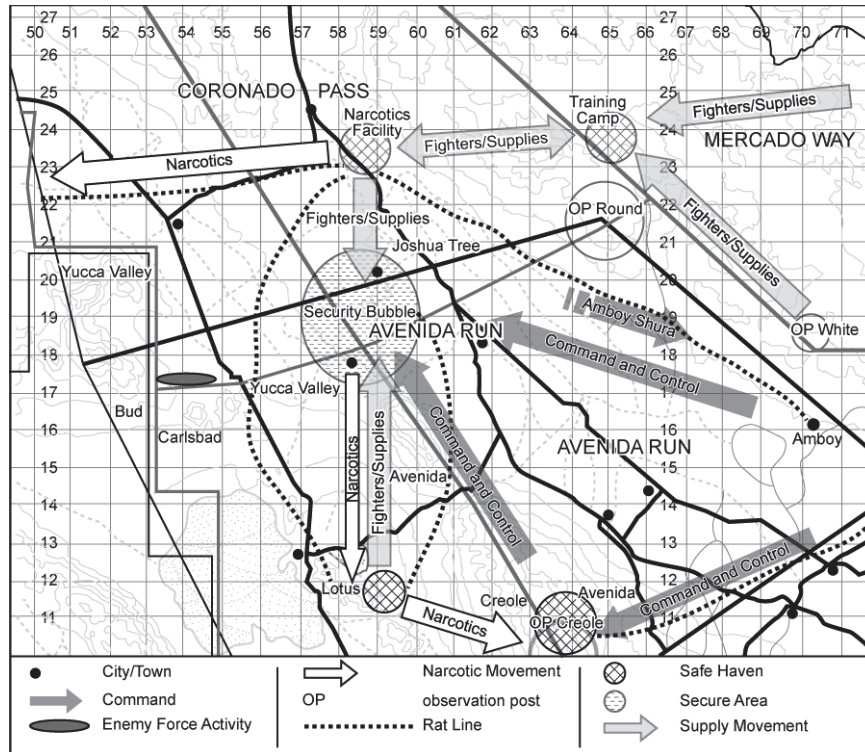
Figure 5-5. *Example of a Marine Corps doctrinal template for an irregular adversary*

5-38. Figure 5-6 is an example of an integrated attack by a task-organized guerilla battalion threat/*adversary* model.
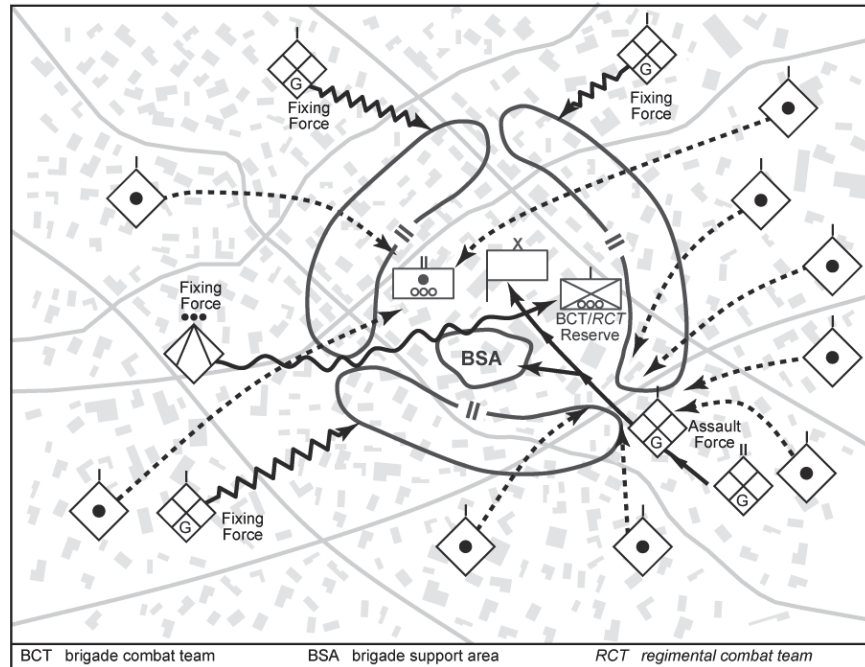
Figure 5-6. Example of an integrated attack by task-organized guerilla battalion threat/*adversary* model

Hybrid Threat/*Adversary* Forces

5-39. There are no threat/*adversary* force models or templates currently developed for specific hybrid threats/*adversary* forces. However, TC 7-100 includes some basic attack and/or defends hybrid force scenarios designed to support exercise design. These scenarios, along with focused research on real-world threat/*adversary* activity, can aid in developing threat/*adversary* templates.

STRENGTH

5-40. Strength describes a unit in terms of personnel, weapons, and equipment. Information concerning strength provides the commander with an indication of enemy capabilities and helps determine the probable COAs or options open to threat/*adversary* commanders. A lack of strength or a preponderance of strength has the effect of lowering or raising the estimate of the capabilities of an enemy force. Likewise, a marked concentration or build-up of units in an area gives the commander certain indications of enemy objectives and probable COAs. During peacetime, changes in the strength of potential threat/*adversary* forces are important factors which may indicate changes in the threat's/*adversary*'s intention. Strength is determined by comparing how a threat/*adversary* organization is doctrinally staffed and equipped with what the organization actually has on hand.

Regular Threat/*Adversary* Forces

5-41. Strength for regular forces is described in terms of personnel, weapons, and equipment. The most important aspect of strength when evaluating a regular force is to determine whether the force has the capability of conducting specific operations. For example, a unit may have adequate weapons systems to conduct an operation, but may not have a sufficient number of trained personnel or crews to man the systems.

Irregular Threat/*Adversary* Forces

5-42. For irregular forces, strength is defined by the capability of direct action teams, political cadre or cells, and, most importantly, popular support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving, logistics, or just withholding information.

Hybrid Threat/*Adversary* Forces

5-43. The strength of a hybrid threat/*adversary* force is determined by understanding the synergy of regular and irregular forces. The hybrid threat/*adversary* force understands that the environment that would produce the most challenges to U.S. forces is one in which conventional military operations occur in concert with unconventional warfare. The hybrid threat/*adversary* force concept is not just one of making do with what is available, but is primarily one of deliberately created complexity.

5-44. Each component of the hybrid threat/*adversary* force brings a capability to bear. The synergy of these capabilities is not to be understated. Operational environments by their very nature provide a myriad of complexities based on their characteristics. The hybrid threat/*adversary* force seeks to introduce additional complexity through the use of an ever-shifting array of forces, technologies, and techniques.

COMBAT EFFECTIVENESS

5-45. Combat effectiveness describes the abilities and fighting quality of a unit. Numerous tangible and intangible factors affect it.

Regular Threats/*Adversary* Forces

5-46. Determining combat effectiveness for regular threat/*adversary* forces is made by assessing the following factors:

- Personnel strength.
- Amount and condition of weapons and equipment.
- Status of training.
- Efficiency of leadership.
- Quality of leadership.
- Length of time a unit is committed in combat.
- Traditions and past performance.
- Personality traits of the unit commanders.
- Geographical area in which committed.
- Morale, spirit, health, nutrition, discipline, and political reliability (or belief in the cause for which they fight).
- Status of technical and logistical support of the unit.
- Adequacy of military schooling at all levels.
- National characteristics of the people.

Irregular Threat/*Adversary* Forces

5-47. Combat effectiveness for irregular threat/*adversary* forces is measured differently from combat effectiveness for regular threat/*adversary* forces. The threat/*adversary* is motivated by many factors, which can be, but are not limited to, a goal of independence, equality, religion or ideology, occupation of a foreign nation, or economical. Combat effectiveness is determined by, but not limited to—

- External support (financial, physical, moral, propaganda). Often threats/*adversaries* are interconnected to other transnational groups, organizations, or governments. Irregular threats/*adversaries* may be dependent on this external support. External support can noticeably increase the significance of irregular threats/*adversaries*. They can establish financial resources (cash, commodities, services of value legally or illegally) to fund operations. The intended use of these resources lends those funds greater significance than their inherent value.

- Fear and intimidation. Threats/*adversaries* use attacks on civilians or elements of the civilian population (murder, kidnapping, extortion) and attacks on U.S. forces and host-nation governmental or political organizations, businesses, civil, critical infrastructures, and security organizations. Irregular threats/*adversaries* also use the threat/*adversary* of ambushes, improvised explosive devices (IEDs), raids, sabotage, terror, and violence. Without a stable environment, the power of intimidation on the local population is significant.

- Political change. Threats/*adversaries* act as a political entity in a vacuum and claim to be able to fix real or perceived political issues. Irregular threats/*adversaries* use persuasion and coercion to reinforce their political means. They conduct propaganda activities to target the population and international public opinion. These activities may enhance the threat's/*adversary*'s legitimacy and undermine that of the host nation.

- Popular support. Threats/*adversaries* use coerced or uncoerced cooperation of the general population. Armed groups involved in insurgent operations directed against the host-nation government draw their strength from the population or at least a segment of the population. These groups establish sanctuary locations among segments of the population and utilize civilian transportation, communications, financial services, and general services to sustain operations. They receive funding by winning the approval of segments of the population or by extorting and utilizing segments of the population to provide indications and warnings of U.S. operations.

Hybrid Threat/*Adversary* Forces

5-48. Determining the combat effectiveness for hybrid threat/*adversary* forces is made by considering the tangible and intangible factors associated with determining the combat effectiveness for regular and irregular threat/*adversary* forces.

DOCTRINE AND TACTICS

5-49. Doctrine and tactics include tactical doctrine as well as tactics employed by specific units. While tactical doctrine refers to the enemy's accepted organization and employment principles, tactics refer to the threat/*adversary* force's conduct of operations. Based on knowledge of a threat's/*adversary's* tactical doctrine, the intelligence staff can determine how the threat/*adversary* force may employ its forces in the offense and defense under various conditions. Analysts integrate tactics in threat/*adversary* templates and other intelligence products. *Identify the adversary force's possible actions (defend, reinforce, attack, withdraw, delay [DRAW-D]).*

Regular Threat/*Adversary* Forces

5-50. Doctrine and tactics for regular threat/*adversary* force refer to the TTP that guide threat/*adversary* force operations. Understanding how the threat/*adversary* force prefers to operate aids the commander's understanding of potential threat/*adversary* COAs. TTP for regular threat/*adversary* forces can generally be grouped in the following categories:

- Offensive tasks.
- Movement to contact.
- Attack.
- Exploitation.
- Pursuit.
- Defensive tasks.
- Area defense.
- Mobile defense.
- Retrograde.

Irregular Threat/*Adversary* Forces

5-51. Tactics and operations for irregular forces include strategy, methods of procedure, and doctrine. Each refers to the threat/*adversary* force's accepted principles of organization and employment of forces. Tactics also involve political, military, psychological, and economic considerations. Irregular force tactics and operations vary in sophistication according to the level of training the individual or organization has received. Irregular forces carefully plan and train for individual and small-group operations. (See FM 3-24/*MCWP 3-33.5* for more information on potential irregular force tactics and operations.)

Hybrid Threat/*Adversary* Forces

5-52. Threats/*adversaries* to the U.S. and its allies employ hybrid forces as part of a sophisticated, comprehensive, and multidimensional strategy to achieve specific goals and objectives. The doctrine and tactics that guide hybrid forces are similar to Army/*Marine Corps* doctrine and tactics in that strategic, operational, and tactical action are coordinated to achieve objectives and end state.

5-53. Hybrid force doctrine is based on countering a threat's/*adversary*'s capabilities. Hybrid forces often study U.S. and allied military forces and their operations and conduct lessons learned based on their assessments and perceptions.

5-54. Hybrid forces use nations that they see as threats*/adversaries* as baselines for planning adaptive approaches for dealing with the strengths and weaknesses of their forces. These forces use the following principles for applying their various instruments of diplomatic political, informational, economic, and military power:

- Access limitation.
- Control tempo.
- Cause politically unacceptable casualties.
- Neutralize technological overmatch.
- *Conduct information operations aimed at local population, international opinion, and their adversaries' domestic population.*
- Change the nature of conflict.
- Allow no sanctuary.
- Employ operational exclusion.
- Employ operational shielding.
- Avoid defeat.

SUPPORT AND RELATIONSHIPS

5-55. The threat*/adversary* force's adoption of a COA should depend on the ability of its support system to support that action. However, depending on the threat*/adversary* force's objectives, possible time constraints, and/or willingness to assume risk—especially as dictated by political leaders or dynamics of political-military circumstances—this could substantially alter adoption of a COA. With knowledge of these factors, analysts can better evaluate the threat*/adversary* force capabilities, strength, and combat effectiveness.

Regular Threat/*Adversary* Forces

5-56. The location of a regular threat*/adversary* force's logistical support structure elements aids intelligence staffs in determining the disposition of maneuver formations. Logistic information critical for effective intelligence analysis includes—

- Classes and types of supply.
- LOCs.
- Logistical requirements.
- Procurement methods.
- Distribution priorities and procedures.
- Transportation networks and modes.
- Installations and terminals.
- Damaged equipment evacuation and salvage procedures.
- Maintenance.

Irregular Threat/*Adversary* Forces

5-57. The effectiveness of unconventional warfare depends heavily on support and relationships. This dependency fluctuates horizontally and vertically between the various groups and levels of operation. The intensity of support activity is based on operations. Critical components of support include, but are not limited to—

- Financing.
- Food.
- Water.
- Weapons and ammunition.
- Bombmaking components.
- Military information support operations materials (paper, ink, printing press).
- Medical.
- Transportation.
- Support of the population.

Hybrid Threat/*Adversary* Forces

5-58. Hybrid forces will incorporate the types of support irregular forces use to sustain themselves with the traditional logistical support associated with conventional military operations.

5-59. Because a hybrid force is a composite of many different groups, these groups will often have no standard, readily identifiable organizational relationship. What brings together the capabilities and intent of the components of the hybrid threat/*adversary* is a common purpose, typically opposition to U.S. goals. This unity of purpose can even bring together groups that normally would be fighting among themselves.

5-60. Affiliated organizations are cooperating toward a common goal despite having no formal command or organizational relationship. Affiliated organizations are typically nonmilitary or paramilitary groups, such as criminal cartels, insurgencies, terrorist cells, or mercenaries.

5-61. Affiliated forces are those irregular forces operating in a military unit's AO that the unit may be able to sufficiently influence to act in concert with it for a limited time. No "command relationship" exists between an affiliated organization and the unit in whose AO it operates. In some cases, affiliated forces may receive support from the military unit as part of the agreement under which they cooperate.

ELECTRONIC TECHNICAL DATA

5-62. Electronic technical data derived from targeting and electronic warfare are required to conduct electronic warfare. For U.S. Army, it is also derived from cyber electromagnetic activities. This data includes communications and noncommunications equipment parameters, such as emitter type and nomenclature, modulation, multiplex capability, pulse duration, pulse repetition frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. This information can be developed into an overlay. In order to produce the overlay, signal intelligence personnel require the assistance and input of the targeting and electronic warfare staff. (For U.S. Army, they also obtain assistance from the cyber electromagnetic activities element.)

Regular Threat/*Adversary* Forces

5-63. For regular threat/*adversary* forces, this data also includes critical threat/*adversary* communications nodes such as command posts and logistical control points. This information supports threat/*adversary* templating. With electronic technical data, a more accurate evaluation of the enemy's vulnerability to electronic countermeasures and deception is made; signals intercept and direction finding for the production of signals intelligence is made easier; and support is given to counter threat electronic warfare by assessing the threat's/*adversary's* electronic warfare capabilities.

Irregular Threat/*Adversary* Forces

5-64. When combating irregular threat/*adversary* forces, the lack of an obvious formal organizational structure or architecture impedes development of an extensive threat/*adversary* communications network diagrams and electronic technical database. The insurgent has communications equipment available ranging from the most modern to the most primitive. Insurgent forces can use high frequency, short-wave, ham radio and Citizen band sets; cellular phones, satellite phones, the Internet, mail, and couriers. While not playing a significant historical role, the insurgent's potential use of radar cannot be ruled out.

Hybrid Threat/*Adversary* Forces

5-65. Hybrid enemy forces will employ a combination of the capabilities used by regular and irregular forces as well as available commercial-off-the-shelf technology and existing civilian communications networks.

CAPABILITIES AND LIMITATIONS

5-66. Capabilities are the broad COAs and supporting operations that the enemy can take to achieve its goals and objectives. The following four tactical COAs are generally open to military forces in conventional operations: attack, defend, reinforce, retrograde/*DRAW-D.*

5-67. Each of these broad COAs can be divided into more specific COAs. An attack may be envelopment, penetration, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement. Other threat/*adversary* force capabilities include support to broad COAs or specific types of operations, including—

- Deception operations.
- Military information support operations.
- Intelligence operations.
- CBRN employment.
- Espionage, sabotage, subversion, and terrorist operations.

5-68. Threat/*adversary* capabilities take the form of statements, such as—

- The threat/*adversary* has the ability to insert up to two infantry battalions in a single lift operation.
- The threat/*adversary* can establish a prepared defense by 14 May.
- The demonstrators can effectively block traffic at up to seven intersections in the AO.

5-69. When identifying threat/*adversary* capabilities, intelligence staffs—

- Start with developed threat/*adversary* models.
- Consider the threat/*adversary* ability to conduct each operation based on all factors related to the current situation. (The enemy may be under-strength in equipment or personnel, short of logistic support, lacking air support, or the enemy's troops may be inexperienced or poorly trained.)

Regular Threat/*Adversary* Forces

5-70. A regular threat/*adversary* force is designed to attack or defend as necessary to accomplish objectives. Determining capabilities and limitations for a regular threat/*adversary* force requires an understanding of the art and science of war, as well as an understanding of the threat/*adversary* force itself.

Irregular Threat/*Adversary* Forces

5-71. The most challenging capability of an irregular threat/*adversary* is its ability to blend in with the population or to hide in complex terrain. This allows the threat/*adversary* to plan and prepare for an operation and attack at a time and place of its own choosing without interference from friendly forces.

Hybrid Theat/*Adversary* Forces

5-72. From a friendly perspective, the most challenging capability of a hybrid force is its ability to adapt and transition. The hybrid force emphasizes speed, agility, versatility, and changeability as the keys to success in a fight against a larger, more powerful opponent.

Adaptation

5-73. Adaptation, broadly defined, is the ability to adjust behaviors based on learning. Adaptation is closely linked to the operational environment and its variables. Threat/a*dversary* forces approach adaptation from two perspectives: natural and directed.

- **Natural** adaptation occurs as an actor (nation-state or non-state) acquires or refines its ability to apply its political, economic, military, or informational power. Natural adaptation can be advanced through acquisition of technology, key capabilities, or resources (financial and material), effective organization, effective use of the information environment, or even key regional or global alliances.
- **Directed** adaptation refers to adaptation, based specifically on lessons learned, to counter U.S. power and influence. Counters to U.S. actions will be ever-changing and likely conducted by a hybrid force. Hybrid forces will offer a mix of capabilities along the range of military operations to counter U.S. military actions. Adversaries will learn from U.S. operations what works and what needs refinement. They will be whatever the U.S. force is not. Like natural adaptation, directed adaptation will inform issues of force design, military strategy, and operational designs.

Transitions

5-74. One of the most dangerous aspects of a hybrid force is the ability of its components to transition in and out of various forms. Military forces, for example, can remove uniforms and insignia and other indicators of status and blend in with the local population. Insurgent forces might abandon weapons and protest innocence of wrongdoing. Criminals might impersonate local police forces in order to gain access to a key facility.

5-75. Hybrid forces will use the difficulties of positive identification of threat/*adversary* actors as threat/*adversary* actors to their advantage. Operational environments will be replete with many actors conducting activities counter to U.S. interests but without a clear visual signature as to their status as threats/*adversaries*. Indeed, often these actors will be providing signatures similar to friendly or neutral actors.

5-76. These concepts of conventional and unconventional warfare and traditional versus adaptive methods are weapons to a hybrid force. These concepts do not have meaning to hybrid forces beyond their ability to be used against their opponents. Hybrid forces see war holistically and do not try to break it up into convenient pieces. Hybrid forces will need to perform certain functions in order for them to succeed. Some functions at some points will best be performed by uniformed military forces. At other times or for other reasons, some functions will be best performed by irregular forces. At some points, both types of forces will be acting together. At others, they will shift between the status of regular and irregular. They may also use deception to shift between combatant and noncombatant status. Hybrid forces will present themselves in many ways but maintain the ability to aggregate at the time and place of their choosing.

CURRENT OPERATIONS

5-77. Current operations are those operations in which an enemy force is currently engaged. This includes operations against U.S. military forces or interests or against the military forces or interests of other nation-states. Analyzing current operations provides up-to-date information on all other threat/*adversary* characteristics.

Regular Threat/*Adversary* Forces

5-78. The Army's/*Marine Corps'* knowledge of regular threat/*adversary* forces is based on its understanding of these forces prior to 11 September 2001 (hereinafter referred to as 9/11). These forces have evolved as the Army/*Marine Corps* has evolved. Intelligence staffs at all echelons continuously study these forces to gain a better understanding of them.

Irregular Threat/*Adversary* Forces

5-79. The Army/*Marine Corps* gained valuable experience in combating irregular forces during Operation Iraqi Freedom and Operation Enduring Freedom. Thus, the Army/*Marine Corps* has learned how diverse and adaptive these threats/*adversaries* can be. It is unlikely that the irregular threats/*adversaries* the Army/*Marine Corps* will face in the future will mirror those it fought in Iraq and Afghanistan. To gain the best understanding of the evolving nature of irregular threats/*adversaries* throughout the world, intelligence staffs analyze these threats/*adversaries* whenever and wherever they appear.

Hybrid Threat/*Adversary* Forces

5-80. Although the Army/*Marine Corps* believes the primary threat/*adversary* it will face in the future will come from hybrid threat/*adversary* forces, little is known about what the character of these threats/*adversaries* will be. Although the Army/*Marine Corps* has developed a hybrid threat/*adversary* force model to use in training combined arms teams, this model provides only limited value in preparing the intelligence staff in understanding this threat/*adversary*. This is because, like the previous contemporary operational environment threat/*adversary* model, it is a generic construct that does not reflect the threat characteristics/*adversary order of battle* of any particular real-world threat/*adversary*. Because of this, it is incumbent upon intelligence staffs at all levels to study these types of threats/*adversaries* wherever they are operating in order to continually increase understanding of this threat/*adversary* category. The intelligence staff also studies historical examples of hybrid threat/*adversary* operations.

HISTORICAL DATA

5-81. Compiling the history of any threat/*adversary* organization involves conducting the research necessary to gather all relevant information regarding the threat/*adversary* and producing the materials needed to communicate that information to the commander and staff. Information briefings and papers are the two most common methods used for this purpose. Both of these methods can be used to support intelligence training, officer professional development, and noncommissioned officer professional development. The history component of the threat/*adversary* data file includes the original sources of information used to compile information briefings and papers. These sources form part of the professional reading required by all of the unit's intelligence personnel.

Regular Threat/*Adversary* Forces

5-82. Regular threat/*adversary* forces develop attributes based on how it has been employed over time and on how it conducted itself during that employment. While not definitive, understanding a unit's lineage can provide insight into the extent a unit will go in order to accomplish its objectives. This also provides insight into what the unit will not do to accomplish its objectives.

Irregular Threat/*Adversary* Forces

5-83. Irregular threat/*adversary* forces also develop attributes based on how it has been employed over time and on how it conducted itself during that employment.

Hybrid Threat/*Adversary* Forces

5-84. The historical record of the operations and activities of hybrid threats/*adversaries* will be one of the results of the analysis of current operations. However, history does provide examples of threat/*adversary* forces using hybrid approaches against a superior force.

Historical Examples of Hybrid Approaches

- 1754 to 1763—Regular British and French forces fought each other amidst irregular Colonialists fighting for the British and American Indians fighting for both sides.
- 1814—Peninsular War ended after the combination of regular and irregular multinational forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- 1954 to 1976—Viet Cong and People's Army of Vietnam combined irregular and regular forces in fighting the French and U.S. forces. Viet Cong would organize into conventional and unconventional units.
- 2006—Hezbollah mixed conventional capabilities (such as anti-armor weapons, rockets, and command and control networks) with irregular tactics (including information operations, non-uniformed combatants, and civilian shielding). The result was a tactical stalemate and strategic setback for Israel.

MISCELLANEOUS DATA

5-85. Intelligence staffs use supporting information to develop threat/*adversary* force characteristics and to construct comprehensive intelligence estimates. This information includes biographic data, personalities, and biometric data, as well as other information important to mission accomplishment. Biographic data contains information on characteristics and attributes of a threat/*adversary* force's members. Knowledge of personalities is important in identifying units and, in some cases, predicting a unit's COA. Personality data is valuable because the tactics and combat efficiency of particular units are closely tied to the commander's character, schooling, and personality traits. In counterinsurgency operations, supporting data may include tribal, clan, or ethnic group traits and their effects on the combat capabilities or limitations of the threat/*adversary* force, as well as biometric data.

5-86. Operations in Iraq and Afghanistan have seen an extensive use of biometric and forensic collection to support counterinsurgency operations. This collection was used to establish the identity, affiliations, and authorizations of an individual, deny anonymity to the adversary, and protect friendly assets, facilities, and forces. Valuable intelligence can and has been gleaned from identity operations. Known as identity intelligence, it is the collection, analysis, protection, exploitation, and management of identity attributes and associated technologies and processes in order to locate, track, and maintain continuity on identities across multiple or disparate instances and/or incidents, or across space and time. Future conflicts will likely involve an adversary who will seek to blend into a civilian populace. Intelligence Marines should seek to deny anonymity to the adversary by directing focused biometric and forensic collections and incorporating identity intelligence into the IPB process.

Regular Threat/*Adversary* Forces

5-87. When evaluating regular forces, miscellaneous data includes biographic data on the commander's and other key leaders in the organization. When combined with the other threat/*adversary* characteristics, this information may provide insight on how an enemy commander may react in a particular situation or attempt to solve a particular problem.

Irregular Threat/*Adversary* Forces

5-88. When evaluating irregular threat/*adversary* forces, miscellaneous data includes information on personalities, culture, and internal organizational processes.

Personalities

5-89. Personality is an important factor, and sometimes it is critical especially when combating irregular forces. Analysts focus on leaders and other important individuals. Personality files help the analyst conduct this analysis. Personality files include, but are not limited to—
- Leaders (political, ideological, religious, military, other).
- Staff members.
- Spokespeople.
- Family members (immediate and extended).
- Previous experience and skill training in professional disciplines, trades, and specialties.
- Media manipulation personnel.
- Trainers.
- Code names and nicknames.

5-90. Analysts use these personality files to help conduct link analysis and build organizational diagrams to determine relationships between critical personalities and their associations to various groups or activities. When combating irregular forces, this task is often known as "network analysis." This thorough analysis is critical to help determine the roles and relationships of many different people and organizations and to assess their loyalties, political significance, and interests. It is important to remember that any relationship or organization can span across illegal, terrorist, and other threat/*adversary* as well as legitimate people, money, and activities.

Culture

5-91. Culture is the ideology of a people or region and defines a people's way of life. A people's culture is reflected in daily manners and customs. Culture outlines the existing systems of practical ethics, defines what constitutes good and evil, articulates the structures and disciplines that direct daily life, and provides direction to establish patterns of thinking and behavior. Cultural issues include, but are not limited to, the following:
- Religion—beliefs, customs, and protocols.
- Political and economic beliefs—ideology and work ethic.
- Tribe—family allegiances and loyalties; family economic interests; and matriarchies versus patriarchies.

- Clan—caste, class, social group, standing, status, hierarchies.
- Ethnicity—race, nationality (for example, Arab, Bedouin, and Turkic; Kurd and Armenian; Tibetan, Korean, Mongolian, and Chinese).
- Regional affiliations—internal to a nation and those that extend past national borders.
- Military attitudes—order, weapons, honor.
- Law and justice—one system of law or multiple systems; property rights; and correction versus punishment.

Internal Organizational Processes

5-92. An organization's flexibility or rigidity is a key determinant as to its strengths and vulnerabilities. This flexibility or rigidity can be accurately estimated by answering several questions:

- Are achievers viewed as potential competitors, or as important organizational contributors? Is the attitude consistent throughout the organization?
- How do organizations replace leader and cadre casualties? What are the primary factors that determine how these replacements are selected?
- Rewards and punishments: what are they and are they consistently applied?
- Are internal rivalries complex, or does organizational discipline have primacy?
- How are policies adjusted and adjudicated: gunfights or dialogue?
- What are potential divisions and policy fractures?
- Which leaders support specific positions, and why?
- Are leader motivations organizational, family, or personal?

Hybrid Threat/*Adversary* Forces

5-93. The miscellaneous data associated with hybrid threat characteristics/*adversary order of battle* are a combination of that required for regular and irregular forces.

CREATE OR REFINE THREAT/*ADVERSARY* MODELS

5-94. Threat/*adversary* models accurately portray how threat/*adversary* forces normally execute operations and how they have reacted to similar situations in the past. This also includes knowledge of threat/*adversary* capabilities based on the current situation. Threat/*adversary* models are initially created by analyzing information contained in various databases. Some threat/*adversary* models are created and developed by higher agencies and organizations; but in immature operational environments or when a new threat/*adversary* emerges, analysts have to develop threat/*adversary* models.

5-95. A threat/*adversary* model is a three-part analytical work aid designed to assist in the development of situation templates during step 4 of the IPB process. Threat/*adversary* models consist of three parts:

- Convert threat/*adversary* doctrine or patterns of operation to graphics.
- Describe the threat's/*adversary*'s tactics and options.
- Identify HVTs.

CONVERT THREAT/*ADVERSARY* DOCTRINE OR PATTERNS OF OPERATION TO GRAPHICS

5-96. Threat/a*dversary* templates graphically portray how the threat/*adversary* might utilize its capabilities to perform the functions required to accomplish its objectives. Threat/a*dversary* templates are scaled to depict the threat's/*adversary*'s disposition and actions for a particular type of operation (for example, offense, defense, insurgent ambush, or terrorist kidnapping operation). When possible, templates should be depicted graphically as an overlay, on a supporting system or through some other means. Threat/a*dversary* templates are tailored to the needs of the unit or staff creating them. They may depict, but are not limited to, unit frontages, unit depths, boundaries, engagement areas, and obstacles.

5-97. The analyst constructs threat/*adversary* templates through an analysis of the intelligence database and an evaluation of the threat's/*adversary*'s past operations. The analyst also determines how the

threat/*adversary* normally organizes for combat and how threats*/adversaries* deploy and employ their forces and assets. In addition, the analyst looks for patterns in how the threats*/adversaries* organize their forces, timing, distances, relative locations, groupings, or use of the terrain and weather.

5-98. Templating requires continuous refinement to accurately portray threat/*adversary* patterns and practices. For example, while there may be no threat/*adversary* template for emplacement of kidnapping cells or money-laundering activities, evaluating the database can indicate specific patterns of kidnapping and money laundering. Because the implementation time is a consistent planning factor, an analyst can use the implementation time evaluation to determine the likelihood of location or participants.

5-99. Threat/a*dversary* templates are tailored to the needs of the unit or staff section creating them. A G-2 section's threat/*adversary* template will differ in scope from the template created by a brigade/*unit* S-2 section. Some threat/*adversary* templates consider the threat/*adversary* forces as a whole, while others focus on a single warfighting function, such as intelligence or fire support, while other products depict pattern analysis, time event charts, and association matrices.

DESCRIBE THE THREAT'S/*ADVERSARY*'S TACTICS AND OPTIONS

5-100. The threat/*adversary* model includes a description of the threat's/*adversary*'s preferred tactics. A description is still needed even if the threat/*adversary* has preferred tactics are depicted in a graphic form. The description—

- Lists the options available to the threat/*adversary* should the operation fail or succeed.
- Prevents the threat/*adversary* model from becoming more than a "snapshot in time" of the operation being depicted.
- Aids in mentally wargaming the operation over its duration and during the development of threat/*adversary* COAs and situation templates.
- Addresses typical timelines and phases of operation, points where unit's transition from one form of maneuver to the next and how each warfighting function contributes to the success of the operation.

5-101. The analyst describes the actions of the supporting warfighting function in enough detail to allow for identification and development of HVTs. The analyst also examines each phase separately because target values may change from phase to phase.

5-102. The analyst describes and makes a determination of what goal or goals the threat/*adversary* is trying to achieve. Threat/*adversary* objectives are often, but not always, what the unit's mission is trying to prevent; they are often actions taken by the threat/*adversary* to prevent unit mission accomplishment. Threat/*adversary* objectives will be specific to the type of threat/*adversary*, the AO, the unit's composition and mission, and other factors. The analyst also describes the threat/*adversary* objective in terms of purpose and end state. A number of different functions must be executed each time a threat/*adversary* force attempts to accomplish a mission.

IDENTIFY HIGH-VALUE TARGETS

5-103. The following techniques may be useful in identifying and evaluating HVTs:
- Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and SALUTE reports. A review of threat/*adversary* TTP and previous threat/*adversary* operations as well as understanding the threat's/*adversary*'s objective, tasks, purpose, and intent will be useful.
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat/*adversary* might react to the loss of each identified HVT. Consider the threat's/*adversary*'s ability to substitute other assets as well as adopt branches or sequels.

5-104. After identifying the set of HVTs, place them in order of their relative worth to the threat's/*adversary*'s operation and record them as part of the threat/*adversary* model. A HVTs value will vary over the course of an operation. Staffs should identify and annotate changes in value by phase of operations. The identification of HVTs assists the staff in the creation of HPTs.

5-105. HPTs can include various threat/*adversary* considerations that can be detrimental to the success of friendly missions. HPTs are incorporated into the scheme of fires, and are used in the creation of target selection standards and attack guidance matrices.

IDENTIFY THREAT/*ADVERSARY* CAPABILITIES

5-106. Threat/*adversary* capabilities are options and supporting operations that the threat/*adversary* can take to influence accomplishing friendly missions. The analysts define capabilities with the use of statements. The following are examples of capability statements:

- "The threat/*adversary* has the capability to attack with up to 8 divisions supported by 150 daily sorties of fixed-wing aircraft."
- "The criminal organization has the ability to pay off local law enforcement agencies."
- "The terrorists have the capability to send destructive viruses over the Internet, which can destroy computer files and archives."
- "The threat/*adversary* can establish a prepared defense by 14 May."
- "The terrorists have the capability of using CBRN weapons."
- "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/*adversary* has the ability to target friendly convoys along main supply routes using remotely detonated IEDs."

5-107. Other capabilities include support to COAs (attack, defend, reinforce, retrograde/*DRAW-D*) or specific types of operations, as well as operations that would allow the threat/*adversary* force to use a COA that would not normally be available or would be severely hindered if the supporting operation were not conducted. Examples of these types of operations include—

- Use of CBRN weapons.
- Intelligence collection.
- Electronic warfare operations.
- Use of air assets (fixed- and rotary-wing).
- Engineering operations.
- Air assault or airborne operations.
- Amphibious operations.
- River operations.
- Propaganda.
- 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.

5-108. When identifying threat/*adversary* capabilities and COAs, start with a full set of threat/*adversary* models and consider the threat's/*adversary*'s ability to conduct each operation based on the current situation and the threat's/*adversary*'s own METT-TC/*METT-T* conditions. Most situations will not present the threat/*adversary* with ideal conditions envisioned by their doctrine. As a result, the threat/*adversary*'s actual capabilities usually will not mirror the ideal capabilities represented by the complete set of threat/*adversary* models.

5-109. The threat/*adversary* could be under-strength in personnel and equipment, may be short of logistic support, or the 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 in order to conduct other operations elsewhere. The evaluation of the threat's/*adversary*'s logistics might indicate a critical shortage of explosives. Analysts should consider the following:

- Avoid limiting the threat/*adversary* models and capabilities strictly to the threat/*adversary*'s conventional forces. For example, student rioters during a noncombatant evacuation operation may be or may become a threat/*adversary* during the operation.
- Avoid overstating the threat/*adversary* model and threat/*adversary* capabilities. The proper use of findings and recommendations developed from threat/*adversary* assessments will in turn develop realistic threat/*adversary* models.
- During any discussion of the threat/*adversary*, cultural awareness is an important factor. By developing an awareness of the culture, friendly units can identify groups or individual members of the population that may be friendly, a threat/*adversary*, somewhere in between, or both.

THREAT/*ADVERSARY* TEMPLATE

5-110. As operations commence, it is imperative to develop foundationally sound and accurate threat/*adversary* models through careful analysis. The analyst analyzes a threat's/*adversary*'s capability, vulnerabilities, doctrinal principles, and preferred TTP. It is from the threat's/*adversary*'s doctrine, training practices, and observed patterns and activities that analysts construct threat/*adversary* templates.

5-111. A threat/*adversary* template is a graphic that depicts the time and distance of relationships of threat/*adversary* forces conducting a specific operation or activity. Depending on the mission variables, developing templates can be time intensive.

5-112. Threat/*adversary* templates show the deployment pattern and disposition preferred by the threat/*adversary* when not constrained by the effects of the operational environment. These templates are normally scaled depictions of threat/*adversary* dispositions for a particular operation. They include—

- The location of all enemy units two levels down. For example, an infantry battalion in the defense template would depict platoon and specialty team locations.
- The distance and/or time between enemy units.
- Graphic control measures associated with the operation (boundaries, routes, other).

5-113. Threat/*adversary* templates graphically portray how the threat/*adversary* prefers to utilize its capabilities to perform the functions required to accomplish its objectives. Threat/*adversary* templates are scaled to depict the threat's/*adversary*'s disposition and actions for a particular type of operation (for example, offense, defense, insurgent ambush, or terrorist kidnapping operation).

5-114. When possible, templates are depicted graphically as an overlay, on a supporting system, or through some other means. Threat/*adversary* templates are tailored to the needs of the unit or staff creating them. They may depict, but are not limited to—

- Unit frontages.
- Unit depths.
- Boundaries.
- Engagement areas.
- Obstacles.

5-115. Threat/*adversary* templates allow analysts and the staff to—

- Fuse all relevant combat information.
- Assist in identifying intelligence gaps.
- Predict threat/*adversary* activities and adapt COAs.
- Synchronize information collection.

5-116. An integrated attack is an offensive action where the threat/*adversary* seeks a military decision by destroying the enemy's will and/or ability to continue fighting through the application of combined arms effects. An integrated attack is often employed when the threat/*adversary* determines overmatch of the enemy and is able to mass all elements of offensive combat power for mission effects. It may also be employed against a more sophisticated and capable opponent if the appropriate advantage and/or opportunity is created or available. (See TC 7-100-2, paragraphs 3-63 to 3-74, for more information on integrated attacks.)

5-117. Integrated attacks are characterized by—

- Not being focused solely on destruction of ground combat power but often on enemy command and control and logistics.
- Fixing the majority of the enemy's force in place with the minimum force necessary.
- Isolating the targeted subcomponents of the enemy's combat system from the enemy's main combat power.
- Using complex terrain to force the enemy to fight at a disadvantage.
- Using deception to degrade the enemy's situational understanding and ability to target threat/*adversary* formations.
- Using flank attack and envelopment, particularly of enemy forces that have been fixed.

5-118. The threat/*adversary* prefers to conduct integrated attacks when most or all of the following conditions exist. The threat/*adversary*—

- Recognizes significant overmatch in combat power over enemy forces.
- Possesses at least air parity over the critical portions of the battlefield/*battlespace*.
- Operates sufficiently free of enemy standoff reconnaissance and attack systems to be able to operate without accepting high levels of risk.

5-119. An integrated attack employs various types of functional forces. The threat/*adversary*, when task-organized with significant combat capabilities, assigns subordinate units functional designations that correspond to their intended roles in the attack. Two types of forces are enabling forces and action forces.

5-120. The most common type of action force in an integrated attack is the exploitation force. Such a force is capable of penetrating or avoiding enemy defensive forces and attacking and destroying the enemy's support infrastructure. An exploitation force ideally possesses a combination of mobility, protection, and firepower that permits it to reach the target with sufficient combat power to accomplish the mission.

5-121. Enabling forces in an integrated attack are employed typically as fixing, assault, and/or support forces. A disruption force exists but is not created specifically for this type of offensive action.

- The fixing force in an integrated attack is required to prevent enemy defending forces, reserves, and quick-response forces from interfering with the actions of the assault and exploitation forces. One or more assault forces may be used in an integrated attack.
- The assault force in an integrated attack has mission tasks to destroy a particular part of the enemy force or seize key positions.
- A support force provides support to the attack with command and control functions, attack by fire effects, and other support/*combat support*, such as smoke; suppressive artillery and rocket fires; air-delivered weapons; combat engineer units; and/or sustainment/*combat service support* capabilities.

5-122. Figures 5-7 through 5-9 on pages 5-26 through 5-28 are examples of threat/*adversary* models.

5-123. Figure 5-7 is an example of a complex battle position for an insurgent organization threat/*adversary* model.

| CBP | constant battlefield picture | S | suspected or assumed hostile |
| INFOWAR | information warfare/*information operations* | | |
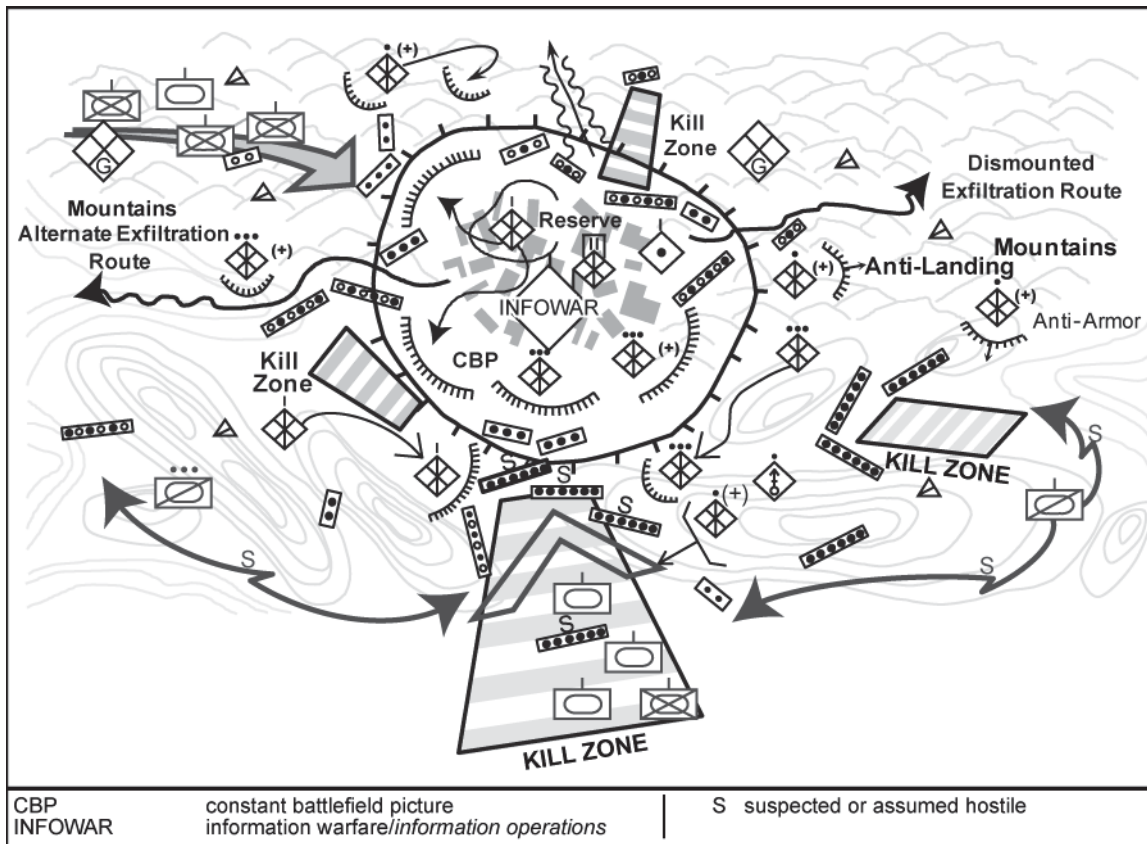
Figure 5-7. Example of a complex battle position: insurgent organization threat/*adversary* model

5-124. Figure 5-8 is an example of a threat/*adversary* template for counterinsurgency operations.
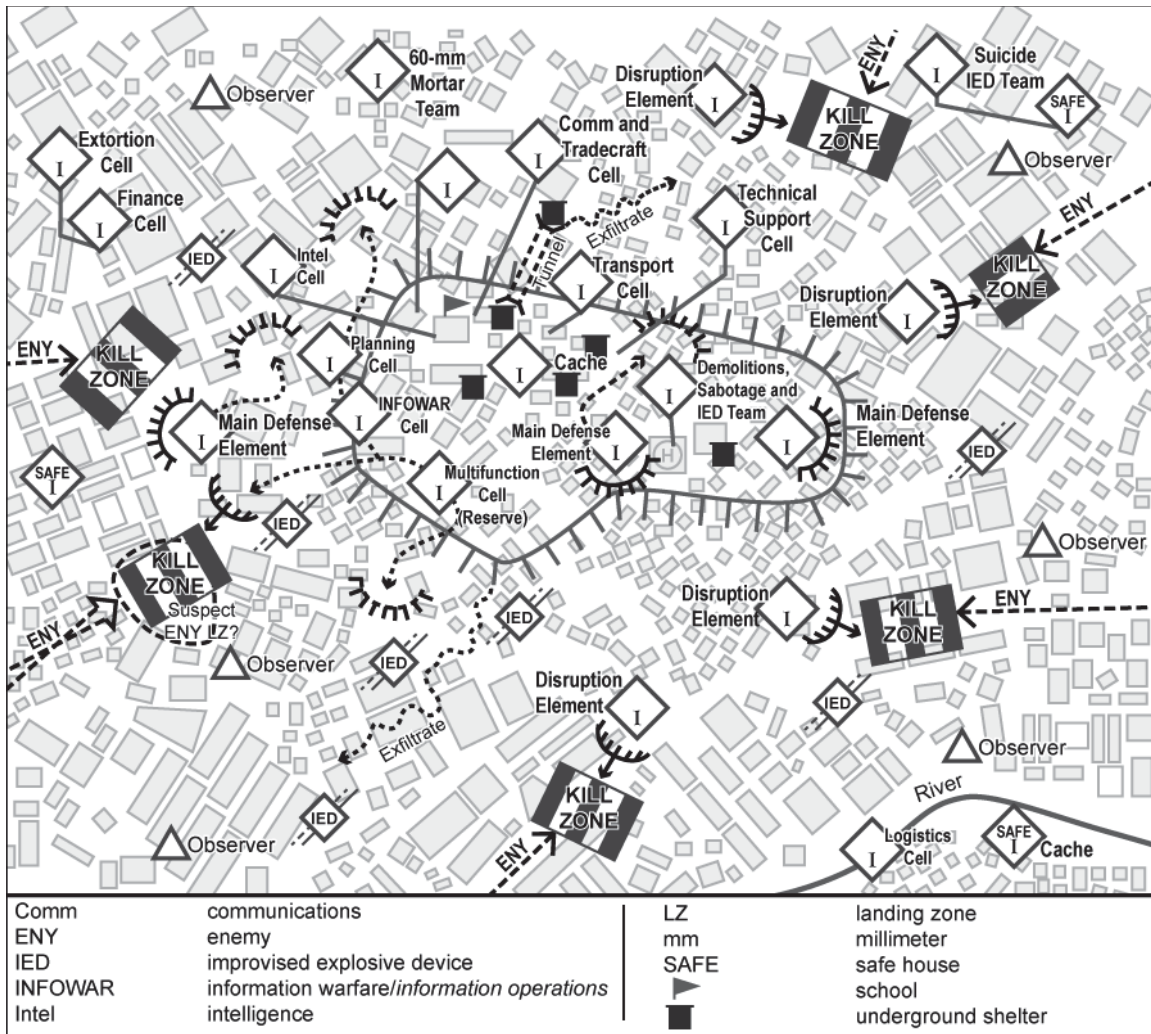
Figure 5-8. Example threat/*adversary* template (counterinsurgency)

5-125. In a threat/*adversary* template, the identification of immediate and subsequent objectives can be terrain-based or force-based. Objectives are more than likely areas deemed as key terrain by the threat/*adversary* commander based on operational timelines.

5-126. The irregular threat/*adversary* opposing friendly forces doctrinally prefers to conduct attacks consisting of—

- IED attacks (see figure 5-9 on page 5-28).
- Convoy ambushes.
- Complex attacks against fixed sites.
- Urban anti-armor ambushes.

5-127. Other attacks that the irregular threat/*adversary* opposing the brigade/*unit* may conduct are—

- Indirect fire attacks.
- Murders and kidnappings.
- Sniper attacks.
- Bombing (vehicle and suicide).
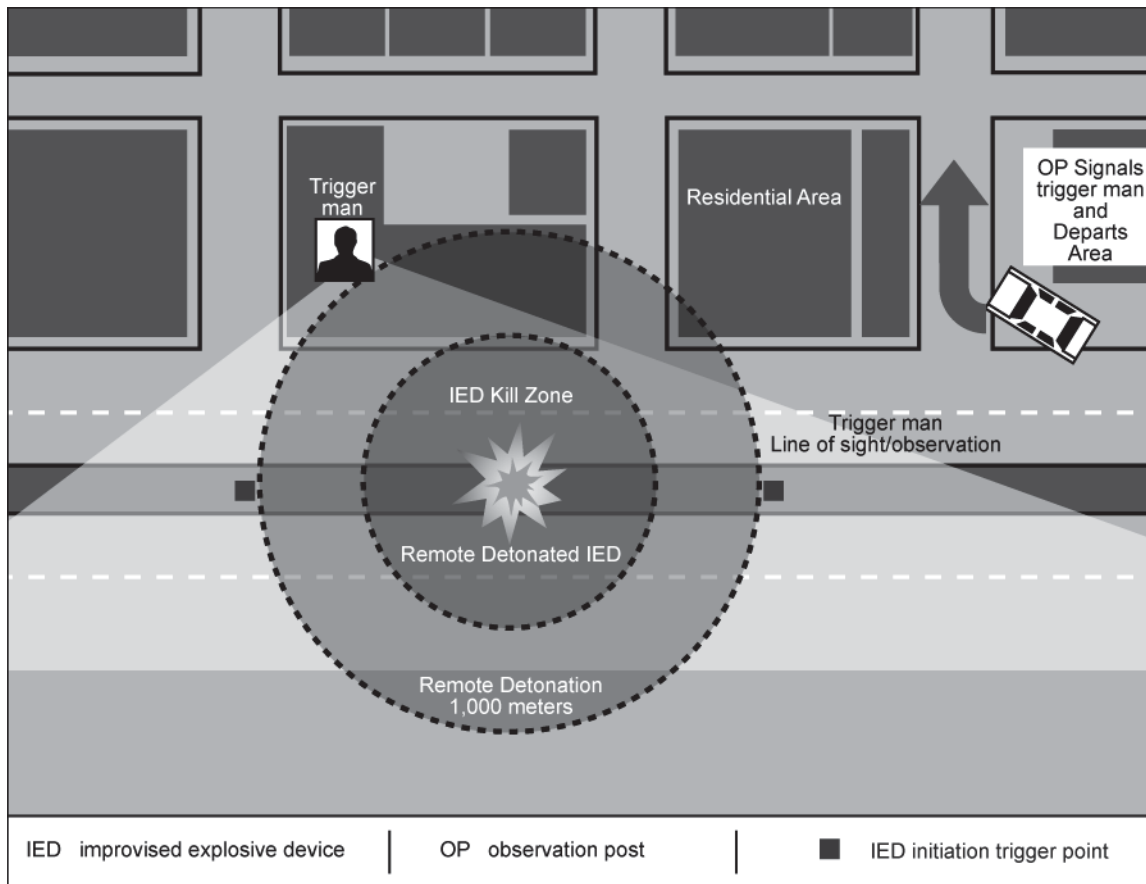
Figure 5-9. Event template (IED attack)

Threat/*Adversary* Capabilities Statement

5-128. Threat/*adversary* capabilities are the broad options the threat/*adversary* has to counter friendly operations and supporting operations the threat/*adversary* can take based on the conclusions made when determining threat characteristics/*adversary order of battle* at the beginning of step 3 of the IPB process. A threat/*adversary* capabilities statement is a narrative that identifies a particular action for which the threat/*adversary* has the capability to complete and the tactics the threat/*adversary* prefers to use to accomplish its objectives. It addresses operations of major units that will be portrayed on the threat/*adversary* template and the activities of each warfighting function. Figure 5-10 is an example of a threat/*adversary* capability statement that illustrates the capabilities of the 231st Brigade Tactical Group.
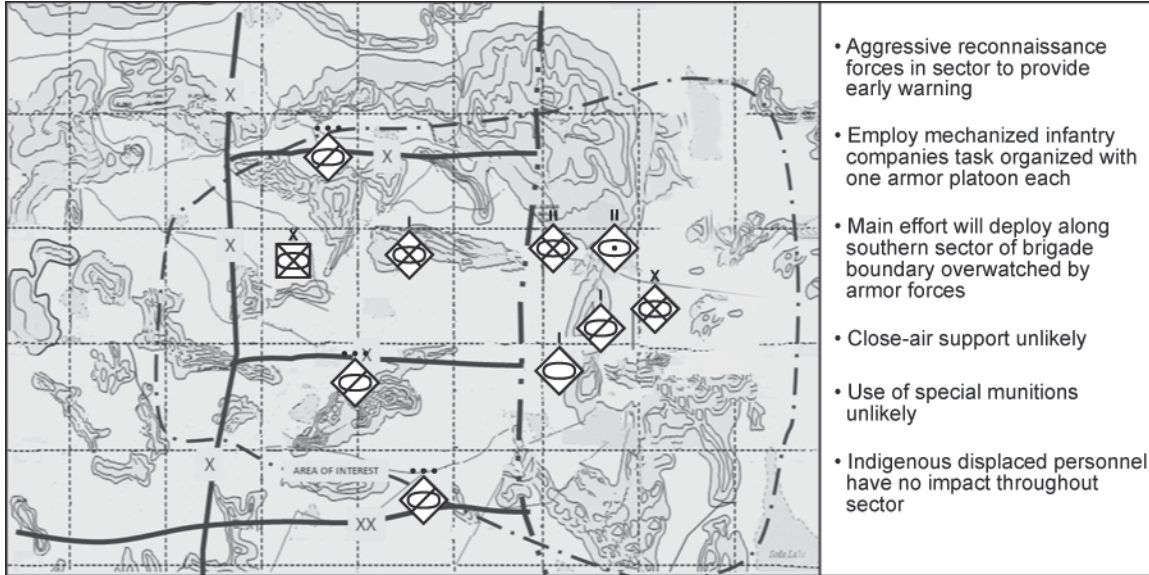
Figure 5-10. Example threat/*adversary* capability statement

HIGH-VALUE TARGET LIST

5-129.   The HVTs identified during step 3 of the IPB process are initially refined during step 4 of the IPB process, and are refined again during the COA analysis step of the MDMP/*COA wargaming step of MCPP*. This data is used to develop the HPTL that is continually refined during execution by targeting groups and boards.

5-130.   HVTs are determined based on analysis of the threat/*adversary* capabilities statement, an analysis of the threat/*adversary* template, and tactical judgment. Mentally wargaming and thinking through the threat/*adversary* operation is the quickest and most efficient method to determine HVTs at this point. Determining how the threat/*adversary* will employ its assets aids in determining the assets critical to the operation. For example, when mentally wargaming a threat/*adversary* air attack against friendly targets supported by a well-prepared air defense system, it is logical to conclude that the threat/*adversary* will need a substantial air defense suppression package as part of its operation to ensure the success of the attack. In this case, the artillery and air assets that form this suppression package are HVTs.

5-131.   In identifying and evaluating HVTs, it may be useful to—

- Identify HVTs from existing intelligence studies, evaluation of the databases, patrol debriefs, and SALUTE reports. A review of threat/*adversary* TTP and previous threat/*adversary* operations as well as understanding the threat's/*adversary*'s objective, tasks, purpose, and intent will be useful.
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat/*adversary* might react to the loss of each identified HVT. Consider the threat's/*adversary's* ability to substitute other assets as well as to adopt branches or sequels.

5-132.   After identifying the set of HVTs, place them in order of their relative worth to the threat/*adversary* operation and record them as part of the threat/*adversary* model. An HVT's value varies over the course of an operation. The staff should identify and annotate changes in value by the phase of operation. The following are additional considerations:

- Use all available intelligence sources (for example, patrol debriefs, SALUTE reports) to update and refine the threat/*adversary* models.
- Categorize the updates to reach a conclusion concerning the threat's/*adversary*'s operations, capabilities, and vulnerabilities.

5-133.   HPTs can include various threat/*adversary* considerations that can be detrimental to the success of friendly missions. During targeting, HVTs are identified and prioritized during the wargaming phase of

planning. In addition, it identifies the subset of HVTs that must be acquired and attacked for the friendly mission to succeed. HVTs may be nominated as HPTs when these targets can be successfully acquired, vulnerable to attacks, and such an attack supports the commander's scheme of maneuver.

5-134.   To ensure all HVTs are identified, the staff determines which assets are critical to the success of the threat's/*adversary*'s main and supporting efforts, as well as those critical to the success of possible threat/*adversary* branches and sequels. Determining how the threat/*adversary* will react to the loss of an asset and its ability to substitute other assets will also aid in this process. HVTs should be prioritized by their relative worth to the threat's/*adversary*'s operation. Target value analysis aids in prioritizing HVTs.

5-135.   *Marine Corps staffs conduct a center of gravity analysis based on the understanding gained through design and task analysis to identify or refine adversary and friendly centers of gravity and to determine which friendly and adversary weaknesses may become critical vulnerabilities. A critical vulnerability is some aspect of the center of gravity that is, or can be made, vulnerable to attack.*

TARGET-VALUE ANALYSIS

5-136.   The TVA is a process led by the fires cell as part of targeting that quantifies the relative value of HVTs with each other in relation to a particular enemy operation. (See FM 3-60 and FM 6-20-40 for more discussion on TVA.) This analysis is based in part on the conclusions the intelligence staff reaches as it evaluates threat characteristics/*adversary order of battle* during IPB. The IPB products required to support TVA are the threat/*adversary* template, the threat/*adversary* capabilities statement, and the HVTL. These products aid the fires cell and the rest of the staff in—

- Providing a focus for the commander's target acquisition effort.
- Identifying priorities for the engagement of enemy targets that will facilitate the success of the mission.
- Identifying effects criteria.

Note. While TVA is conducted initially during IPB, it is a separate process that is repeated throughout the operations process as part of targeting. To be effective, TVA depends on the most current intelligence related to the enemy. Initially based on the threat/*adversary* templates developed during step 3 of the IPB process, TVA should be refined based on the threat/*adversary* COAs developed during step 4 of the IPB process, and refined continually based on changes to the enemy situation overlay during operations. Whenever conducted, the intelligence staff supports TVA with the most up-to-date enemy-related intelligence it has.

5-137.   *For the Marine Corps, TVA is a method of identifying and ranking potential HVT sets in a COA. The target analyst, in coordination with the G-3/S-3, G-2/S-2, fire support coordinator, and other staff members, wargame the COAs to—*

- *Finalize individual staff estimates.*
- *Develop a fire support plan and a scheme of maneuver, as well as friendly and adversary decision support templates.*
- *Determine critical assets required by the adversary commander to accomplish the commander's mission.*

5-138.   See JP 3-60 for more information on TVA.

Chapter 6

Step 4 of the IPB Process—Determine Threat/*Adversary* Courses of Action

WHAT IS IT?

6-1. Step 4 of the IPB process identifies and describes threat/*adversary* COAs that can influence friendly operations. Example 1 is a classic vignette from *The Defence of Duffer's Drift*, by Sir Ernest Swinton, which illustrates the proper use of tactics, IPB, and the practical application of doctrine. Example 2 examines PMESII-PT/*PMESII* and ASCOPE from the threat's perspective.

Example 1

A Boer S-2 tells his commander: "Sir, the enemy platoon leader's likely objective is to retain control of the only crossing point suitable for wheeled traffic over the Silliasvogel River. He can defend the crossing, known as Duffer's Drift, with his 50 Soldiers in any one of the following ways:

- He can leave it undefended until tomorrow (being inexperienced and thinking that we will not arrive until the next day). He can dig his platoon into a small enclosure just on the other side of the drift. A variant of this COA would be for him to establish a trench line astride the main road.

- He can occupy and fortify the Kraal village that overlooks the drift.

- He can occupy the riverbed itself with only a small outpost in the Kraal village. This goes against every canon in British doctrine; however, we must consider this COA because it is so dangerous to the accomplishment of our mission.

The S-2 tells his commander: "Sir, I think the platoon leader will adopt one of these COAs, in order of probability as I gave them. We need to conduct reconnaissance of the riverbed and the Kraal in order to find out which of these COAs he has chosen."

Example 2

While evaluating the threat/*adversary*, another technique is to consider PMESII-PT/*PMESII* and ASCOPE through the perspective of the threat/*adversary* force. As the threat/*adversary* is evaluated, consider how PMESII-PT/*PMESII* and ASCOPE will impact how the enemy will operate. Also, while evaluating the threat/*adversary*, consider how the friendly actions may impact enemy operations and enemy COAs.

DESIRED END STATE

6-2.   The desired end state of step 4 of the IPB process is the development of graphic overlays (enemy situation templates) and narratives (enemy COA statements) for each possible enemy COA that has been identified. The staff uses these products during the friendly COA development and friendly COA analysis steps of MDMP/*COA wargaming step of MCPP*:

- Replicate the set of COAs that the enemy commander and staff are considering.
- Identify all COAs that will influence the friendly command's mission.
- Identify those areas and activities that, when observed, will discern which COA the enemy commander has chosen. The primary outputs associated with step 4 may include—
  - Representing the enemy action or enemy COAs with associated COA statements and HVTLs.
  - Developing an event template and associated event matrix.
  - Determining the HVTL and providing input to HPTs and the HPTL.
  - Providing input into the collection plan.
  - Updating the intelligence estimate.
  - Providing input into PIRs.
  - Providing input into OPORDs and/or OPLANs (annexes and/or appendixes).

SO WHAT?

6-3.   The "so what" in this step is determining the enemy COAs necessary to aid the development of friendly COAs.

- Success results in the friendly commander will avoid being surprised with an unanticipated enemy action, thus quickly narrowing the set of possible threat/*adversary* COAs to the one the enemy has chosen.
- Consequences of failure:
  - Failure to identify which of the possible COAs the enemy has chosen, leading to surprise of the friendly command.
  - The enemy commander may have the information needed to exploit the opportunities the operational environment provides in a way the friendly commander did not anticipate.

HOW TO DO IT: (THE PROCESS)

6-4.   Determining threat/*adversary* COAs is a two-step process consisting of the actions discussed below and shown in figure 6-1:

- Develop threat/*adversary* COAs.
- Develop the event template and matrix.
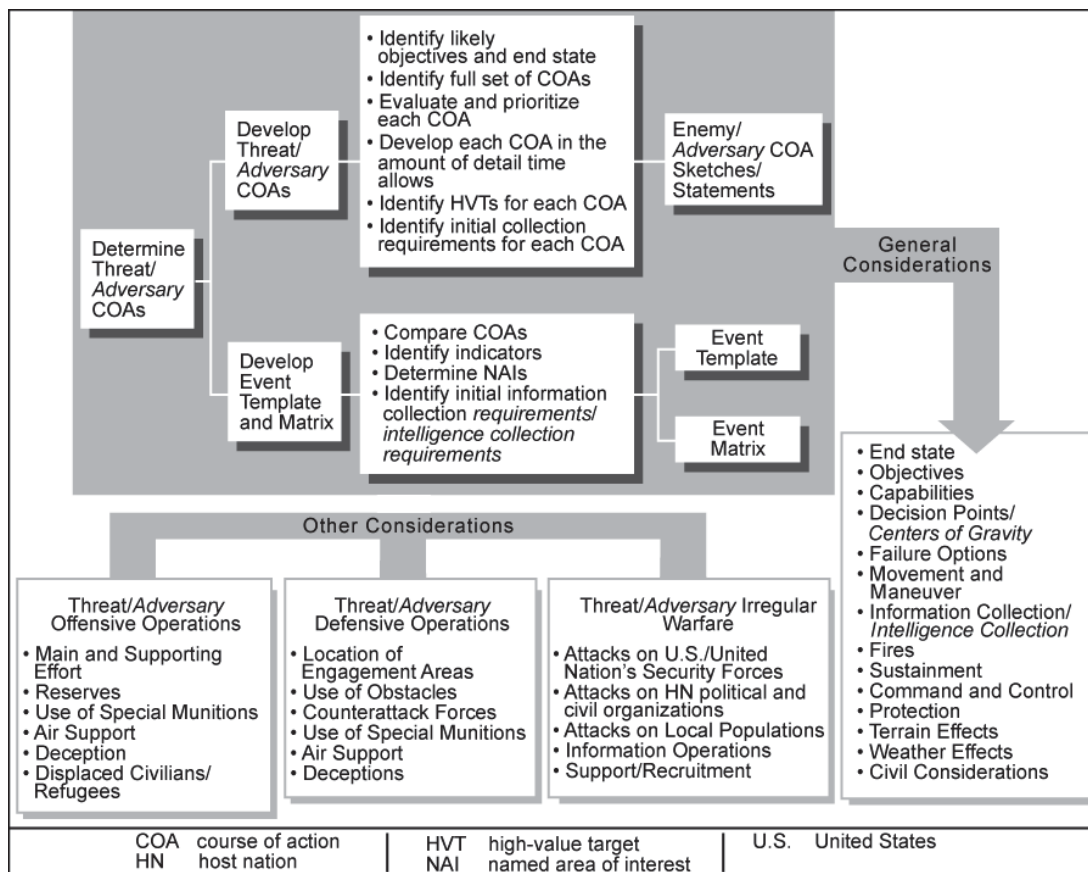
Figure 6-1. Determine threat/*adversary* COAs

DEVELOP THREAT/*ADVERSARY* COURSES OF ACTION

6-5.   Threat/*adversary* COA development is a six-step process that requires an understanding of the threat characteristics/*adversary order of battle* discussed in chapter 5, and the effects of terrain, weather, and civil considerations on operations discussed in chapter 4. Population effects to operations will be clearly annotated with full details so that during the wargame the population and the effects and threat/*adversary* actions will be portrayed during the wargame. The most important element in determining enemy COAs is in understanding enemy operational art and tactics. As mentioned in chapter 5, there are three types of threat/*adversary* forces that U.S. forces may encounter: regular, irregular, and hybrid. The process to determine COAs these forces may employ is identical, mirrors friendly COA development, and consists of the following:

- Identify likely objectives and end state.
- Identify the full set of COAs available to the threat/*adversary*.
- Evaluate and prioritize each threat/*adversary* COA.
- Develop each COA in the amount of detail time allows.
- Identify HVTs for each COA.
- Identify initial collection requirements for each COA.

6-6.   In order to plan for all possible contingencies, the commander understands all COAs a threat/*adversary* commander can use to accomplish his objectives. To aid in this understanding, the staff determines all valid threat/*adversary* COAs and prioritizes them from most to least likely. The staff also determines which threat/*adversary* COA action is the most dangerous to friendly forces. To be valid, threat/*adversary* COAs should be feasible, acceptable, suitable, distinguishable, and complete—the same criteria used to validate friendly COAs.

6-7.   When determining COAs for regular and hybrid threats/*adversaries* where the threat/*adversary* operates under the command and control of a unified command structure, the staff will develop COAs focused on the objectives and end state of that command structure. However, when faced with multiples threats/*adversaries* with varied and competing objectives, such as those encountered during stability tasks, the staff will have to develop COAs for each of these threats/*adversaries*.

6-8.   Threat/*adversary* COAs are developed in the same manner as friendly COAs. When developing a threat/*adversary* COA, the intelligence staff accounts for all relevant enemy activity; this includes all possible branches and sequels the threat/*adversary* commander may adopt. (See ADRP 5-0/*MCWP 5-1* for further discussion of the development of friendly COAs.) Intelligence staffs can use this same methodology when developing threat/*adversary* COAs.

IDENTIFY LIKELY OBJECTIVES AND END STATE

6-9.   Based on the results of analysis of mission variables conducted earlier in the IPB process, the staff now identifies the enemy's likely immediate and subsequent objectives and desired end state. These elements are included in the threat/*adversary* COA statement developed for each COA.

6-10.   An objective is a clearly defined, decisive, and attainable goal toward which every operation is directed. The end state is a set of required conditions that define achievement of the commander's objectives. Enemy objectives are normally terrain or force oriented. For example, an enemy may attack to destroy a friendly force or to seize key terrain; defend to delay a friendly force or retain control of key terrain; or conduct guerrilla operations to disrupt friendly operations.

6-11.   The end state is the desired conditions that, if achieved, meet the conditions of policy, orders, guidance, and directives issued by the commander. For example, the end state for an attack to destroy may be the destruction of all friendly forces down to platoon level and friendly forces incapable of conducting a coordinated defense.

6-12.   For regular forces, objectives can be either terrain or force oriented, and the end state is usually based on effect and time. For example, the objective of a lead echelon infantry brigade/*unit* performing an attack may be to neutralize defending forces. The brigade's/*unit's* end state may be to prevent defending forces from affecting the movement of second echelon forces. Additionally, the brigade's/*unit's* operations are synchronized in time with higher headquarters operations to ensure combat power is applied where and when needed to ensure success.

6-13.   For irregular forces, while the end state remains based on effect, objectives are not always linear or time-based. Often, the objectives for irregular forces are driven by event rather than time. For example, the objective of an extremist group may be to prevent U.S. forces from providing security to the general population by increasing the amount of time spent on resources. The group's end state may be to convince the population to rely on security provided by the extremist group rather than U.S. forces. In this case, the group's operations are synchronized with the operations of U.S. forces attacking patrols, convoys, combat outposts, and security forces.

IDENTIFY THE FULL SET OF COAs AVAILABLE TO THE THREAT/*ADVERSARY*

6-14.   A regular force has two primary types of operations it can conduct: attack or defend. Based on its objectives, the enemy must select one of these options. Once selected, the threat/*adversary* generally has multiple options to consider when developing its plan.

6-15.   An irregular force can conduct an attack or defend on a small scale, for short periods, or in complex terrain, but it is difficult to sustain these types of operations without degradation to their effectiveness and their operations. The primary types of operations irregular forces can conduct are activities associated with insurgent or guerilla operations, raids, ambushes, sabotage, and acts of terror.

6-16.   A hybrid force can combine the capabilities of regular and irregular forces to engage U.S. forces from all points in order to overwhelm U.S. capabilities.

6-17.   Regardless of the type of force and the type of operation being conducted, enemy forces may plan operations based on **task, purpose, method,** and **end state**. Activities within its operations are planned to support that task and purpose. The staff identifies the tasks, purpose, and end state for each COA developed. By

identifying these for each COA, the intelligence staff will be better able to determine the chosen threat/*adversary* COA during the conduct of operations. Regardless of the type of force, when developing a threat/*adversary* COA, the staff determines—

- Current enemy situation.
- Mission (includes **task** and **purpose**).
- Enemy/*adversary* objectives, **methods**, and end state.
- Commander's intent, purpose, and **end state**.
- Task organization.
- Capabilities.
- Vulnerabilities.
- HVTs.
- Decision points (essential in determining branches and sequels).
- Decisive point/*center of gravity* (source of strength, power, and resistance).
- Failure options.
- Branches and sequels.
- Intent for—
    - Movement and maneuver.
    - Reconnaissance and surveillance.
    - Fire support.
    - Logistics.
    - Threat/*adversary* command and control.
    - Protection.
    - Information activities.
    - Denial and deception.
- How terrain and weather will affect threat/*adversary* operations. *For the Marine Corps, this includes a G-2/S-2 red cell analysis. In addition to enemy composition and disposition, METOC parameters are factored in to determine what, if any advantage or disadvantage weather conditions will have on the enemy forces, and how the enemy can use anticipated weather conditions to move against friendly forces.* (*See MCWP 5-1 for more information on red cell analysis.*)
- How civil considerations will affect threat/*adversary* operations.
- How displaced civilians and displaced persons will affect threat/*adversary* operations.
- How the presence and actions of U.S. forces will affect threat/*adversary* operations (reverse IPB).

6-18. In addition, for enemy offensive tasks, the staff focuses on determining—

- Main, supporting, and reinforcing efforts.
- Use of reserves.
- Use of special munitions.
- Use of air support.

6-19. In addition, for enemy defensive tasks, the staff focuses on determining—

- Location of engagement areas and obstacles.
- Location, type, and size of security zone forces.
- Location, type, and size of counterattack forces.
- Use of special munitions.
- Use of air support.

6-20. In addition, for irregular warfare, the staff generally considers—

- Guerilla and terror attacks on U.S. forces and host-nation governmental, civil, and security organizations.
- Guerilla and terror attacks on local populations.

6-21. Functional analysis graphically portrays how the threat/*adversary* might utilize its capabilities to perform the functions required to accomplish its objectives. Functional analysis depicts the threat's/*adversary*'s disposition and actions for a particular type of operation. When possible, the results of functional analysis are depicted graphically as an overlay, on a supporting intelligence system, or through some other means. (See appendix B for a discussion on functional analysis.)

6-22. Once the staff has identified all valid threat/*adversary* COAs, it compares each COA to the others and prioritizes them by number. For example, if four COAs have been developed, COA 1 is the enemy's most likely COA and COA 4 is the least likely. Additionally, the staff determines which COA is the most dangerous to U.S. forces. The most likely COA may also be the most dangerous. Additionally, a COA needs to answer six basic questions:

- Who—the organizational structure of the threat/*adversary* organization, including external organizations providing support.
- What—the type of operation: attack, defend, other.
- When—the earliest time the action can begin.
- Where—the battlefield/*battlespace* geometry that frames the COA (boundaries, objectives, routes, other).
- How—the threat/*adversary* will employ its assets to achieve its objectives.
- Why—the threat's/*adversary's* objectives.

EVALUATE AND PRIORITIZE EACH ENEMY/*ADVERSARY* COA

6-23. The commander approves a plan that is optimized to counter the most likely enemy COA, while allowing for contingency options should the threat/*adversary* choose another COA. Therefore, the staff evaluates each enemy COA and prioritizes it according to how likely it is that the threat/*adversary* adopts that option. Generally, threat/*adversary* forces are more likely to use a COA that offers the greatest advantage while minimizing risk. However, based on the situation and its objectives, the threat/*adversary* may choose to accept risk to achieve a desired end state. It is impossible to predict what COA the threat/*adversary* will choose. Therefore, the staff develops and prioritizes as many valid threat/*adversary* COAs as time allows but at a minimum develops the most likely and most dangerous COAs.

DEVELOP EACH COA IN THE AMOUNT OF DETAIL TIME ALLOWS

6-24. A threat/*adversary* COA consists of the following products:

- Situation template for the threat/*adversary* COA.
- Threat/*adversary* COA statement.
- HVTs and HVTL for the threat/*adversary* COA.

Situation Template for the Threat/*Adversary* COA

6-25. When constructing a situation template, the staff uses the threat/*adversary* template developed as part of the threat/*adversary* model during step 3 of the IPB process as a base. That template is modified based on the significant effects the operational environment will have on the threat/*adversary* COA. For example, an enemy may prefer to establish battle positions 1 to 1.5 kilometers apart. The terrain, however, may force the enemy to increase this distance in order to protect its flanks. Another example is, the enemy prefers to attack on high speed AAs but also prefers to avoid complex terrain. Therefore, the location of an urban area along a high speed, optimal AA may force the threat/*adversary* to use a suboptimal approach.

6-26. A threat/*adversary* situation template is a depiction of a potential threat/*adversary* COA as part of a particular threat/*adversary* operation. Situation templates are developed using the threat's/*adversary*'s current

situation, based on threat/*adversary* doctrine and the effects of terrain, weather, and civil considerations. Situation templates can be simple sketches, reserving in-depth development and analysis for later when more time is available.

6-27. A technique is to design a sketch to depict an enemy action or COA which is a graphic representation that will show key outputs or a graphic representation of an enemy action or enemy COA. Each enemy COA has a corresponding situation template. Figure 6-2 is an example of a situation template.
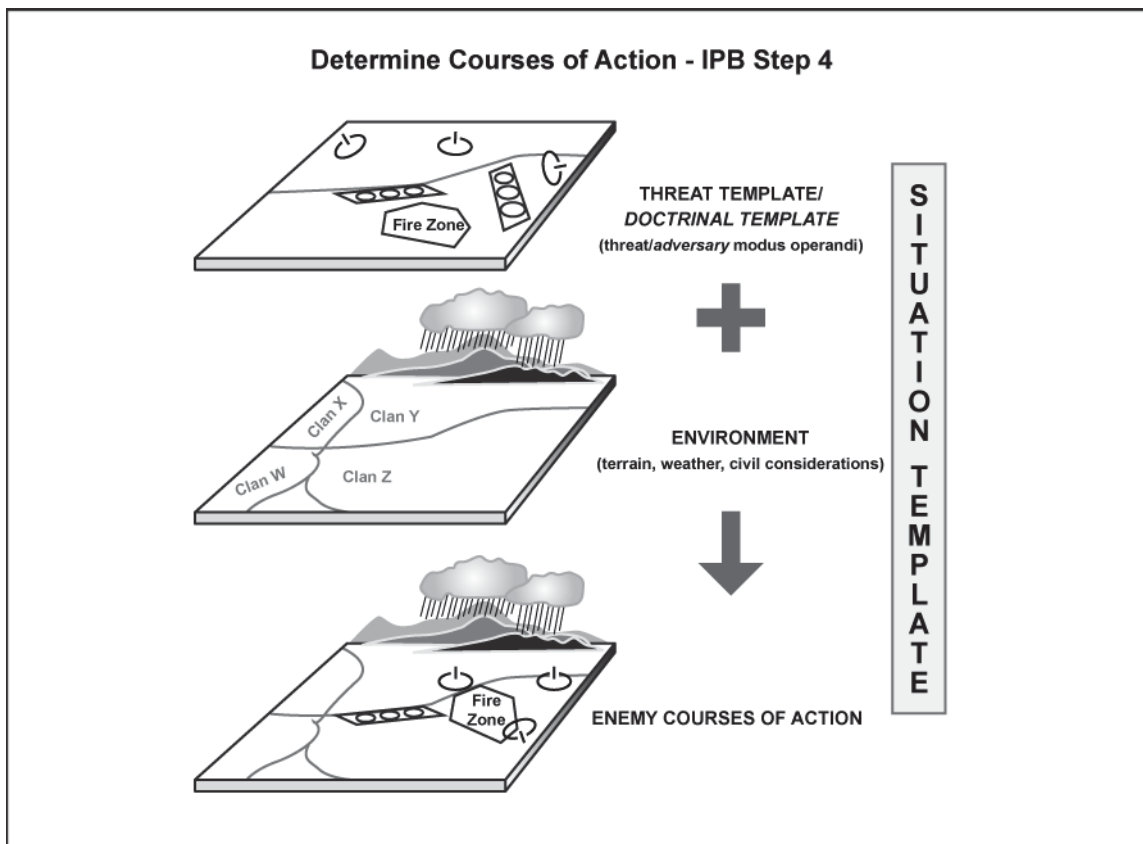
Figure 6-2. Example of a situation template

6-28. A threat/*adversary* situation template is a graphic depiction along with the analysis of expected enemy dispositions related to a specific COA. Situation overlays usually depict the most critical point in the operation as determined by the commander, the operations officer, and the intelligence officer. However, the operation may require several overlays representing different "snapshots in time." This is especially true when developing overlays for enemy offensive tasks where there may be several critical points in the engagement. Chapter 5 contains the figures that show examples of a threat/*adversary* template and situation template.

6-29. Generally, there will not be enough time during the MDMP/*MCPP* to develop enemy situation overlays for all COAs. A good technique is to develop alternate or secondary COAs, write a COA statement, and produce a HVTL to use during the mission analysis briefing and COA development. Once these tools and products are complete, the staff constructs overlays depicting the enemy's most likely and most dangerous COA to use during friendly COA analysis.

6-30. There are three primary types of enemy situation overlays the staff may have to develop: enemy in the offense, enemy in the defense, and irregular forces conducting guerrilla or terror operations. During IPB, these overlays are largely based on assumption and depict enemy locations and activities that are usually templated. This is especially true of overlays depicting enemy offensive tasks or guerilla and/or terror activities. Because the enemy is more static in defensive tasks, the staff may have information related to enemy locations that aids the development of the overlay.

6-31. When developing an overlay depicting regular forces conducting offensive or defensive tasks, the staff should template enemy locations and activities two levels down. For example, a friendly brigade combat team/unit would construct an overlay showing maneuver companies and specialty platoons. One of that brigade's battalions/*an element two levels down from the unit* would refine that overlay for its zone or sector showing maneuver platoons and specialty teams.

6-32. When developing an overlay depicting irregular forces, the staff at every echelon templates enemy locations and activities at the cellular level. For example, whether at corps, division, brigade, or battalion/*regardless of the level of the unit* the staff templates enemy cells where these cells are believed to be operating. Staffs template where they believe the activity associated with each cell can occur. This activity is determined by evaluating enemy activity through predictive and pattern analysis.

6-33. *For the Marine Corps, once the complete set of adversary COAs has been identified, analysts develop each COA in as much detail as the situation requires and time allows. The order in which each COA is developed is based on its probability of adoption and the commander's guidance. To ensure completeness, each COA must answer the following five questions:*

- *What (type of operation)?*
- *When (time the action will begin)?*
- *Where (sectors, zones, axis of attack)?*
- *How (method by which the adversary will employ his assets)?*
- *Why (objective or end state of the adversary)?*

Overlays Depicting the Enemy in Offensive Tasks

6-34. The staff constructs an enemy offensive overlay using an 11-step process that includes the following steps:

- Step 1—Draw the enemy line of departure. This graphic-control measure is normally placed where the friendly limit of advance is. H-Hour is the time the enemy crosses the enemy line of departure or friendly limit of advance. When the enemy begins movement from assembly areas, to the line of departure or limit of advance, its actions in time and space occur on an H-countdown. Enemy movement that occurs past the line of departure or limit of advance happens on an H+ countdown. This information will be depicted on the enemy attack timeline accompanying the overlay.
- Step 2—Draw the enemy's immediate and subsequent objectives as identified in the enemy COA statement. Enemy offensive objectives are normally terrain or force oriented. For example, a force-oriented immediate objective may be to defeat first echelon defending forces and facilitate the passage of second echelon forces. A subsequent objective for this operation may be the destruction of friendly second echelon defending forces. Reverse IPB can aid in determining these objectives. Although the commander has not approved the plan yet, the staff will already have a rough idea of how to construct the defense based on the results of IPB so far.
- Step 3—Draw the enemy left and right boundaries. This determination is made on the doctrinal frontage for the enemy attack and the effects of terrain on movement. The MCOO developed during step 2 of the IPB process will show AAs, as well as the optimal and suboptimal movement routes, available to the enemy attacking force.
- Step 4—Draw all available attack routes the enemy may use to conduct its attack and secure its immediate and subsequent objectives. The MCOO and weather effects matrix/*operational impacts chart* will aid this analysis also.
- Step 5—Template the point of penetration. This area is where the enemy's main effort will attempt to move through the main defensive line. This area will most likely be at the end of a high-speed optimal attack route that allows the enemy to use speed and mass to quickly overwhelm the defense. It may also be at perceived weak points in the defense.
- Step 6—Template the locations of enemy ground reconnaissance assets from the line of departure along attack routes to the immediate and subsequent objectives. These locations will normally be associated with the enemy commander's decision points and locations where reconnaissance assets can provide observation in support of targeting.

- Step 7—Template the initial and subsequent field artillery firing positions the enemy will use to support the attack. Templating where the range fans for each type of enemy indirect fire system need to be to support actions on each enemy objective aids in this analysis.
- Step 8—Template potential locations the enemy may employ special munitions to isolate part of the friendly defense; delaying reorientation of the defense or the use of counterattack forces.
- Step 9—Template air AAs that enable the enemy's use of close air support on immediate and subsequent objectives.
- Step 10—Template enemy movement formation and attack timeline. There are several ways to do this. One way is to template how the enemy movement formation looks as the advance guard main body enters the defense's engagement area. Another technique is to show how the enemy movement formation looks at different points along attack routes. This technique requires the development of multiple enemy attack formations as it moves through the defense's sector.
- Step 11—Label enemy commander's decision points. Indicate on the overlay the areas where the enemy commander has to make a decision regarding the movement of forces to achieve the desired objectives and end state associated with the COA.

6-35. Figure 6-3 is an example of an enemy situation overlay showing a mechanized infantry brigade in the attack.
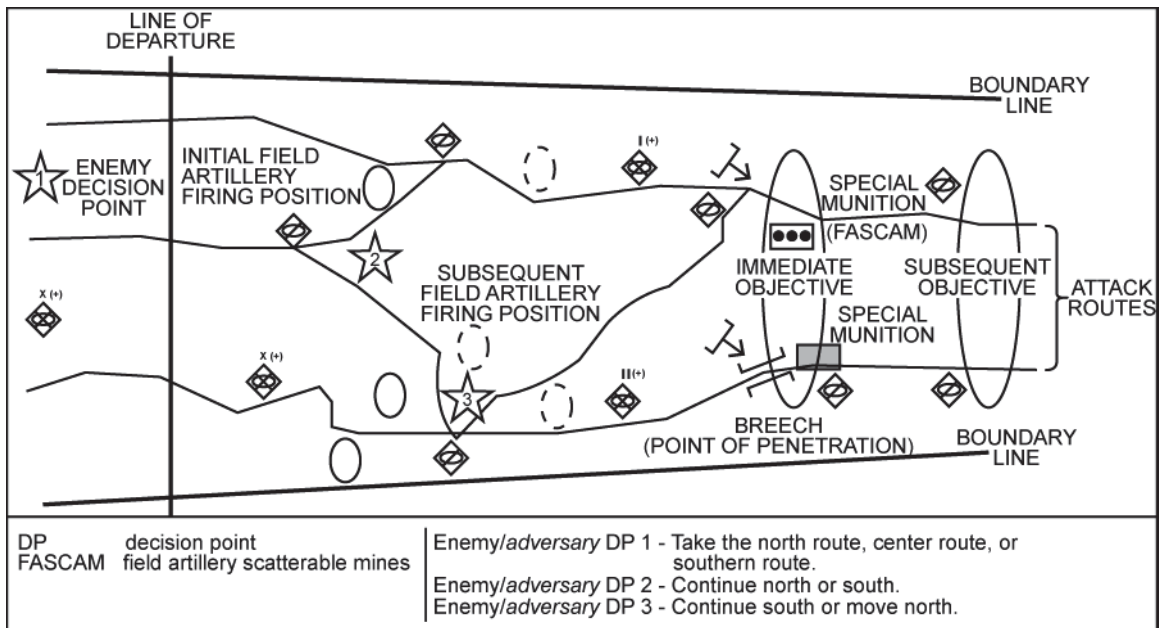

Figure 6-3. Example enemy offensive situation overlay

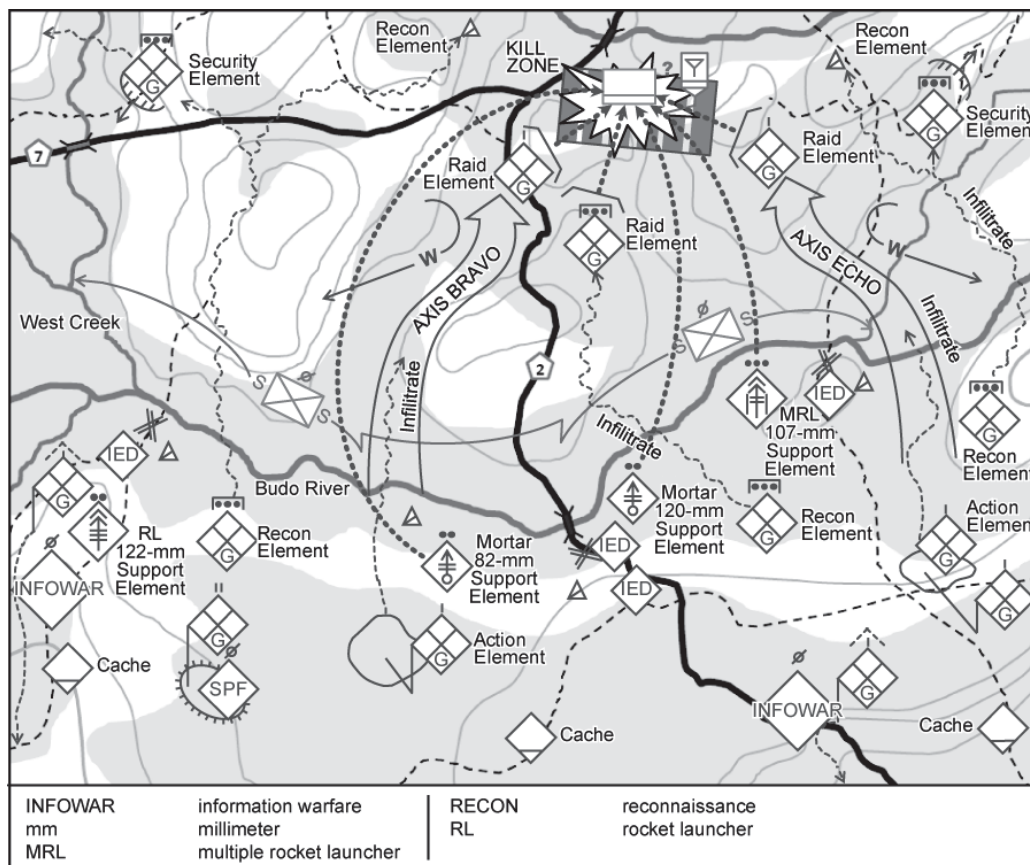6-36. Figure 6-4 is an example of an enemy reconnaissance attack.

Figure 6-4. Example enemy reconnaissance attack

Overlays Depicting the Enemy in Defensive Tasks

6-37. The staff constructs an enemy defensive overlay using a 10-step process that includes the following steps:

- Step 1—Template the location of enemy battle positions. Enemy battle positions are determined based on the assessed locations of enemy units, what is known about enemy operational art and tactics, and the effects of terrain and weather on the construction of a defense.
- Step 2—Template the location of enemy obstacles. The location of obstacles is determined based on assessed locations of enemy obstacles and unit locations, what is known about enemy operational art and tactics, and the methods available to the enemy to tie its obstacle plan into the terrain.
- Step 3—Template the location of enemy engagement areas. The templated location of enemy battle positions and obstacles aids in determining the location of engagement areas.
- Step 4—Draw the control measures (internal and external boundaries) associated with the defense. The frontage of the enemy defense can be determined by the structure presented by the configuration of battle positions, obstacles, and engagement areas templated in steps 1 through 3.
- Step 5—Template the field artillery firing positions the enemy will use to support the defense. Templating where the range fans for each type of enemy indirect fire system need to be to support enemy forces in the security zone and in the main battle area aids in this analysis.

- Step 6—Template the locations of enemy observation posts, antitank ambushes, and forward positions located in the security zone. These locations will normally be associated with the enemy commander's decision points, locations where reconnaissance assets can provide observation in support of targeting, and locations where the enemy can disrupt or deceive attacking forces.
- Step 7—Template potential locations where the enemy may employ special munitions to channel attacking forces into engagement areas; separate echelons or force attacking forces to adopt a protective posture from CBRN attack.
- Step 8—Template air AAs that enable the enemy's use of close air support on the main defensive belt to support the defense.
- Step 9—Template the location of enemy counterattack forces and the movement routes these forces can use to support the defense. When templating movement routes, identify the movement times associated with each route.
- Step 10—Label enemy commander's decision points. Indicate on the overlay the areas where the enemy commander has to make a decision regarding the movement of forces to achieve the desired objectives and end state associated with the COA.

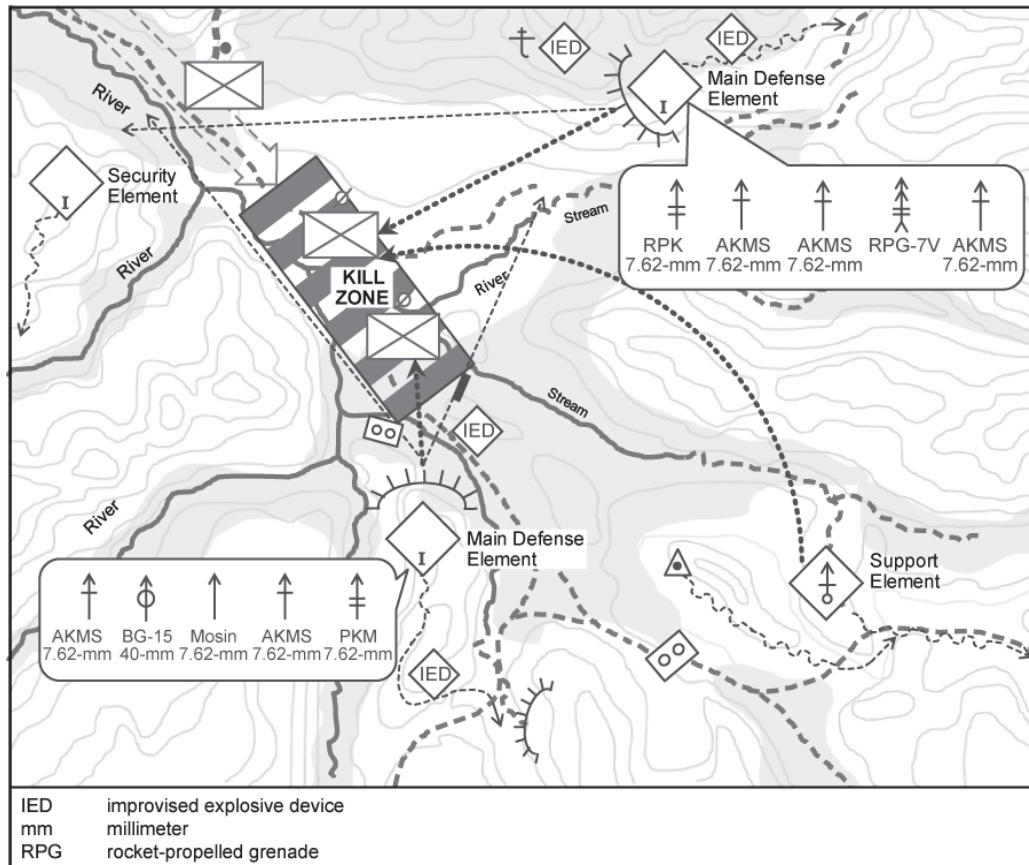6-38. Figure 6-5 is an example of an enemy defensive situation overlay.

Figure 6-5. Example enemy defensive situation overlay

Overlays Depicting Irregular Forces

6-39. Overlays depicting irregular forces conducting operations typically focus on armed forces in a tactical array. The process and example at figure 6-6 depicts an enemy situation overlay showing an irregular force operating in an urban area.

6-40. Staffs consider whether they need to create overlays that depict the less visible elements of the threat/*adversary* to include auxiliary support networks, and popular support groups as well as the activities they engage in. Additionally, staffs should capture the process they use to template the overlay so that they and subordinate staffs can replicate the process as required.

6-41. The staff constructs an irregular forces overlay using a 10-step process that includes the following steps:

- Step 1—Template the physical objectives irregular forces may attack. These objectives are typically friendly unit locations and movement routes. These objectives may also be elements or individuals associated with host-nation political, civil, and security organizations; critical infrastructure; or elements of the civilian population.
- Step 2—Template ingress and egress routes around objectives. Analysis of these routes includes consideration of nontraditional approaches associated with infiltration and sabotage.
- Step 3—Template range fans around objectives. This analysis is based on the ranges of enemy indirect fire and air defense systems.
- Step 4—Template potential locations of reconnaissance and surveillance assets. This analysis includes consideration of physical areas of observation around and on the objective. It also focuses on identifying TTP the enemy uses to conduct reconnaissance.
- Step 5—Template potential ambush sites along movement routes and near objectives. This analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.
- Step 6—Template potential sniper locations along movement routes and near objectives. This analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.
- Step 7—Template potential IED attack locations along movement routes and near objectives. This analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.
- Step 8—Template potential cache sites. This analysis is based on pattern and predictive analysis, as well as on analysis of TTP.
- Step 9—Template the bed-down area for direct action cells and HPTs (individuals). This analysis is based on pattern and predictive analysis.
- Step 10—Draw the AO for each direct action cell. This analysis is based on pattern and predictive analysis.
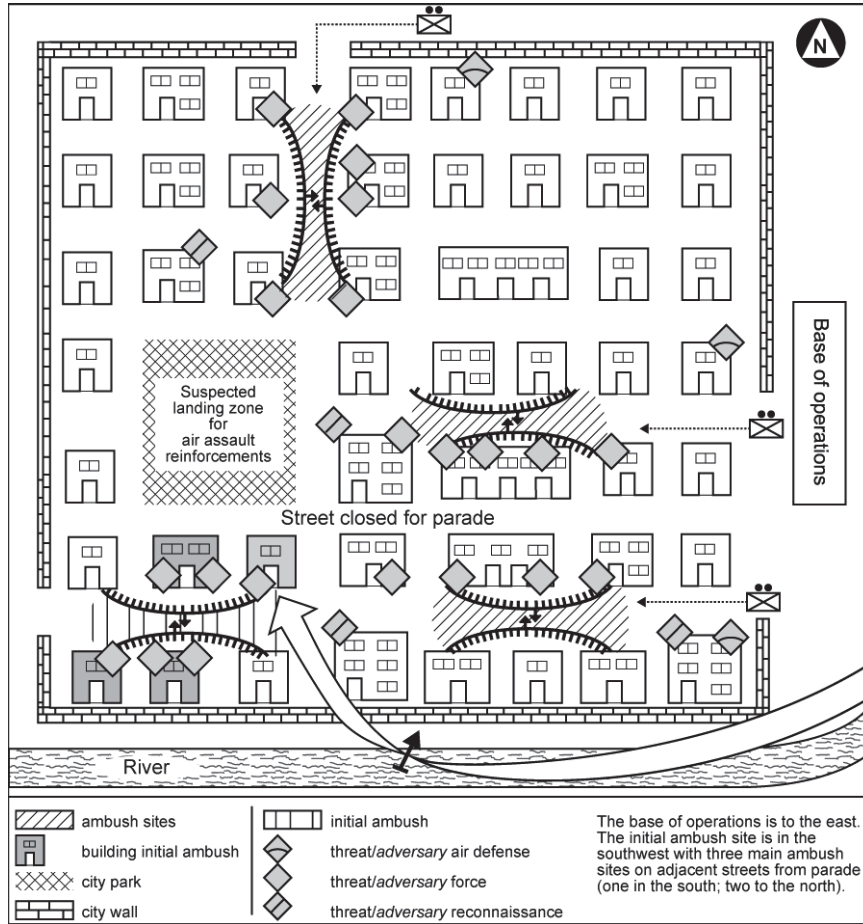
Figure 6-6. Example irregular force situation overlay

Threat/*Adversary* COA Statements

6-42. As stated previously, every threat/*adversary* COA includes a threat/*adversary* COA statement, which is a narrative that describes the situation overlay. Figure 6-7 is an example of a threat/*adversary* COA statement.

Current enemy situation.
Enemy mission.
Enemy objectives and end state.
Enemy task organization.
Capabilities.
Vulnerabilities.
Decision points.
Decisive point/*Center of gravity*.
Failure options.
Commander's intent for—
  - Movement and maneuver.
  - Information collection/*Intelligence collection*.
  - Fires.
  - Sustainment.
  - Threat/a*dversary* command and control.
  - Protection.
  - Information activities.
  - Denial and deception.

Figure 6-7. Example threat/*adversary* COA statement

HVTs and HVTL for the Threat/*Adversary* COA

6-43. An HVT is an asset an enemy commander requires for the successful completion of a mission. Identifying HVTs involves mentally wargaming an enemy COA to determine what assets are required to complete the mission. This process involves—

- Using the HVTL developed as part of the threat/*adversary* model in step 3 of the IPB process as a guide.
- Determining the effect on the threat/*adversary* COA if each of these targets is lost.
- Identifying possible threat/*adversary* responses if the target is lost.

6-44. Based on the situation, one or more of the targets taken from the threat/*adversary* model may be validated as HVTs. Additionally, targets that were not identified in the threat/*adversary* model may turn out to be HVTs.

6-45. Later on, in planning, the staff will use the HVTLs developed for each threat/*adversary* COA to construct the HPTL. The HPT is an asset that if lost to the enemy will significantly contribute to the success of friendly operations.

IDENTIFY INITIAL COLLECTION REQUIREMENTS FOR EACH COA

6-46. After identifying the full set of potential threat/*adversary* COAs, the staff develops the tools necessary to determine which COA the threat/*adversary* will implement. Because the threat/*adversary* has not acted yet, this determination cannot be made during IPB. However, the staff can develop the information requirements and indicators necessary to support the construction of an information collection plan/*intelligence collection plan* that can provide the information necessary to confirm or deny threat/*adversary* COAs and locate enemy targets. Information requirements are those items of information that need to be collected and processed in order to meet the intelligence requirements of the commander. An indicator is an item of information which reflects the intention or capability of a threat/*adversary* to adopt or reject a COA.

6-47. *For the Marine Corps, after identifying potential adversary COAs, the analyst must determine which one the enemy will adopt. Initial collection requirements are designed to help answer the challenge. The identification of initial intelligence collection requirements revolves around predicting specific areas and activities, which, when observed, will reveal which COAs the adversary has chosen. The areas where the analyst expects key events to occur are designated NAIs. The activities that reveal the selected COA are called indicators.*

6-48. Chapters 7, 8, and 9 discuss the types of information needed to support offensive, defensive, and stability tasks. These requirements are generally related to confirming or denying a threat/*adversary* COA and locating enemy HVTs.

DEVELOP THE EVENT TEMPLATE AND MATRIX

6-49. An event template is a graphic overlay used to confirm or deny enemy COAs. The event template is used as a guide during the COA analysis step of the MDMP/*COA wargaming step of MCPP* to describe enemy actions throughout wargaming. Additionally, the event template is used to develop the information collection overlay/*intelligence collection overlay* and the decision support template during COA analysis. The event template is used during the execution phase of the operations process to aid in determining which COA the enemy has adopted. An event template is always accompanied by an event matrix.

6-50. The event template is comprised of the following elements: time-phase lines, NAIs, and enemy decision points. Time-phase lines are linear geographic areas that depict when enemy activity will occur. NAIs are usually selected to capture indications of enemy COAs, but also may be related to conditions of the operational environment. A decision point is a point in time and space when the enemy commander anticipates making a decision regarding a specific COA.

6-51. An event matrix is a table that associates the NAI and enemy decision points identified on the event template with indicators to aid in determining which COA the enemy commander is implementing. An indicator is an item of information which reflects the intention or capability of an enemy to adopt or reject a COA.

6-52. The initial event template and matrix are normally developed prior to COA analysis, refined during COA analysis, and further refined during execution as the situation changes. In addition to using the event template and matrix to support its own planning, the staff normally disseminates the event template to subordinate units to aid in the development of subordinate unit information collection plans/*intelligence collection plans.*

EVENT TEMPLATE

6-53. Constructing an event template is an analytical process that involves comparing the multiple enemy COAs developed earlier in step 4 of the IPB process to determine the time or event and the place or condition in which the enemy commander must make a decision on a particular COA. Figure 6-8 and figure 6-9 on page 6-16 are examples of how to illustrate the basic mechanics of this process. The figures only display some minimal, but not all-inclusive information, for what is included on the event template.
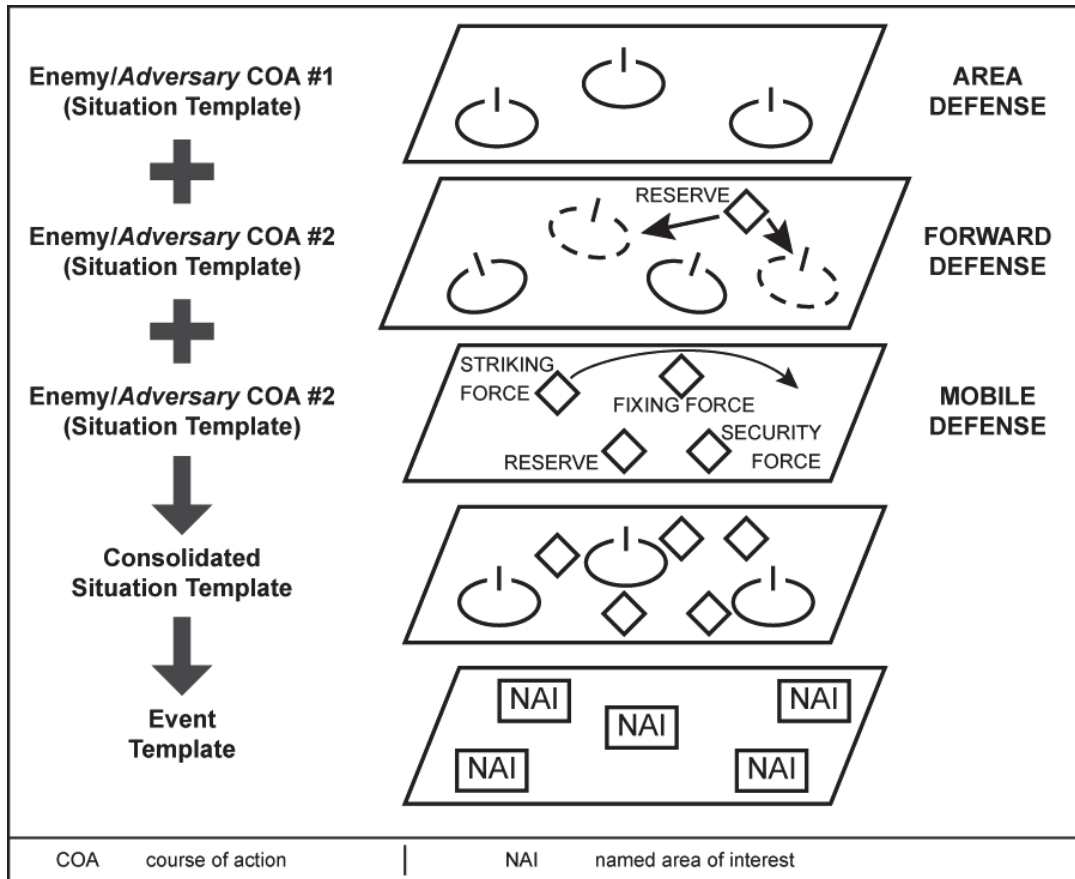

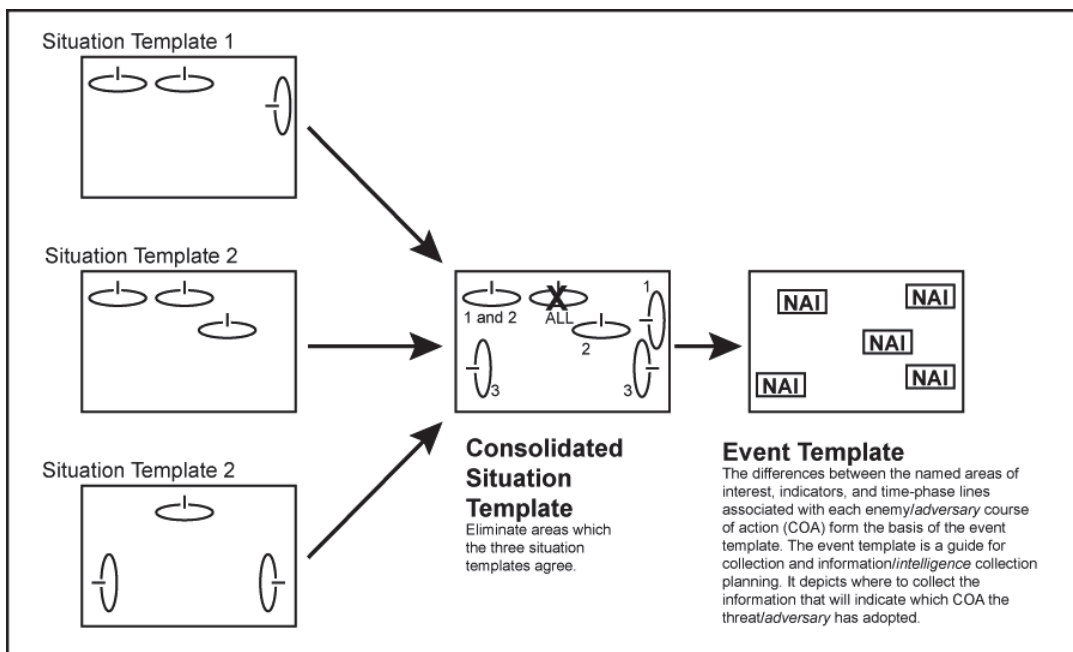**Figure 6-8. Example of an event template – 1**

Figure 6-9. Example of an event template – 2

EVENT MATRIX

6-54.   Constructing an event matrix is an analytical process that involves determining the indicators of enemy activity that aid in identifying the decisions the enemy commander has made. Table 6-1 illustrates the basic mechanics of this process.

Table 6-1. Constructing an event matrix

Named area of interest	Indicators	Enemy decision point	Time (Hour)	Enemy course of action (COA) indicated
1, 2, 3	• Establishment of battle positions and obstacles • Presence of armored vehicles • Presence of engineer assets	1	H–12	COA 1 area defense
1, 3 4	• Establishment of battle positions and obstacles • Presence of armored vehicles • Presence of engineer assets • Identification of company (+) sized reserve	2	H–12	COA 2 forward defense
1, 2, 3 5, 6	• Absence of maneuver and engineer assets • Presence of mobile armored formation	3	H–3	COA 3 mobile defense

6-55. Figure 6-10 is an example of a completed event template for an enemy conducting offensive operations. This figure is for illustrative purposes and is not based on a tactical scenario.
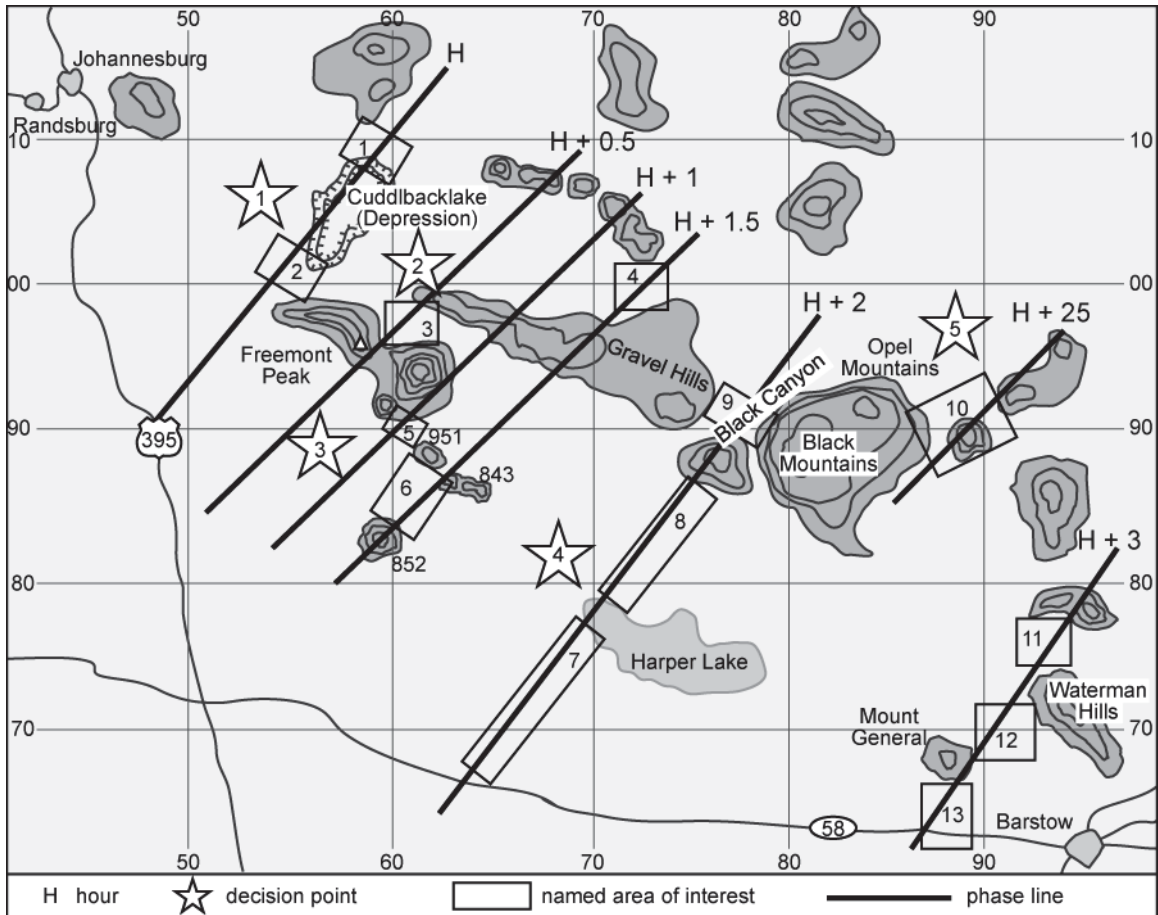
Figure 6-10. Example event template (regular threat)

6-56. Figure 6-11 is an example of a completed event template for an enemy conducting irregular warfare. This figure is for illustrative purposes and is not based on a tactical scenario.
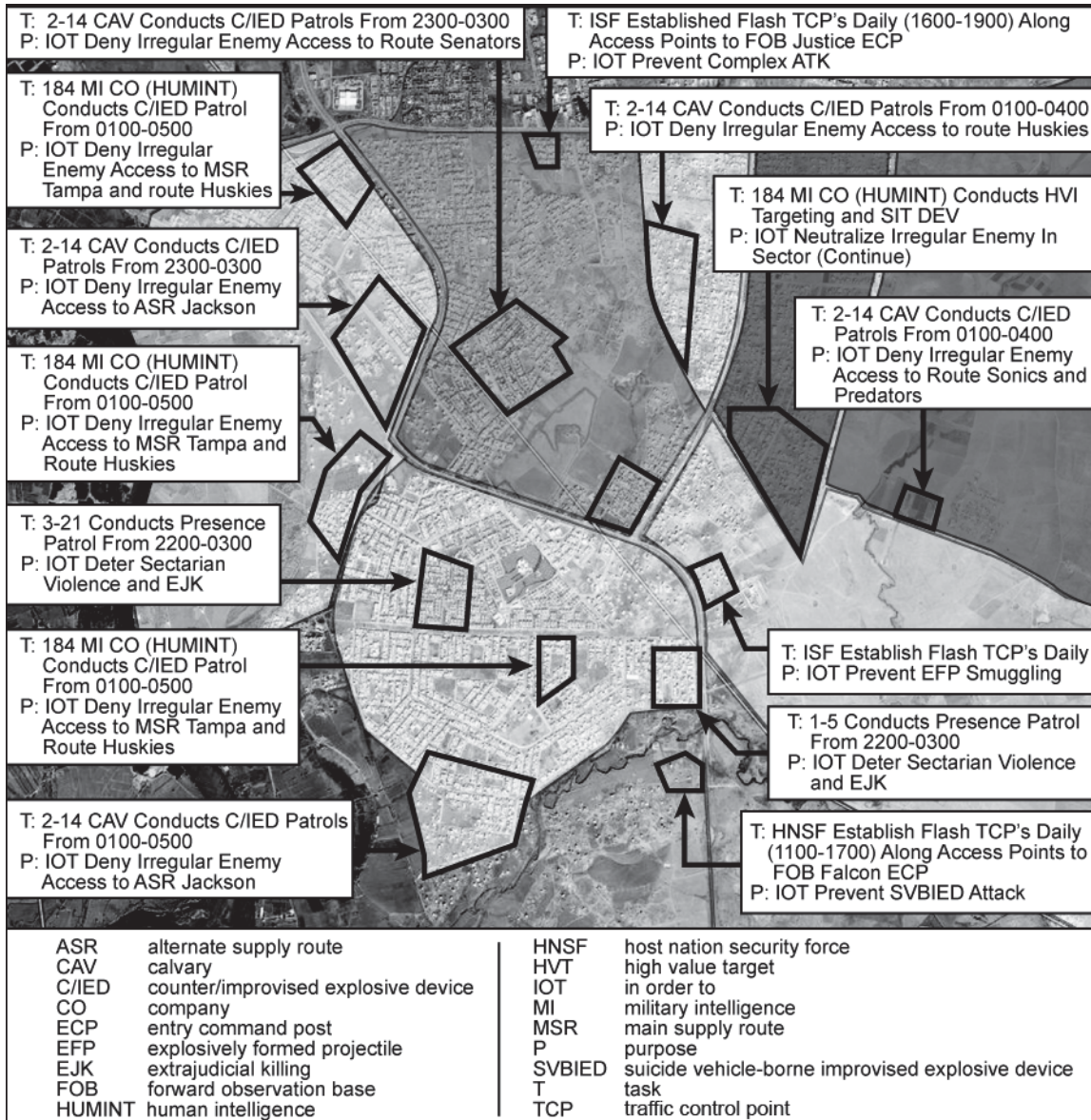
Figure 6-11. Example event template (irregular threat)

Note. When constructing an event template for an enemy or multiple enemies conducting irregular warfare operations, it is often challenging to discern the tactical enemy decisive point. A way to overcome this is to construct the event template based on conclusions formed based on a pattern and link analysis.

PART THREE

Considerations for Specific Operations, Unique Environments, and Missions

---

Chapter 7

IPB for Specific Operations

7-1. **Unified action** is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). Under unified action, commanders synchronize military actions with activities of other government agencies, NGOs, IGOs, and the private sector.

7-2. For the Army, the Army's contribution to unified action, as well as its operational concept, is unified land operations. Unified land operations describes how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution. Chapter 7 discusses specific considerations for IPB conducted in support of unified land operations. (See ADP 3-0 for further discussion of unified land operations.) Army forces conduct decisive and sustainable land operations through the simultaneous combination of offensive, defensive, and stability operations appropriate to the mission and environment.

7-3. *For the Marine Corps, this chapter discusses specific considerations for IPB in support of specific operations. Intelligence analysts must identify areas that favor each type of MAGTF operation (such as offensive, defensive, force protection, and peace enforcement). They tailor their intelligence analysis and products depending on which type of operation they face. (See MCWP 5-1 for information on planning for specific types of operations.)*

IPB CONSIDERATIONS FOR OFFENSIVE TASKS/*OPERATIONS*

7-4. **Offensive tasks** are conducted to defeat, destroy, or neutralize an enemy force. A commander may also conduct offensive tasks to secure decisive terrain, to deprive the enemy of resources, to gain information, to deceive and divert the enemy, to hold the enemy in position, to disrupt his attack, and to set the conditions for future successful operations (ADRP 3-90). *Offensive operations are operations conducted to take the initiative from the enemy, gain freedom of action, and generate effects to achieve objectives. The four types of offensive operations are movement to contact, attack, exploitation, and pursuit (MCRP 5-12C).* Intelligence requirements generally associated with offensive operations are as follows:

- Determine what type of defense the enemy is employing:
  - Area defense.
  - Mobile defense.
  - Retrograde.

- Determine location, disposition, and orientation of enemy defense:
  - Main battle area.
  - Battle positions.
  - Battle handover lines.
  - Obstacles.
  - Engagement areas.
  - Reserves.
  - Fire support assets.
  - Specialty teams.
  - Close air support and other aviation supporting the defense.
  - Other assets supporting the defense.
- Determine the enemy commander's—
  - End state.
  - Objectives.
  - Decision points.
  - Decisive point/c*enter of gravity.*
  - Failure option.
- Determine enemy commander's intent for—
  - Denial and deception operations.
  - Information activities.
  - Reconnaissance and surveillance.
  - Fires.
- Identify terrain and weather effects that support enemy defensive tasks:
  - Physical areas that allow the commander to tie in obstacles and battle positions to existing terrain features.
  - Air and ground AAs (close air support, reserve, and counterattack forces).
  - Terrain that canalizes attacking forces.
  - Prevailing winds, temperature inversion, humidity, precipitation, visibility, illumination, and other weather effects.
- Identify terrain and weather effects that support friendly movement and maneuver:
  - Air and ground AAs.
  - Primary and alternate attack routes.
  - Landing zones.
  - Terrain management (mission command/*command and control*, air defense, signal, and reconnaissance).
  - Prevailing winds, temperature inversion, humidity, illumination, and other weather elements.
- Determine the impact of civil considerations and displaced civilians on friendly and enemy operations:
  - Rural communities.
  - Refugee camps.
  - Refugee movement.
  - Aid organizations located in the AO.

7-5. In addition to the intelligence requirements listed in paragraph 7-4, each of these operations has its own unique requirements. (See ADRP 3-90/*MCDP 1-0* for additional information on offensive tasks/*operations.*)

MOVEMENT TO CONTACT

7-6. A movement to contact is an offensive task designed to develop the situation and to establish or regain contact. It may also include preliminary diversionary actions and preparation fires. The extent and nature of the movement to contact depends on whether threat/*adversary* forces were previously in contact. If forces are not in contact, then the central feature of the movement-to-contact operations is gaining or reestablishing contact with the enemy. Conducting movement to contact relies heavily on assumptions made during IPB. This is because the relationship of friendly and enemy forces in time and space is an unknown. In addition to the considerations listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- Enemy location and intent.
- Location and time of potential meeting engagements.
- Location of danger areas (enemy defensive locations along routes, engagement areas, observation posts, and obstacles) where friendly forces may encounter enemy forces.
- Attack routes that protect friendly forces from ground observation or surprise by the enemy.
- Natural and/or manmade obstacles along attack routes that can affect friendly advance.
- Location, type, and size of security forces along attack routes.
- Location of enemy flanks and other weak points in the enemy's posture.
- Threats to friendly force flanks and rear.
- Location and extent of CBRN contaminated areas.

ATTACK

7-7. An attack is a type of offensive task that destroys or defeats enemy forces, seizes and secures terrain, or both. Movement supported by fires characterizes the conduct of an attack. An attack differs from a movement to contact because enemy main body dispositions are at least partially known. In addition to the considerations listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- Location of areas where friendly forces could become disoriented, such as rough or restrictive terrain.
- The most favorable routes to the objective.
- Areas friendly forces can use to support flanking fire and maneuver, such as support by fire and attack by fire positions.

EXPLOITATION

7-8. An exploitation is a type of offensive task that rapidly follows a successful attack and is designed to disorganize the enemy in depth. The objective of exploitation is to complete the enemy's disintegration. Exploitation takes advantage of previous successes and friendly force continuing activities. In addition to the considerations listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- Location of enemy reserves prior to commitment.
- Location of enemy countermobility assets prior to their employment on routes friendly forces are using to conduct the exploitation.
- Location of enemy forces attempting to reestablish the defense.
- Location of enemy logistics and/or resupply operations.

PURSUIT

7-9. A pursuit is a type of offensive task designed to catch or cut off an enemy force attempting to escape, with the intent to destroy it. A commander often plans for an enemy retrograde operation as either a branch or sequel to an operation. When recommending pursuit, the staff must consider possible enemy deception (whether the enemy is in retreat or attempting to draw friendly forces into a position where they can be destroyed by conventional means or by weapons of mass destruction). In addition to the considerations

listed in paragraph 7-4, conducting this type of operation includes considering the following intelligence requirements during IPB:

- Possible routes the enemy might use to conduct retrograde operations.
- Availability and condition of pursuit routes.
- Location and accessibility of blocking points.
- Location of critical terrain features that affect enemy and friendly movement.
- Location of enemy uncommitted forces.
- Identity of fire support and air assets that can affect friendly force movement.
- Indications the enemy can no longer maintain defensive positions nor cohesively execute defensive tasks.
- Indications the enemy can only conduct limited counterattacks.
- Indications the enemy is increasing reconnaissance efforts.
- Indications the enemy is destroying weapons and equipment.
- Decrease of enemy indirect fire throughout the AO (intensity and effectiveness).
- Increase of enemy indirect fire in one or more sectors of the front at a time when the amount of overall defensive fires is decreasing.
- Indications of retreating forces.
- Location of enemy second echelon defensive lines.
- Location, type, strength, and size of bypassed units.
- Presence of new forces on the battlefield/*battlespace.*
- Indications of increased resistance.

IPB CONSIDERATIONS FOR DEFENSIVE TASKS/*OPERATIONS*

7-10. For the U.S. Army, a **defensive task** is a task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks (ADRP 3-90). *For the Marine Corps, defensive operations are operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable to offensive and stability operations. The three types of defensive operations are area, mobile, and retrograde (MCRP 5-12C.)* Intelligence requirements generally associated with defensive operations are as follows:

- Determine, locate, and/or track the enemy's main and supporting efforts.
- Locate and/or track enemy reserves.
- Locate and/or track enemy reconnaissance assets.
- Identify enemy's use of special munitions (CBRN, artillery scatterable mines).
- Locate and/or track enemy close air support.
- Locate enemy information capabilities.
- Identify enemy deception operations.
- Determine enemy commander's end state.
- Determine enemy commander's objectives.
- Determine enemy commander's decision points.
- Determine enemy decisive point/*center of gravity.*
- Determine enemy's failure option.

- Determine enemy commander's intent for—
  - Reconnaissance and surveillance.
  - Fires.
  - Denial and deception.
  - Defensible terrain.
  - Battle positions.
  - Engagement areas.
  - Indirect fire assets positions.
  - Counterattack routes for reserves plan.
- Develop TAIs for indirect fire and close air support.
- Determine the impact of civil considerations and displaced civilians on friendly and enemy operations for—
  - Rural communities.
  - Refugee camps.
  - Refugee movement.
  - Aid organizations located in the AO.

7-11. There are three types of defensive operations forces may engage in: area defense, mobile defense, and retrograde. In addition to the intelligence requirements listed in paragraph 7-10, each of these operations has its own unique requirements. (See ADRP 3-90/*MCDP 1-0* for additional information on defensive tasks/*operations*.)

AREA DEFENSE

7-12. Area defense is a type of defensive operation that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright. The focus of the area defensive task is on retaining terrain where the bulk of the defending force positions itself in mutually supporting, prepared positions. Units maintain their positions and control the terrain between these positions. The decisive operation focuses on fires into engagement areas possibly supplemented by a counterattack. The reserve may or may not take part in the decisive operation. The commanders can use their reserves to reinforce fires; add depth, block, or restore the position by counterattack; seize the initiative; and destroy enemy forces. In addition to the considerations listed in paragraph 7-10, conducting this type of operation includes considering the following intelligence requirements during IPB:

- The location of natural lines of resistance, well-defined AAs, IVLs, and other terrain features that support defensive tasks.
- Whether the terrain better supports a forward defense or a defense in depth.

MOBILE DEFENSE

7-13. Mobile defense is a type of defensive operation that concentrates on the destruction or defeat of the enemy through a decisive attack by a striking force. A mobile defense focuses on defeating or destroying the enemy by allowing the enemy to advance to a point where he is exposed to a decisive counterattack by the striking force. The decisive operation is a counterattack conducted by the striking force. The striking force is a dedicated counterattack force constituting the bulk of available combat power. A fixing force supplements the striking force. The commanders use their fixing force to hold attacking enemy forces in position, to help channel attacking enemy forces into ambush areas, and to retain areas from which to launch the striking force. In addition to the considerations listed in paragraph 7-10, conducting this type of operation includes considering the following intelligence requirements during IPB:

- Methods to deceive the enemy regarding the purpose of the defense.
- Terrain that will hide the striking force.

RETROGRADE

7-14. Retrograde is a type of defensive operation that involves organized movement away from the enemy. The enemy may force these operations, or a commander may execute them voluntarily. The higher commander of the force executing the retrograde must approve the retrograde operation before its initiation in either case. A retrograde is a transitional operation; it is not conducted in isolation. It is part of a larger scheme of maneuver designed to regain the initiative and defeat the enemy. In addition to the considerations listed in paragraph 7-10, conducting this type of operation includes considering the following intelligence requirements during IPB:

- Possible routes friendly forces can use to conduct retrograde operations.
- Possible pursuit routes enemy forces may use.
- Blocking points enemy forces may use to prevent the retrograde.
- Areas enemy movement can be disrupted through the use of obstacles, indirect fire, and close air support.

7-15. As in supporting planning for offensive operations, the primary intelligence products and work aids necessary to support planning for defensive operations are a MCOO, weather effects matrix/*operational impacts chart*, enemy organizational charts, enemy capabilities statement, enemy situation overlays with COA statements, event template with matrix, relative target value matrix, HVTL, and intelligence requirements specific to the enemy operation.

IPB CONSIDERATIONS FOR COUNTERINSURGENCY OPERATIONS AND STABILITY TASKS

7-16. **Counterinsurgency operations** are those military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency (JP 1-02). Counterinsurgency operations are usually conducted simultaneously with stability tasks.

7-17. **Stability operations** is an overarching term encompassing various military missions, tasks, and activities conducted outside the Unites States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (JP 3-0).

7-18. The lines of operations in counterinsurgency and stability operations, as discussed in FM 3-24/*MCWP 3-33.5* and FM 3-07, often overlap and can include establishing civil security, establishing civil control, restoring essential services, supporting governance, and supporting economic and infrastructure development.

7-19. The purpose of IPB in counterinsurgency and stability tasks is the same as in offensive and defensive tasks/*operations*. However, the nature of these operations and the intelligence requirements associated with them are unique. The principal difference is the focus and degree of detail of analysis required for the civil aspects of the environment. Unlike major combat/*major operations*, an environment dominated by offensive and defensive tasks/*operations* directed against an enemy force, counterinsurgency, and stability tasks encompass various military missions, tasks, and activities that are not enemy-centric.

7-20. One of the consistent observations from commands involved in Operation Iraqi Freedom and Operation Enduring Freedom is that planning can become too enemy-centric and ignore other lines of operations. The lesson learned is that while enemy analysis needs to be done, so does the analysis related to all the lines of operations the commander has identified as important. This means that the analysis of civil considerations may have equal or greater importance to the analysis of enemy forces.

7-21. FM 3-24/*MCWP 3-33.5* constitutes the Army/*Marine Corps* current doctrine on counterinsurgency and contains the operational discussion that intelligence personnel need to understand to conduct effective IPB in support of counterinsurgency. The primary intelligence requirements associated with counterinsurgency are associated with the following questions:

- What are the drivers of instability? (Examples include fraudulent elections, rule-of-law issues, sectarian tensions, political and civil government credibility, completion for resources, lack of essential services, and others.)
- What is the nature or type of the insurgency? (Who are the insurgents and what do they want?)
- What is the insurgent strategy? (How do they intend to achieve what they want?)
- What are the insurgents' motivations (strategic goals)?
- What are the insurgents' objectives (operational objectives)?
- What popular support does the insurgency have (active or passive, tribal, ethnic, other)?
- What are the insurgents' capabilities, vulnerabilities (command and control, maneuver, fire support, intelligence, logistics, other)?

7-22. FM 3-07 constitutes the Army's current doctrine on stability tasks and contains the operational discussion that intelligence personnel need to understand to conduct effective IPB in support of stability tasks. The primary intelligence requirements associated with stability tasks are generally based on lines of operations identified by the commander and are focused on aiding governments in securing the environment, restoring essential services, and promoting infrastructure and economic development.

Note. For the Marine Corps, see MCWP 3-33.5 for additional information on counterinsurgency and the operational discussion that intelligence personnel need to understand to conduct effective IPB in support of counterinsurgency. See also MCDP 1-0 for additional information on stability operations.

7-23. *Counterinsurgency and stability operations are conducted in support of a host-nation or interim government or as part of an occupation when no government exists. These operations involve both coercive and constructive actions by the military force. They are designed to establish a safe and secure environment; facilitate reconciliation among local or regional adversaries; establish political, legal, social, and economic institutions; and facilitate the transition to legitimate local governance.*

7-24. Counterinsurgency and stability operations promote and protect U.S. national interests by influencing the threat, political, and information aspects of the operational environment through a combination of peacetime developmental, cooperative activities, and coercive actions in response to crises. Regional security is supported by a balanced approach that enhances regional stability and economic prosperity simultaneously. When conducting IPB for stability tasks, a good technique is to balance the analytical effort in the same manner. Commanders and staffs should be wary of becoming too focused on enemy forces and not conducting necessary analysis on civil considerations. In fact, a greater emphasis may need to be placed on civil considerations than on the enemy during counterinsurgency operations and stability tasks. The purpose of counterinsurgency operations and stability tasks is to—

- Provide a secure environment (isolate insurgents from the local populace).
- Gain support for the host-nation government.
- Meet the critical needs of the populace.
- Build support for host-nation governments and institutions.
- Shape the environment for interagency and host-nation success.

7-25. IPB can help the commander gain the situational understanding needed to accomplish these tasks by—

- Understanding the root cause or causes of the insurgency.
- Identifying external and internal support for the insurgency.
- Understanding how the insurgents appeal to the population.
- Identifying the targets/audiences on which insurgents focus.

- Identifying groups or populations vulnerable to insurgent influence activities and determine why they are vulnerable.
- Understanding insurgent motivation and depth of commitment.
- Understanding insurgent TTP.
- Understanding the conditions the insurgents want to create to achieve their objectives.
- Identifying and verifying identities and tracking insurgents, criminals, and known or suspected terrorists.
- Identifying demographics for groups supporting, neutral to, or hostile to insurgent organizations and operations.
- Identifying the means to gain legitimacy among the population and its leaders (formal and informal).
- Accurately assessing the needs and security requirements of the population.
- Providing assessments for all lines of operations.
- Identifying the themes insurgent organizations use.
- Assessing the effects or consequences of friendly operations.

7-26. There are five lines of operations associated with counterinsurgency and stability tasks that require extensive IPB:

- Establish civil security.
- Establish civil control.
- Restore essential services.
- Support governance.
- Support economic and infrastructure development.

7-27. In addition to providing intelligence about these lines of operations, IPB provides intelligence about people. U.S. forces must understand the people of the nation in which they are operating in order to accomplish the missions they are given. Commanders and planners require accurate intelligence assessments into the culture, perceptions, values, beliefs, interests, and decisionmaking processes of the individual and groups that comprise the various social networks that comprise the population.

ESTABLISH CIVIL SECURITY

7-28. Establishing civil security is the first responsibility of military forces in counterinsurgency and stability operations and involves providing for the safety of the host nation, including protection from active enemy forces. When dealing with internal and external enemy forces that pose a direct threat to the host nation and its people, there are three basic subtasks associated with civil security that require detailed IPB:

- Protect external borders.
- Combat internal threats/*defeat insurgencies*.
- Separate insurgents from the general population.

7-29. Table 7-1 identifies types of intelligence requirements that may be associated with each of these three subtasks.

Table 7-1. Example civil security intelligence requirements

Protect external borders	*Combat internal threats/defeat insurgencies*	*Separate insurgents from the general population*
- Identify all external state and nonstate actors attempting to influence U.S. operations. - Identify objectives of these groups and individuals. - Identify the tactics, techniques, and procedures these groups and individuals are using to accomplish their objectives. - Identify physical locations these groups and individuals are using to transport weapons, equipment, personnel, money, media, and ideas across the border. - Identify the locations, methods, and operations of organizations within the host nation aiding external state and nonstate actors. - Identify good locations for friendly observation posts, checkpoints, engagement areas, and friendly approach and withdrawal routes.	- Identify all regular and irregular forces that pose a military threat to U.S. and host-nation security forces. - Identify threat characteristics/*adversary order of battle* for each threat/*adversary* group. - Develop threat/*adversary* templates for each threat/*adversary* group. - Develop an enemy situation overlay for each threat/*adversary* group. - Identify high-value targets. - Identify and verify individuals as insurgents, known or suspected terrorists, and/or criminals. - Identify actors in the civilian population providing support to enemy forces. - Identify external actors providing support to the enemy. - Identify groups and populations that are vulnerable to enemy influence (persuasion, coercion, other).	- Identify the objectives and concerns of stakeholders. - Determine methods to protect the population from insurgents. - Locate sectarian fault lines. - Locate sectarian and ethnic enclaves. - Identify conditions that can promote civilian opposition to insurgents.

7-30. When conducting stability tasks, U.S. forces will generally not have to prepare for an attack by a regional power across an international border. The primary cross-border threats/*adversaries* U.S. forces will encounter are—

- Foreign nation special forces.
- Terrorist organizations.
- Regionally based irregular forces.
- Criminal organizations.

7-31. The primary threat/*adversary* activity U.S. forces will have to counter are—

- Infiltration of foreign operatives and fighters.
- Movement of weapons, equipment, money, and other resources needed to support an insurgency.
- Criminal smuggling.

7-32. Commanders need to know what external forces and/or individuals are supporting enemy forces in their AO in order to develop friendly COAs to counter these forces. Failure by the intelligence staff to provide this intelligence can result in the unchecked reinforcement and resupply of these forces. Although commanders may not be able to act directly against these forces, they can request support from the next higher command. Detailed intelligence on these forces provided by the intelligence staff can assist commanders in gaining this support. Table 7-2 on page 7-10 illustrates four steps as a way of presenting this information.

Table 7-2. TTP for evaluating external threat/*adversary* organizations

Step	Requirement	Tactics, techniques, and procedures (TTP)
1	Identify all external state and nonstate actors attempting to influence U.S. operations and their objectives. Include— • Identity. • Location. • Objectives. • Operations. • Methods. • Defeat mechanisms.	• Identify all organizations and their objectives during mission analysis/*problem framing*. • Develop organizational charts for each of these groups during mission analysis/*problem framing*. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these organizations.
2	Within the area of operations, identify physical locations these groups or individuals are using to transport weapons, equipment, personnel, money, media, and ideas across the border.	• Develop a situation template (digital overlay) that depicts the border-crossing points, movement routes, safe houses, cache sites, and high-value targets associated with each organization. • Develop a course of action statement describing the operations of each of these organizations during mission analysis/*problem framing*. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain situation template as part of the joint common database.
3	Identify TTP these groups or individuals are using to accomplish their objectives.	• Identify these methods during mission analysis/*problem framing*. • Develop special assessments (text and graphics) that describe TTP in detail. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these TTP.
4	Identify good locations for friendly observation posts, checkpoints, engagement areas, and friendly approach and withdrawal routes.	• Develop a digital terrain overlay (geospatial and imagery intelligence) during mission analysis/*problem framing* that describes these locations. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain digital terrain overlays as part of the joint common database.

Combat Internal Threats/*Defeat Insurgencies*

7-33. When engaged in stability operations, U.S. forces can be contested by one or more armed and organized groups that oppose U.S. presence and objectives in the area. These groups will vary in size and capability. Their motivations and objectives may or may not be the same. They may actively oppose each other or they may work together. The one characteristic these groups share is to achieve their goals through violence. Beyond that, these groups can be generally characterized as follows. They—

- Are generally un-located and not easily detected by U.S. information collection assets/*intelligence collection assets*.
- Are often unidentified early in an operation.
- Usually operate under a decentralized chain of command.
- Are organized under a cellular, militia, or special forces structure.
- Operate in complex terrain usually within urban centers or severely restricted natural terrain.

- Are a thinking and adaptable enemy that modify TTP, as needed, to operate against conventional forces.
- Target four general groups:
  - Host-nation political and civil authorities.
  - Host-nation military and police forces.
  - The general population.
  - U.S armed forces and other international military and civilian agencies.
- Sustain themselves through external and/or internal support mechanisms.
- Establish sanctuary in complex terrain or among civilian populations.
- Generally avoid massing forces.
- Generally employ—
  - Commercial-off-the-shelf communications technology (telephone, cell phone, Internet).
  - Tactical radios.
  - Nonelectronic methods of command and control.
  - Civilian transportation (public transportation, privately owned vehicles).
  - Small arms and crew-served weapons.
  - IEDs.
  - Mortars.
  - Shoulder-fired antiaircraft weapons.
- Are capable of operations directed against U.S. forces, such as—
  - IED attack.
  - Mortar attack.
  - Complex attack.
  - Sniper attack.
  - Drive-by shooting.
  - Infiltration.
  - Ambush.
  - Sabotage.
  - Suicide bombing.
  - Information activities.
  - Information for effect.
  - Misinformation.
  - Disinformation.
  - Propaganda.
  - Reconnaissance and surveillance.
- Can conduct operations directed against host-nation political targets, civil targets, security targets, and the general population (in addition to the above list):
  - Assassination and murder.
  - Kidnapping.
  - Coercion.
  - Intimidation.
  - Recruitment.

7-34. The commander needs detailed intelligence on all of the insurgent organizations in the AOs in order to prevent their activity from affecting the command's ability to complete all other assigned stability tasks. Failure by the intelligence staff to provide this intelligence can result in a continual escalation of insurgent activity that may prevent the command from accomplishing the mission. When evaluating this type of enemy, intelligence staffs maintain up-to-date data files relating to the threat characteristics/*adversary order of battle*, historical reporting, and current reporting to produce the predictive assessments the commander needs to plan operation.

7-35. Table 7-3 illustrates a way of evaluating insurgent operations.

Table 7-3. TTP for evaluating internal threat/*insurgency* operations

Step	Requirement	Tactics, techniques, and procedures (TTP)
1	Identify all regular and irregular forces that pose a military threat to U.S. and host-nation security forces.	• Identify all organizations and their objectives during mission analysis/*problem framing*. • Develop organizational charts for each of these groups during mission analysis. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these organizations.
2	Within the area of operations, identify physical locations these groups or individuals are using to transport weapons, equipment, personnel, money, media, and ideas across the border.	• Develop a situation template (digital overlay) that depicts the border-crossing points, movement routes, safe houses, cache sites, and high-value targets associated with each organization. • Develop a course of action statement describing the operations of each of these organizations during mission analysis/*problem framing*. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain a situation template as part of the joint common database.
3	Identify TTP these groups or individuals are using to accomplish their objectives.	• Identify these methods during mission analysis/*problem framing*. • Develop special assessments (text and graphics) that describe TTP in detail. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain up-to-date data files for each of these TTP.
4	Identify good locations for friendly observation posts, checkpoints, engagement areas, and friendly approach and withdrawal routes.	• Develop a digital terrain overlay (geospatial and imagery intelligence) during mission analysis/*problem framing* that describes these locations. • Present this information during the mission analysis/*problem framing* briefing. • Include this information as part of the intelligence estimate. • Maintain digital terrain overlays as part of the joint common database.

Separating Insurgents from the General Population

7-36. Paramilitary elements, terrorists, militias, and other insurgent groups of elements conducting irregular warfare depend on the cooperation of the general population. These groups do not have the capability to sustain operations against armed conventional forces without that support. Denying support from the general population to these groups is a critical component of an overall strategy to prevent them from influencing other stability tasks. Armed groups involved in insurgent operations directed against the host-nation government draw their strength from the population. These groups—

- Establish sanctuary locations among segments of the population.
- Utilize civilian transportation, communications, financial services, and general services to sustain operations.
- Receive funding by winning the approval of segments of the population or by extortion.
- Utilize segments of the population to provide indications and warnings of U.S. operations.

- Conduct information activities targeting the population.
- Use the threat of violence or specific actions to coerce the population.

7-37. In order to separate these forces from the population, commanders need to understand how and why the population is supporting these forces. There are many factors that may influence a local population's perspective and sway its support one way or another. Safety from the violence of war and crime, economic viability, religious freedom, view toward government, and view toward U.S. presence are some examples. The intelligence staff continually reevaluates the role the population is playing in the conflict and provides the information the commanders need to conduct operations that can influence the population to support their programs. Steps 1 and 2 in table 7-4 illustrate a way of presenting this information.

Table 7-4. TTP for evaluating the general population's role in a conflict

Step	*Requirement*	*Tactics, techniques, and procedures (TTP)*
1	Conduct an initial assessment of the population during intelligence preparation of the battlefield/*battlespace.*	• This can be a long and difficult process. Begin this assessment during predeployment. • Integrate civil affairs personnel and assessments in the intelligence preparation of the battlefield/*battlespace* process. • Consider how successful insurgent groups have conducted population surveys to determine how these groups view and use the population. • Maintain a civil considerations assessment that accurately describes the civil aspects of the environment, assesses effects of friendly operations on the population, and identifies strategies that can influence the population to aid in combating enemy forces. • Determine how the enemy is using the population as part of its operations. • Determine the positive and negative effects of every type of friendly operation. • When determining intelligence gaps, include those related to the population. This will assist civil reconnaissance as well as information collection operations/*intelligence collection operations* in general.
2	Continually reassess information collected as part of civil and infrastructure reconnaissance.	• Continually update the civil considerations assessment. • Include the civil considerations assessment in all intelligence briefings. • Include the civil considerations/*human environment* assessment in targeting and information collection working groups/*intelligence collection working groups*.

ESTABLISH CIVIL CONTROL

7-38. When mission and conditions warrant, U.S. forces may be required to implement populace and resources control measures to achieve civil control and protect the populace. The military activities associated with establishing civil control generally involve developing interim mechanisms for establishing rule of law and restoring the justice system. Generally, the military role is to—

- Occupy and assert transitional military authority.
- Establish public order and safety.
- Establish military government.
- Transition to other authority.
- Establish interim criminal justice system.
- Support—
    - Law enforcement and policing reform.
    - Judicial reform.
    - Property dispute resolution processes.
    - Corrections reform.
    - War crimes courts and tribunals.
    - Public outreach and community rebuilding programs.
- Work with the following types of groups to accomplish the task:
    - Host-nation political and civil leaders.
    - Host-nation military and police forces.
    - Leaders of host-nation religious and ethnic groups.
    - U.S., host-nation, and international aid organizations.
    - Host-nation judicial bodies.
    - Local populations.

7-39. Establishing civil control goes hand-in-hand with establishing civil security and involves developing interim mechanisms for establishing rule of law. When attempting to establish civil control, the commander has two primary intelligence requirements:

- Identify the appropriate methods necessary to regulate selected behavior and activities of individuals and groups to reduce the overall risk to the general population.
- Determine the reliability, capability, and support requirements of the key individuals and organizations assisting with this task.

7-40. During IPB, the commander and staff assess the indigenous nation's ability to combat crime, as well as identify—

- All vulnerable elements of the population and assess their needs.
- Methods to communicate with the public to promote reconciliation.
- Security requirements for humanitarian aid organizations and indigenous security forces.
- What civilian police functions need to be performed by U.S. military forces.
- Major crime issues.
- Critical infrastructure related to criminal justice and security institutions that need to be protected.

7-41. Civil affairs/*G-3/S-3*, military police, and the staff judge advocate office and other sources of information—including local nationals, local government officials, NGOs, and IGOs—can provide Department of State information on establishing civil control for—

- Public order and safety.
- Criminal justice system reform.
- Law enforcement reform.
- Judicial system reform.
- Corrections system reform.

- War crimes courts and tribunals.
- Conflict resolution.
- Public outreach and community rebuilding.

RESTORE ESSENTIAL SERVICES

7-42. The military activities associated with restoring essential services generally involve supporting indigenous populations and institutions as well as civilian relief agency operations addressing the effects of humanitarian crises such as famine, dislocated civilians, displaced persons, and human trafficking. Generally, the military role is to provide—

- An initial response that provides for immediate humanitarian needs (food, water, shelter, and medical support).
- A transformational response where military forces build on unified action partner capacity to operate and maintain essential civil services.

7-43. During IPB, the commander and staff should determine the nature and scope of the humanitarian crisis as well as determine the following:

- Civilian dislocation/displaced person relief programs:
  - Identify the size and location of dislocated civilian populations.
  - Identify food, water, shelter, and medical needs.
  - Assess the capability of local physical transport, distribution, and storage to deliver relief supplies (including government and relief agencies).
  - Determine the command's capability to provide services or augment the efforts of other organizations.
  - Identify other threats to the affected population (human rights abuses, minefields, hostile forces, other).
- Famine relief programs:
  - Assess the effects of conflict on food and availability.
  - Determine food and water security requirements.
  - Estimate total food and water needs.
  - Assess the capability of local physical transport, distribution, and storage to deliver food and water (including government and relief agencies).
  - Identify most vulnerable populations.
  - Identify security requirements for relief distribution networks.
  - Identify other threats to the affected population (human rights abuses, minefields, hostile forces, other).
- Nonfood relief programs:
  - Identify security requirements for relief distribution networks.
  - Identify areas that need emergency nonfood items.
- Humanitarian demining:
  - Identify mined areas.
  - Identify populations and individuals injured by mines.
  - Determine medical support required to treat injuries.
  - Determine how best to educate the population to recognize and avoid mines.
- Human rights initiatives:
  - Identify previous human rights violations.
  - Identify vulnerable populations.
  - Determine how to secure vulnerable populations.
  - Determine how best to support IGOs and NGOs.

- Public health and education programs:
  - Identify public health hazards (malnutrition, water contamination, sewage).
  - Identify deficiencies in the existing medical infrastructure.
  - Assess the need for additional medical personnel and facilities.
  - Identify requirements to open schools.

7-44. Civil affairs/*G-3/S-3*, military police, and the staff judge advocate office staff proponents and other sources of information including local nationals, local government officials, NGOs, and IGOs can provide Department of State information for restoring essential services, such as—

- Civilian dislocation programs.
- Famine prevention programs.
- Nonfood relief programs.
- Humanitarian demining programs.
- Human rights initiatives.
- Public health programs.
- Education programs.

SUPPORT GOVERNANCE

7-45. When a legitimate and functional host-nation government is present, military forces operating in support of a state have a limited role. However, if the host-nation government cannot adequately perform its basic civil functions, some degree of military support to governance may be necessary. Supporting governance is the fourth stability task that may need to be analyzed during IPB. During IPB, the commander and staff assess whether the indigenous government is adequately performing its basic civil functions. If the indigenous government is not adequately performing its basic civil functions, the commander and staff will—

- Identify founding documents that establish the nature of government of the host nation (for example, United Nations mandate, declaration of independence, constitution or bylaws).
- Implement representative facets to government (councils, elections).
- Support civil administration and unified action partners by assisting in the development an internal defense and development plan.
- Identify critical essential public infrastructure and services that must be restored and maintained.
- Establish public information and education programs that support the authority and legitimacy of the host nation.
- Promote public health and welfare through foreign humanitarian assistance (FHA) and humanitarian civil assistance programs in support of the internal defense and development plan.

7-46. The operations office staff proponent and other sources of information including local nationals, local government officials, NGOs, and IGOs can provide Department of State information on supporting governance for—

- Transitional administrations.
- Local governments.
- Anti-corruption initiatives.
- Elections.

SUPPORT ECONOMIC AND INFRASTRUCTURE DEVELOPMENT

7-47. The most effective long-term measure of conflict prevention and resolution is the sustainment of a viable government that is actively engaged in meeting the needs of its citizens; including economic development. A nation's economy affects its ability to govern and provide security for its people. The status of a nation's infrastructure affects the sustainment and growth of its economy. Understanding the economy and the state of infrastructure in the AO is critical to a commander's ability to plan and conduct operations that improve economic conditions.

7-48. Support economic and infrastructure development is the fifth and last stability task that may need to be analyzed during IPB. During IPB, the commander and staff—

- Assess overall economic conditions within the AO.
- Assess overall infrastructure conditions within the AO.

7-49. When assessing economic conditions, while not all-inclusive, the commander and staff consider the following information:

- Ability of legal border-crossing sites and other ports of entry to assist the legal flow of commerce.
- Positive and negative effects of cross-border smuggling of commercial goods.
- Positive and negative effects of any existing underground economy.
- Status of financial services being provided by the private sector within the AO.
- Threats to critical financial institutions, infrastructure, personnel, and transactions.
- Corruption within existing financial institutions.
- How the various groups of a local population are earning their living (agriculture, trade, industry).
- Where the most important items the population consumes come from.
- Weather or terrain effects on the availability of commodities.
- How conflict has impacted the availability and movement of commerce.
- What measures the population has taken to adapt to a disrupted economy.
- Current and projected level of job growth without intervention.
- Existence of ongoing host-nation and/or international economic recovery programs.
- The economic impact of criminal organizations, insurgent groups, and corrupt political and civil elements on the host-nation government, assistance providers, and U.S. military forces.
- Availability and distribution of currency.
- The best use of the commander's emergency response program.
- Status of dislocated civilian population and ongoing relief efforts.
- Measures of effectiveness that can be used for assistance programs and civic action programs.

7-50. The answers to these questions can help the commander avoid actions that might disrupt economic recovery and target efforts that improve local economic conditions through infrastructure development. Table 7-5 shows the intelligence staff where this information is found. Additional sources of information are local nationals, local government officials, NGOs, and IGOs.

Table 7-5. Information sources for supporting economic developments

Economic category	Staff proponent	Information sources
Economic Generation and Enterprise Creation	Civil Affairs/*G-3/S-3*	Department of Treasury
Monetary Programs	Civil Affairs/*G-3/S-3*	Department of Treasury
National Treasury Operation	Civil Affairs/*G-3/S-3*	Department of Treasury
Public Sector Investment Programs	Civil Affairs/*G-3/S-3*	Department of Commerce
Private Sector Development	Civil Affairs/*G-3/S-3*	Department of Commerce
Natural Resource Protection	Civil Affairs/*G-3/S-3*	Department of Interior
Agricultural Development	Civil Affairs/*G-3/S-3*	Department of Agriculture
Transportation Infrastructure Programs	Civil Affairs/*G-3/S-3*	Department of Commerce
Telecommunications Infrastructure Programs	Civil Affairs/*G-3/S-3*	Department of Commerce
General Infrastructure Programs	Civil Affairs/*G-3/S-3*	Department of Commerce

7-51. When assessing infrastructure conditions, the intelligence staff considers—

- The condition of existing infrastructure and whether rehabilitation or new infrastructure development is needed.
- The organizations and individuals responsible for maintaining infrastructure and providing services.

- The capability of responsible organizations and individuals to meet the requirements of the population.
- Corruption and favoritism in the delivery of services.
- The expectations and perceptions of local communities regarding the provision of services made possible by functional infrastructure.

7-52. The answers to these questions can help the commander prioritize infrastructure development projects, maximize existing resources, and potentially leverage external resources. Data collected during infrastructure reconnaissance can help answer these questions. Infrastructure reconnaissance as described in FM 3-34-170 results in the collection of the technical information on public systems, services, and facilities necessary to develop the situational understanding of local capability to support the infrastructure requirements of local populace within a specific area. Table 7-6 shows the intelligence staff where to find this information (*memory aid is SWEAT-MSO*.) Additional sources of information are local nationals, local government officials, NGOs, and IGOs.

7-53. When assessing economic and infrastructure conditions, the intelligence staff conducts an analysis of the economic and infrastructure conditions within a targeting area during initial IPB in order to focus the commander and staff on these problem sets during the remainder of planning. This analysis is briefed during the intelligence portion of the mission analysis/*problem framing* briefing and included as part of the intelligence estimate issued with the OPLAN and/or OPORD. Additionally, in order to support continued operations, this analysis is continually updated to ensure planning teams and assessment working groups have the most current data.

Table 7-6. Information sources for supporting infrastructure development (*SWEAT-MSO*)

Infrastructure category	Staff proponent	Information sources
SEWAGE	Engineer	Engineer reconnaissance teams, infrastructure survey teams, scouts, and combat patrols.
WATER	Engineer	Same as Sewage.
ELECTRICITY	Engineer	Same as Sewage.
ACADEMICS	Civil Affairs/*G-3/S-3*	Civil Affairs teams/*G-3/S-3.*
TRASH	Engineer	Same as Sewage.
MEDICAL	Medical Services	Civil Affairs teams/*G-3/S-3.*
SAFETY	Military Police	Same as Sewage.
OTHER:		
Roads and railroads	Engineer	Same as Sewage.
Bridges and waterways	Engineer	Same as Sewage.
Airports	Engineer	Same as Sewage.
Housing	Engineer	Same as Sewage.
Communications	Engineer	Same as Sewage.
Food supply	Civil Affairs/*G-3/S-3*	Civil Affairs teams/*G-3/S-3.*
Hazardous materials	Engineer	Same as Sewage.
Population concerns related to all above	Civil Affairs/*G-3/S-3*	Civil Affairs teams and human terrain teams/*foreign area officers, regional affairs officers, and other cultural enablers.*

UNDERSTANDING THE POPULATION

7-54. Counterinsurgency and stability tasks are conducted in and around populations. These populations can aid or hinder friendly operations. Understanding these populations aids all aspects of counterinsurgency and stability planning and operations.

7-55. In general, when conducting counterinsurgency operations and stability tasks, people are the decisive point/*center of gravity* and the key terrain for both threat/*adversary* and friendly forces.

7-56. IPB aids the understanding of populations (people) through the analysis of civil considerations as discussed in part one of this publication. Understanding the population aids the commander in developing a plan that can separate the population from the insurgents and gain the support of the population for the host-nation government and its security forces, including U.S. forces. Intelligence requirements associated with understanding the population are as follows:

- Identify and define the dominant and secondary cultures within the host-nation society.
- Determine how the society—groups, institutions, organizations, and networks—functions (social network analysis).

7-57. Counterinsurgency and stability tasks are conducted in and around populations. These populations can aid or hinder friendly operations. Understanding these populations aids all aspects of counterinsurgency and stability planning and operations.

7-58. In general, when conducting counterinsurgency operations and stability tasks, people are the decisive point/*center of gravity* and the key terrain for both threat/*adversary* and friendly forces.

7-59. IPB aids the understanding of populations (people) through the analysis of civil considerations as discussed in part one of this publication. Understanding the population aids the commander in developing a plan that can separate the population from the insurgents and gain the support of the population for the host-nation government and its security forces, including U.S. forces. Intelligence requirements associated with understanding the population are as follows:

- Identify and define the dominant and secondary cultures within the host-nation society.
- Determine how the society—groups, institutions, organizations, and networks—functions (social network analysis).
- Identify language:
  - Identify the languages spoken by the host-nation society, the insurgents, and multinational security forces.
  - Identify social manners, behaviors, and nonverbal cues that can aid in communicating with the population through interpreters.
- Identify power and authority:
  - Determine how formal and informal power and authority are apportioned within the society:
    - Formal power and authority: central government, local government, government agencies.
    - Informal power and authority: political parties; political interest groups; unions; and religious, tribal, and ethnic groups.
  - Determine how each formal and informal power holder acquires, maintains, and uses power to attract and maintain followers—
    - Through the use of coercive force.
    - Through the expenditure of social capital (reciprocity and exchange, patron-client relationships).
    - Through the application of economic power.
  - Consider the state of the formal economic system (weak or strong, supplanted or supported by an informal economic system).
  - Consider the state of any informal economic systems (smuggling, black market, barter and exchange, tribal or clan networks).
  - Determine how the primary and secondary cultures in the society perceive their interests.

- Determine security:
    - Do these cultures believe they are safe from harm?
    - Do these cultures have faith in the police, the military, and the judiciary?
- Identify basic necessities: Are these groups satisfied with the availability of—
    - Food.
    - Water.
    - Clothing.
    - Shelter.
    - Medical treatment.
- Identify economic well-being: Are these groups optimistic about long-term economic viability for themselves and their children?
- Identify political participation: Do these groups believe they are part of, and can affect change, within the political process?

Chapter 8

IPB Considerations for Unique Activities, Tasks, and Processes

IPB SUPPORT TO PROTECTION/*FORCE PROTECTION*

8-1.   Protection relates to those actions taken by commanders to preserve the force so they can apply maximum combat power. Preserving the force includes protecting personnel (combatants and noncombatants), physical assets, and information of the United States and multinational military and civilian partners. The protection warfighting function facilitates the commander's ability to maintain the force's integrity and combat power.

8-2.   Intelligence personnel may support command protection/*force protection* programs by identifying, collecting, reporting, analyzing, and disseminating intelligence regarding <u>foreign</u> threats to the Army. Inside the United States, intelligence personnel must limit collection to foreign intelligence and international terrorism threat data. Criminal and domestic terrorism threat information is restricted to law enforcement agencies.

8-3.   Protection determines the degree to which potential threats/*adversaries* can disrupt operations and counters or mitigates those threats/*adversaries*. Emphasis on protection increases during preparation and continues throughout execution including in-transit (fort-to-port), redeployment, and home-station operations. Protection is a continuing activity; it integrates all protection capabilities to safeguard bases, secure routes, and protect forces. Supporting tasks that routinely require IPB support include the following:

- Apply antiterrorism measures.
- Implement operations security.
- Implement information protection/*information security*.
- Conduct operational area security.
- Coordinate air and missile defense.
- Conduct personnel recovery operations.
- Conduct force health protection operations.

APPLY ANTITERRORISM MEASURES

8-4.   For U.S. Army, **terrorism** is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (U.S. Code, Title 18, Section 2331). *For the Marine Corps, terrorism is the unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political (JP 3-07.2).* U.S. Code, Title 22, Section 2656f, defines terrorism as premeditated politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents. The Army/*Marine Corps* adds to this definition by recognizing that terrorist groups will target U.S. forces as well as noncombatants.

8-5.   **Antiterrorism** is defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces (JP 3-07.2). It is an element of protection and a consideration during planning and operations. During IPB, the staff identifies potential terrorist threats and other threat activities. Based on this analysis, the staff recommends actions to reduce vulnerabilities to terrorist acts and attacks. Additionally, based on the analysis of terrorist organizations and

capabilities conducted during IPB, the staff develops plans and orders to counter terrorist attacks. Intelligence requirements generally associated with antiterrorism are—

- Identify the individual components (organization) of terrorist networks operating in the AO and area of interest: direct action cells, support cells, intelligence cells, command and control cells, financiers, and others.
- Determine the goals and objectives associated with each network.
- Determine the strengths and weaknesses within each network.
- Identify the HVTs and individuals associated with each network.
- Determine the location of each of the components of the network.
- Identify the targets each network will attack.
- Identify the TTP the networks will employ to conduct their operations.
- Determine the friendly resources and activities that need protection from terrorist attack in order to accomplish the mission.
- Determine what types of actions the force can take to mitigate terrorist attacks on noncombatants.

IMPLEMENT OPERATIONS SECURITY

8-6. JP 3-13.3 defines operations security as a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities that can be observed by *adversary* intelligence systems. Criticality, vulnerability, and threat assessments conducted by counterintelligence personnel contribute to IPB support to operations security. This information should be included into a threat/*adversary* vulnerability assessment. Intelligence requirements associated with operations security are—

- Identify essential elements of friendly information:
  - Locations of headquarters elements.
  - Location and activities of assets critical to operational success.
  - Information collection/*intelligence collection*.
  - Fires.
  - Engineer.
  - Sustainment.
  - Information related to friendly force operations.
  - Information related to friendly strengths and weaknesses.
  - Other information as required based on mission.
- Identify indicators associated with the conduct of friendly operations. The same type of indicators associated with threat/*adversary* operations apply to friendly operations. (See chapter 7 for indicators associated with offensive, defensive, and stability tasks.)
- Identify threats to critical resources, information, and personnel:
  - Identify threat/*adversary* information collection assets/*intelligence collection assets*.
  - Determine threat/*adversary* capability to detect and attack friendly critical resources, assets, and personnel.

IMPLEMENT INFORMATION PROTECTION

8-7. Information protection are those active or passive measures used to safeguard and defend friendly information and information systems. Information protection comprises information assurance, defensive cyberspace operations, and electronic protection. *Marine Corps uses the joint term "information security," which is the security discipline concerned with implementation of a system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure information that is authorized protection by executive order, statute, or regulation. Information security includes protection of classified, controlled unclassified, and sensitive compartmented information.*

Information Assurance

8-8. Information assurance is the protection and defense of information and information systems on data networks and computer systems. Intelligence requirements associated with information assurance are—

- Identify the structure of the friendly communications network.
- Identify potential threats to the network.
- Identify vulnerabilities within the network.

Defensive Cyberspace Operations

8-9. Computer network defense utilizes defensive cyberspace operations to protect against unauthorized activity. Computer network defense includes monitoring, detection, analysis, response, and restoration activities. Intelligence requirements associated with computer network defense are—

- Identify threat/*adversary* organization capabilities to disable, corrupt, or compromise friendly information systems.
- Identify internal threats/*insurgencies* that can disable, corrupt, or compromise friendly information systems.

Electronic Protection

8-10. Electronic protection involves actions such as communications avoidance or anti-jamming measures to protect personnel, facilities, and equipment from friendly and enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Intelligence requirements associated with electronic protection are—

- Identify threat/*adversary* electronic surveillance capabilities.
- Identify threat/*adversary* electronic attack capabilities.

CONDUCT PERSONNEL RECOVERY OPERATIONS/*TACTICAL RECOVERY OF AIRCRAFT AND PERSONNEL*

8-11. The U.S. Army conducts personnel recovery operations that are conducted to recover and return Soldiers, Army civilian personnel, selected Department of Defense contractors, and other personnel as determined by the Secretary of Defense who are isolated, missing, detained, or captured. Intelligence requirements associated with personnel recovery are the same as those for any operation—determining the effects of enemy, terrain, weather, and civil consideration in the area friendly forces are conducting personnel recovery operations. Intelligence requirements also include information on isolated, missing, detained, or captured personnel needing recovery similar to the requirements in a noncombatant evacuation operation and includes—

- Identifying the location, disposition, capabilities, and possible COAs for all enemy forces.
- Anticipating the number of isolated, missing, detained, or captured personnel (total number by area) categorized by medical status.

8-12. *The U.S. Marine Corps participates and/or supports combat search and rescue. It conducts tactical recovery of aircraft and personnel (TRAP). TRAP includes rescue or extraction, by surface or air, of downed aircraft and/or personnel and equipment; aircraft sanitation; and advanced trauma life support in a benign or hostile environment. (See MCDP 1-0 for more information on TRAP.)*

CONDUCT FORCE HEALTH PROTECTION OPERATIONS

8-13. Throughout history, the number of casualties sustained from disease and nonbattle injuries have far outweighed the number of combat casualties, thereby reducing the operational effectiveness of military forces. Disease and nonbattle injuries may be the result of endemic and epidemic diseases. Table 8-1 on page 8-4 lists some examples of these types of injuries.

Table 8-1. Examples of types of non-combat-related injuries

Disease	Health threat	Stressors	Plants	Animals	Accidents
• Arthropod • Waste • Waterborne	• Occupational • Environmental • Extreme heat • Extreme cold • Altitude • Toxic industrial materials • Radiation: (ionizing and non-ionizing) • Hazardous noise	• Psychological • Physiological (from traumatic and/or continuous operations)	• Poison ivy • Poison oak	• Insects • Venomous snakes • Spiders	• Self-inflicted wounds • Injuries from accidents • Injuries from recreational activities

8-14. Intelligence requirements associated with force health protection include—

- Location of facilities that use or manufacture toxic industrial materials (such as research laboratories, gas stations, refineries, or chemical plants).
- Location and operational status of sanitation facilities and services (waste disposal facilities, water treatment plants and services, such as trash pickup and landfills).
- Types and locations of medical facilities (clinics, hospitals, medical training facilities, research facilities).
- Types of transportation available to move patients from point of injury, incident site, or between hospital facilities (dedicated evacuation platforms versus vehicles of opportunity).
- Leading causes of death, birth rates, nutrition status, and accessibility to medical care for the local population.
- Displaced persons camps to include camp leaders, sanitation facilities, and nutrition status.

IPB SUPPORT TO BUILDING PARTNERSHIP CAPACITY/ *ESTABLISHING GENUINE PARTNERSHIPS*

8-15. Operations may require inter-organizational efforts to build the capacity of partners to secure populations, protect infrastructure, and strengthen institutions as a means of protecting common security interests. The intelligence requirements associated with building partnership capacity are normally the same as those associated with stability operations.

8-16. *For the Marine Corps when establishing genuine partnerships, partnership is an arrangement between U.S. and host-nation forces in which they operate together to achieve mission success while building capability and capacity. Partnership requires mutual respect despite the differences in size, skill, training, capability or culture of the partnering forces. (See MCDP 1-0 for more information on establishing genuine partnerships.)*

SMALL-SCALE JOINT OPERATIONS

8-17. Small-scale joint operations 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 small-scale joint operations that Army/*Marine Corps* forces may participate in are noncombatant evacuations, raids, show of force, FHA, sanction enforcement, and elimination of weapons of mass destruction.

8-18. However, the threat of terrorist attack is possible as are attacks from the general population. During these types of operations, the commander is primarily concerned with protection, operations security, and targeting operations. Threat/*adversary* resolution is normally not clear. It usually consists of terrorist, guerilla, paramilitary, political, or religious groups opposing an established government that is being supported by the U.S. Government. These groups are usually not well-defined at the tactical level and are probably un-located. Echelon-above-brigade intelligence organizations/*high-level unit intelligence*

organizations and host-nation agencies generally will not provide the resolution required to satisfy the CCIRs, but they can provide enough information initially to focus information collection operations/*intelligence collection operations.*

PEACE OPERATIONS

8-19. 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 and are characterized by irregular forces, a failing government, absence of the rule of law, terrorism, human rights abuses, collapse of civil infrastructure, and the presence of dislocated civilians.

8-20. Attacks by insurgent and terrorist groups are likely, and U.S. forces may have to conduct limited offensive tasks in accordance with rules of engagement against these groups in support of stability tasks. Enemy forces will try to mitigate U.S. information collection/*intelligence collection* capability by adopting command and control; maneuver; fires, intelligence; and logistics TTP that reduce their signature and vulnerability to U.S. collection systems. When conducting IPB and developing a collection plan, the commander considers the enemy's ability to develop low-cost, low-technology counter-information collection solutions/*intelligence collection solutions.*

IRREGULAR WARFARE

8-21. Irregular warfare is a violent struggle among state and non-state 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.

8-22. Types of operations the unit may be employed in to counter irregular warfare are foreign internal defense, support to insurgency, counterinsurgency, combating terrorism, and irregular warfare. Traditionally, these missions are conducted by Special Forces. However, if Special Forces and host-nation forces cannot defeat irregular threats or *adversaries*, conventional friendly forces can assume the lead role. Operation Iraqi Freedom and Operation Enduring Freedom are good examples of this.

8-23. Just as in limited interventions and peace operations, U.S. forces will generally be opposed by an undefined and un-located enemy that operates within complex terrain. The tactics and operational art employed by these forces will vary from conflict to conflict as will the structure of the threats/*adversaries* themselves. In most cases, current intelligence doctrine will not provide all of the tools the unit needs to counter these threats. When this occurs, commanders will have to modify doctrine and develop methods that work in the moment.

8-24. In addition to operations discussed previously, the Army/*Marine Corps* participates in other operations. 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; force protection and operations security are two of the commander's primary intelligence concerns. U.S. national and theater intelligence agencies will provide the initial analysis and information collection/*intelligence collection* support to units preparing for these missions. Additionally, these units may receive limited support from host-nation agencies. The commander and staff should consider both of these sources of information when planning for operations.

This page intentionally left blank.

Chapter 9

IPB Considerations for Unique Environments

IPB CONSIDERATIONS FOR AN URBAN ENVIRONMENT

9-1.   An urban operation is a military operation where manmade construction and high population density are the dominant features. FM 3-06 constitutes Army doctrine for urban operations and discusses IPB considerations in detail. (*For the Marine Corps, see MCWP 3-35.3 for additional information on military operations on urbanized terrain.*) JP 3-06 also provides extensive discussion on IPB in the urban environment.

9-2.   Chapter 4 of this publication discusses terrain analysis conducted for both natural and urban terrain. This section discusses intelligence requirements normally associated with planning considerations for urban operations. The primary terrain effect when operating in an urban environment is the multidimensional nature of the environment. Urban areas are a blend of horizontal, vertical, interior, exterior, and subterranean forms superimposed on the natural relief, drainage, and vegetation. The characteristics of urban environments affect friendly and enemy forces based on their doctrine and tactics. IPB in urban operations evaluates the effect of the characteristics of the urban environment on both.

UNIQUE URBAN CHARACTERISTICS

9-3.   Offensive and defensive tasks/*operations* and stability tasks are the three types of operations conducted by the Army/*Marine Corps* in urban environments. Chapter 7 discusses IPB for these three types of operations. In addition to the general intelligence requirements associated with IPB, urban environment in IPB emphasizes the effects of the following characteristics:

- An urban area is a topographical complex where manmade construction or high population density is the dominant feature. Evaluation of urban areas during IPB is directed on the physical aspects of the area and their effects on operations. This approach is effective when population density is not a factor in the operation. Chapters 3 and 4 discuss how to evaluate the physical aspects of urban terrain and associated civil considerations.

- An urban environment includes the physical aspects of the urban area as well as the complex and dynamic interaction and relationships between its key components—the terrain (natural and manmade), the society, and the supporting infrastructure—as an overlapping and interdependent system of systems. This approach is necessary when population density is a factor in the operations. Chapter 7 discusses IPB support to stability tasks.

EVALUATING THE MILITARY ASPECTS OF THE TERRAIN IN AN URBAN ENVIRONMENT

9-4.   Evaluating the effects of terrain in an urban environment differs in many respects from that of open terrain. The analysis of the five military aspects of terrain defined in the OAKOC/*KOCOA* considerations still applies. This analysis, however, must be in the context of urban battlefield/*battlespace* characteristics.

9-5.   A standard MCOO developed from a military map will not be of much use to leaders at the company level and below. Standard military maps do not have the detail required to allow a thorough analysis of urban terrain. Many standard military maps are old and do not reflect the more recent buildings, streets, and sometimes significant urban growth. In addition, standard maps do not show the subsurface aspects of the urban environment: sewers, subways, and underground water systems. While these military maps show key public buildings and areas such as hospitals, clinics, stadiums, and parks, they do not clearly identify the water facilities, communication facilities, fuel supply, storage facilities, and temporary conditions (for example, construction sites).

9-6.   Terrain analysis software is available to assist in analyzing urban terrain. Familiarization with terrain analysis products and what they can provide assists the G-2/S-2 in explaining and coordinating with geospatial engineers the units' needs in better tailored urban terrain products. A number of sources of information are available such as the U.S. Army Engineer School Reachback Operations Center and National Geospatial-Intelligence Agency, which provide specific types of imagery products, 3-dimensional maps, and types of products to overlay demographics on an urban map.

9-7.   The Center for Army Lessons Learned has documented over 10 years of terrain analysis techniques that are available based off products that were developed from urban operations from multiple campaigns such as Operation Iraqi Freedom, Horn of Africa, Philippines, and from hurricane responses. (See FM 3-34.170/*MCWP 3-17.4* for additional information on geospatial engineering and for urban considerations such as sewage, water, electricity, academics, trash, medical, safety, and other *[SWEAT-MSO]* considerations).

9-8.   Terrain analysis is done on maps or other imagery that contains this information. Additionally, while conducting terrain analysis for an entire city may be effective for major combat operations/*major operations,* it is not useful for the types of operations associated with stability tasks. In stability tasks, analysis focuses on the requirements of small units (squad, platoon, and company) to move from an operating base to an objective. (Chapter 4 fully discusses the evaluation of terrain effects on operations.)

IPB CONSIDERATIONS FOR A COLD WEATHER OR MOUNTAIN ENVIRONMENT

9-9.   In addition to the general requirements associated with IPB, cold weather or mountain environment in IPB emphasizes the effects of cold on personnel and material, the effects of the winter environment on friendly and enemy operations, and planning considerations unique to the winter battlefield/*battlespace* and cold regions. The primary consideration when planning military operations in this type of environment is time. In addition to the increased amount of time consumed in actual movement, allowance must be made for other time-consuming tasks that are not present in temperate zone operations. These include, among others, erecting and striking tents, performing maintenance, constructing roads, starting and warming engines, moving supplies, and hundreds of other small tasks that must be performed while wearing bulky cold weather clothing.

> *Note.* While not normally considered when conducting IPB, time allowances need to be emphasized in cold weather operations.

9-10. Mountain terrain is characterized by steep slopes, great variations in relief, natural obstacles, and a lack of accessible routes—all of which can restrict mobility, increase movement times, limit the effectiveness of some weapons and equipment, and complicate sustainment operations. This physically challenging terrain is the primary terrain effect in cold weather or mountain operations and affects operations in greater detail than it does in temperate or desert environments. Like other regions of the world, mountainous terrain has native inhabitants that can be hostile if not treated properly. To prevent conflict, these inhabitants should be treated as friends and have their customs, taboos, privacy, and property respected.

UNIQUE COLD WEATHER OR MOUNTAIN CHARACTERISTICS

9-11. Offensive and defensive tasks/*operations* are the two types of operations conducted by U.S. forces in mountain environments. Chapter 7 discusses IPB for these two types of operations. (See FM 3-97.6/*MCWP 3-35.1* for a detailed discussion on mountain operations.) In addition to the general intelligence requirements associated with IPB, a mountain environment in IPB emphasizes the effects the following characteristics have on operations:

- Cold
- Altitude.
- Slope.
- Relief.
- Natural obstacles.
- Movement routes.
- Blowing snow and fog.

Cold

9-12. Temperature is the primary terrain effect in cold weather or mountain operations and has the ability to affect operations to a greater detail than it does in temperate or desert environments. In a cold weather environment the effects of weather are directly tied to the use of clothing. The use of cold weather clothing is affected by two types of weather conditions: wet and dry. These conditions are amplified by humidity, coupled with temperature and wind velocity; high humidity (wet conditions); and low humidity (dry conditions).

9-13. Cold-dry conditions occur when average temperatures are lower than 14 degrees Fahrenheit. The ground is usually frozen and snow is usually dry in the form of fine crystals. Strong winds cause low temperatures to seem colder and increase the need for protection of the entire body (wind chill). During these periods, troops should have available additional insulating layers of clothing. This is particularly true when entering static situations from a period of strenuous exercise. Cold-wet conditions also occur when temperatures are near freezing and variations in day and night temperatures cause alternate freezing and thawing. This freezing and thawing is often accompanied by rain and wet snow, causing the ground to become muddy and slushy. During these periods troops should wear clothing that consists of a water-repellent, wind-resistant outer layer and inner layers with sufficient insulation to provide ample protection in moderately cold weather (above 14 degrees Fahrenheit). (See FM 3-97.6/*MCWP 3-35.1* for a detailed discussion on cold conditions in this unique environment.)

Altitude

9-14. The primary effect of mountainous terrain on personnel is exhaustion caused by altitude. The lack of oxygen at high altitudes negatively affects both the mind and the body. This effect is compounded by the rigorous physical activity necessary to move through the terrain. Additionally, factors such a Soldier's/*Marine's* age, fatigue-level, physical conditioning, previous injury, illness, diet, and use of medications can magnify the effect mountainous terrain can have. As Soldiers/*Marines* ascend in altitude, the proportion of oxygen in the air decreases. Without proper acclimatization, this decrease in oxygen saturation can cause altitude sickness and reduced physical and mental performance.

9-15. Soldiers/*Marines* cannot maintain the same physical performance at high altitude that they can at low altitude, regardless of their fitness level. Exposure to altitudes over 3,000 meters can cause changes in senses, moods, and personality. Altitude also affects the lift capability of certain types of aircraft, reducing the load they can carry and, in some cases, preventing their use altogether. Additionally, decreased molecular density in high elevations results in an increase in fuel consumption necessary to gain and maintain lift.

Slope

9-16. In terrain analysis, slope indicates the steepness, incline, or grade. Mountain slopes generally vary between 15 and 45 degrees. Cliffs and other rocky precipices may be near vertical, or even overhanging. Aside from obvious rock formations and other local vegetation characteristics, actual slope surfaces are usually found as some type of relatively firm earth or grass. Grassy slopes may include grassy clumps known as tussocks, short alpine grasses, or tundra (the latter more common at higher elevations and latitudes).

9-17. Many slopes will be scattered with rocky debris deposited from the higher peaks and ridges. Extensive rock or boulder fields are known as talus. Slopes covered with smaller rocks, usually fist-sized or smaller, are called scree fields. Slopes covered in talus often prove to be a relatively easy ascent route. On the other hand, climbing a scree slope can be extremely difficult, as the small rocks tend to loosen easily and give way. However, this characteristic often makes scree fields excellent descent routes. Before attempting to descend scree slopes, commanders should carefully analyze the potential for creating dangerous rockfalls and take necessary avoidance measures.

9-18. In winter, and at higher elevations throughout the year, snow may blanket slopes, creating an environment with its own distinct effects. Some snow conditions can aid travel by covering rough terrain with a consistent surface. Deep snow, however, greatly impedes movement and requires Soldiers/*Marines* be well-trained in using snowshoes, skis, and over-snow vehicles.

9-19. Steep snow-covered terrain presents the risk of snow avalanches as well. Snow can pose a serious threat to Soldiers/*Marines* not properly trained and equipped for movement under such conditions. Avalanches have taken the lives of more Soldiers/*Marines* engaged in mountain warfare than all other terrain hazards combined. Another hazard is becoming "snowblind" due to the snow's high reflectivity value, or albedo. This condition results when solar radiation reflects off the snow and into the eyes of personnel in a snow-covered area. The effect is identical to a sunburn, and all exposed body parts are susceptible to this hazard.

9-20. Commanders operating in arctic and subarctic mountain regions, as well as the upper elevations of the world's high mountains, may be confronted with vast areas of glaciation. Valleys in these areas are frequently buried under massive glaciers and present additional hazards, such as hidden crevices and ice and snow avalanches. The mountain slopes of these peaks are often glaciated and their surfaces are generally composed of varying combinations of rock, snow, and ice. Although glaciers have their own peculiar hazards requiring special training and equipment, movement over valley glaciers is often the safest route through these areas. (ATTP 3-97.11, FM 3-97.6, and *MCWP 3-35.1* contain more information on avalanches and glaciers and their effects on operations.)

Relief

9-21. Relief is the vertical and horizontal dimension of land surface. Mountains are generally classified according to relief. Mountains are commonly classified as low or high, depending on their local relief and, to some extent, elevation. Low mountains have a local relief of 300 to 900 meters (1,000 to 3,000 feet) with summits usually below the timberline. High mountains have a local relief usually exceeding 900 meters (3,000 feet) and are characterized by barren alpine zones above the timberline.

Natural Obstacles

9-22. Natural obstacles associated with mountain terrain include deep defiles, cliffs, rivers, landslides, avalanches, crevices, scree slopes, and areas of dense vegetation or deadfalls, as well as the physical terrain of the mountain itself.

Movement Routes

9-23. Movement routes associated with mountain terrain include manmade and animal trails, streambeds, and the bottom and top of ravines, as well as exiting LOCs.

Blowing Snow and Fog

9-24. Because of the potential of blowing snow and fog, defensive positions are located on high ground, thus forcing the enemy to attack uphill in deep snow. Each weapon is assigned a field of fire oriented at man-height level on the likely enemy approaches. This increases the likelihood of effective fire during periods of restricted visibility caused by blowing snow and fog. Ice or vapor fogs are common in extreme low temperatures. Such fogs are primarily the result of natural phenomena, but also result from many other causes such as vehicle exhausts, cooking, breathing, and weapons firing. Fogs of this nature hang overhead and could be clear markers of a position. They will also limit visibility.

9-25. The observed fire of automatic and direct fire weapons is handicapped considerably by the fog, smoke, and whirling snow caused by muzzle blast. Placing observers away from the weapons positions may be necessary to control the fire. Placing tarpaulins under the guns, or packing or icing the snow, assists in reducing the effect of muzzle blast. Pauses in firing or change of position may be necessary in order to obtain better fire effect.

EVALUATING THE MILITARY ASPECTS OF THE TERRAIN IN A MOUNTAIN ENVIRONMENT

9-26. Paragraphs 9-27 through 9-33 describe how terrain affects operations in a mountain environment. This discussion follows the outline of the terrain analysis process summarized by the OAKOC/*KOCOA* considerations.

Observation and Fields of Fire

9-27. Although mountainous terrain generally permits excellent long-range observation and fields of fire, steep slopes and rugged terrain affect a Soldier's/*Marine's* ability to accurately estimate range and cause large areas to be hidden from observation. The existence of sharp relief and dead space facilitates unobserved approaches, making surveillance difficult despite long-range observation. Four factors that influence what can be seen and hid in mountainous terrain are—

- The ability to observe and identify targets in conditions of bright sunlight.
- The ability to estimate range in clear air.
- The ability to apply wind corrections.
- The ability to shoot accurately up and down vertical slopes.

Avenues of Approach

9-28. In mountainous terrain, there are few easily accessible AAs, and they usually run along valleys, defiles, or the crests and spurs of ridges. This type of geography allows the defender to economize in difficult terrain and to concentrate on dangerous AAs. A typical offensive tactic is to conduct a coordinated assault with the main effort along accessible AAs, and supporting efforts by one or more maneuver elements on difficult and unexpected AAs.

9-29. Normally, high rates of advance and heavy concentration of forces are difficult or impossible to achieve along mountainous AAs. Relief features may create large areas of dead space that facilitate covert movement. Units may use difficult and unlikely AAs to achieve surprise; however, these are extremely high-risk operations and are prone to failure unless forces are well trained and experienced in mountaineering techniques. In mountainous terrain, the analysis of AAs are based on a thorough reconnaissance and evaluated in terms of the following factors:

- Ability to achieve surprise.
- Vulnerability of attack from surrounding heights.
- Ability to provide mutual support to forces attacking on other AAs.
- Effect on rates of march.
- Increase in the number of litter patients and requirements for litter bearers.
- Effect on command and control.
- Ability to support sustainment operations.

● Access to secure rest and halt sites.
● Potential to fix enemy forces and reduce the possibility of retreat.

Key Terrain

9-30. Key terrain generally increases in importance with an increase in elevation and a decrease in accessibility. In the mountains, however, terrain that is higher than that held by the enemy force is often key, but only if the force is capable of fighting there. A well-prepared force capable of maneuver in rugged terrain can gain an even greater advantage over an ill-prepared enemy at higher elevation levels.

9-31. The vast majority of operations in the mountains require that the commander designate decisive terrain in his concept of operations to communicate its importance to his staff and subordinate commanders. In operations over mountainous terrain, the analysis of key and decisive terrain is based on the identification of these features at each of the three operational terrain levels. There are few truly impassable areas in the mountains. Commanders recognize that what may be key terrain to one force may be an obstacle to another force. They also recognize that properly trained combatants can use high obstructing terrain as a means to achieve decisive victories with comparatively small-sized combat elements.

Obstacles

9-32. As stated in paragraph 9-17, obstacles associated with mountain terrain include deep defiles, cliffs, rivers, landslides, avalanches, crevices, scree slopes, and areas of dense vegetation or deadfalls, as well as the physical terrain of the mountain itself. Obstacles vary in their effect on different forces. Evaluation of obstacles considers the degree to which obstacles restrict operations, and at the ability of friendly and enemy forces to exploit the tactical opportunities that exist when obstacles are employed. Manmade obstacles used in conjunction with restrictive terrain are extremely effective in the mountains; however, their construction is costly in terms of time, materiel, transportation assets, and labor. Commanders need to know the location, extent, and strength of natural obstacles so they can be incorporated into their scheme of maneuver.

Cover and Concealment

9-33. The identification and proper use of the cover and concealment provided by mountainous terrain is fundamental to all aspects of mountain operations. The ridge systems found in mountainous terrain may provide unobserved approaches through many areas that are hidden from observation by the vegetation and relief. The difficulties a force encounters in finding available cover and concealment along ridges are fewer than those on the peaks, especially above the timberline. Uncovered portions of an approach leave a force exposed to observation and fire for long periods. A defending force can easily detect movement in this region, leaving an attacking force with three primary options to improve cover and concealment:

● Identify and exploit AAs the defender would consider unlikely because of the difficulty of ascent and descent.
● Conduct movement during periods of restricted visibility.
● Employ overwhelming route security.

IPB CONSIDERATIONS FOR A JUNGLE ENVIRONMENT

9-34. FM 90-5 defines a jungle environment as an area where all seasons are nearly alike. FM 90-5/*FMFM 7-28* divides jungle environments into two zones: those areas close to the equator and those areas away from the equator. In areas close to the equator, rains occur throughout the year. In areas away from the equator, jungles have distinct wet and dry seasons. Both zones have high temperatures (averaging 78 to 95+ degrees Fahrenheit), heavy rainfall (400+ inches annually), and high humidity (90 percent) throughout the year.

9-35. Jungle environments are comprised of densely forested areas, grasslands, cultivated areas, and swamps. The vegetation in the jungle diminishes the ability to see. The jungle canopy compounds this issue by preventing ambient light from penetrating. As a result, night observation devices are mostly ineffective under the canopy. Dense vegetation also limits the ability to hear by trapping noise. The potential lack of

road networks and areas that are impassable to vehicles seriously degrade mounted operations. Casualties who would be ambulatory in other types of terrain will become litter patients in the jungle as they are unable to navigate difficult terrain. This will significantly increase evacuation times and will necessitate diverting some troops to become litter bearers.

9-36. High incidences of rust, corrosion, and fungal infestation caused by high humidity and moisture force strict daily maintenance on weapons and equipment. The jungle climate, relief, and foliage combine to reduce the effective range of radio communication and electronic surveillance. Civil considerations are generally not a major factor when planning and conducting jungle operations, although the existence of noncombatants in the area must be considered, consistent with planning offensive and defensive tasks/*operations*. Like other regions of the world, the jungle has native inhabitants that can be hostile if not treated properly. To prevent conflict, these inhabitants should be treated as friends and have their customs, taboos, privacy, and property respected.

UNIQUE JUNGLE ENVIRONMENT CHARACTERISTICS

9-37. Offensive and defensive tasks/*operations* are the two types of operations conducted by U.S. forces in jungle environments. Chapter 7 discusses IPB for these two types of operations. (See FM 90-5/*FMFM 7-28* for details on jungle environment conditions.) In addition to the general intelligence requirements associated with IPB, a jungle environment in IPB emphasizes the effects the following characteristics have on operations:

- Mosquitoes, sandflies, and other insects.
- Leeches.
- Poisonous snakes.
- Crocodiles and caymans.
- Wild animals.
- Poisonous vegetation.
- Waterborne diseases.
- Fungal diseases.

EVALUATING MILITARY ASPECTS OF THE TERRAIN IN A JUNGLE ENVIRONMENT

9-38. Paragraphs 9-39 through 9-43 describe how terrain affects operations in a jungle environment. This discussion follows the outline of the terrain analysis process summarized by the OAKOC/*KOCOA* considerations.

Observation and Field of Fire

9-39. Observation and fields of fire in the jungle are limited because of dense vegetation. Often, observation and fields of fire must be created or improved upon. When this is necessary, Soldiers/*Marines* clear away only what is absolutely necessary in order to retain as much natural concealment as possible. When in properly constructed fighting or observation positions, the Soldier's/*Marine's* eyes and weapon will be at ground level. In this way, the Soldier/*Marine* is concealed from the enemy, is protected by cover, but still can detect any approaching enemy. If a small tree is in a Soldier's/*Marine's* field of fire, only the branches that deny observation should be removed. The cuttings on the tree are darkened with mud. Overly cleared areas or fresh, improperly concealed cuttings are easy to spot. Additionally, restricted lines of sight can prevent visual contact between units, interlocking fires, and the use of tube-launched optically tracked munitions. Adjustment of indirect fire support is difficult due to limited visibility and may have to be accomplished by sound.

Avenues of Approach

9-40. Moving over jungle terrain is difficult because of the lack of clear AAs or routes. There may not be adequate topography survey or map data to identify AAs during planning because of the isolation of jungle environments, the rugged ground, and the presence of a canopy and dense forest. When using aerial photography to identify AAs, these photographs should be less than four months old because trails and

other clearings can be overgrown during that time. In many cases, AAs may need to be created. The use of indigenous people (military and civilian) to identify existing AAs and movement routes is an effective way to quickly identify these terrain features. AAs in the jungle include rivers, streams, valley floors, ridgelines, animal trails, and trails made by man. Because sound in the jungle does not travel far, movement along AAs is generally closer than believed.

Key Terrain

9-41. The aspects of terrain and enemy discussed above result in fewer set-piece battles. Rather than conventional attacks conducted against conventional defenses, jungle battles are more often ambushes, raids, and meeting engagements. Battles are not fought for high ground as frequently as conventional battles. Orientation is on the enemy rather than on the terrain. Hills in the jungle are often too thickly vegetated to permit observation and fire and, therefore, do not always qualify as key terrain. In the jungle, roads, rivers and streams, fording sites, and landing zones are more likely to be key terrain features.

Obstacles

9-42. Rivers and other large bodies of water as well as cliffs are the predominant natural obstacles in a jungle environment. Depending on the type of operation, swamps and heavily forested areas may become obstacles as well.

Cover and Concealment

9-43. Jungle terrain generally provides good concealment from both air and ground observation because of dense vegetation. Natural cover (trees, rocks, logs) provides adequate cover from small arms fire but provides only minimal protection from grenades and indirect fire if not improved upon. When constructing fighting positions, ample natural resources are available to build cover that blends in with the surroundings. Lowland and swamp areas provide good concealment but poor cover because they are generally too wet to permit the digging of fighting positions. Tree limbs can block or deflect mortars, grenades, and small arms fire.

IPB CONSIDERATIONS FOR A DESERT ENVIRONMENT

9-44. FM 90-3/*MCWP 3-35.6* defines a desert environment as an arid, barren region incapable of supporting normal life due to lack of water. Temperatures vary according to latitude and season, from over 136 degrees Fahrenheit in the deserts of Mexico and Libya to the bitter cold of winter in the Gobi (East Asia). In some deserts, day-to-night temperature fluctuation exceeds 70 degrees Fahrenheit. Desert terrain also varies considerably from place to place, the sole common denominator being lack of water with its consequent environmental effects, such as sparse, if any, vegetation.

9-45. The basic land forms are similar to those in other parts of the world, but the topsoil has been eroded due to a combination of lack of water, heat, and wind to give deserts their characteristic barren appearance. The bedrock may be covered by a flat layer of sand or gravel, or may have been exposed by erosion. Other common features are sand dunes, escarpments, wadis, and depressions. Although civil considerations are generally not a major factor when planning and conducting desert operations, consider the impact of noncombatants in the area; consistent with planning offensive and defensive tasks.

UNIQUE DESERT ENVIRONMENT CHARACTERISTICS

9-46. Offensive and defensive tasks/*operations* are the two types of operations conducted by U.S. forces in desert environments. Chapter 7 discusses IPB for these two types of operations. In addition to the general intelligence requirements associated with IPB, a desert environment in IPB emphasizes the effects the following characteristics have on operations:

- Water.
- Terrain.
- Heat and cold.
- Wind.
- Dust and sand.

- Humidity.
- Temperature variations.
- Thermal cross-over.
- Optical path bending.
- Static electricity.
- Solar radiation.

Water

9-47. Although water can be found in the desert, and the location of known and possible water sources is identified during IPB, carrying enough water to accomplish the mission is a primary planning consideration when operating in the desert. This is because even though water is there it may be impossible to find or reach it. If water is accessible, it may not be potable. Also, dependency on local water sources can make movement predictable and expose the force to enemy attack. When planning how much water to carry, consider the following uses:

- Personnel (drinking only).
- Personnel (uses other than drinking).
- Medical treatment.
- Vehicle and equipment cooling systems.
- Decontamination.
- Food preparation.
- Construction.
- Laundry.

Terrain

9-48. Terrain varies from nearly flat with high trafficability, to lava beds and salt marshes with little or no trafficability. Tracked vehicles are well suited for desert operations. Wheeled vehicles may be acceptable as they can go many places that tracked vehicles can go; however, their lower speed average in poor terrain may be unacceptable during some operations. Vehicles should be equipped with extra fan belts, tires (and other items apt to malfunction), tow ropes (if not equipped with a winch), extra water cans, and desert camouflage nets. Air-recognition panels, signal mirrors, and a tarpaulin for crew sun protection are very useful.

Heat and Cold

9-49. Heat affects personnel as well as weapons and equipment. The extreme heat of the desert can cause heat exhaustion and heatstroke and puts troops at risk of degraded performance. For optimum mental and physical performance, body temperatures must be maintained within narrow limits. Therefore, it is important that the body loses the heat it gains during work. The amount of heat accumulation in the human body depends upon the amount of physical activity, level of hydration, and the state of personal heat acclimatization. Unit leaders must monitor their troops carefully for signs of heat distress and adjust schedules, work rates, rest, and water consumption according to conditions.

9-50. The desert can be dangerously cold, particularly at night. The dry air, wind, and clear sky can combine to produce bone-chilling discomfort and even injury. The ability of the body to maintain body temperature within a narrow range is as important in the cold as in the heat. Loss of body heat to the environment can lead to cold injury; a general lowering of the body temperature can result in hypothermia, and local freezing of body tissues can lead to frostbite. Hypothermia is the major threat from the cold in the desert, but frostbite also occurs. *This effect is mitigated by periods of extensive cloud cover—METOC forecasters will factor this into the planning in a desert environment during bivouac operations.*

Wind

9-51. Desert winds, by their velocity alone, can be very destructive to large and relatively light materiel, such as aircraft, tents, and antenna systems. To minimize the possibility of wind damage, materiel should be sited to benefit from wind protection and be firmly picketed to the ground. Desert winds also move dust and sand from the desert floor into sensitive areas of weapons and equipment, thus causing malfunction and damage.

Dust and Sand

9-52. Dust and sand are the greatest threats to the efficient functioning of weapons and equipment in the desert. It is almost impossible to avoid particles settling on moving parts and acting as an abrasive. Sand mixed with oil forms an abrasive paste that destroys the working of fine parts. The existence of dust and sand requires additional time and resources for maintenance in accordance with applicable maintenance manuals.

Humidity

9-53. Some deserts are humid. Where this is the case, humidity plus heat causes rust on bare metal and mold in enclosed spaces such as optics. Bare metal surfaces on equipment not required for immediate use must be kept clean and very lightly lubricated. Items such as optics should be stored in dry conditions; those in use are kept where air can circulate around them and should be purged at frequent intervals. Aircraft are washed daily, particularly if there is salt in the air, using low-pressure sprays.

Temperature Variations

9-54. Temperature variation is the change in ambient temperature between daytime and nighttime hours. In deserts with relatively high dew levels and high humidity, overnight condensation can occur wherever surfaces (such as metal exposed to air) are cooler than the air temperature. Condensation can affect such items as optics, fuel lines, and air tanks. Draining fuel lines both at night and in the morning (whenever necessary) and cleaning optics and weapons frequently can mitigate the effect of temperature variation.

Thermal Cross-Over

9-55. Thermal cross-over is the natural phenomenon that normally occurs twice daily when temperature conditions are such that there is a loss of contrast between two adjacent objects on infrared imagery. Small arms may be affected by thermal cross-over. Soldiers/*Marines* should modify direct fire control procedures, as needed. Modern U.S. tanks are designed to compensate for thermal cross-over. Enemy tanks may not have this capability.

Optical Path Bending

9-56. Optical path bending, also called refraction, occurs when light passes through one medium to another. This condition can exist when the air is warmer above the desert floor. Heat shimmer is an indication that refraction exists. Refraction can occur during daytime conditions with a clear sky over flat terrain with winds less than 10 miles per hour. Refraction can also occur during nighttime conditions with a clear sky over flat terrain with winds less than 4 miles per hour. Refraction can affect the ability of direct fire weapons systems to engage targets beyond 1,500 meters.

Static Electricity

9-57. Static electricity is the buildup of an electric charge on the surface of objects that remains until the charge is bleed off to a ground or neutralized by discharge. Static electricity is prevalent and poses a danger in the desert. It is caused by atmospheric conditions, coupled with an inability to ground out, due to dryness of the terrain. It is particularly prevalent with aircraft or vehicles having no conductor contact with the soil. The difference of electrical potential between separate materials may cause an electrical discharge between them when contact is made; if flammable gases are present, they may explode and cause a fire.

Solar Radiation

9-58. Solar radiation is generated by the sun's rays. Solar radiation can be detrimental to some plastics, lubricants, pressurized gases, chemicals, and infrared tracking and guidance systems. These materials must be kept out of constant direct sunlight to avoid damage. Over exposure to solar radiation can cause sunburn and damage eyesight. Soldiers/*Marines* need to implement personal protective measures such as applying sun screen and using sunglasses to avoid injury.

EVALUATING MILITARY ASPECTS OF THE TERRAIN IN A DESERT ENVIRONMENT

9-59. Paragraphs 9-60 through 9-64 describe how terrain affects operations in a desert environment. This discussion follows the outline of the terrain analysis process summarized by OAKOC/*KOCOA* considerations.

Observation and Fields of Fire

9-60. Observation and fields of fire are generally excellent in most desert areas. The atmosphere is stable and dry, allowing unrestricted view over vast distances. Flat desert terrain permits direct-fire weapons to be used to their maximum range. Open terrain and a predominantly clear atmosphere generally offer excellent long-range visibility; however, at certain times of the day visibility may be limited or distorted by heat. Additionally, the desert is not absolutely flat, so weapons are sited to provide mutual support. Dead space can also be a problem. Even though the landscape appears flat, upon close inspection it can be undulating with relatively deep wadis and depressions creating IVLs. These areas should be covered by indirect fire.

Avenues of Approach

9-61. AAs are not clearly defined in desert environments. AAs may be wider and of greater availability permitting maneuver from virtually any direction, making wide envelopments possible. Modern sensor technology, limited natural concealment, and improved observation make the element of surprise a challenge. In mountainous and canyon topography avenues are more limited, and the wadis and valleys are likely to be the only possible access routes. Any roads that do exist are probably in valleys.

Key Terrain

9-62. Key terrain in the desert can be manmade features, mountain passes, high ground, and/or valleys. Staff sections provide recommendations of key terrain so that these are analyzed for their benefit to friendly and enemy/*adversary* forces. For example, for the S-6, the only piece of high ground in the AO may be key due to the limitations of frequency modulation communications that require retransmission. Some deserts provide high ground that is crucial for observation. In an open or arid environment, a draw or wadi could be viewed as key terrain. The relative flatness and great distances of some deserts make even large sand dunes dominant features. Flat areas in otherwise rough terrain are vital for airborne operations and aerial resupply. Key terrain in the desert can also include facilities that could provide water or villages.

Obstacles

9-63. There are natural obstacles in the desert. The wadis and steep slopes of escarpments, mountains, hills, and dunes hinder cross-country movement. Sand dunes may stretch for miles and prevent direct movement across their length. Sand dunes are often more than 100 feet in elevation and consist of loose sand with high, steep downwind faces that make vehicular traversing next to impossible. Aerial reconnaissance immediately before any large movement is advisable because sand dunes migrate with shifting winds, and they may not be where maps or even photographs show them. Additionally, dry lake beds and salt marshes may have a crust on the top that can deceive a vehicle driver. A top crust forms on the surface, but below the crust the soil is moist, which is similar to marsh conditions. The surface may appear to have good trafficability, but the crust will collapse with the weight of a vehicle and the vehicle becomes mired. Sandy deserts are ideal for employing minefields. Although windstorms can reveal previously buried mines, these mines can still channel movement and deny access to certain areas.

Cover and Concealment

9-64. Areas in the desert may be wide and provide very limited cover and concealment. Flat sandy terrain provides little, if any, natural cover or concealment, especially from aerial attack or reconnaissance. Ground concealment and protection from fire can be found behind dunes or in wadis. Some arid regions have vegetation that can provide limited concealment from ground observation. In rocky, mountainous deserts, cover and concealment are best found behind boulders and in crevices. Daytime vehicular movement will likely be visible and eliminate the possibility of surprise, as dust trails created by the traffic can be spotted for miles. At night noise and light discipline is critical, as both sound and light travel great distances because of the unobstructed flatness of the terrain and atmospheric stability. Camouflage can be effectively employed to improve on natural cover and concealment.

IPB SUPPORT TO CYBER ELECTROMAGNETIC ACTIVITIES/ *CYBERSPACE OPERATIONS*

9-65. **Cyberspace** is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12). Cyber capabilities and leveraging cyberspace are critical for the future force to be able to command and control on-the-move while reducing operational risk. Cyberspace can be viewed in three layers (physical, logical, and cyber-persona), all of which can be integrated into the traditional IPB process and aforementioned intelligence disciplines:

- The physical network layer includes the geographic component and the physical network components. The geographic component is the physical location of elements of the network. The physical network component includes all the hardware and infrastructure (wired, wireless, optical) that support the network and the physical connections (wires, cables, radio frequency, routers, servers, and computers). These items are subject to lethal as well as cyber threats.
- The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network. An example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator.
- The cyber-persona layer consists of the people actually on the network.

9-66. The G-2/S-2 will work closely with the G-6/S-6, the defense information agency, and related entities to ascertain enemy cyber TTP, AAs, and enemy COAs. For U.S. Army, the G-2/S-2 will also work closely with the cyber electromagnetic activities elements and the local regional computer incident response team.

9-67. The G-6/S-6 assists the G-2/S-2 in IPB by drawing on intelligence products focused on vulnerabilities and threats in the cyberspace domain and the electromagnetic spectrum. This process provides the commander with an assessment of the operational environment, which includes the cyberspace domain and electromagnetic spectrum within its assigned physical AO. For U.S. Army, the cyber electromagnetic activities element also assists with this assessment.

9-68. The AO, area of influence, and area of interest are defined terms that include the relevant portions of the cyberspace domain and the electromagnetic spectrum. The AO involves a portion of the cyberspace domain as part of its whole. An area of influence may be a geographic area, a portion of the cyberspace domain, or both. The cyberspace domain and electromagnetic spectrum are key terrain considerations.

9-69. The G-6/S-6 assists with the assessment of enemy cyberspace and electromagnetic warfare capabilities, to include an examination of doctrinal principles and TTP, and observed patterns of enemy operations in the cyberspace domain and electromagnetic spectrum leading to a determination of possible enemy COAs. An enemy or adversary COA may involve AAs that reside solely within the cyberspace domain or electromagnetic spectrum themselves. Intelligence in the cyberspace domain involves extensive coordination, and this effort is dependent on the operating environmentand available analytical resources. For U.S. Army, the cyber electromagnetic activities element also provides this assistance to the G-2/S-2.

9-70. See JP 3-12 for more information on IPB considerations for the cyberspace domain and cyberspace operations. For the Army, see FM 3-38 for more information on cyber electromagnetic activities necessary for IPB.

Chapter 10

IPB Considerations for Unique Missions

CONDUCTING IPB IN SUPPORT OF COUNTERDRUG ACTIVITIES

10-1. Unique missions are those operations not routinely conducted by the Army/*Marine Corps*. IPB, with modification, supports the planning for these operations. This chapter discusses IPB tactics and procedures for counterdrug, counter-IED, site exploitation, peace operations, and humanitarian, disaster relief, and noncombatant evacuation operations.

10-2. The purpose of Army/*Marine Corps* support to counterdrug activities is to assist law enforcement agencies in the identification and interdiction of suspected drug trafficking within and along the approaches to the continental United States. Planning for a counterdrug support mission requires the same IPB as any other military operation. To the greatest extent possible, estimates are coordinated with supported law enforcement agencies.

10-3. When conducting intelligence activities inside the United States, or targeted at U.S. persons or groups, additional restrictions and requirements apply. Furthermore, Army intelligence employees may only participate in counterdrug missions inside the United States that have been approved under Procedure 12 of AR 381-10.

10-4. JP 3-07.4 constitutes the current doctrine the Army/*Marine Corps* uses to conduct counterdrug activities. In order to conduct IPB required for this type of operation, commanders and staffs must understand the nature of counterdrug activities and the intelligence requirements associated with them.

10-5. **Counterdrug activities** are those measures taken to detect, interdict, disrupt, or curtail any activity that is reasonably related to illicit drug trafficking. This includes, but is not limited to, measures taken to detect, interdict, disrupt, or curtail activities related to substances, materiel, weapons, or resources used to finance, support, secure, cultivate, process, or transport illegal drugs (JP 3-07.4). Counterdrug activities conducted by the Army/*Marine Corps* are normally conducted as part of a joint force. Planning for counterdrug activities below the strategic level is conducted using the joint operation planning process (JOPP). Step 2 of the JOPP is mission analysis. IPB begins during step 2 and continues throughout the JOPP.

10-6. IPB support to counterdrug activities is conducted using the IPB process. This is an intellectual process of analysis and evaluation that is modified from traditional military joint intelligence preparation of the operational environment. Using the IPB process identifies likely trafficking routes and the most efficient allocation of scarce resources to locate, track, and apprehend drug traffickers.

10-7. In steps 1 and 2 of the IPB process, in addition to identifying and describing the enemy, terrain, and weather concerns, the staff evaluates the effect the population may have on friendly and drug trafficking operations to—

- Identify and describe the AOs and areas of interest.
- Identify and describe significant threat/*adversary*, terrain and weather, and civil considerations characteristics of the operational environment.

10-8. Discussion of the threat/*adversary* should be limited to identifying all drug trafficking networks for further analysis and discussion during steps 3 and 4 of the IPB process. Discussion of terrain and weather should be limited to identifying significant effects of these factors. Discussion of civil considerations, however, should discuss in detail how these considerations affect friendly and drug trafficking operations. This analysis focuses on identifying—

- Whether the local population is supporting drug trafficking and how. (This includes governmental, civil, military, and law enforcement organizations.)
- If the local population is supporting drug trafficking organizations, how can friendly forces separate them from these organizations and co-opt them into friendly operations?

TERRAIN ANALYSIS

10-9. Terrain analysis conducted in support of counterdrug activities is conducted as part of the IPB process and follows the OAKOC/*KOCOA* considerations. Terrain analysis focuses on the effects terrain can have on the operations of friendly forces and on drug traffickers. The standard terrain products and work aids used during traditional IPB can be used as part of IPB support to counterdrug activities without modification, specifically the MCOO and terrain effects matrix. (Refer to chapter 4 for additional details on these products.)

WEATHER ANALYSIS

10-10. Weather analysis conducted in support of counterdrug activities is conducted as part of the traditional IPB process. Weather analysis focuses on the effects weather can have on the operations of friendly forces and on drug traffickers. The standard weather products and work aids used during the traditional IPB process can be used as part of IPB support to counterdrug activities without modification. These products are—

- Weather forecast and conditions chart.
- Weather effects chart/*operational impacts chart*.
- Lunar illumination data.

THREAT EVALUATION

10-11. During step 3 of the IPB process—evaluate the threat/*adversary*—intelligence personnel conducting IPB support to counterdrug activities conduct a functional analysis of drug trafficking networks to develop a database that includes data on—

- Organizational structure.
- Locations (AOs).
- Disposition.
- TTP.
- Command and control structure.
- Intelligence-gathering capabilities.
- Counterintelligence capabilities.
- Logistics operations.
- Funding and finance.
- Personal data on known smugglers.
- Capabilities and limitations.

10-12. Threat/*adversary* evaluation is critical to threat integration. Without a complete and accurate evaluation of drug trafficking networks, threat/*adversary* integration efforts will be flawed and will result in inaccurate intelligence estimates being used to plan operations.

10-13. In step 4 of the IPB process—determine threat/*adversary* COAs—intelligence personnel conducting IPB analyze what is known about the drug traffickers' modes of operation. The intelligence personnel integrate that analysis with the analysis conducted in the operational area evaluation and terrain

and weather analysis to make a judgment on when, how, and where the drug traffickers will move. The following products are developed during threat integration:

- Drug trafficking situation overlay that depicts—
  - Primary and alternate drug smuggling routes.
  - Escape routes.
  - Crossing sites (includes official entry points, as well as obstacles that must be navigated, such as rivers, other).
  - Locations of drug cultivation, manufacture, and storage.
  - Locations and identity of groups and/or individuals—
    - Directing drug trafficking operations.
    - Funding drug trafficking operations.
    - Providing logistics support to drug trafficking operations.
    - Providing intelligence and security support to drug trafficking operations.
    - Transporting drugs.
- Drug trafficking situation statements that describe the battlefield/*battlespace* geometry and activities depicted on the drug trafficking situation overlay.
- HVTL identifying the individuals, organizations, and systems associated with the drug trafficking situation overlay.
- Drug traffickers' TTP list describing all TTP associated with the drug-smuggling operation.
- Indicator list describing the indicators associated with specific types of drug activity.
- Drug trafficking event template that identifies the locations where potential activities may occur relating to drug trafficking.

10-14. The development of all of these products is critical to the development of the decision support template, information collection overlay/*intelligence collection overlay*, and the overall development of a successful interdiction strategy. The format and construct of these products are similar to the threat-related products constructed as part of traditional IPB. Table 10-1 shows this comparison.

Table 10-1. IPB products in support of counterdrug activities

IPB products for counterdrug activities	*Traditional IPB products*
Drug trafficking situation overlay	Enemy situation overlay
Drug trafficking situation statement	Enemy course of action statement
High-value target list	High-value target list
Drug trafficker tactics, techniques, and procedures list	Threat/*adversary* tactics, techniques, and procedures list
Indicator list	Indicator list
Drug trafficking event template	Event template

IPB SUPPORT TO COUNTER-PROLIFERATION

10-15. The proliferation of weapons of mass destruction remains a threat, which adds an even more deadly complication to the environments where U.S. forces potentially have to operate, and may create additional mission requirements. The mission to counter the weapons of mass destruction threat is not limited to defeating ballistic missiles, interceding to prevent weapons of mass destruction proliferation, and ensuring the security of weapons easily smuggled in small quantities. It extends to addressing advanced weapons programs such as nuclear, chemical, and biological munitions that can be protected by a host of defensive and deception techniques. U.S. forces deny threat/*adversary* sanctuaries, destroy critical enemy capabilities, recover personnel or sensitive equipment, safeguard and/or seize weapons of mass destruction or associated materials, and cause the threat/*adversary* to disperse forces.

10-16. Potential proliferation of weapons of mass destruction material, weapons, delivery means, and technology could quickly become a global crisis posing a physical threat. Prevention and countering the

threat/*adversary* is a high priority for U.S. forces. Protection and detection are key elements of countering weapons of mass destruction proliferation.

IPB SUPPORT TO COUNTER-IMPROVISED EXPLOSIVE DEVICE OPERATIONS

10-17.   An IED attack is the result of a planned tactical operation with several key elements that work in a coordinated and synchronized manner to attain a desired result. Successful IED defeat operations begin with a thorough understanding of the enemy and the common activities associated with an IED attack. Activities include leadership, planning, financing, materiel procurement, bombmaking, target selection, recruiting, and attack execution. A holistic approach to understanding the requirements of an IED attack assists commanders and planners in identifying vulnerabilities.

10-18.   IED defeat operations are unit activities that are planned, prepared for, executed, and assessed to identify, deter, and mitigate the effects of an IED attack. As part of the broader mission of the unit, these activities are conducted to predict, detect, prevent, avoid, neutralize, and protect the force from IED attack. IED defeat operations are not a staff- or function-specific responsibility. IED defeat cuts across the warfighting functions and requires the entire staff to consider all options to eliminate the IED threat. The goal is to identify and defeat enemy leaders, suppliers, trainers, enablers, and executors responsible for the employment of IEDs, while protecting the force from the effects of an IED attack.

10-19.   Counter-IED operations are those actions taken by a command to prevent IED attacks on U.S. forces; multinational partners; host-nation governmental, civil, military, law enforcement agencies; and host-nation civilian populations. Counter-IED operations are integrated into any operation where there is an IED threat. The primary components of counter-IED operations are attack the network, defeat the device, and train the force. (See ATP 3-90.37/*MCIP 3-17.02* for more information on counter-IED operations.)

- Attack the network, which aims to find and eliminate bombmakers and their sources of supply—
  - Identifies and locates sources of bombmaking materials.
  - Identifies and locates bombmaking facilities.
  - Determines supply routes used to transport bombmaking material.
  - Determines methods of transport for bombmaking material.
  - Identifies and locates bombmakers.
  - Identifies and locates entities financing IED operations.
  - Locates and identifies enemy forces using IEDs as part of their operations.
  - Identifies enemy current TTP and changes to TTP associated with IEDs.
- Defeat the device, which aims to identify and/or detonate the IED at the point of attack prior to its being used successfully by the enemy—
  - Identifies what types of IEDs are being used.
  - Identifies where IEDs are being used.
  - Identifies the TTP associated with the employment of each IED.
  - Identifies the locations where the enemy will employ IEDs.
- Train the force aims at educating units and personnel on the types of devices being used to attack them; the TTP the enemy is employing; and the TTP friendly forces can use to recognize and protect themselves from IEDs. Train the force incorporates the elements of defeat the device component into IED training.

IPB SUPPORT TO SITE EXPLOITATION AND/OR EXPLOITATION OF SENSITIVE SITES

10-20.   The Army/*Marine Corps*, during operations in Iraq and Afghanistan, routinely conducted site exploitation and/or exploitation of sensitive sites against strategically important sites of significant intelligence value. A sensitive site is a geographically limited area with special diplomatic, informational,

military, or economic sensitivity to the United States. Recent examples of sensitive sites include the following:

- War crimes sites.
- Critical hostile government facilities.
- Areas suspected of containing persons of high rank or those sought after by the U.S. Government.
- Document storage areas containing enemy or terrorist classified files, research, and production facilities involving breakthrough technologies.
- Any place containing or suspected to have enemy research, production, storage, employment, or use of CBRN weapons.

10-21. Exploitation of these types of sites can involve exploiting personnel, documents, electronic files, biometrics, forensics, and other foreign materiel captured at the site for intelligence value, while neutralizing the threat/*adversary* posed by the site or any of its contents.

SITE EXPLOITATION

10-22. A commander conducts site exploitation to—

- Answer information requirements (usually the CCIRs).
- Gather intelligence for future operations (already planned or not yet anticipated).
- Gather evidence to support prosecution.

10-23. Site exploitation is normally an implied task associated with other missions, and planning for site exploitation usually occurs during the planning of those missions. (See ATTP 3-90.15 for more information on site exploitation operations.) Intelligence requirements generally associated with site exploitation are identifying—

- Characteristics and limits of the AO (search area).
- Terrain analysis of military characteristics of the terrain leading to and including the search area (analysis of surface, subsurface, and supersurface areas).
- Location, type, size, and interior schematics (floor plan) of buildings in the search area.
- Location, size, and capabilities of security forces in and around the search area.
- Location and identity of high-value individuals within the search area.
- Enemy TTP for concealing information, material, or persons. For example:
    - Creating false walls in buildings.
    - Burying containers.
    - Using women and children as couriers.
- Enemy TTP for reacting to the presence of U.S. forces. For example:
    - Using security forces to delay, disrupt, or destroy.
    - Using reconnaissance assets.
    - Using fire support (mortars).
    - Using boobytraps and IEDs.
    - Using obstacles.
    - Destroying material or information media.
    - Evacuating information media, material, or persons.
    - Using escape routes.
- The presence and attitude of noncombatants in and around the search area.
- Location of indigenous law enforcement facilities.
- Location of indigenous security forces (military and law enforcement).
- Objects or entities listed on the no-strike list.
- Presence of cultural sites and natural resources in the search area.
- Presence of critical infrastructure.

- Environmental hazards in and around the search area.
- Constraints. For example:
    - Rules of engagement.
    - Search restrictions.
    - Use of force.
- Status and availability of—
    - Weapons technical intelligence collectors.
    - Multifunctional teams.
    - Forensic collection kits.
    - Document and media exploitation assets.
    - Linguists and their associated classifications.
    - Forensic laboratories and facilities.
    - Equipment, such as the biometric identity management tool, remote detection assets, and voice language translation tools.
    - Theater assets that can assist with or conduct exploitation of sensitive sites.

EXPLOITATION OF SENSITIVE SITES

10-24. Exploitation of sensitive sites differs from site exploitation in that the site contains information, materials, or persons that could cause embarrassment, compromise, or threat to U.S. security or national interests. Additionally, sensitive sites can be more dangerous, or present different types of danger, to Army/*Marine Corps* personnel. This is especially true of research and development facilities where the presence and concentration of CBRN material can cause immediate and long-term harm to personnel. Equally as important, exploitation of these sites may be beyond the capability of a tactical unit.

10-25. Some sensitive sites will also be protected sites under international law. Intelligence personnel must take extra care not to cause damage or degradation to a protected site. If exploitation is likely to result in damage, consult the servicing Judge Advocate for further guidance. In addition to intelligence requirements associated with site exploitation, intelligence requirements generally associated with sensitive site exploitation are identifying—

- Possible presence of CBRN.
- Possible CBRN facility.
- Locations containing evidence of war crimes.
- Terrorist training camps.
- Enemy prisoner of war locations.
- Research and production facilities involving breakthrough technologies.
- Government buildings and infrastructure of strategic value.
- Official government residences.
- Sites suspected of harboring high-value individuals or other enemy leaders.

IPB SUPPORT TO PEACE OPERATIONS

10-26. Peace operations include—

- Peacekeeping.
- Peace enforcement.
- Peace building.
- Peacemaking.
- Conflict prevention.

Note. Only the IPB considerations for peacekeeping and peace enforcement are discussed below. (See FM 3-07.31/*MCWP 3-33.8* for multi-Service TTP on peace operations.)

PEACEKEEPING

10-27.   The objectives of peace operations include keeping violence from spreading, containing violence that has occurred, and reducing tension among factions. Accomplishing these objectives creates an environment in which other instruments of national power are used to reduce the level of violence to stable peace. Peace operations are usually interagency efforts. They require a balance of military and diplomatic resources. (JP 3-07.3 contains joint TTP for peace operations.)

10-28.   **Peacekeeping** is defined as military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement (JP 3-07.3).

Define the Operational Environment/*Battlespace Environment*

10-29.   Consider the following to define the operational environment/*battlespace environment*:
- Identify and locate all outside influences; for example, political groups, media, and any third-nation support.
- Identify significant sociocultural and economic issues. These might include such things as living conditions, religious beliefs, cultural distinctions, allocation of wealth, and political grievances.
- Identify the legal mandates, geographical boundaries, rules of engagement, and other limitations that may affect parties involved.
- Identify the organization and structure of all players in the AO and area of interest.
- Review the history of the AO and area of interest pertinent to the current situation.
- Be aware of the media and its influence on the population of both the AO and area of interest.

Describe Environmental Effects on Operations/*Describe the Battlespace Effects*

10-30.   Consider the following to describe the environmental effects on operations/*describe the battlespace effects*:
- Sociocultural information (for example, root cause of conflict, desire for conflict resolution).
- Weather and terrain. Analyze the effects of weather on visibility among all parties, as well as its effect on activities such as demonstrations and on mobility and operations. Identify terrain that allows all threat/*adversary* groups access to the peacekeeper and its effect on mobility and the separation of the various factions. Analyze the terrain to identify likely current disposition of threat/*adversary* groups.
- Legal (for example, legal COAs available to all involved parties, the likelihood of belligerents to obey laws and treaty provisions, legal limits on use of force).
- Food distribution warehouses or food sources.
- Boat docks to unload relief supplies.
- Civilian relief agencies.
- Nomadic campsites.
- Sources of water.
- Sites of religious, political, or cultural significance.
- Communication structure and capabilities of the parties within the AO.

Evaluate the Threat/*Adversary*

10-31.   Use the following IPB considerations to evaluate the threat/*adversary*:
- Identify all threat/*adversary* groups. Determine which factions or groups are likely to violate the peace.
- Determine any relationships among the groups or factions.
- Identify political organizations and their objectives.
- Identify political and religious beliefs that directly affect or influence the conduct of the belligerents.

- Identify threat/*adversary* military capabilities and key personnel.
- Identify local support to all threat/*adversary* parties.
- Identify threat/*adversary* tactics for the offense and defense.

Determine Threat/*Adversary* Courses of Action

10-32.   Use the following IPB considerations to determine threat/*adversary* COAs:
- Template threat/*adversary* actions, to include combat operations/*major operations*, support functions, terrorist acts, and any other actions that would violate the peace.
- Template threat/*adversary* responses to violations of the peace.
- Template the responses of the threat/*adversary*, the host-nation or foreign-nation government, and local indigenous populations and institutions to friendly force peacekeeping operations.
- Template or analyze faction activity as it relates to past events to analyze potential trends.
- Wargame terrorist actions and other activities where belligerents could reasonably avoid being held accountable.

Peace Enforcement

10-33.   **Peace enforcement** is the application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order (JP 3-07.3).

Define the Operational Environment/*Battlespace Environment*

10-34.   Consider the following to define the operational environment/*battlespace environment*:
- Identify and locate all outside influences; for example, political groups, media, and any third-nation support.
- Identify significant sociocultural and economic issues that may potentially adversely affect the effort to enforce the peace. These might include such things as living conditions, religious beliefs, cultural distinctions, allocation of wealth, and political grievances.
- Identify the legal mandates, geographical boundaries, rules of engagement, and other limitations that may affect parties involved. Determine which resolutions are being enforced.
- Identify the organization and structure of all players in the AO and area of interest.
- Review the history of the AO and area of interest pertinent to the current situation.
- Be aware of the media and its influence on the population of both the AO and area of interest.

Describe Environmental Effects on Operations/*Describe the Battlespace Effects*

10-35.   Consider the following to describe environmental effects/*battlespace effects*:
- Sociocultural information (for example, root cause of conflict, desire for conflict resolution).
- Weather and terrain. Analyze the effects of weather on visibility among all parties, as well as its effect on activities such as demonstrations and on mobility and operations. Identify terrain that allows all threat/*adversary* groups access to the peace enforcer and its effect on mobility and the separation of the various factions. Analyze the terrain to identify likely current dispositions of threat/*adversary* groups.
- Legal (for example, legal COAs available to all involved parties the likelihood of belligerents to obey laws and treaty provisions, legal limits on use of force). This is critical to peace enforcement operations, as the focus is to get the parties to comply with agreed-to resolutions or sanctions.
- Civilian relief agencies.
- Sources of water.
- Sites of religious, political, or cultural significance.
- Communication structure and capabilities of the parties within the AO.

Evaluate the Threat/*Adversary*

10-36. Use the following considerations to evaluate the threat/*adversary*:

- Identify all threat/*adversary* groups.
- Determine which factions or groups are likely to violate the resolutions.
- Determine any relationships among the groups or factions.
- Identify political organizations and their objectives.
- Determine who wants to violate the resolutions.
- Identify political and religious beliefs that directly affect or influence the conduct of the belligerents. Determine whether these beliefs are contrary to the goals of the peace enforcement operation.
- Identify threat/*adversary* military capabilities and key personnel.
- Determine whether the parties can defeat efforts to enforce the peace.
- Determine the tactics the threat/*adversary* will use to affect the will of the peace enforcer.
- Identify local support to all threat/*adversary* parties.
- Identify threat/*adversary* tactics for the offense and defense.

Determine Threat/*Adversary* Courses of Action

10-37. Use the following IPB considerations to determine threat/*adversary* COAs:

- Template threat/*adversary* actions, to include combat operations/*major operations*, support functions, terrorist acts, and any other actions that would violate the peace.
- Template threat/*adversary* responses to violations of the peace.
- Template the responses of the threat/*adversary*, the host-nation or foreign-nation government, and local indigenous populations and institutions to friendly force peace enforcement operations.
- Template or analyze faction activity as it relates to past events to analyze potential trends.
- Wargame terrorist actions and other activities where belligerents could reasonably avoid being held accountable.

IPB SUPPORT TO HUMANITARIAN AND DISASTER RELIEF AND OTHER OPERATIONS

10-38. Humanitarian, disaster relief, and other operations (such as noncombatant evacuation operations) assist governments and security organizations in easing human sufferance caused by manmade or natural disasters.

10-39. Humanitarian and disaster relief provided by U.S. forces is limited in scope and duration. The relief provided is designed to supplement or complement the efforts of the host-nation civil authorities or agencies that may have the primary responsibility for providing relief.

DEFINE THE OPERATIONAL ENVIRONMENT/*BATTLESPACE ENVIRONMENT*

10-40. In defining the operational environment/*battlespace environment* in support of relief, the staff will—

- Identify areas or activities that might generate displaced civilian movement.
- Consider threats to the AO, such as severe weather, gangs; criminal organizations or religious, ethnic, and racial factions.
- Identify all military, paramilitary, host-nation, international, IGOs, and NGOs; indigenous populations and institutions; and transnational corporations.
- Determine the status of any hostile military or paramilitary forces in the area. Identify the key civilian leaders, community elders, tribal leaders, and their respective supporters.
- Assess host-nation infrastructure.
- Determine the condition of LOCs, utilities, transportation systems, and government services.

- Determine the status of sanitation conditions within the AO.
- Identify storage facilities and requirements.
- Determine the effects of rules of engagement and other force protection measures on threat/*adversary* operations.
- Determine the type and location of all land minefields.
- Determine the geography within the AO and its effect on the mission.

DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS/*BATTLESPACE EFFECTS*

10-41. In describing the environmental effects on operations/*battlespace effects* in support of FHA, the staff will—

- Consider the effects of terrain on locations of land minefields.
- Determine if weather has had an effect on minefield location; for example, has the thawing and freezing of the ground affected known or suspected minefields?
- Determine the effect weather and terrain will have on displaced civilian movement, military operations, civil affairs or military information support operations, mass actions, food supplies, and general mobility.
- Identify the population sectors. The staff looks at urban or rural areas where real or potential threats/*adversaries* can blend into the population or gain influence over the population.
- Focus on demographics. Consider, for example, the effects of—
    - Urban and rural population patterns.
    - Ethnic, religious, and racial divisions.
    - Language divisions.
    - Tribe, clan, and sub-clan loyalties.
    - Health hazards.
    - Political sympathies.
- Consider the effects of the infrastructure on—
    - Location, activity, and capacity of care distribution points (food, health care).
    - Sources of food and water.
    - Housing availability.
    - Hospital capabilities.
    - Utility services.
    - Law enforcement agencies and emergency services and their respective capabilities.
- Determine the LOCs that can be used by friendly forces and potential threats/*adversaries* to affect movement of FHA.
- Locate agricultural areas and other sources of subsistence.
- Determine the present and potential effects of severe weather on executing the FHA mission and displaced civilian movement.
- Determine if the environment is permissive or hostile to the introduction of friendly forces.
- Identify key targets and facilities. The staff should consider that the targets and facilities may also be key terrain.

Evaluate the Threat/*Adversary*

10-42. In evaluating the threat/*adversary* in support of FHA, the staff will—

- Consider weather and the environment as potential threats/*adversaries*. Weather will affect the ability to conduct relief operations. For example, if the target of a relief effort is a village isolated by mudslides or another natural disaster, inclement weather may limit or curtail air operations to the site. Consider that the environment may pose threats to the health of both friendly forces and host-nation personnel in the forms of waterborne diseases, spoiled or contaminated foodstuffs, and other environmental hazards.

- Identify and evaluate the threat posed by any groups that may oppose friendly force operations.
- Consider groups that may clandestinely oppose the operation even though they publicly pledge support.
- Consider civilians and local populace (for example, NGOs, indigenous populations, and institutions) that may become hostile as the operation progresses.
- Evaluate the threat posed by gangs, paramilitaries, terrorist groups or individuals, insurgents, guerilla forces, or other organized forces.
- Identify and evaluate potential trouble spots and contentious issues. Look for riot or similar threat/*adversary* indicators.

Determine Threat/*Adversary* Courses of Action

10-43. In determining threat/*adversary* COAs in support of FHA, the staff will—
- Identify threat/*adversary* COAs that seek to embarrass friendly forces during the FHA mission; for example, will the threat/*adversary* use relief workers to embarrass friendly forces?
- Identify the possibility of threat/*adversary* military action against civilians (relief workers and host-nation personnel).
- Evaluate the threat/*adversary* imposed by a degradation of the capabilities of host-nation law enforcement.
- Evaluate the possibility of unknown or new minefields and other obstacles in the AO.
- Assess threat/*adversary* propaganda capability.

10-44. A noncombatant evacuation operation is a small-scale limited operation conducted to assist the Department of State in evacuating U.S. citizens, Department of Defense civilian personnel, and designated host-nation and third-country nationals whose lives are in danger from locations in a foreign nation to an appropriate safe haven. Although normally considered in connection with hostile action, evacuation may also be conducted in anticipation of, or in response to, any natural or manmade disaster. (See JP 3-68 for more information on noncombatant evacuation operations.)

10-45. A noncombatant evacuation operation is a joint operation, and planning is normally conducted by joint task forces using the JOPP. Therefore, commanders and staff use the joint intelligence preparation of the operational environment (JIPOE) process during planning, not IPB. JIPOE begins during step 2 of JOPP—mission analysis—and continues throughout the JOPP. Intelligence requirements generally associated with noncombatant evacuation operations are—
- Location, disposition, capabilities, and possible COAs for all enemy forces.
- Location of evacuation sites (landing zones, ports, beaches).
- Anticipated number of evacuees (total number by area) categorized by medical status. Categories include—
  - Persons not requiring assistance.
  - Persons requiring medical assistance prior to evacuation.
  - Persons requiring medical assistance prior to and during evacuation.
  - Persons requiring emergency medical evacuation.
- Locations of assembly areas and major supply routes.
- Location of command posts.
- Key personnel (name, location, and methods of contact).
- Description of the embassy communications system, transportation fleet, and warden system.
- Quantity of Class I (subsistence supplies) on hand at the embassy.
- Quantity of Class III (fuel) on hand at the embassy or available elsewhere.
- Availability of class VIII (medical supplies) on hand at the embassy.
- Standard map products of the local area with annotations identifying critical landmarks.
- Rules of engagement.

10-46.   Every U.S. embassy is required to maintain an emergency action plan that includes much of the information the staff needs to support JIPOE. A copy of this action plan is also maintained by the theater headquarters. The joint task force staff should obtain a copy of the emergency action plan prior to beginning JIPOE and coordinate with the theater command and staff and the embassy throughout JIPOE.

10-47.   Additionally, the National Geospatial-Intelligence Agency maintains a geospatial intelligence base for contingency operations; this intelligence base contains specific maps, charts, imagery, and other geospatial intelligence products to support noncombatant evacuation operations planning. Other intelligence sources that can aid JIPOE are as follows:

- The Defense Intelligence Agency maintains various databases that provide details on diplomatic facilities and associated areas for use in evacuation planning.
- The *Marine Corps Intelligence Activity* produces joint expeditionary support products containing maps, charts, imagery, points of entry, and route studies for use during expeditionary operations including evacuation planning and execution.
- United States Transportation Command maintains the port and airfield collaborative environment Web site, which provides detailed overviews of ports and strategic airfields (capable of C-130s and above) worldwide.
- Each Joint Intelligence Operations Center maintains Web sites and databases that provide varying degrees of intelligence support for particular countries.
- The Department of State Web site maintains the most current situational information available for the country of interest.
- The Central Intelligence Agency maintains basic information and maps for all countries of the world in the factbook data file on its Web site.
- Joint task force staffs may also be augmented with a National Intelligence Support Team that provides liaison to national intelligence agencies. (See JP 2-0 for more information on national intelligence support teams.)

Appendix A

Marine Corps Planning Process Tools

A-1. *This appendix only applies to the Marine Corps. For the MCPP, commanders and their staffs use MCPP tools to record, track, and analyze critical planning information. These tools help the commander and the staff better understand the environment, facilitate the commander's decisionmaking, assist in the preparation of plans and orders, and increase tempo. The MCPP tools must serve the needs of the commander and the requirements of the situation. Commanders and staffs can tailor these tools to meet their needs and use other tools available that are appropriate for their particular situation.*

A-2. *Table A-1 identifies commonly used overlays, templates, matrices, worksheets, graphics, and narratives on how each tool supports the MCPP. The examples in this appendix (shown in figures or tables) are at the MEF level, but these tools may be employed at any level of command. The formats and uses of these tools may be modified as required. (See MCWP 5-1 for additional information on the MCPP.)*

Table A-1. *Marine Corps planning process tools*

Tools	*Problem framing*	*COA development*	*COA wargame*	*Comparison and decision*	*Orders development*	*Transition*
Modified combined obstacle overlay (figure A-1 on page A-3)	X	X	X			
Adversary template (figure A-2 on page A-4)	X	X	X			
Situation template (figure A-3 on page A-5)	X	X	X			
Event template (figure A-4 on page A-6)	X	X	X			
Event matrix (table A-3 on page A-6)	X	X	X			
Decision support template (figure A-5 on page A-7)		X	X	X	X	X
Decision support matrix (table A-4 on page A-8)		X	X	X	X	X
COA graphic and narrative (figure A-6 on page A-9)		X	X	X	X	
Synchronization matrix (table A-5 on page A-10)		X	X	X	X	X
COA wargame worksheet (table A-6 on page A-11)			X	X	X	
Comparison and decision matrix with comments (table A-7 on page A-12)				X		

INTELLIGENCE PREPARATION OF THE BATTLESPACE PRODUCTS

A-3. The IPB is a systematic process of analyzing and visualizing the portions of the mission variables of the enemy, terrain and weather, and, when appropriate, civil considerations in a specific area of interest and for a specific mission. By applying IPB, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space. A continuous planning activity undertaken by the entire staff, IPB builds an extensive database for each potential area in which a unit may be required to operate. The IPB describes the environment in which the command is operating and the effects of that environment on the command's operations. Battlespace and weather evaluations assist in identifying obstacles, mobility corridors, and AAs; predicting weather effects for numerous mobility options; and estimating sea conditions. The IPB process consists of the following steps:

- *Define the operational environment.*
- *Describe the effects on operations.*
- *Evaluate the adversary.*
- *Determine the adversary's COAs.*

A-4. In conventional military operations, determining adversary COAs will normally include templating with an adversary assessment. Templating continues from planning to execution, both to assess current operations and to support planning for future operations. In irregular warfare, adversary templating will focus on pattern analysis, which involves tracking, analyzing, and identifying specific trends, such as IEDs or population support, over time.

A-5. The IPB products graphically display the results of the IPB process. Table A-2 identifies the major IPB products and shows their integration with the planning process. Note that both the G-2/S-2 and the G-3/S-3 are responsible for specific products. While IPB starts as an intelligence effort, it expands to an operational process and has logistic and communications applications that are not shown in the table. Paragraphs A-6 through A-11 provide a short description of each product.

Table A-2. *IPB integration throughout the Marine Corps planning process*

Products	Problem Framing	COA Development	COA Wargame	Comparison and Decision	Orders Development	Transition
Modified combined obstacle overlay	←G-2/S-2→					
Adversary template	←G-2/S-2→					continuous[1]
Situation template	←G-2/S-2→					continuous[1]
Pertinent adversary COAs	←G-2/S-2——→					continuous[1]
Refined and prioritized adversary COAs and event templates and matrices	←G-2/S-2————→					continuous[1]
Initial decision support template	←	G-2/S-2/OPT——→				continuous[1]
Decision support template matrix	←	G-2/S-2/OPT————	→			continuous[1]
Note[1]. Templates are updated throughout the operation. COA course of action OPT operational planning team						

MODIFIED COMBINED OBSTACLE OVERLAY

A-6. *The MCOO (see figure A-1) is a graphic of the battlespace's effects on military operations. It is normally based on a product depicting all obstacles to mobility and it is modified as necessary. Modifications can include cross-country mobility classifications, objectives, AAs and mobility corridors, likely obstacles, defensible battlespace, likely engagement areas, key terrain, cultural factors, built-up areas, and civil infrastructure.*
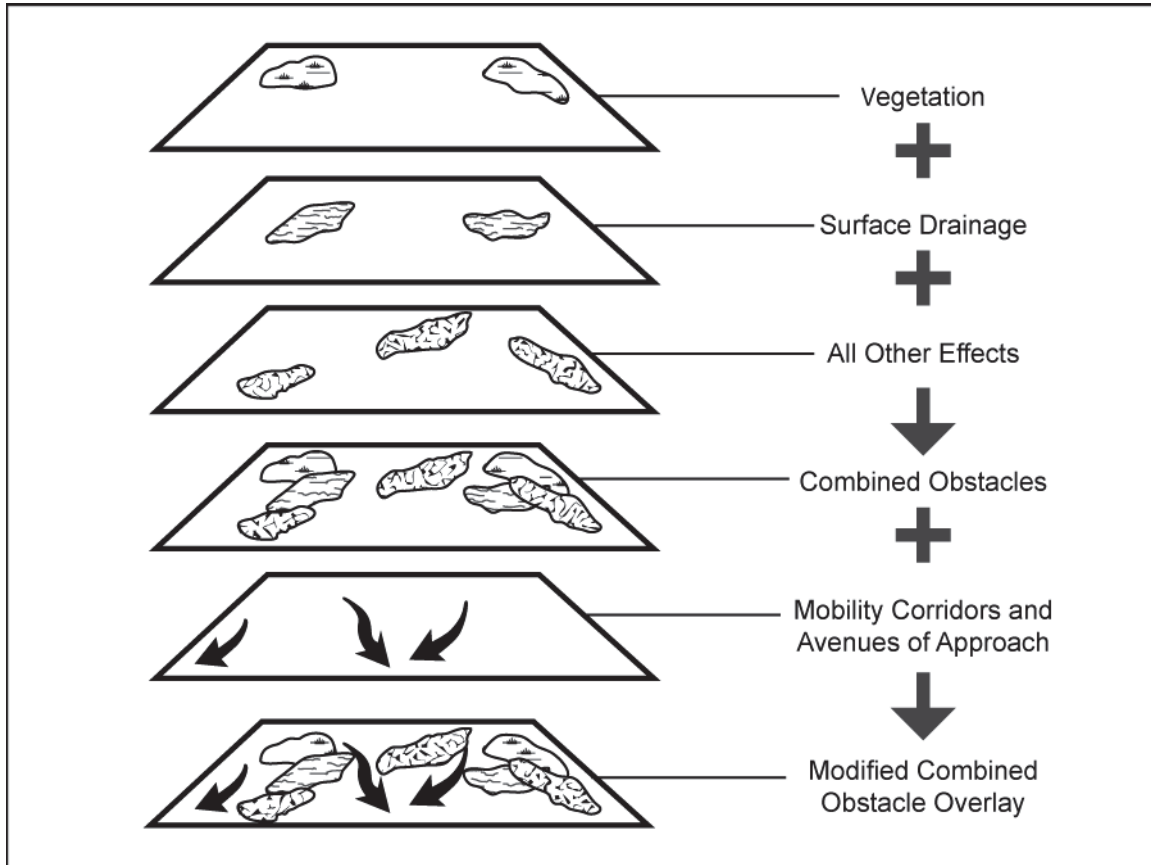
Figure A-1. *Modified combined obstacle overlay*

ADVERSARY TEMPLATE

A-7. *Adversary templates (see figure A-2) are models based on postulated adversary doctrine. They illustrate the disposition and activity of adversary forces conducting a particular operation arrayed on ideal terrain. Adversary templates depict the adversary's nominal organization, frontages, depths, boundaries, and control measures for combat. They are usually scaled for use with a map background and are one part of an adversary model. In irregular warfare, adversary templating will focus on pattern analysis, which involves tracking, analyzing, and identifying specific trends, such as IEDs or population support, over time.*
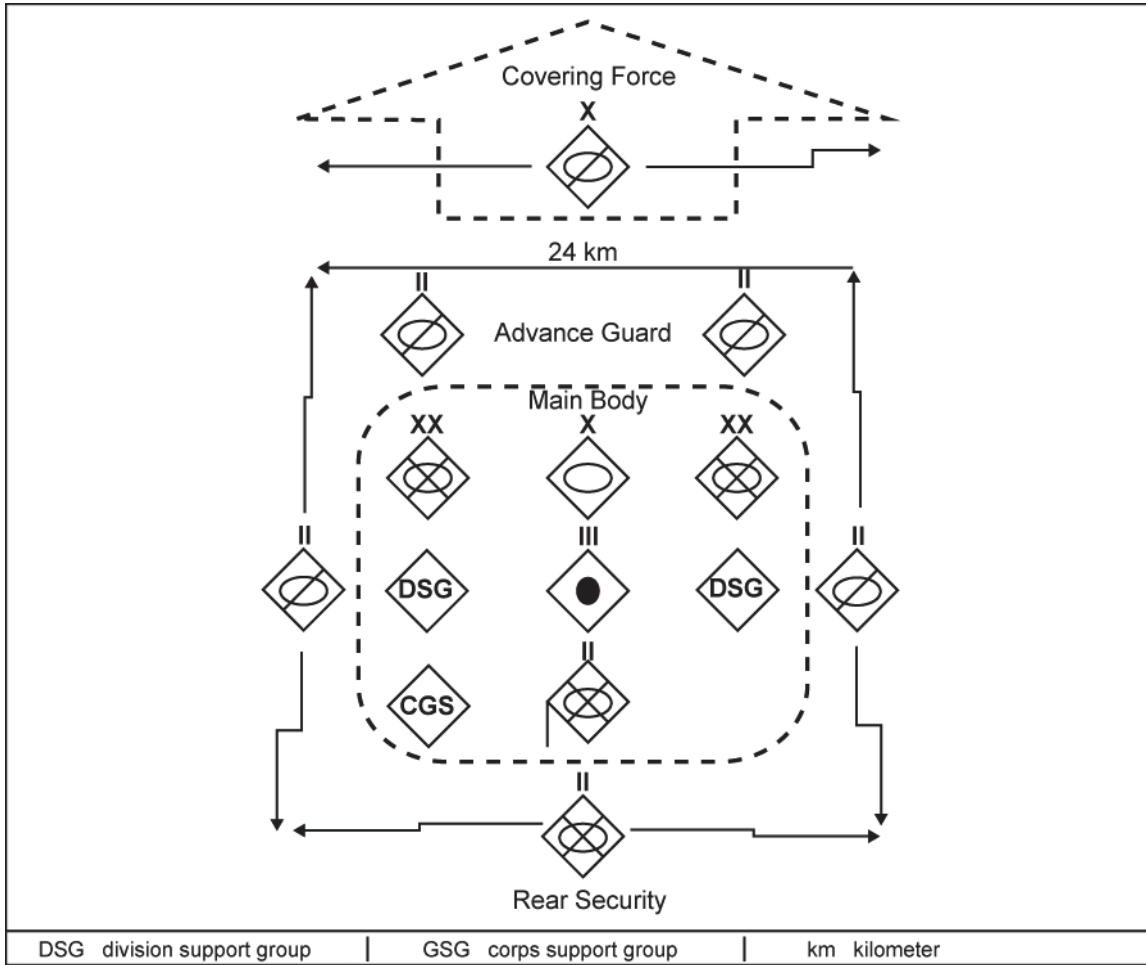
Figure A-2. *Adversary template*

SITUATION TEMPLATE

A-8. *A situation template (see figure A-3) is an adversary template that has been modified to depict adversary dispositions based on the effects of the battlespace and the pursuit of a particular COA. This template accounts for the adversary's current situation with respect to the terrain, training and experience levels, logistic status, losses, and dispositions. Normally, the situation template depicts adversary units two levels down and critical points in the COA. Situation templates are one part of an adversary COA model. Models may contain more than one situation template to depict locations and formations at various times.*
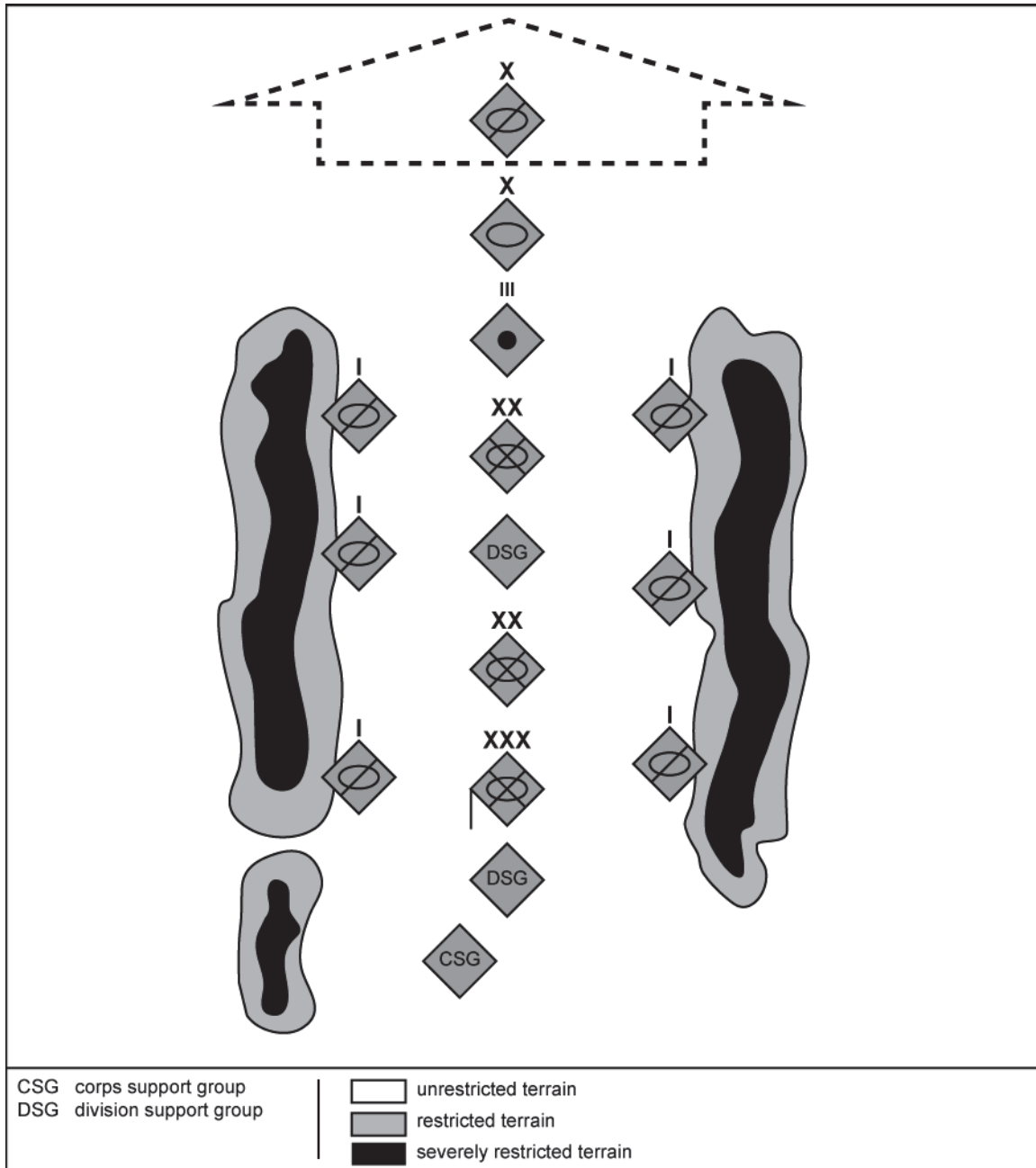
Figure A-3. *Situation template*

EVENT TEMPLATE AND MATRIX

A-9. *The event template is derived from the situation template and depicts the NAIs, areas where activity—or lack of activity—will indicate which COA the adversary has adopted. The NAIs are described in paragraphs 1-36, 6-47, 6-50, and 6-51.. Event templates contain time-phase lines that depict movement of forces and the expected flow of the operation. Movement rates depend on the terrain (MCOO) and the adversary COA (DRAW-D). The event template is the IPB starting point for COA wargaming. The event matrix depicts types of activity expected in each NAI, when the NAI is expected to be active, and any additional information to aid in collection planning. (See figure A-4 and table A-3.)*
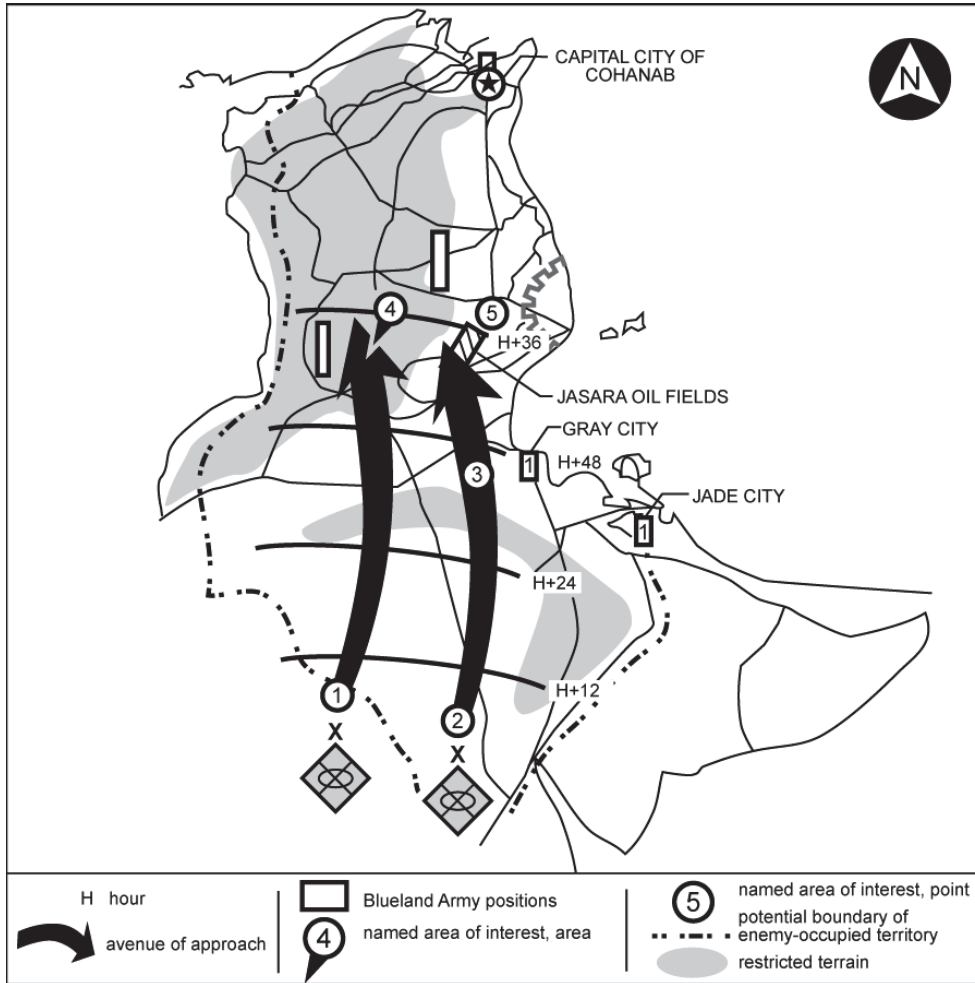
Figure A-4. *Event template*

Table A-3. *Event matrix*

Named area of interest	No earlier than	No later than	Event or indicator
1	*H+6*	*H+12*	*Brigade-sized forces moving north.*
2	*H+6*	*H+12*	*Brigade-sized forces moving north.*
3	*H+12*	*H+24*	*Orangeland forces enter Blueland. Northern operational group driving on Jasara oil fields.*
4	*H+14*	*H+24*	*Orangeland forces seize junction of highways 7 and 8. Northern operational group turns northwest toward Jasara.*
5	*H+18*	*H+24*	*Orangeland forces enter Tealton. Northern operational group driving on Jasara.*

DECISION SUPPORT TEMPLATE AND MATRIX

A-10. *The decision support template is normally developed during COA wargaming. It is derived from adversary, situational, and event templates. The decision support template depicts decision points, time-phase lines associated with movement of adversary and friendly forces, the flow of the operation, and other information required to execute a specific friendly COA.*

A-11. *The decision support template is a key planning tool for use during transition and execution. The decision support matrix provides a recap of expected events, decision points, and planned friendly actions in a narrative form. It shows where and when a decision must be made if a specific action is to take place. It ties decision points to NAIs, TAIs, CCIRs, collection assets, and potential friendly response options. The decision support template and matrix may be refined as planning progresses after the wargame. (See figure A-5 and table A-4 on page A-8.)*
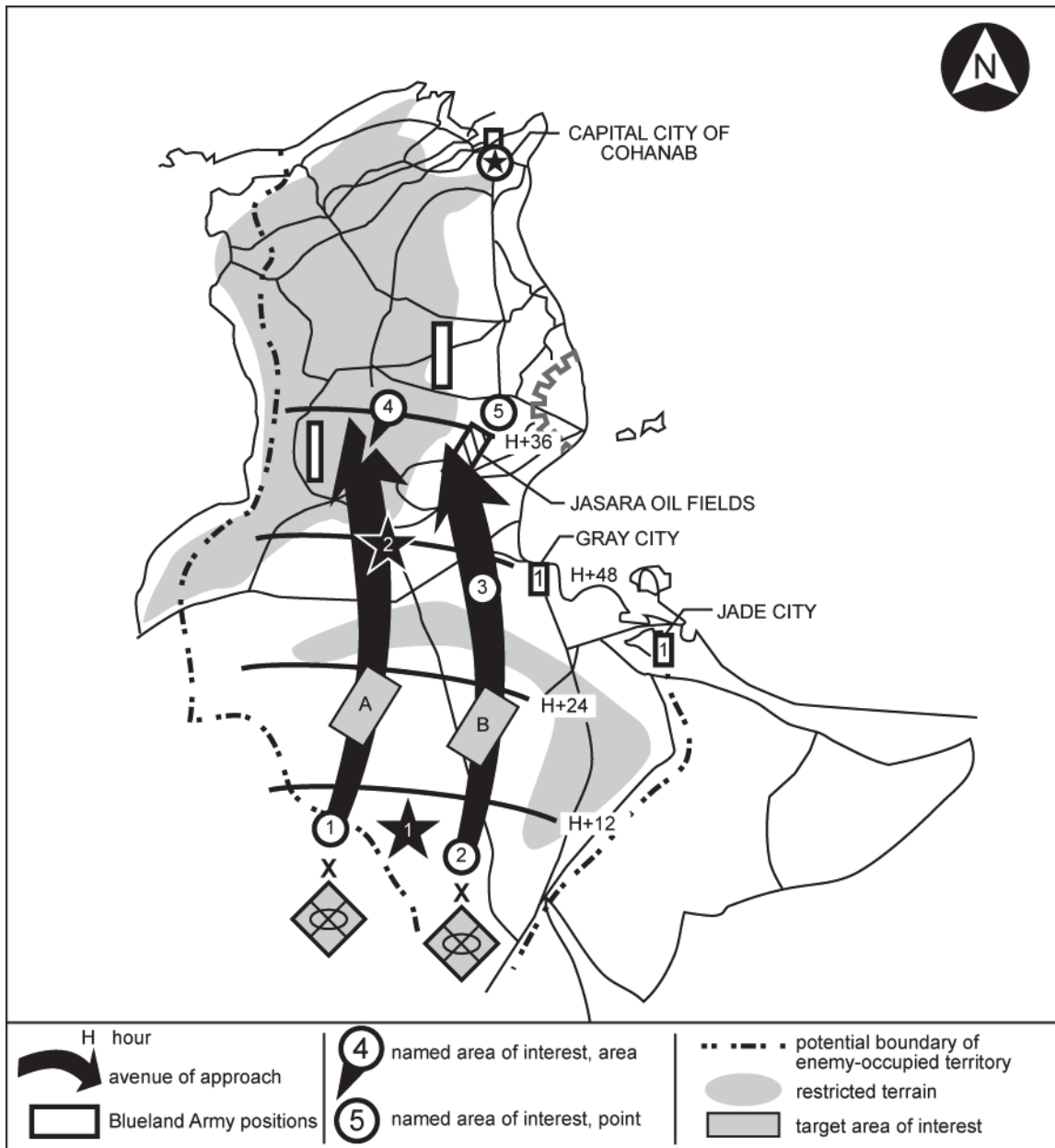
Figure A-5. *Decision support template*

Table A-4. *Decision support matrix*

Event Number	Event	No earlier than/no later than	Named area of interest	Target area of interest	Friendly action
1	*Orangeland forces enter Blueland. Northern operational group division driving on Tealton.*	*H+14/H+24*		*A, B*	*Covering force withdraws; Marine aircraft wing conducts interdiction west of phase line Teal (see figure A-6).*
2	*Orangeland forces seize junction of Highways 7 and 8. Northern operational group turns northwest on Jasara.*	*H+18/H+24*	*3, 4*	*C*	*1st and 3d Marine divisions execute branch plan Hawk.*

PLANNING SUPPORT TOOLS

A-12. *Planning support tools support the commander's and staff's planning effort by recording and displaying critical planning information on the COAs and the commander's decisions and guidance. They aid the commander in decisionmaking by displaying critical information in a useful format. Planning support tools include the COA graphic and narrative, synchronization matrix, COA wargame worksheets, and the comparison and decision matrix.*

COURSE OF ACTION GRAPHIC AND NARRATIVE

A-13. *The COA graphic and narrative (see figure A-6) is a visual depiction and written description of a COA. It clearly portrays how the organization will accomplish the mission, identifying the* **who** *(notional task organization),* **what** *(tasks),* **when, where, how,** *and* **why** *(intent). It should include the tasks and purpose of the main effort, supporting efforts, and reserve. It also includes maneuver control measures, such as boundaries. The COA narrative and graphic, when approved by the commander, forms the basis for the concept of operations and operations overlay in the OPLAN or OPORD.*
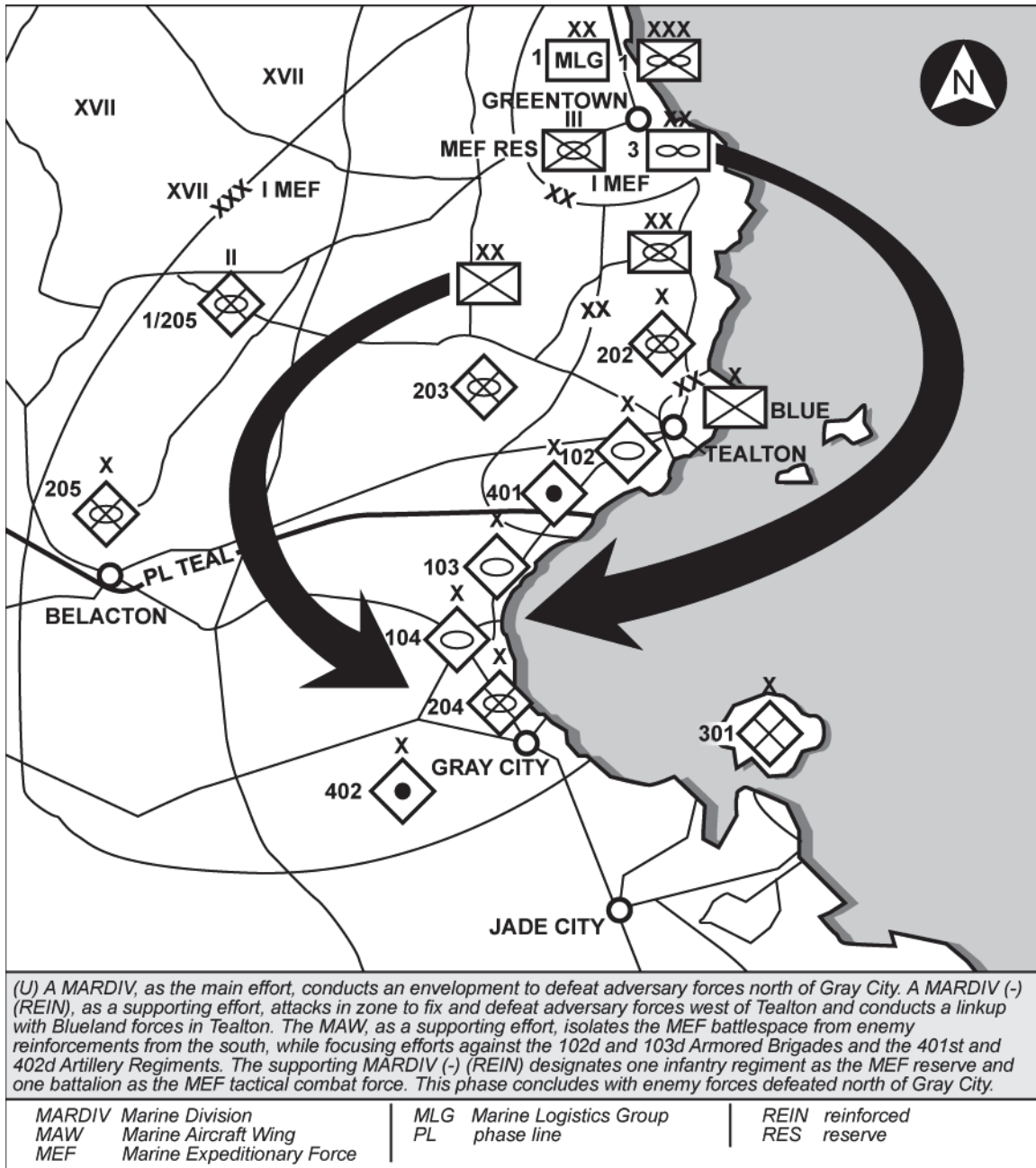
Figure A-6. *Course of action graphic and narrative*

(U) A MARDIV, as the main effort, conducts an envelopment to defeat adversary forces north of Gray City. A MARDIV (-) (REIN), as a supporting effort, attacks in zone to fix and defeat adversary forces west of Tealton and conducts a linkup with Blueland forces in Tealton. The MAW, as a supporting effort, isolates the MEF battlespace from enemy reinforcements from the south, while focusing efforts against the 102d and 103d Armored Brigades and the 401st and 402d Artillery Regiments. The supporting MARDIV (-) (REIN) designates one infantry regiment as the MEF reserve and one battalion as the MEF tactical combat force. This phase concludes with enemy forces defeated north of Gray City.

MARDIV Marine Division	MLG Marine Logistics Group	REIN reinforced
MAW Marine Aircraft Wing	PL phase line	RES reserve
MEF Marine Expeditionary Force		

SYNCHRONIZATION MATRIX

A-14. *A synchronization matrix (see table A-5) is a planning support tool designed to integrate the efforts of the force. It can be organized across the warfighting functions, lines of operations, or other activities based on the situation. It can also record the results of the COA wargame. It depicts, over time, the diverse actions of the entire force necessary to execute the COA. When completed, it provides the basis for an execution matrix or Annex X (Execution Checklist) to the OPLAN or OPORD.*

Table A-5. *Synchronization matrix*

Time	Event	Pre-D-day	D-day - D+2	D+3 - D+4	D+5 - D+6
Adversary action					
Decision points				1	2
Intelligence		Marine expeditionary force (MEF) conducts reconnaissance in zone			
	NAI		1, 2	3, 4	5
Force protection	Survivability	Establish combat air patrol over MEF area of operations			
	CBRN		Priority of support to ACE		
Maneuver	Deep		Marine aircraft wing (MAW) attacks northern operational group armor and artillery, C2, and CSS facilities	MAW attacks 102, 103, 401, and 402	
	Security		Covering forces conduct security operations		
	Close		1st and 3^d Marine Divisions (MARDIVs) complete rupture of adversary defenses	1st MARDIV attacks adversary forces south of phase line Teal The 2^d MARDIV conducts linkup with Blueland forces	
	Reserve	3^d MARDIV—one regiment to MEF reserve			
	Rear	3^d MARDIV—one battalion to tactical combat force			
	Mobility	Priority of main supply route development in main effort zone			
	Countermobility			Complete execution of barrier plan south	

ACE	aviation combat element		CSS	combat service support
C2	command and control		NAI	named area of interest
CBRN	chemical, biological, radiological, and nuclear			

COURSE OF ACTION WARGAME WORKSHEET

A-15. *The COA wargame worksheet (see table A-6) is used during the wargame to record friendly action, adversary reaction, and friendly counteraction involved in each COA. It is also used to capture critical information that may be identified during the wargame, such as potential CCIR, decision points, and NAIs.*

Table A-6. *Course of action wargame worksheet*

COA 1, Stage A; Box; Most likely							
Action	**Reaction**	**Counteraction**	**Assets**	**Time**	**D P**	**CCIR**	**Remarks**
MARDIV envelops Orangeland forces north of Gray City	102^d and 103^d Armored Brigades CATK	MAW interdicts moving threat/adversary forces MARDIV engages and destroys threat/adversary armor at long range	Surge MAW attack assets to interdict threat/adversary armor	D+3	3	Will 102^d and 103^d Armored Brigades move west to CATK	MARDIV has priority of close-air support
CATK – counterattack COA – course of action		D – day DP – decision point			MARDIV – Marine division MAW – Marine aircraft wing		

COURSE OF ACTION COMPARISON AND DECISION MATRIX

A-16. *The COA comparison and decision matrix is a planning support tool designed to assist the commander and staff in recording the advantages and disadvantages of each COA as it is compared against the commander's evaluation criteria. It also provides a venue for further discussion. It may reflect various techniques for weighing the COA against the commander's evaluation criteria (see table A-7 on page A-12). The commander may use the COA comparison and decision matrix to aid his decisionmaking process during the selection of a COA for execution. Commanders and staffs should guard against relying on numerical "rankings" or other simplistic methods that can fail to underscore the complexity involved in the decisionmaking process.*

PLANNING SUPPORT TOOLS FOR STABILITY OPERATIONS

A-17. The following planning support tools have emerged and evolved as a result of lessons learned from Operation Iraqi Freedom and Operation Enduring Freedom.

CIVIL CONSIDERATIONS

A-18. *Civil considerations are a factor in all types of military operations, but they are of particular significance in stability operations. If the mission is to support civil authorities, civil considerations define the mission. Civil considerations generally focus on the immediate impact of civilians on 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. 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.*

A-19. *Civil considerations can either help or hinder friendly or adversary forces and will influence the selection of a COA. An appreciation of civil considerations—the ability to analyze their impact on operations—enhances several aspects of operations, such as the selection of objectives; location, movement, and control of forces; use of weapons; and protection measures. Civil considerations comprise six characteristics— areas, structures, capabilities, organizations, people, and events—expressed in the acronym ASCOPE. (See figure A-7 on page A-12.)*

Table A-7. *Comparison and decision matrix with comments*

Commander's evaluation criteria	COA 1	COA 2	COA 3
Force protection	Moderate casualties	High casualties Increased chemical, biological, radiological, and nuclear threat	Light casualties
Tempo, surprise		Achieving surprise unlikely	High change of achieving surprise
Shapes the battlespace	ACE interdiction of adversary lines of communications limits adversary's ability to reinforce		Deception likely to be effective
Asymmetrical operations	ACE operates against second echelon armor forces GCE mechanized forces attack adversary dismounted infantry	Marine expeditionary forces mechanized forces against adversary mechanized forces	
Maneuver	Frontal attack followed by penetration	Frontal attack	Turning movement
Decisive actions	ACE disrupts deployment of second echelon forces through interdiction		Isolate first echelon forces. Disrupt lines of communications, logistic facilities, and assembly areas
Simplicity		Simplest	Demanding command and coordination requirements
ACE aviation combat element		GCE ground combat element	
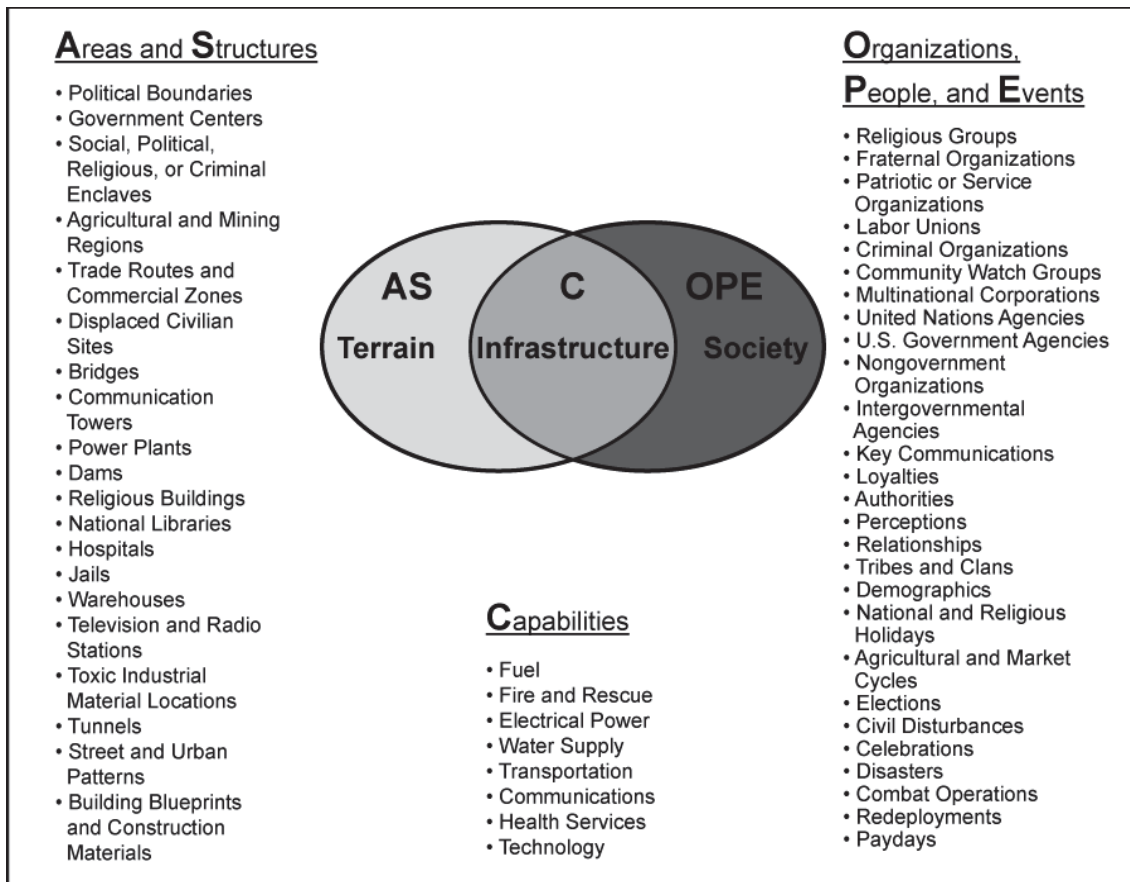
Figure A-7. *Sample civil considerations*

AREAS

A-20. *Areas are key localities or aspects of the terrain within a commander's operational environment that are not normally thought of as militarily significant. Failure to consider key civil areas, however, can seriously affect the success of any military mission. Civil-military operations planners analyze key civil areas from two perspectives: how do these areas affect the military mission and how do military operations impact civilian activities in these areas? At times, the answers to these questions may dramatically influence major portions of the COAs being considered.*

STRUCTURES

A-21. *Structures are architectural objects, such as bridges, communications towers, power plants, and dams, and are often identified as traditional HPTs. Other structures, such as churches, mosques, national libraries and hospitals, are cultural sites generally protected by international law or other agreements. Still other structures are facilities with practical applications, such as jails, warehouses, schools, television stations, radio stations, and printing plants, which may be useful for military purposes. Structures analysis involves determining their location, functions, capabilities, and application in support of military operations. It also involves weighing the military, political, economic, religious, social, and informational consequences of removing them from civilian use; the reaction of the populace; and replacement costs.*

CAPABILITIES

A-22. *Civil capabilities can be viewed from several perspectives. The term "capabilities" may refer to—*

- *Existing capabilities of the populace to sustain itself, such as through public administration, public safety, emergency services, and food and agriculture systems.*
- *Capabilities with which the populace needs assistance, such as public works and utilities, public health, public transportation, economics, and commerce.*
- *Resources and services that can be contracted to support the military mission, such as interpreters, laundry services, construction materials, and equipment. Local vendors, the host nation, or other nations may provide these resources and services. In hostile territory, civil capabilities include resources that may be taken and used by military forces consistent with international law. Analysis of the existing capabilities of the AO is normally conducted based on civil affairs functional specialties. The analysis also identifies the capabilities of partner countries and organizations involved in the operation. In doing so, civil-military operations planners consider how to address shortfalls, as well as how to capitalize on capability strengths.*

ORGANIZATIONS

A-23. *Civil organizations are groups that may or may not affiliate with government agencies. They can be church groups, fraternal organizations, patriotic or service organizations, or community watch groups. They might be IGOs or NGOs. Organizations can assist the commander in keeping the populace informed of ongoing and future activities in an area of operations and influencing the actions of the populace. They can also form the nucleus of humanitarian assistance programs, interim governing bodies, civil defense efforts, and other activities.*

PEOPLE

A-24. *People, both individually and collectively, can have a positive, negative, or no impact on military operations. The "people" element of ASCOPE includes civilians or nonmilitary personnel encountered in an AO. The term may also extend to those outside the AO whose actions, opinions, or political influence can affect the military mission. In all military operations, U.S. forces must be prepared to encounter and work closely with civilians of all types. When analyzing people, Marines should consider historical, cultural, ethnic, political, economic, and humanitarian factors. Working with the "people" assists Marines in identifying the key communicators as well as the formal and informal processes used to influence people. Regardless of the nature of the operation, military forces will usually encounter civilians living and operating in and around the supported unit's AO. Major categories of civilians likely to be encountered include—*

- *Local nationals, such as town and city dwellers, farmers, other rural dwellers, and nomads.*
- *Local civil authorities, such as elected and traditional leaders at all levels of government.*
- *Expatriates.*
- *Foreign employees of IGOs or NGOs.*
- *U.S. Government and third-nation government agency representatives.*
- *Contractors, who may be U.S. citizens, local nationals, or third-nation citizens providing contract services.*
- *Department of Defense civilian employees.*
- *The media, including journalists from print, radio, and visual media.*

EVENTS

A-25. *As there are many different categories of civilians, there are many categories of civilian events that may affect the military mission. Some examples are planting and harvest seasons, elections, riots, and voluntary and involuntary evacuations. Likewise, there are military events that impact the lives of civilians in an AO. Some examples are combat operations, including indirect fires, deployments, and redeployments. Civil-military operations planners determine what events are occurring and analyze the events for their political, economic, psychological, environmental, and legal implications.*

Appendix B
Functional Analysis

B-1. Functional analysis shows graphically how the threat/*adversary* might utilize its capabilities to perform the functions required to accomplish its objectives. It depicts the threat's/*adversary*'s disposition and actions for a particular type of operation (for example, offense, defense, movement to contact, insurgent ambush, and/or terrorist kidnapping operation).

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

B-3. A threat/*adversary* employs functional tactics. It determines the functions it needs to perform as part of an action to bring about its success. Then it allocates appropriate actors to each function and synchronizes the effort.

B-4. A number of different functions are executed each time a threat/*adversary* force attempts to accomplish a mission. The threat/*adversary* commanders identify the specific functions they intend their various subordinate forces or elements to perform. The functions do not change, regardless of where the force or element might happen to be located on the battlefield/*battlespace*. However, the function of a particular force or element may change during the course of the battle.

B-5. Functional analysis may predict likely threat/*adversary* COAs of any type, such as—
- The methodology and technique an insurgent force will use to emplace and explode an IED along convoy routes.
- The methods used by a criminal organization to rob banks.
- Convoy procedures a drug trafficking ring will use to transport large amounts of drugs, such as the distance between vehicles, number of vehicles, where security forces are placed, and how many are in the convoy.
- How the security force will react to or deploy against a police force.

B-6. Functional analysis consists of three steps:
- Determine threat/*adversary* objectives.
- Determine threat battlefield/*adversary battlespace* functions.
- Determine threat/*adversary* capabilities available to perform each function.

DETERMINE THREAT/*ADVERSARY* OBJECTIVES

B-7. Functional analysis begins with a determination of what goal or goals the threat/*adversary* is trying to achieve. Threat/*adversary* objectives are often, but not always, what the unit's mission is trying to prevent. These objectives are also often actions taken by the threat to prevent unit mission accomplishment. The objectives are specific to the type of threat, the AO, the unit's composition and mission, and other factors.

B-8. Some examples of these objectives are—
- Cause friendly unit casualties in order to weaken political resolve in the U.S. and among multinational partners.
- Destroy friendly aircraft while on the ground during a refueling operation.
- Kidnap and ransom a friendly civil leader.
- Prevent friendly security forces from discovering a hidden drug laboratory.

- Seize an important crossroads to facilitate maneuver of a larger force.
- Describe the objectives in terms of purpose and end state.

DETERMINE THREAT BATTLEFIELD/*ADVERSARY BATTLESPACE* FUNCTIONS

B-9. The threat/*adversary* executes a number of different functions each time a threat force attempts to accomplish a mission. While the various functions required to accomplish any given mission can be quite diverse, they can be divided into four very broad categories: action, enabling, fixing, and security.

ACTION

B-10. The action function (also known as the exploitation, decision, or mission function) is performed by the set of capabilities that actually accomplishes a given mission. If the threat/*adversary* objective is to destroy a city with a weapon of mass destruction, then the weapon of mass destruction is performing the action function. If the threat objective is to seize a friendly capital city and it employs a weapon of mass destruction 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 weapon of mass destruction is performing a different function.

B-11. The action function is performed by the set of capabilities that actually accomplish a given mission. One part of the unit or grouping of units conducting a particular action is normally responsible for performing the primary function or task that accomplishes the goal or objective of that action. In general terms, therefore, that part can be called the action force or action element. In most cases, however, the higher commander will give the action force or element a more specific designation that identifies the specific function it is intended to perform, which equates to achieving the objective of the higher command's mission.

B-12. For example, if the objective of the action is to conduct an assault, the element designated to complete that action is the assault element. In larger offensive actions, an action force that completes the primary offensive mission by exploiting a window of opportunity created by another force is called the exploitation force. In defensive actions, the unit or grouping of units that performs the main defensive mission in the battle zone is called the main defense force or main defense element. However, in a maneuver defense, the main defensive action is executed by a combination of two functional forces: the contact force and the shielding force.

ENABLING

B-13. The enabling function (also known as the assault 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. The enabling function is performed by a set of capabilities that acts to assist those capabilities performing the action function. In relation to the forces or elements conducting the action function, all other parts of the organization or grouping of organizations conducting an action provide enabling functions of various kinds. In general terms, therefore, each of these parts can be called an enabling force or enabling element. However, each subordinate force or element with an enabling function can be more clearly identified by the specific function it performs.

B-14. For example, a force that enables by fixing enemy forces so they cannot interfere with the primary action is a fixing force. Likewise, an element that creates a breach that enables an assault element to assault the enemy forces on the far side of an obstacle is a breach element.

B-15. In larger offensive actions, one force can enable another by conducting an assault that enables another force to exploit the effects of that assault in order to accomplish the primary objective. Thus, that type of enabling force can be called the assault force. In this case, the force that conducts the initial assault is not the one that is actually intended to achieve the objective of the higher command's mission. The role of the assault force is to create an opportunity for another force—the exploitation force—to accomplish the objective. Thus, the assault force, conducting the first part of a two-part offensive action, acts as an

enabling force. In order to create a window of opportunity for the exploitation force to succeed, the assault force may be required to operate at a high degree of risk and may sustain substantial casualties. However, other types of enabling forces or elements may not even need to make contact with the enemy.

B-16. If the mission is to enter an enemy base and set off an explosive device, an enabling function would be to penetrate the perimeter defenses of the base or to assist in the infiltration of the element emplacing the device. In the defense, an enabling function might be to counterattack to restore a portion of the area of responsibility to threat/*adversary* control. There are three specific types of enabling functions common that warrant additional attention: disruption, fixing, and security.

B-17. Disruption forces or elements operate to prevent U.S. forces from executing friendly COAs the way U.S. forces want to and to prevent U.S. forces interfering with the threat's/*adversary*'s COA. U.S. forces can—

- Disrupt enemy preparations or actions.
- Destroy or deceive enemy reconnaissance.
- Begin reducing the effectiveness of key components of the enemy's combat system.

FIXING

B-18. 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 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 from maneuvering.

B-19. Fixing is accomplished when a part of the enemy force does not participate in actions that could lead to the failure of the threat/*adversary* COAs. This is accomplished in a variety of ways, including—

- Suppressing a force with fires.
- Deceiving it with information warfare/*information operations*.
- Forcing it to conduct disaster relief and humanitarian assistance.
- Involving it in a firefight away from the main action.
- Restricting its movement with countermobility effects.
- Depriving it of logistics resources.

SECURITY

B-20. The security function is performed by a set of capabilities that acts to protect other capabilities from observation, destruction, or becoming fixed. Security is provided by isolating the battlefield/*battlespace* from enemy elements that could alter the outcome. This can be accomplished by providing early warning and reaction time or actively delaying or destroying arriving enemy forces.

OTHER FUNCTIONS

B-21. The threat/*adversary* commander may designate a subordinate unit or grouping to conduct a deception action (such as a demonstration or feint). This unit or grouping is, therefore, a deception force or deception element. Its function is to lead the enemy to act in ways prejudicial to enemy interests or favoring the success of a threat/*adversary* action force or element.

B-22. A threat/*adversary* commander may also designate some subordinates to perform various support functions. These support elements can provide the following types of support:

- Perform support by fire (in which case, it can be called more specifically a support by fire element).
- Provide support or sustainment/*combat or combat service support*.
- Provide command and control functions.

B-23. At a commander's discretion, some forces or elements may be held out of initial action, in reserve, pending determination of their specific function, so that the commander may influence unforeseen events or

take advantage of developing opportunities. These forces or elements are designated as reserves (reserve force or reserve element). If and when such units are subsequently assigned a mission to perform a specific function, they receive the appropriate functional force or element designation. For example, a reserve force in a defensive operation might become the counterattack force.

DETERMINE THREAT/ADVERSARY CAPABILITIES AVAILABLE TO PERFORM EACH FUNCTION

B-24. Once it is known which functions the threat/*adversary* needs to perform and what goal the threat/*adversary* commander is seeking to accomplish through the performance of those functions, the last step is to identify what capabilities the threat/*adversary* has to execute each function.

B-25. 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 depending on the location, threat/*adversary*, and environment. These may even vary from street to street. In one battlefield/*battlespace,* the threat/*adversary* may employ an infantry platoon equipped with infantry-fighting vehicles and sophisticated thermal sensors to execute the security function. In another, the same function may be performed by a civilian in a third-floor apartment window using a cellular phone.

B-26. Both of the examples below are assaults:

- In figure B-1 each of the functions is performed by readily recognized military formations. Air defense and antitank units perform the security function; direct and indirect fire weapons enable the action, while infantry units perform the action function of the assault.
- In figure B-2 the same functions are being performed, but by significantly different actors. The security function is performed individually with communications devices. The enabling function is being performed by sniper teams and a rioting crowd and the assault itself conducted by insurgents initially posing as members of that crowd.

B-27. In both cases, each type of element is performing the same function. The security elements are providing early warning of arriving enemy forces and, if possible, delaying their ability to influence the decisive point. The support elements are providing activities that enable the action element to accomplish its mission. The action elements are executing the task that accomplishes the goal—in this case the enemy's destruction and the seizure of his position.

B-28. Briefly stated, functional analysis is the application of the knowledge of common and necessary military functions to specific threat capabilities. It is a methodology that—

- Forces analysts and the staff to learn and understand tactics and not rote memorizations.
- Reduces the ability of the enemy/*adversary* to deceive analysts and the staff.
- Is transportable between theaters and works all along the range of military operations.
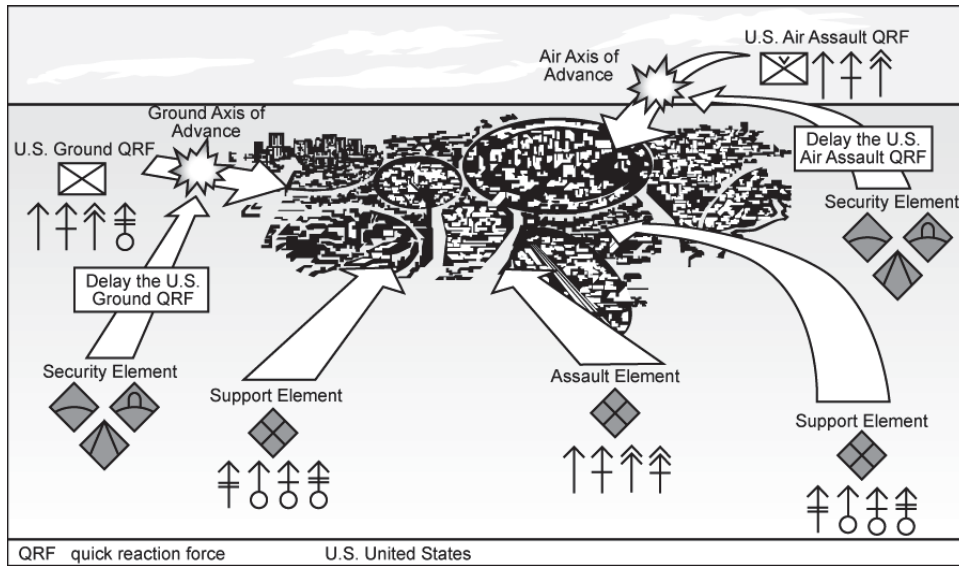
Figure B-1. Enemy attacking fixed position
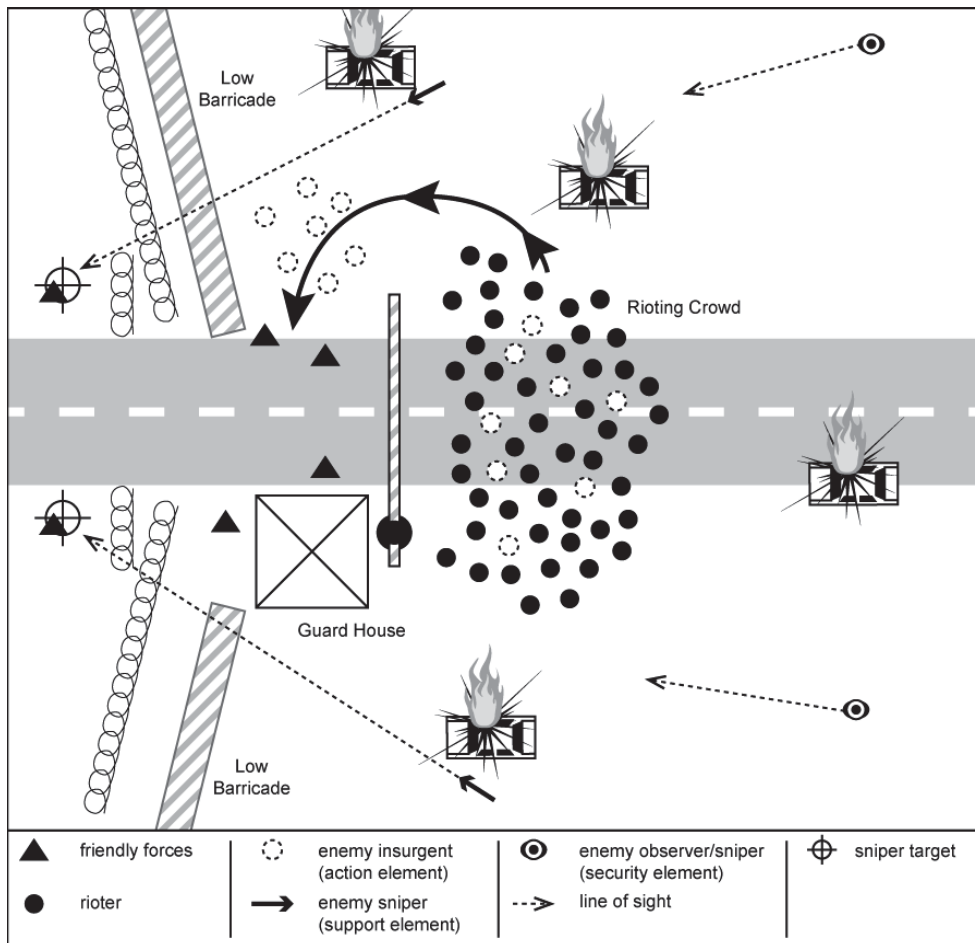
Figure B-2. Sniper and riot-enabled insurgency assault

This page intentionally left blank.

Glossary

For acronyms and terms with Army definitions (Army) precedes the definition. For acronyms and terms with *Marine Corps* definitions (Marine Corps) precedes the definition. The two terms for which ATP 2-01.3/*MCRP 2-3A* is the proponent are marked with an asterisk (*). The proponent publication for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

AA	avenue of approach
AO	area of operations
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AFTTP	Air Force tactics, techniques, and procedures
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
ATTP	Army tactics, techniques, and procedures
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirement
COA	course of action
DA	Department of the Army
DRAW-D	*defend, reinforce, attack, withdraw, delay (Marine Corps)*
EEFI	essential element of friendly information
FHA	foreign humanitarian assistance
FM	field manual
FMFM	*Fleet Marine Force Manual*
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-6	assistant chief of staff, signal
G-9	assistant chief of staff, civil affairs operations
GIRH	*Generic Intelligence Requirements Handbook (Marine Corps)*
HPT	high-payoff target
HPTL	high-payoff target list
HTT	human terrain team (Army)
HVT	high-value target
HVTL	high-value target list
IED	improvised explosive device
IGO	intergovernmental organization

IPB	intelligence preparation of the battlefield (Army)/*intelligence preparation of the battlespace (Marine Corps)*
IVL	intervisibility line
JIPOE	joint intelligence preparation of the operational environment
JOPP	joint operations planning process
JP	joint publication
KOCOA	*key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach (Marine Corps)*
LOC	line of communications
MAGTF	*Marine air-ground task force(Marine Corps)*
MAW	*Marine aircraft wing (Marine Corps)*
MCDP	*Marine Corps doctrinal publication (Marine Corps)*
MCIA	*Marine Corps Intelligence Activity (Marine Corps)*
MCIP	*Marine Corps interim publication (Marine Corps)*
MCO	*Marine Corps order*
MCOO	modified combined obstacle overlay
MCPP	*Marine Corps Planning Process(Marine Corps)*
MCRP	*Marine Corps reference publication (Marine Corps)*
MCWP	*Marine Corps warfighting publication (Marine Corps)*
MDMP	military decisionmaking process (Army)
MEF	*Marine expeditionary force (Marine Corps)*
METOC	*meteorological and oceanographic (Marine Corps)*
METT-T	*mission, enemy, terrain and weather, troops and support available—time available (Marine Corps)*
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, civil considerations (mission variables) (Army)
NAI	named area of interest
NGO	nongovernmental organization
NTTP	Navy tactics techniques and procedures
NWP	*Navy warfare publication (Marine Corps)*
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (military aspects of terrain) (Army)
OPLAN	operation plan
OPORD	operation order
PIR	priority intelligence requirement
PMESII	*political, military, economic, social, information, and infrastructure (Marine Corps)*
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, time (operational variables) (Army)
R2P2	*rapid response planning process (Marine Corps)*
RDSP	rapid decisionmaking and synchronization process (Army)
S-2	intelligence staff officer
S-3	operations staff officer

S-4	logistics staff officer
S-6	signal staff officer/*communications staff officer(0602)*
S-9	civil affairs operations staff officer (Army)
SALUTE	size, activity, location, unit, time, and equipment
SIPRNET	SECRET Internet Protocol Router Network
SME	subject matter expert
TC	training circular
TLP	troop leading procedures
TRAP	*tactical recovery of aircraft and personnel (Marine Corps)*
TTP	tactics, techniques, and procedures
UNS	*Universal Need Statement (Marine Corps)*
U.S.	United States

SECTION II – TERMS

adversary template

(Marine Corps) A model that portrays the adversary's frontage depths, echelon spacing, and force composition as well as the disposition of adversary combat, combat support, and combat service support units for a given operation. It portrays how the adversary would like to fight if he was not constrained.

antiterrorism

(joint) Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called **AT**. (JP 3-07.2)

area of influence

(joint) A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. (JP 3-0)

area of interest

(joint) That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called **AOI**. (JP 3-0)

area of operations

(joint) An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called **AO**. (JP 3-0)

avenue of approach

(joint) An air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. Also called **AA**. (JP 2-01.3)

battlespace

(Marine Corps) The environment, factors, and conditions that must be understood to successfully apply combat power, protect the forces, or complete the mission. This includes the air, land, sea, space, and the included enemy and friendly forces; facilities; weather; terrian; the electromagnetic spectrum; and the information environment within the operational areas, areas of interest, and areas of influence. (MCRP 5-12C)

begin morning civil twilight

(joint) The period of time at which the sun is halfway between beginning morning and nautical twilight and sunrise, when there is enough light to see objects clearly with the unaided eye. Also called **BMCT**. (JP 2-01.3)

begin morning nautical twilight

(joint) The start of that period where, in good conditions and in the absence of other illumination, the sun is 12 degrees below the eastern horizon and enough light is available to identify the general outlines of ground objects and conduct limited military operations. Also called **BMNT**. (JP 2-01.3)

civil considerations

The influence of manmade infrastructure, civilian institutions, and the attitudes and activities of the civilian leaders, populations, and organizations within an area of operations on the conduct of military operations. (ADRP 5-0)

collection

(Marine Corps) Acquisition of information and the provision of this information to processing. (JP 1-02). The gathering of intelligence data and information to satisfy the identified requirements. (MCRP 5-12C)

commander's critical information requirement

(joint) An information requirement identified by the commander as being critical to facilitating timely decision making. (JP 3-0)

concealment

Protection from observation or surveillance. (ADRP 1-02)

cover

(joint) In intelligence usage, those measures necessary to give protection to a person, plan, operation, formation, or installation from the enemy intelligence effort and leakage of information. (JP 2-01.2)

decision support template

(joint) A combined intelligence and operations graphic based on the results of wargaming that depicts decision points, timelines associated with the movement of forces and the flow of the operation, and other key items of information required to execute a specific friendly course of action. (JP 2-01.3) *(Marine Corps) A staff product initially used in the wargaming process that graphically represents the decision points and projected situations and indicates when, where, and under what conditions a decision is most likely to be required to initiate a specific activity (such as a branch or sequel) or event (such as lifting or shifting of fires). (MCRP 5-12C)*

end evening civil twilight

(joint) The point in time when the sun has dropped 6 degrees beneath the western horizon, and is the instant at which there is no longer sufficient light to see objects with the unaided eye. Also called **EECT**. (JP 2-01.3)

end of evening nautical twilight

(joint) The point in time when the sun has dropped 12 degrees below the western horizon, and is the instant of last available daylight for the visual control of limited military operations. Also called **EENT**. (JP 2-01.3)

event matrix

(joint) A cross-referenced description of the indicators and activity expected to occur in each named area of interest. (JP 2-01.3)

event template

(joint) A guide for collection planning. The event template depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted. See also **area of interest**. (JP 2-01.3)

high-payoff target list

A prioritized list of high-payoff targets. (FM 3-60)

high-value target

(joint) A target the enemy commander requires for the successful completion of the mission. Also called **HVT**. (JP 3-60)

hybrid threat

>   The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, and/or criminal elements unified to achieve mutually benefitting effects. (ADRP 3-0)

information environment

>   (joint) The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

intelligence

>   (joint) 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities.. (JP 2-0) *(Marine Corps) Knowledge about the enemy or the surrounding environment needed to support decisionmaking. Intelligence is one of the six warfighting functions. (MCRP 5-12C)*

intelligence estimate

>   (joint) The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy and the order of probability of their adoption. (JP 2-0)

*intelligence preparation of the battlefield/*battlespace*

>   (Army) The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. Also called **IPB**. *(Marine Corps) The systematic, continuous process of analyzing the threat and environment in a specific geographic area. Also called **IPB**.*

intelligence requirement*(s)*

>   (joint) 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. Also called **IR**. (JP 2-0) *(Marine Corps) Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called **IRs**. (MCRP 5-12C)*

key terrain

>   (joint) Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (JP 2-01.3)

line of communications

>   (joint) A route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move. Also called **LOC**. (JP 2-01.3)

*line of sight

>   The unobstructed path from a Soldier's/*Marine's* weapon, weapon site, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another.

mobility corridor

>   (joint) Areas that are relatively free of obstacles where a force will be canalized due to terrain restrictions allowing military forces to capitalize on the principles of mass and speed. (JP 2-01.3)

modified combined obstacle overlay

>   (joint) A joint intelligence preparation of the operational environment product used to portray the militarily significant aspects of the operational environment, such as obstacles restricting military movement, key geography, and military objectives. Also called **MCOO**. (JP 2-01.3)

named area of interest

>   (Army) The geographical area where information that will satisfy a specific information requirement can be collected. (ADRP 1-02) *(Marine Corps) A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of*

interest will help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

obstacle

(joint) Any natural or man-made obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force. (JP 3-15)

operational environment

(joint) A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called **OE**. (JP 3-0)

priority intelligence requirement

(joint) An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment. Also called **PIR**. (JP 2-0) *(Marine Corps) An intelligence requirement associated with a decision that will critically affect the overall success of the command's misison. (MCRP 5-12C)*

request for information

(joint) 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. Also called **RFI**. (JP 2-0, part 1 of a 2-part definition)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

situation template

(joint) A depiction of assumed adversary dispositions, based on that adversary's preferred method of operations and the impact of the operational environment if the adversary should adopt a particular course of action. (JP 2-01.3)

sociocultural factors

(joint) The social, cultural, and behavioral factors characterizing the relationships and activities of the population of a specific region or operational environment. (JP 2-01.3)

target

(joint) 1. An entity or object that performs a function for the adversary considered for possible engagement or other action. 2. In intelligence usage, a country, area, installation, agency, or person against which intelligence operations are directed. 3. An area designated and numbered for future firing. (JP 3-60, parts 1, 2, and 3 of a 4-part definition)

targeting

(joint) The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

terrain analysis

(joint) The collection, analysis, evaluation, and interpretation of geographic information on the natural and man-made features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (JP 2-03)

terrorism

(Army) The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (U.S. Code, Title 18, Section 2331) *(Marine Corps) The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political. (JP 3-07.2)*

References

REQUIRED PUBLICATIONS

These documents must be available to the intended user of this publication.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new _pubs/jointpub.htm.

JP 1. *Doctrine for the Armed Forces of the United States.* 25 March 2013.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 8 November 2010.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online at http://www.apd.army.mil.

ADRP 1-02. *Terms and Military Symbols.* 24 September 2013.

RELATED PUBLICATIONS

These documents are cited in this publication.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new _pubs/jointpub.htm.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01.2. *Counterintelligence and Human Intelligence in Joint Operations.* 26 August 2011. (This classified publication is available on the SIPRNET. Contact the preparing agency of this manual for access instructions.)

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment.* 21 May 2014.

JP 2-03. *Geospatial Intelligence in Joint Operations.* 31 October 2012.

JP 3-0. *Joint Operations.* 11 August 2011.

JP 3-04. *Joint Shipboard Helicopter and Tiltrotor Aircraft Operations.* 6 December 2012.

JP 3-06. *Joint Urban Operations.* 20 November 2013.

JP 3-07.2. *Antiterrorism.* 14 March 2014.

JP 3-07.3. *Peace Operations.* 1 August 2012.

JP 3-07.4. *Counterdrug Operations.* 14 August 2013.

JP 3-12. *Cyberspace Operations*. 5 February 2013. (This classified publication is available on the SIPRNET. Contact the preparing agency of this manual for access instructions.)

JP 3-13. *Information Operations.* 27 November 2012.

JP 3-13.3. *Operations Security.* 4 January 2012.

JP 3-15. *Barriers, Obstacles, and Mine Warfare for Joint Operations.* 17 June 2011.

JP 3-59. *Meteorological and Oceanographic Operations*. 7 December 2012.

JP 3-60. *Joint Targeting.* 31 January 2013.

JP 3-68. *Noncombatant Evacuation Operations.* 23 December 2010.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://www.apd.army.mil.

ADP 3-0. *Unified Land Operations.* 10 October 2011.

ADP 5-0. *The Operations Process.* 17 May 2012.

ADRP 2-0. *Intelligence*. 31 August 2012.

ADRP 3-0. *United Land Operations.* 16 May 2012.

ADRP 3-90. *Offense and Defense.* 31 August 2012.

ADRP 5-0. *The Operations Process.* 17 May 2012.

AR 380-5. *Department of the Army Information Security Program.* 29 September 2000.

AR 381-10. *U.S. Army Intelligence Activities.* 3 May 2007.

ATP 2-01. *Plan Requirements and Assess Collection.* 19 August 2014.

ATP 3-34.80. *Geospatial Engineering.* 23 June 2014.

ATP 3-90.37. *Countering Improvised Explosive Devices.* 29 July 2014.

ATP 5-19. *Risk Management.* 14 April 2014.

ATTP 3-90.15. *Site Exploitation Operations.* 8 July 2010.

ATTP 3-97.11/*MCRP 3-35.1D*. *Cold Region Operations.* 28 January 2011.

FM 3-06. *Urban Operations*. 26 October 2006.

FM 3-07. *Stability*. 2 June 2014.

FM 3-07.31/MCWP 3-33.8/AFTTP 3-2.40. *Multi-Service Tactics, Techniques, and Procedures for Conducting Peace Operations.* 26 October 2003.

FM 3-24/*MCWP 3-33.5*. *Insurgencies and Countering Insurgencies.* 13 May 2014.

FM 3-34.170/*MCWP 3-17.4*. *Engineer Reconnaissance.* 25 March 2008.

FM 3-38. *Cyber Electromagnetic Activities.* 12 February 2014.

FM 3-55. *Information Collection.* 3 May 2013.

FM 3-60. *The Targeting Process*. 26 November 2010.

FM 3-97.6. *Mountain Operations*. 28 November 2000.

FM 4-02. *Army Health System.* 26 August 2013.

FM 6-20-40. *Tactics, Techniques, and Procedures for Fire Support for Brigade Operations (Heavy).* 5 January 1990.

FM 7-15. *The Army Universal Task List.* 27 February 2009.

FM 90-3/*MCWP 3-35.6*. *Desert Operations*. 24 August 1993.

FM 90-5/*FMFM 7-28*. *Jungle Operations*. 16 August 1982.

TC 7-100. *Hybrid Threat.* 26 November 2010.

TC 7-100.2. *Opposing Force Tactics*. 9 December 2011.

NAVY AND MARINE CORPS PUBLICATIONS

Most Marine Corps doctrinal publications are available online at https://www.doctrine.usmc.mil/.

Cultural Intelligence Indicator Guide. Quantico, VA: U.S. Marine Corps Intelligence Activity. October 2009. Available online at https://www.intelink.gov/mcia, accessed on 15 October 2014.

Generic Intelligence Requirements Handbook. Quantico, VA: U.S. Marine Corps Intelligence Activity. June 2003. Available online at https://www.intelink.gov/mcia, accessed on 15 October 2014.

MCDP 1-0. Marine Corps Operations. 9 August 2011.

MCIP 3-17.02. Marine Air-Ground Task Force Counter-Improvised Explosive Device Operations. 24 January 2011.

MCO 3900.15B. Marine Corps Expeditionary Force Development System (EFDS). 10 March 2008. Available online at http://www.marines.mil/News/Publications/ELECTRONICLIBRARY. aspx, accessed on 15 October 2015.

MCRP 5-12C. Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms. 16 November 2011.

MCWP 2-2. MAGTF Intelligence Collection. 30 July 2004.

MCWP 2-3. MAGTF Intelligence Production and Analysis. 27 September 2001.

MCWP 3-35.1. Mountain Warfare Operations. 28 February 2014.

MCWP 3-35.3. Military Operations on Urbanized Terrain (MOUT). 26 April 1998.

MCWP 3-35.7. MAGTF Meteorology and Oceanography Support. 30 June 1998.

MCWP 5-1. Marine Corps Planning Process. 24 August 2010.

NWP 3-59M/MCWP 3-35.10.Operational Level Integration of METOC Capabilities. December 2013.

PUBLIC LAWS AND OTHER PUBLICATIONS

Title 18, United States Code, Section 2331, Chapter 113B, *Terrorism.* Available online at http://uscode.house.gov/, accessed on 19 June 2014.

Title 22, United States Code, Section 2656f, Chapter 38, *Annual Country Reports on Terrorism.* Available online at http://uscode.house.gov/, accessed on 19 June 2014.

Swinton, Ernest Dunlop. *The Defence of Duffer's Drift.* Washington, DC: The United States Infantry Association. Available online at www.gutenberg.org, accessed on 23 October 2014.

RECOMMENDED READINGS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

JP 3-16. *Multinational Operations.* 16 July 2013.

JP 3-24. *Counterinsurgency.* 22 November 2013.

JP 4-0. *Joint Logistics.* 16 October 2013.

JP 4-02. *Health Service Support.* 26 July 2012.

JP 5-0. *Joint Operation Planning.* 11 August 2011.

ARMY PUBLICATIONS

ADP 2-0. *Intelligence.* 31 August 2012.

ADP 3-90. *Offense and Defense.* 31 August 2012.

ADP 6-0. *Mission Command.* 17 May 2012.

ADRP 3-37. *Protection.* 31 August 2012.

ADRP 6-0. *Mission Command.* 17 May 2012.

ATP 1-02.1/*MCRP 3-25B/NTTP 6-02.1/AFTTP3-2.5. Multi-Service Brevity Codes.* 20 September 2012.

ATP 3-37.2. *Antiterrorism.* 3 June 2014.

FM 3-24.2. *Tactics in Counterinsurgency.* 21 April 2009.

FM 3-50. *Army Personnel Recovery.* 2 September 2014.

FM 3-90.1. *Tank and Mechanized Infantry Company Team.* 9 December 2002.

FM 7-100.1. *Opposing Force Operations.* 27 December 2004.

FM 7-100.4. *Opposing Force Organization Guide.* 3 May 2007.

TC 3-97.61. *Military Mountaineering.* 26 July 2012.

NAVY AND MARINE CORPS PUBLICATIONS

MCWP 2-1. Intelligence Operations. 10 September 2003.

MCWP 3-1. Ground Combat Operations. 4 April 1995.

MCWP 3-17. Engineering Operations. 14 February 2000.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Web site: www.apd.army.mil.

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

Index

Entries are by paragraph number unless indicated otherwise.

Entries are by paragraph number unless indicated otherwise.

Entries are by paragraph number unless indicated otherwise.

Entries are by paragraph number unless indicated otherwise.

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1430301

By Direction of the Commandant of the Marine Corps:

K. J. GLUECK, JR.
Lieutenant General, U.S.
Marine Corps
Deputy Commandant
Combat Development
and Integration

DISTRIBUTION:

Active Army, the Army National Guard, and the United States Army Reserve. Not to be distributed; electronic media only.