ATP 2-01.3

Intelligence Preparation of the Battlefield

MARCH 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 2-01.3/MCRP 2-3A, dated 10 November 2014.

Headquarters, Department of the Army

Army Techniques Publication
No. 2-01.3

Headquarters
Department of the Army
Washington, DC 1 March 2019

Intelligence Preparation of the Battlefield

Contents

DISTRIBUTION RESTRICTION DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes ATP 2-01.3/MCRP 2-3A, dated 10 November 2014.

PART THREE CONSIDERATIONS FOR OPERATIONS AND ENVIRONMENTS

Figures

Tables

Preface

ATP 2-01.3 constitutes current doctrine on how to systematically evaluate the effects of significant characteristics of the operational environment (OE) for specific missions. This publication—

- Describes how the commander and staff examine mission variables to understand how these variables may affect operations.
- Discusses intelligence preparation of the battlefield (IPB) as a critical component of the military decision-making process, how IPB supports decision making, and the integrating processes and continuing activities.
- Facilitates a common understanding, foundational concepts, and methods of the IPB process.

The principal audience for ATP 2-01.3 is tactical Army commanders and staffs. Commanders and staffs of Army 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 also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and in some cases host-nation and other nation's laws and regulations when applicable. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 27-10.)

ATP 2-01.3 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ATP 2-01.3 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which ATP 2-01.3 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

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 the judge advocate for assistance.

ATP 2-01.3 applies to the Active Army, the Army National Guard/Army National Guard of the United States, U.S. Army Reserve, unless otherwise stated.

The proponent of ATP 2-01.3 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Directorate of Doctrine and Intelligence System Training, 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-DST-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.

This page intentionally left blank.

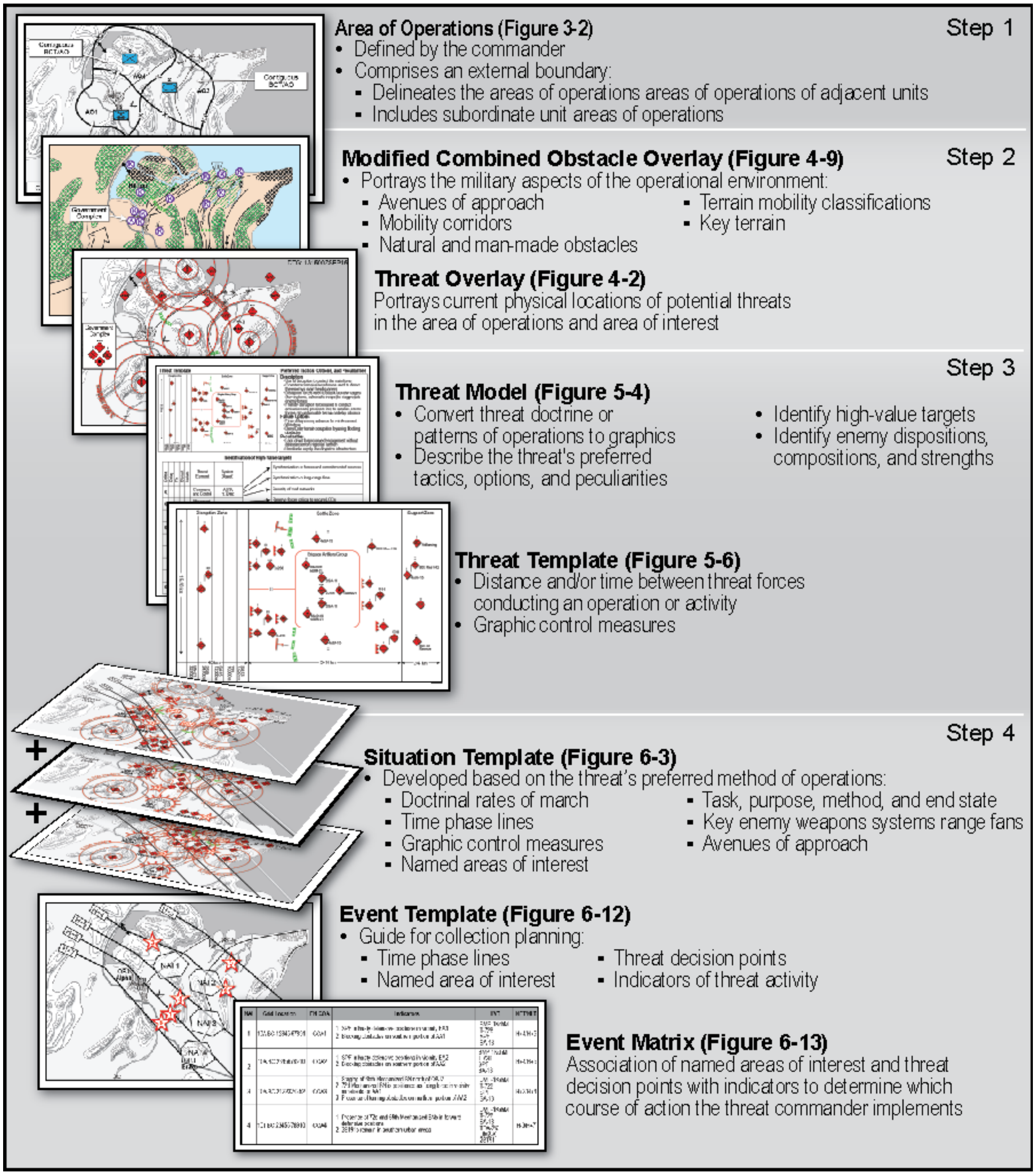
Acknowledgement

The term Cyber Kill Chain, including Cyber Kill Chain methodology, in paragraphs D-33 through D-37, has been used with permission from Lockheed Martin Corporation, www.lockheedmartin.com, *Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense, 2015*. The copyright owner has granted permission to reproduce material from its works. With Lockheed Martin Corporation's permission, some of the text has been paraphrased and adapted for military purposes.

This page intentionally left blank.

Introduction

IPB is a collaborative staff effort led by the J-2/G-2/S-2 and the intelligence staff. IPB products developed and continuously updated facilitate situational understanding and assist commanders and staffs in identifying relevant aspects within the area of operations and area of interest that can affect mission accomplishment. The introductory figure lists and summarizes the relevant IPB products.



Step 1

Area of Operations (Figure 3-2)

- Defined by the commander
- Comprises an external boundary:
  - Delineates the areas of operations areas of operations of adjacent units
  - Includes subordinate unit areas of operations

Step 2

Modified Combined Obstacle Overlay (Figure 4-9)

- Portrays the military aspects of the operational environment:
  - Avenues of approach
  - Mobility corridors
  - Natural and man-made obstacles
  - Terrain mobility classifications
  - Key terrain

Threat Overlay (Figure 4-2)

Portrays current physical locations of potential threats in the area of operations and area of interest

Step 3

Threat Model (Figure 5-4)

- Convert threat doctrine or patterns of operations to graphics
- Describe the threat's preferred tactics, options, and peculiarities
- Identify high-value targets
- Identify enemy dispositions, compositions, and strengths

Threat Template (Figure 5-6)

- Distance and/or time between threat forces conducting an operation or activity
- Graphic control measures

Step 4

Situation Template (Figure 6-3)

- Developed based on the threat's preferred method of operations:
  - Doctrinal rates of march
  - Time phase lines
  - Graphic control measures
  - Named areas of interest
  - Task, purpose, method, and end state
  - Key enemy weapons systems range fans
  - Avenues of approach

Event Template (Figure 6-12)

- Guide for collection planning:
  - Time phase lines
  - Named area of interest
  - Threat decision points
  - Indicators of threat activity

Event Matrix (Figure 6-13)

Association of named areas of interest and threat decision points with indicators to determine which course of action the threat commander implements

Introductory figure. Products of the IPB process

The IPB process is unique—it impacts the range of military operations, is relevant across all echelons, and is the fundamental element used in all planning and decision making. IPB serves as the initial framework for analysis of the battlefield in all operations.

The revision of this publication addresses complex OE in which U.S. forces will operate across all domains (air, land, space, maritime, and cyberspace) and the information environment and worldwide. The goal of this revision is to—

- Highlight staff processes and products to assist commanders and staffs in identifying when and where to leverage friendly capabilities in the scope of an operation.
- Add some unique considerations for IPB supporting certain missions not addressed in the 2014 version of this publication.

ATP 2-01.3 updates and describes the fundamentals of IPB. It contains eight chapters and four appendixes:

- **Chapter 1** provides the fundamentals of IPB and introduces topics such as the operational framework, peer threats, multi-domain operations, and identifying windows of opportunity.
- **Chapter 2** discusses IPB support to decision making and the relationship between IPB and the military decision-making process.
- **Chapter 3**, step 1 of the IPB process, discusses the analysis of the significant characteristics of or activities within the OE that may influence friendly and threat courses of action and command decisions, as well as the physical space the mission will occupy.
- **Chapter 4**, step 2 of the IPB process, discusses how the significant characteristics of the OE can affect friendly and threat operations.
- **Chapter 5**, step 3 of the IPB process, discusses threat force capabilities and the doctrinal principles and tactics, techniques, and procedures threat forces prefer to employ.
- **Chapter 6**, step 4 of the IPB process, identifies and describes how threat courses of action can influence friendly operations.
- **Chapter 7** discusses IPB support to offense, defense, and stability tasks and the unique characteristics of littoral, urban, and subterranean environments.
- **Chapter 8** discusses unique aspects of each domain, the information environment, and the electromagnetic spectrum.
- **Appendix A** provides a checklist to the S-2 on the *how to* of IPB.
- **Appendix B** provides analysts with tools to use when performing IPB.
- **Appendix C** describes the threat characteristics for regular, irregular, and hybrid threats.
- **Appendix D** discusses the cyberspace domain and how to integrate cyberspace considerations into the IPB process.

This publication—

- Introduces acronyms at their first use in the front matter of this publication (preface and introduction), and again in the body of the publication (chapters and appendixes).
- Introduces G-*X* and S-*X* (such as G-2 and S-2) acronyms at their first use without defining them as it hinders readability. Definitions for these acronyms can be found in the glossary.
- Uses *U.S.* as a modifier (for example, U.S. forces) and *United States* as a noun (for example, the United States, a country in North America).
- Uses the term *threat*, which includes all enemies and adversaries that are part of the OE.
- Refers to *staffs* as the operations, intelligence, and other coordinating and special staff sections unless indicated otherwise.
- Uses *holdings* to annotate many different feeds (for example, biometrics). Holdings 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.
- Avoids discussing specific disciplines and complementary intelligence capabilities.

PART ONE

Fundamental Principles, Process Activities, and Relationships

Chapter 1

Intelligence Preparation of the Battlefield Fundamentals

INTELLIGENCE PREPARATION OF THE BATTLEFIELD (IPB) DEFINED

1-1. ***Intelligence preparation of the battlefield* 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.** IPB allows commanders and staffs to take a holistic approach to analyzing the operational environment (OE). A holistic approach—

- Describes the totality of relevant aspects of the OE that may impact friendly, threat, and neutral forces.
- Accounts for all relevant domains that may impact friendly and threat operations.
- Identifies windows of opportunity to leverage friendly capabilities against threat forces.
- Allows commanders to leverage positions of relative advantage at a time and place most advantageous for mission success with the most accurate information available.

1-2. IPB results in intelligence products that are used during the military decision-making process (MDMP) to assist in developing friendly courses of action (COAs) and decision points for the commander. Additionally, the conclusions reached and the products (which are included in the intelligence estimate) developed during IPB are critical to planning information collection and targeting operations. IPB products include—

- Threat situation templates with associated COA statements and high-value target (HVT) lists.
- Event templates and associated event matrices.
- Modified combined obstacle overlays (MCOOs), terrain effects matrices, and terrain assessments.
- Weather effects work aids—weather forecast charts, weather effects matrices, light and illumination tables, and weather estimates.
- Civil considerations overlays and assessments.

1-3. The J-2/G-2/S-2 leads the staff effort and begins preparing for IPB during generate intelligence knowledge, which is associated with the intelligence support to force generation task of the intelligence warfighting function and incorporated into the Army design methodology. (See FM 2-0 and ADRP 1-03 for intelligence warfighting function tasks and measures of performance, respectively.)

1-4. During generate intelligence knowledge, intelligence staffs create data files for their OE based on existing information and their evaluation of the information and intelligence related to the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time [PMESII-PT]). The intelligence staff can also access holdings maintained by the military intelligence brigade-theater (also called MIB-T). This theater-aligned unit processes, refines, and stores intelligence products daily, which benefit nonregionally aligned units.

1-5. When generating intelligence knowledge, the intelligence staff should begin by determining the information needed to collect on the OE. As the staff begins to collect data on the OE, the data should be organized into baseline data files in accordance with the commander's guidance. These files must be compatible with the unit's mission command information systems. Generally, tactical echelons create primary data files based on the enemy, terrain and weather, and civil considerations. Strategic and operational echelons create data files based on the commander's operational requirements.

1-6. Given the limited time available to collect and evaluate information and intelligence on the operational variables, the information obtained from these data files may not be specific enough to support the IPB process and the MDMP. However, the commander and staff can use the information to assist in framing the OE during the Army design methodology.

1-7. Throughout the operations process, the commander and staff continually collect information and analyze the operational variables in order to provide increased situational understanding due to possible contingency operations. *Situational understanding* is the product of applying analysis and judgment to relevant information to determine the relationship among the operational and mission variables to facilitate decision making (ADP 5-0).

1-8. Upon receipt of a warning order or mission, the commander and staff draw relevant information categorized by the operational variables and filter it into the mission variables used during mission analysis. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC). During IPB, the staff focuses on the relevant aspects of the OE as they pertain to the staff's warfighting function. The staff focuses primarily on the mission variables of enemy, terrain and weather, and civil considerations. However, depending on the staff's echelon, the type of OE, the type of operation, and changes in the OE, the staff may need to update its analysis to ensure the mission focus is both relevant and accurate.

1-9. To be effective, IPB must—

- Be a continuous process with all staff members providing input.
- Account for all domains, the information environment, and the electromagnetic spectrum (EMS). (See chapter 8.)
- Define the commander's area of interest (AOI) by its geographic boundaries to focus collection and analysis within the AOI.
- Describe how the enemy, terrain and weather, and civil considerations will affect friendly and threat operations.
- Include relevant aspects of the OE for decisive, shaping, and sustaining operations. (See FM 3-0 for more on these operations.)
- Support each step of the MDMP with IPB products.
- Determine how the interactions of friendly forces, threat forces, and local populations affect each other to continually create outcomes that positively affect friendly operations. This aspect of IPB is not the sole responsibility of the intelligence staff. It involves the commander and the entire staff collaborating to determine these effects.
- Support the operational framework considerations—physical, temporal, cognitive, and virtual. (See paragraph 1-60.)
- Facilitate the commander's ability to visualize the desired end state and a broad concept of how to shape current conditions into that end state.
- Support the commander in directing the intelligence effort.
- Facilitate understanding threat characteristics and the threat's goals, objectives, and COAs.

1-10. IPB is most effective and best aids the commander's decision making when the intelligence staff integrates the expertise of the other staff sections and supporting elements into its analysis. (See paragraphs 1-27 through 1-33.) This is especially true when operating in environments where the effects of the operational and mission variables are complex, multidimensional, and not easily determined.

1-11. IPB assists commanders in reducing uncertainty by evaluating how the enemy, terrain and weather, and civil considerations may affect operations and decision making. Most intelligence requirements are generated because of IPB and its interrelationship with decision making.

1-12. A key aspect of IPB is refinement. The conclusions 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. (See FM 6-0 for more information on the running estimate.) This refinement ensures the commander's decisions are based on the most current information and intelligence available.

IPB PROCESS ACTIVITIES

1-13. The IPB process consists of the following four steps:

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

Note. Although there are four steps to the IPB process, it is important to note that IPB is a continuous process. Continuous analysis and assessment are necessary to maintain situational understanding of an OE in constant flux.

STEP 1—DEFINE THE OPERATIONAL ENVIRONMENT

1-14. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An OE for any specific operation comprises more than the interacting variables that exist within a specific physical area. It also involves interconnected influences from the global or regional perspective (such as politics, economics) that affect OE conditions and operations. Thus, each commander's OE is part of a higher commander's OE. Defining the OE results in the identification of—

- Significant characteristics of the OE that can affect friendly and threat operations.
- Gaps in current intelligence holdings.

1-15. Step 1 is important because it assists the commander in defining relative aspects of the OE in time and space. This is equally important when considering characteristics of multi-domain OEs. Aspects of these OEs may act simultaneously across the battlefield but may only factor in friendly or threat operations at specific times and locations.

1-16. During step 1, the intelligence staff must identify those significant characteristics related to the mission variables of enemy, terrain and weather, and civil considerations that are relevant to the mission. The intelligence staff evaluates significant characteristics to identify gaps and initiate information collection. The intelligence staff then justifies the analysis to the commander. Failure to identify or misidentifying the effect these variables may have on operations at a given time and place can hinder decision making and result in the development of an ineffective information collection strategy. During step 1, the area of operations (AO), AOI, and area of influence must also be identified and established. (Chapter 3 discusses step 1 fully.)

1-17. Understanding friendly and threat forces is not enough; other factors, such as culture, languages, tribal affiliations, and operational and mission variables, can be equally important. Identifying the significant characteristics of the OE is essential in identifying the additional information needed to complete IPB. Once approved by the commander, this information becomes the commander's initial intelligence requirements—which focus the commander's initial information collection efforts and the remaining steps of the IPB process.

1-18. Additionally, where a unit will be assigned and how its operations will synchronize with other associated operations must be considered. For example, the G-2/S-2 should be forming questions regarding where the unit will deploy within the entire theater of operations and the specific logistics requirements needed to handle the operation's contingency plans.

STEP 2—DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

1-19. During step 2 of the IPB process, the intelligence staff describes how significant characteristics affect friendly operations. The intelligence staff also describes how terrain, weather, civil considerations, and friendly forces affect threat forces. This evaluation focuses on the general capabilities of each force until the development of threat COAs in step 4 of IPB and friendly COAs later in the MDMP. The entire staff determines the effects of friendly and threat force actions on the population.

1-20. If the intelligence staff does not have the information required to form conclusions, it uses assumptions to fill information gaps—always careful to ensure the commander understands when assumptions are used in place of facts to form conclusions. (Chapter 4 discusses step 2 fully.)

STEP 3—EVALUATE THE THREAT

1-21. The purpose of evaluating the threat is to understand how a threat can affect friendly operations. Although threat forces may conform to some of the fundamental principles of warfare that guide Army operations, these forces will have obvious, as well as subtle, differences in how they approach situations and problem solving. Understanding these differences is essential to understanding how a threat force will react in a given situation.

1-22. Threat evaluation does not begin with IPB. The intelligence staff conducts threat evaluations and creates threat models during generate intelligence knowledge of the intelligence support to force generation task. Using this information, the intelligence staff refines threat models, as necessary, to support IPB. When analyzing a well-known threat, the intelligence staff may be able to rely on previously developed threat models. When analyzing a new or less well-known threat, the intelligence staff may need to evaluate the threat and develop threat models during the MDMP's mission analysis step. When this occurs, the intelligence staff relies heavily on the threat evaluation conducted by higher headquarters and other intelligence agencies.

1-23. In situations where there is no threat 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. (Chapter 5 discusses step 3 more fully.)

STEP 4—DETERMINE THREAT COURSES OF ACTION

1-24. During step 4, the intelligence staff identifies and develops possible threat COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat COAs to assist in developing and selecting friendly COAs during COA steps of the MDMP. Identifying and developing all valid threat COAs minimize the potential of surprise to the commander by an unanticipated threat action.

1-25. Failure to fully identify and develop all valid threat COAs may lead to the development of an information collection strategy that does not provide the information necessary to confirm what COA the threat has taken and may result in friendly forces being surprised and possibly defeated. When needed, the staff should identify all significant civil considerations (this refers to those civil considerations identified as OE significant characteristics) to portray the interrelationship of the threat, friendly forces, and population activities.

1-26. The staff develops threat COAs in the same manner friendly COAs are developed. The COA development discussion in ADRP 5-0 is an excellent model for developing valid threat COAs that are suitable, feasible, acceptable, unique, and consistent with threat doctrine or patterns of operation. Although the intelligence staff has the primary responsibility for developing threat COAs, it needs assistance from the rest of the staff to present the most accurate and complete analysis to the commander. (Chapter 6 discusses step 4 fully.)

STAFF COLLABORATION

1-27. Precise intelligence is critical to targeting threat capabilities at the right time and place to open windows of opportunity across domains. Commanders and staffs receive effective intelligence when they direct and participate in intelligence warfighting function activities. Close interaction between the commander, G-2/S-2, G-3/S-3, and the rest of the staff is essential, as the entire staff supports unit planning and preparation through the integrating processes and continuing activities.

1-28. From the perspective of fighting for intelligence, the first aspect of supporting operations is developing good information requirements and designating priority intelligence requirements (PIRs) resulting from IPB and the completion of the MDMP. Commanders and staffs must have detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute friendly operations. Staff collaboration assists in developing this detailed knowledge and accounts for possible threat COAs.

1-29. Commanders drive intelligence, intelligence facilitates operations, and operations enable intelligence; this relationship is continuous. Commanders provide tactical and operational experience as it relates to various OEs and missions; they also provide an understanding, visualization, and description of the problem. Commanders assist in shaping the focus and scope of IPB to facilitate an effective MDMP.

1-30. G-2/S-2s facilitate the IPB effort; however, G-2/S-2s and their staffs cannot provide all of the information the commander requires for situational understanding. Other staff sections or supporting elements must assist the intelligence staff in producing and continuously refining all IPB products. Total staff integration ensures a holistic view of the OE, reduces the initial time required for IPB development, and assists the commander in timely decision making. This coordination also improves the quality and accuracy of IPB products.

1-31. Staff sections bring their expertise to IPB as follows:

- The chief of staff or executive officer—
  - Ensures IPB is performed as a collaborative effort.
  - 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 will take, how much time is allocated to mission analysis, and how much time within mission analysis can be suballocated to IPB.
- The G-1/S-1 assists in analyzing the OE to identify its relevant aspects and how they will impact the following, including but not limited to—
  - Casualty assistance operations.
  - Personnel accountability.
  - Essential human resources services.
  - Personnel support activities.
- The G-2/S-2 analyzes the mission variables of enemy, terrain and weather, and civil considerations and assists the commander in improving the understanding of how these variables can affect operations. The G-2/S-2 does this through the production of an intelligence assessment that supports the MDMP, the integrating processes of targeting and risk management, and the continuing activities of information collection and security operations. The rest of the staff assists the G-2/S-2 in this effort. The G-2/S-2 also informs the staff on intelligence capabilities, limitations, and operations. (Appendix A provides the "how to" of IPB as a checklist for the S-2.) Additionally, the G-2/S-2—
  - Facilitates generating intelligence knowledge.
  - Continually coordinates with the staff, outside agencies, and organizations for input to situational understanding.
  - Identifies AOIs and areas of influence.
  - Assists the staff with threat capabilities, vulnerabilities, and intent.
  - Conducts terrain analysis.
  - Determines the threat's composition and disposition.
  - Develops threat templates by warfighting function.

  - With assistance from the other staff sections, determines threat missions, objectives, schemes of maneuver, and desired end states.
  - Coordinates with the staff to identify HVTs and threat COAs.
  - Determines named areas of interest (NAIs) with staff input.
- The G-3/S-3 provides subject matter expertise on the art and science of military operations and—
  - Reviews the G-2/S-2's evaluation of threat COAs.
  - Reviews the G-2/S-2's identification and evaluation of the threat's composition and disposition.
  - Assists the G-2/S-2 with terrain and weather effects on friendly and threat operations.
  - Ensures the G-2/S-2 and other staff members understand the AO and other friendly maneuver limitations and parameters specified by higher headquarters.
  - Ensures the G-2/S-2 and other staff members understand available friendly maneuver forces.
  - Assists in selecting high-payoff targets (HPTs), target areas of interest (TAIs), and decision points.
  - Assists in developing the decision support template (DST).
  - Evaluates threat COAs to ensure they are valid from an operational perspective.
  - Evaluates threat situation templates, COA statements, HVT lists, and civil considerations overlays and assessments to ensure they contain the information necessary to support friendly COA development and analysis.
  - Evaluates the event template and matrix to ensure they contain the information necessary to support friendly COA analysis and the development of the DST.
- The G-4/S-4 provides subject matter expertise on sustainment operations and assists the G-2/S-2 in—
  - Identifying and evaluating threat and host-nation logistics capabilities.
  - Potential supply routes and resupply points.
  - Identifying and evaluating threat logistics capabilities.
- The G-5/S-5 is the principal staff officer for planning mid- to long-range operations. Coordination with the G-5/S-5 ensures the synchronization of IPB and information collection for future operations or the next phase of an operation. The G-5/S-5 also assists in developing branches and sequels as well as deception plans.
- The G-6/S-6 provides subject matter expertise on friendly communications systems and assists the G-2/S-2 in identifying and evaluating friendly communications systems' vulnerabilities to cyberspace and electronic attack. Additionally, the G-6/S-6 coordinates with the spectrum manager to determine friendly forces' vulnerabilities to known threat systems.
- The G-9/S-9 provides subject matter expertise on civil affairs operations. This staff assists the G-2/S-2 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.
  - Identifying protected targets. (The civil affairs staff, along with the chief of fires or fire support officer, provides this assistance.)
  - Creating and maintaining civil considerations overlay, assessments, and data files and/or databases.
  - Providing information on the neutral population, and how it supports/opposes the host nation and friendly and threat forces.

1-32. The intelligence staff coordinates with key supporting elements, whose expertise supports IPB:

- The operations security officer, co-located with the S-3, provides subject matter expertise on friendly vulnerabilities during the phases of an operation. For example, friendly forces may be vulnerable to different threat capabilities; the operations security officer can assist in identifying by phase which threat assets and capabilities should be the focus of information collection and targeting.

- Information operations provide subject matter expertise on shaping operational activities in and through the information environment and cyberspace. (See FM 3-13.) The information operations officer is responsible for—
  - Integrating information-related capabilities.
  - Assisting the G-2/S-2 to identify and evaluate threat information capabilities and deception and denial capabilities, as well as the means to influence the population.
  - Providing information on friendly, neutral, and threat key communicators to use as part of a nonlethal engagement strategy through various information-related capabilities.
- The chief of fires at division and above and the fire support officer at brigade and below provide subject matter expertise on fires. The fires (artillery and air defense) subject matter expert—
  - Assists the G-2/S-2 in—
    - Developing threat fires-related HVTs.
    - Evaluating threat fire support operations, including identifying potential friendly HPTs from the threat perspective.
    - Assessing potential threat artillery.
    - Developing situation and event templates of probable threat employment of fire support assets.
    - Positioning threat fire support assets on the situation template.
  - Coordinates with the G-2/S-2 in identifying types of threat artillery and evaluating likely threat artillery and/or missile positions.
  - Assists the staff in identifying and evaluating potential engagement areas and kill zones.
  - Assists, in coordination with the G-2/S-2 and the staff weather officer, in determining what effect weather and terrain will have on threat artillery systems.
  - Participates in the selection of HPTs, TAIs, and decision points.
  - Coordinates with the G-2/S-2 and the G-3/S-3 in determining the fire support effort to the friendly information collection effort and in countering the threat information collection effort.
  - Assists the staff on protection from threat air.
- The engineer coordinator provides subject matter expertise on mobility and countermobility and assists the G-2/S-2 in developing threat obstacle plans for the situation template. The engineer coordinator—
  - Assists the staff in identifying and assessing obstacles along friendly and avenues of approach (AAs).
  - Assists the G-2/S-2 with terrain analysis and those terrain analysis products that support IPB.
  - Assists the G-2/S-2 in developing the MCOO.
  - Provides staff input concerning threat mobility, countermobility, and survivability doctrine, tactics, and equipment capabilities.
  - Assists in developing situation and event templates regarding the probable employment of threat engineer assets and obstacle emplacement.
  - Coordinates with the G-2/S-2 and the G-3/S-3 in determining engineer support to the friendly information collection effort and in countering the threat information collection effort.
  - Provides engineer reconnaissance input, including the military load-capacity of bridges. (See ATP 3-34.81.)
- The chemical, biological, radiological, and nuclear (CBRN) officer provides subject matter expertise and assists the G-2/S-2 in determining the locations of CBRN assets, production, and storage facilities; the availability of precursor chemicals and materials; and the potential areas of CBRN employment. The CBRN officer—
  - Provides input to the G-2/S-2 on threat CBRN doctrine, capabilities, and employment.
  - Assists the staff in templating likely locations of threat CBRN assets.
  - Advises the staff on threat doctrine concerning the use of obscurants, likely triggers for its employment, and types of obscurant-generating equipment.

    - Assists the staff in locating water sources that friendly and threat forces could use for CBRN decontamination operations.
    - Advises the G-2/S-2, in coordination with the staff weather officer, on the impact of the weather and terrain on friendly and threat CBRN operations.
- The air defense artillery (ADA) officer provides subject matter expertise on ADA and assists the G-2/S-2 in determining the locations of ADA assets and potential areas of employment. The ADA officer—
    - Advises the G-2/S-2, in coordination with the staff weather officer, on the impact of the weather and terrain on friendly and threat ADA operations.
    - Provides input to the G-2/S-2 on threat ADA doctrine, capabilities, and employment.
    - Assists the staff in templating likely locations of threat ADA assets.
    - Assists the staff in determining weather and terrain effects on friendly and threat ADA operations.
    - Provides staff input concerning threat ADA doctrine, tactics, capabilities, and equipment.
    - Assists in developing threat HVTs.
    - Assists in identifying threat air AAs and assessing threat fixed-wing and rotary-wing air defense capabilities. ***Note.*** An air AA refers to the air route of a threat aerial or tactical ballistic missile force of a given size leading to its objective or to the key terrain in its path. (See ATP 3-01.16.)
- The spectrum manager provides subject matter expertise on procedures for using the EMS and for avoiding communications interferences.
- The electronic warfare (EW) officer—
    - Provides subject matter expertise on ground-based, airborne, and functional EW employment considerations.
    - Assists in developing threat EW-, communications-, and radar-related HVTs.
    - Has additional responsibilities as the cyberspace planner. (See FM 3-12.)
    - Assists the G-2/S-2 in determining the locations of EW assets and potential areas and methods of employment.
    - Assists in determining friendly forces' vulnerabilities to known threat systems.
- The surgeon provides subject matter expertise for the analysis and disposition of captured enemy medical materiel and for the analysis of any medications carried by captured or detained threat personnel.

1-33. External assets, such as the following, provide additional subject matter expertise for input to the IPB process: red teams, red cells, foreign-area officers, international affairs officers, cultural enablers, State Department officers, regional experts, psychological operations units, and other special operations units.

RELATIONSHIPS

1-34. As one of the integrating processes, IPB is integral to targeting, risk management, information collection, planning, and decision making. (See chapter 2.) IPB is also related to the generate intelligence knowledge and situation development tasks.

TARGETING

1-35. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). During steps 3 and 4 of IPB, the intelligence staff identifies HVTs associated with each threat capability or COA. This assists the fires cell in conducting target-value analysis. A *high-value target* is a target the enemy commander requires for the successful completion of the mission (JP 3-60).

1-36. The following techniques may be useful in identifying and evaluating HVTs:

- Identify HVTs from existing intelligence studies, database evaluations, patrol debriefs, and size, activity, location, unit, time, and equipment (also called SALUTE) reports. Reviewing threat tactics, techniques, and procedures (TTP) and previous threat operations as well as understanding the threat task, purpose, method, and end state are useful.
- Identify assets that are key to executing the primary operation, branches, or sequels.
- Determine how the threat might react to the loss of each identified HVT. Consider the threat's ability to substitute other assets and adopt branches or sequels.
- Consider AO and AOI effects and potentially broader effects.
- Consider how the threat may use multiple capabilities to create the effects of one or more HVTs.
- Consider how the threat may use assets by phases of an operation, which may lead to classifying certain threat assets, functions, or systems as HVTs across all domains, the information environment, and the EMS.
- Consider the multi-domain nature of complex OEs and how threat forces may use assets to disrupt friendly operations at multiple echelons and locations.
- After identifying HVTs, place them in order of their relative worth to the threat's operation and record them as part of the threat model. The value of an HVT varies throughout an operation.

1-37. 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. The staff develops HPTs, which can include various threat considerations that can be detrimental to the friendly mission's success.

1-38. The intelligence staff, aided by other staff sections, also identifies indicators associated with those targets that can assist in determining their locations and activities. Identifying HVTs during IPB is essential to developing HPTs during the COA development step of the MDMP, and to refining those targets throughout the operations process, particularly during targeting boards and meetings. (Chapter 6 discusses the identification of HVTs and indicators.)

1-39. During targeting meetings, the intelligence officer, along with other staff sections or supporting elements, assesses friendly capabilities, friendly missions, and the effects of friendly actions on the civilian populace. As HPTs are developed, the analysis of the enemy, terrain and weather, and civil considerations conducted during IPB assists in developing intelligence target packages on those targets. (See ATP 3-60.)

RISK MANAGEMENT

1-40. *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0). IPB assists in identifying, quantifying, and mitigating risks. For example, a commander may consider attacking a target on the protected target list. However, because the entire staff performs IPB, which provides an understanding of the OE based on analysis of the mission variables, the true impact of attacking the target can be articulated (the reason the target is on the protected target list), and the commander can make an informed decision to balance risk with mission benefit. 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.)

INFORMATION COLLECTION

1-41. Information collection relies on IPB results. The staff's continuous input to IPB provides an analysis of the OE and the options it presents to friendly and threat forces. It also provides the following information required to plan information collection activities:

- Characteristics of the AOI that will influence friendly and threat operations (including civil considerations).
- Threat 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, doctrine, tactics, techniques, and behavior.
- Possible and likely threat COAs.
- HVTs.

1-42. The Army executes information collection through the operations and intelligence processes (with an emphasis on intelligence analysis and leveraging national to tactical intelligence). Even if the mission is new, the intelligence staff can identify and tap into ongoing or existing information collection activities or joint intelligence, surveillance, and reconnaissance (also called ISR) collection that may offer relevant information to fill gaps. These requirements identify the critical pieces of information the commander must know to successfully conduct (plan, prepare, execute, and assess) operations.

1-43. Ideally, information collection should enable staffs to develop a perception of the threat and the situation on the battlefield that matches the actual threat and situation on the battlefield. In reality, information collection does not eliminate all information gaps that concern commanders and staffs. Intelligence staffs, in conjunction with the other staff sections, should be prepared to fill gaps with reasonable assumptions and continually send out additional requests for information to refine IPB.

1-44. There is a relationship between IPB and information collection—the IPB products that feed intelligence drive information collection requirements. This means that the IPB process identifies intelligence gaps that are translated into information requirements and PIRs, which are then answered through collection.

1-45. The staff collaborates on information considerations and integrates available resources into an integrated information collection plan. Well-stated information requirements assist the commander in accomplishing the mission by illustrating those key knowledge gaps and earmarking them for collection.

1-46. Developing requirements also supports the commander's decision making regarding targeting. To target the threat effectively, the staff develops NAIs and TAIs. A *named area of interest* is the geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected, usually to capture indications of adversary courses of action (JP 2-01.3). A *target area of interest* is the geographical area where high-value targets can be acquired and engaged by friendly forces (JP 2-01.3). NAIs should not be tied to a specific terrain; rather, they should be based on threat locations or suspected locations.

NAI Example

Instead of focusing on an area surrounding a hilltop named 1631 where the enemy may have placed an air defense unit, analysts should focus NAIs on the enemy's unit or functional capability. For example, analysts should focus on the suspected locations where the enemy may place its combined arms reserve or subterranean locations to conduct a counterattack. To refine the locations, analysts should study the enemy's doctrinal or historical use of the combined arms reserve, 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.

1-47. Units need to conduct information collection consistently and continuously. To be effective, information collection must be based on IPB results; it must be adjusted as IPB results are refined through the situation development process. Conversely, the results of reconnaissance, surveillance, security operations, and intelligence operations—the primary means for information collection—drive the refinement of IPB results 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.

GENERATE INTELLIGENCE KNOWLEDGE

1-48. Not all information required to conduct IPB will be readily available to intelligence staffs upon receipt of mission. Generate intelligence knowledge is critical for G-2/S-2s to maintain analytical proficiency and situational awareness of possible impending missions and contingencies. Generate intelligence knowledge begins before mission receipt and provides the relevant knowledge required about the OE for the conduct of operations. Once the intelligence officer and other staff sections collect data on the OE, they organize the data into databases. The information obtained is refined into knowledge for use in mission analysis through functional analysis. (See ATP 2-33.4 for more on 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. Sources for generating intelligence knowledge include but are not limited to—

- Internet:
  - Nonsecure Internet Protocol Router Network (also called NIPRNET).
  - SECRET Internet Protocol Router Network (also called SIPRNET).
  - Joint Worldwide Intelligence Communications System (also called JWICS).
  - Intelligence databases.
- Other military Services or agencies:
  - United States (U.S.) Air Force.
  - U.S. Marine Corps Intelligence Department.
  - Marine Corps Intelligence Activity.
  - National Geospatial-Intelligence Agency (also called NGA).
  - National Ground Intelligence Center (also called NGIC).
  - Defense Intelligence Agency (also called DIA).
  - Office of Naval Intelligence (also called ONI).
  - U.S. Coast Guard.
  - Army and other Service special operations forces.
- Outside agencies:
  - Central Intelligence Agency (also called CIA).
  - National Security Agency (also called NSA).
  - U.S. Agency for International Development (also called USAID).
- Outside organizations:
  - World Health Organization (also called WHO).
  - International Committee of the Red Cross (also called ICRC).
- University research.
- Country studies.
- Area estimates.
- Intelligence summaries.
- Open-source information.

1-49. The types of useful information obtained from sources for generating intelligence knowledge include but are not limited to—

- Order of battle data files.
- Current situation.
- Geography.
- Economy.
- Population.
- Government and military leadership.
- Centers of gravity.
- Demographics.
- Regional partners.
- Threat systems and functions.
- Past conflicts.
- Rule of law status.
- Infrastructure development.

1-50. Information gained though generate intelligence knowledge can also be used to identify intelligence gaps for possible contingencies, therefore reducing the time needed for research in the event of mission receipt. Generate intelligence knowledge is the foundation for performing IPB and mission analysis. The primary product of the generate intelligence knowledge task is the initial data file, which is created based on the analysis of the operational variables (PMESII-PT). (See FM 2-0 for more information on the generate intelligence knowledge task.)

SITUATION DEVELOPMENT

1-51. Situation development is a process for analyzing information and producing current intelligence concerning the relevant aspects of the OE (the mission variables of enemy, terrain and weather, and civil considerations) within the AO before and during operations. The process assists the intelligence staff in recognizing and interpreting indicators of threat intentions and objectives. Situation development—

- Confirms or denies threat COAs.
- Provides threat locations.
- Explains what the threat is doing in relation to the friendly force commander’s intent.
- Provides an estimate of threat combat effectiveness.

1-52. The locations and actions of noncombatant elements and nongovernmental and other civilian organizations in the AO that may impact operations should also be considered. Through situation development, the intelligence officer—

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

1-53. Situation development assists commanders in their decision making, including when to execute branches and sequels. The intelligence staff uses the products developed during IPB as a baseline to begin situation development.

MULTI-DOMAIN UNDERSTANDING OF THE OPERATIONAL ENVIRONMENT

1-54. The interrelationship of the air, land, maritime, space, and cyberspace domains, the information environment (which includes cyberspace), and the EMS requires a multi-domain situational understanding of the OE. (See FM 3-0.) Seeing, understanding, and responding to windows of vulnerability or opportunity within each domain and the information environment can reduce risk to the force and enhance success in chaotic and high-tempo operations, such as large-scale combat operations. This makes situational understanding essential to managing risk.

1-55. When commanders and staffs seek to understand friendly and threat capabilities, they consider how, when, and why those capabilities are employed in each domain, the information environment, and the EMS. From this understanding, commanders can better identify windows of opportunity during operations. This allows a portion of the joint force to establish a decisive point for the multi-domain convergence of capabilities, which must be supported by continuous intelligence operations across the domains for the best effect. Since many friendly capabilities are not organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations.

> ***Note.*** *Decisive point* is a geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an enemy or contribute materially to achieving success (JP 5-0).

1-56. During large-scale combat operations against a peer threat, ground-force commanders may be required to conduct tactical activities, such as a deliberate attack, to shape the OE and gain a position of relative advantage for activities, such as joint fires, within the other domains. Once that position is achieved, operations would continue to increase the position of relative advantage in order to create a longer window of superiority to facilitate follow-on missions and operations across the domains.

> ***Note.*** *Position of relative advantage* is a location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage (ADRP 3-0).

1-57. Intelligence supports the commander by visualizing the threat and detecting possible threat COAs. Army forces must integrate and synchronize these actions across multiple domains to create opportunities to dislocate, isolate, disintegrate, and destroy enemy forces. (See FM 3-0 for more information on these defeat mechanisms.) Army forces strive to use intelligence, mobility, protection, and firepower to strike the enemy unexpectedly in multiple domains and from multiple directions, denying the enemy freedom to maneuver by creating multiple dilemmas that the enemy commander cannot effectively address. Intelligence supports these operations by facilitating situational understanding and supporting decision making. Intelligence assists commanders in seeing through the fog and friction of war.

1967 Arab-Israeli Six-Day War

Tensions between Israel and the Arab alliance of Egypt, Jordan, Iraq, and Syria were heightened following the 1948 Arab-Israeli War. Closed to Israeli shipping since 1950 by Egypt, the Straits of Tiran, located in the Red Sea between the Sinai Peninsula and Tiran Island, were critical to the shipping of oil and other imports to Israel. The re-opening of the straits was a chief Israeli objective. Egypt's blockade of the straits continued to cause strained relations between Egypt and Israel, leading up to May 1967 when Egypt President Gamal Abdel Nasir deployed Egyptian forces along Egypt's border with Israel and banned Israeli ships from using the Gulf of Aqaba, the location of Israel's primary port in Eilat. Sensing further Egyptian and Arab military alliance actions, Israel Prime Minister Levi Eshkol ordered a preemptive strike against Egyptian Air Force assets still on the ground. The strike destroyed more than 90 percent of the Egyptian Air Force and facilitated Israeli freedom of action in the air domain to counter an overwhelming Egyptian force in the land domain. Without Egyptian Air Force availability to provide cover to mobilized Egyptian armored assets, Egyptian tank units were soundly defeated in less than 96 hours.

Window of Opportunity	Exploit the Window	Position of Relative Advantage
Israeli Air Force superior to the Egyptian Air Force.	Israeli Air Force establishes freedom of action in the air domain.	Israeli Air Force destroys mobilized Egyptian tank units.

IPB Products to Identify

Threat overlay, threat model, threat template, situation template, threat model, threat template, situation template, and event template and matrix

Enable

- **DST and matrix. *Note.*** Although not IPB products, the DST and matrix assist in identifying friendly actions to counter threat COAs. (See figure 6-14 on page 6-23.)
- **Information collection matrix. *Note.*** Although not an IPB product, the information collection matrix can assist in answering information gaps and identifying indicators of threat intentions. (See figure 6-15 on page 6-24.)

Importance of Domain Interdependence

1-58. Domain interdependence refers to the reliance on one or multiple domains to leverage effects or information. Domains provide a means of viewing the OE based on how capabilities are arrayed and employed. An OE does not comprise a single domain; a capability's effects are not limited to a single domain; and a capability is not employed in a single domain. For example, a satellite is launched from the ground and uses space as a medium for flight. The satellite may collect information from multiple domains and transmit that information using cyberspace as a medium to reach the ground, where the information can be processed, exploited, and disseminated. It is important for commanders and staffs to understand interdependence in order to visualize when and where capabilities can be leveraged by friendly, neutral, and threat forces.

1-59. Because a multitude of effects (including threat, terrain, and weather) can cross multiple domains, the interdependence of the domains, the information environment, and the EMS must be considered when performing IPB. To do this, the S-2, with assistance from other staff members and possibly outside organizations, must address the operational framework considerations and view the OE holistically.

Operational Framework Considerations

1-60. A thorough IPB effort and intelligence analysis assist each echelon in focusing operations on all significant aspects of the OE in time and space across multiple domains. This prevents each echelon from focusing only on the close fight and current operations. A broad focus across the operational framework considerations assists commanders and staffs in better identifying friendly windows of opportunity and threat windows of vulnerability within and across each domain and the information environment. An *operational framework* is a cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations (ADP 1-01). Table 1-1 lists the operational framework considerations and how IPB and subsequent intelligence analysis support each consideration. (See FM 3-0 for details on operational framework considerations.)

Table 1-1. IPB and intelligence analysis support to operational framework considerations

Operational framework considerations	*Intelligence preparation of the battlefield (IPB) and intelligence analysis support*
Physical considerations include geography, terrain, infrastructure, populations, distance, weapons ranges and effects, and known threat locations.	• Intelligence support begins well before the deployment of forces, through generate intelligence knowledge, which addresses the operational variables. Information gained during generate intelligence knowledge is used by commanders and staffs to assist in framing the operational environment during the Army design methodology. • IPB provides detailed analysis of the mission variables of threat, terrain and weather, and civil considerations to determine effects on operations. • IPB and intelligence analysis assist in determining relevant aspects within an area of operations (such as civil considerations characteristics) that are critical in determining how friendly operations may be impacted during the consolidation of gains. • Intelligence analysis is critical to the designation of a deep area, the fire support coordination line, and the area of interdiction.
Temporal considerations are related to time, including when capabilities can be used, how long they take to generate and employ, and how long they must be used to achieve desired effects.	• IPB is a process that is both geographically and temporally specific. • Developing threat courses of action during IPB is based on identifying threat objectives, goals, timelines, and end states. • IPB provides a temporal context using rates of movement, time phase lines, phases of threat fires, and other templates to capture threat timing.
Cognitive considerations relate to people and how they behave. They include information pertaining to threat decision making, threat will, the nation's will, and the population's behavior.	• IPB accounts for aspects associated with the center of gravity and the threat's morale and willingness to continue operations. • Intelligence support to continuous operational assessments considers many relevant aspects of the operational environment, including sociocultural factors. • IPB also considers all significant aspects of the operational environment associated with the various civil considerations.
Virtual considerations pertain to activities and entities, both friendly and threat, residing in cyberspace.	• IPB and intelligence analysis, in coordination with the cyberspace electromagnetic activities section, provide intelligence on the threat's likely activities within the information environment, which includes cyberspace.

HOLISTIC VIEW OF THE OPERATIONAL ENVIRONMENT

1-61. During IPB, each staff section and supporting element provide input. This ensures a holistic view of the OE. Subsequently, the IPB effort assists in identifying domain windows of opportunity to exploit threat vulnerabilities. A holistic view of the OE assists the commander in understanding and visualizing the multi-domain extended battlefield. Analysis of the five domains and where, how, and when information flows is required to understand how friendly and threat force capabilities may be impacted by aspects within each domain. Friendly, threat, and neutral capabilities often depend on a variety of aspects, such as nodes, systems, and subsystems across the five domains. Knowing how threat forces may use their capabilities throughout the five domains, the information environment, and the EMS is essential to understanding the threat's intent and desired end state as well assessing the impacts friendly and threat operations may have on the OE. The holistic view of the OE encompasses—

- The physical areas and factors of the five domains.
- The information environment. (See chapter 8 for a detailed discussion.)
- The systems perspective, which includes the relationships and interdependencies of friendly, threat, and neutral PMESII-PT systems, subsystems, objects, and affiliated attributes.

1-62. Analysts must also consider the conditions, circumstances, and influences that affect the employment of capabilities and the decisions of the commander. This includes understanding those considerations, both independently and as a composite, to apply combat power, protect the force, and complete a mission. Physical areas, nonphysical aspects, factors, and a systems perspective are means of identifying and understanding the conditions, circumstances, and influences within the OE. These means may be outcomes of IPB or identified before IPB—either way, each staff member participating in the IPB process must consider them.

Physical Areas and Factors

1-63. Within the OE, physical areas include the assigned operational area and the associated AOI and area of influence necessary to conduct operations within the air, land, maritime, space, and cyberspace domains and the information environment. Factors, including but not limited to terrain, threat forces, weather, and the location of man-made obstacles and structures, can impact operations in a given physical area. The identification of physical areas and factors residing within the OE is critical to understanding effects on friendly and threat operations. (See JP 2-01.3 for a detailed discussion of physical areas and factors.)

Systems Perspective

1-64. A systems perspective focuses on a multitude of systems in the OE and their associated functions. The identification of which systems are associated with specific functions and their interdependence with other systems is critical to understanding when and where threats may decide to use them. A systems perspective generates understanding that facilitates identifying potential cues and warnings, lines of operations, centers of gravity, and decision points. No single staff section or capability attached to or organic to the commander can employ a systems perspective in isolation. Just as IPB is a staff process, so is employing a systems perspective to facilitate IPB. (For additional information on systems perspective, see JP 2-01.3 and JP 3-0.)

IPB AND THE ARMY'S STRATEGIC ROLES

1-65. Operations to shape, prevent, conduct large-scale ground combat, and consolidate gains summarize the Army's strategic roles as part of a joint force. Each strategic role presents a unique set of intelligence requirements discussed fully in FM 2-0. Table 1-2 on page 1-16 discusses IPB throughout each strategic role.

Table 1-2. IPB and the Army's strategic roles

Army strategic role	*Intelligence preparation of the battlefield (IPB) support*
Shape	Time is usually not a constraint. Each echelon performs generate intelligence knowledge, warning intelligence, and IPB to support operational planning, regionally aligned activities, and training focused on large-scale combat operations. IPB and other intelligence products are constantly refined. A large portion of the IPB products generated are pushed down from the joint level to military intelligence brigades-theater and then customized for each specific echelon.
Prevent	
Conduct large-scale ground combat	Time is often a major constraint. When possible, the staff uses intelligence products developed before combat. At echelons corps and below, despite multi-domain considerations, the focus is on tactical considerations, especially threat characteristics (including the correlation of forces data), weather, terrain, and other significant characteristics of the operational environment. Each echelon must effectively perform IPB and quickly generate those products that drive the rest of the military decision-making process.
Consolidate gains	Time is usually not a constraint. IPB products tend to flow both top down and bottom up. Often, the IPB focus shifts to address not only the threat but also stability tasks, the local environment, and the information environment. At echelons corps and below, more complexities within the operational environment become important considerations.

Chapter 2

IPB Support to Planning and Decision Making

IPB AND PLANNING

2-1. Commanders conduct planning to—

- Understand a problem or situation.
- Envision a desired future.
- Develop COAs, with assistance from their staffs, that can bring about that desired future.

2-2. During planning, commanders focus their activities on understanding, visualizing, and describing the OE, while directing and assessing operations. IPB is one of the processes commanders use to assist in planning. IPB supports the MDMP and troop leading procedures—two of the three methodologies that assist commanders and staffs in planning.

MILITARY DECISION-MAKING PROCESS

2-3. The *military decision-making process* is an interactive planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). (See ADRP 5-0 for more information on the MDMP.) The MDMP is a seven-step planning process:

- Step 1—Receipt of mission.
- Step 2—Mission analysis.
- Step 3—COA development.
- Step 4—COA analysis (war game).
- Step 5—COA comparison.
- Step 6—COA approval.
- Step 7—Orders production, dissemination, and transition.

2-4. The MDMP 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 or operation order for execution.

2-5. Figure 2-1 shows the relationship between the IPB steps and the MDMP steps.

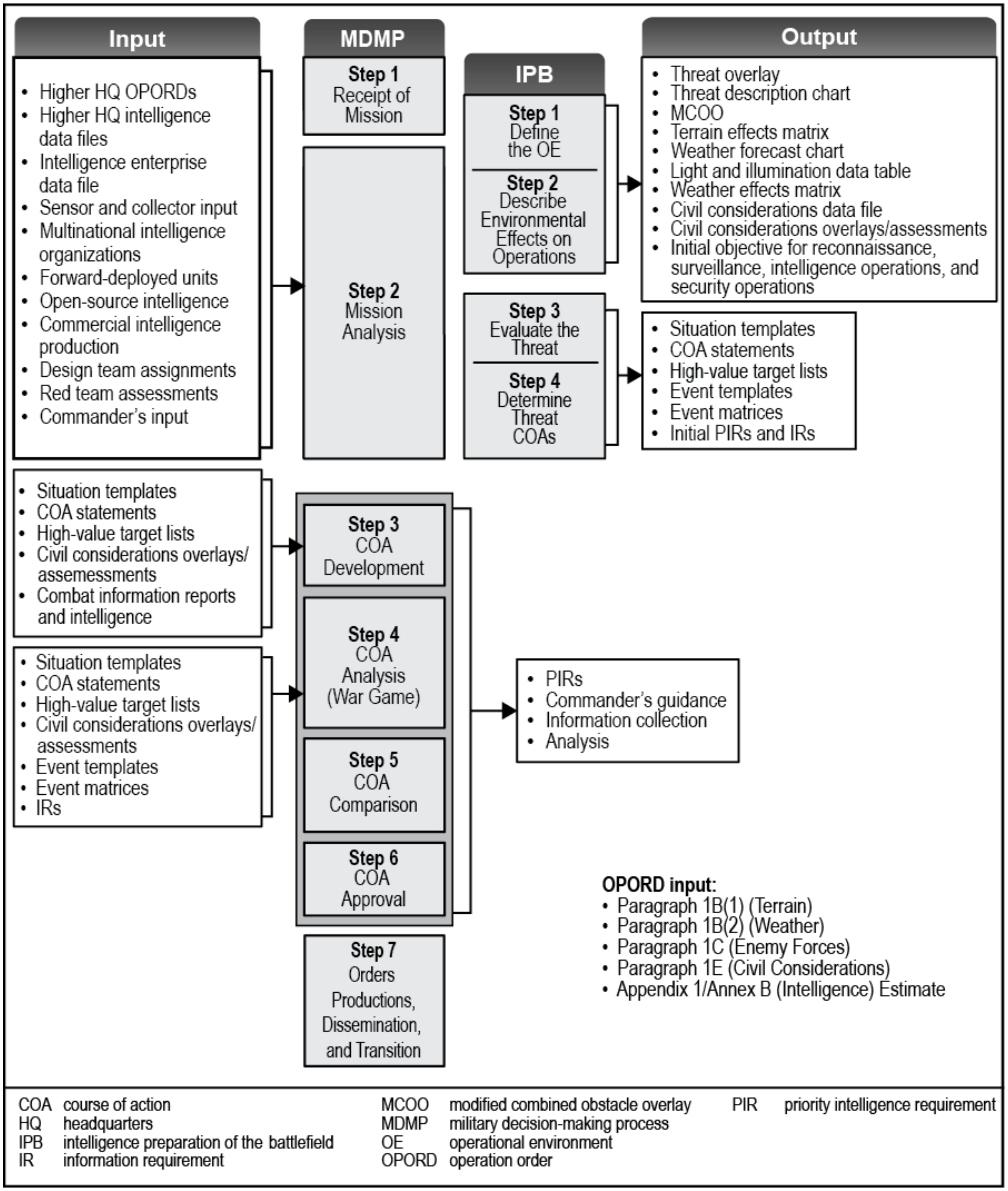

Input
MDMP
IPB
Output
• Higher HQ OPORDs
• Higher HQ intelligence data files
• Intelligence enterprise data file
• Sensor and collector input
• Multinational intelligence organizations
• Forward-deployed units
• Open-source intelligence
• Commercial intelligence production
• Design team assignments
• Red team assessments
• Commander's input
Step 1 Receipt of Mission
Step 2 Mission Analysis
Step 1 Define the OE
Step 2 Describe Environmental Effects on Operations
• Threat overlay
• Threat description chart
• MCOO
• Terrain effects matrix
• Weather forecast chart
• Light and illumination data table
• Weather effects matrix
• Civil considerations data file
• Civil considerations overlays/assessments
• Initial objective for reconnaissance, surveillance, intelligence operations, and security operations
Step 3 Evaluate the Threat
Step 4 Determine Threat COAs
• Situation templates
• COA statements
• High-value target lists
• Event templates
• Event matrices
• Initial PIRs and IRs
• Situation templates
• COA statements
• High-value target lists
• Civil considerations overlays/ assemessments
• Combat information reports and intelligence
• Situation templates
• COA statements
• High-value target lists
• Civil considerations overlays/ assessments
• Event templates
• Event matrices
• IRs
Step 3 COA Development
Step 4 COA Analysis (War Game)
Step 5 COA Comparison
Step 6 COA Approval
Step 7 Orders Productions, Dissemination, and Transition
• PIRs
• Commander's guidance
• Information collection
• Analysis
OPORD input:
• Paragraph 1B(1) (Terrain)
• Paragraph 1B(2) (Weather)
• Paragraph 1C (Enemy Forces)
• Paragraph 1E (Civil Considerations)
• Appendix 1/Annex B (Intelligence) Estimate
COA course of action
HQ headquarters
IPB intelligence preparation of the battlefield
IR information requirement
MCOO modified combined obstacle overlay
MDMP military decision-making process
OE operational environment
OPORD operation order
PIR priority intelligence requirement

Figure 2-1. IPB and the MDMP steps

Understand the Situation and Mission

2-6. During the mission analysis step of the MDMP, the staff conducts IPB 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 operation order:

- Intelligence gaps.
- Information requirements.
- Threat situation templates with associated COA statements and HVT lists.
- Event templates with associated event matrices.
- Relative combat power matrices for threat forces.
- Geospatial intelligence tactical decision aids required to support continual planning (terrain effects).
- Weather tactical decision aids required to support continued planning (operational climatology or weather forecast 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 Courses of Action

2-7. In the COA development step of the MDMP, friendly COAs are broad potential solutions to an identified problem. These solutions are based on conclusions reached during initial IPB and any refinement of those conclusions that occurs between the conclusion of mission analysis and the beginning of COA development. The primary IPB product required for COA development is the threat situation template with the associated COA statement.

Decide on a Course of Action that Best Accomplishes the Mission

2-8. In the COA analysis step of the MDMP, deciding on a COA enables commanders and staffs to identify difficulties or coordination problems and probable consequences of planned actions for each COA being considered. The primary IPB products required for deciding a COA are—

- Threat situation templates with associated COA statements.
- Event templates with associated event matrices.
- Relative combat power matrices for threat forces.

2-9. During stability tasks, additional products may be required, such as civil considerations overlays and assessments. Information collection operations conducted during the mission analysis step of the MDMP provide pertinent combat information that informs COA development. This information confirms or denies the threat situation template and the associated COA statement.

Produce an Operation Plan or Operation Order for Execution

2-10. At the conclusion of the MDMP, the staff prepares the operation plan or order 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.

TROOP LEADING PROCEDURES

2-11. The troop leading procedures extend the MDMP to the small-unit level. The MDMP and troop leading procedures are similar but not identical. *Troop leading procedures* is 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.

2-12. The sequence of actions assists leaders in effectively using available time to issue orders and execute tactical operations. Troop leading procedures consist of eight steps. The sequence of the steps is not rigid. Leaders modify the sequence to meet the mission, situation, and available time. Some of the following steps may be performed concurrently while other steps may be performed 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.

2-13. The intelligence staff at the battalion intelligence cell develops and provides the IPB products required by the company commander to use troop leading procedures. Commanders should not need to do any other refinement of these products. The following includes standard IPB products provided by the battalion to assist the commander in using the troop leading procedures:

- Threat situation templates and COA statements.
- Terrain and weather products.
- Tactical decision aids (such as MCOOs and terrain effects evaluations, weather forecast charts, weather effects matrices, and light and illumination data tables).
- Civil considerations tools and products.

Note. Company commanders coordinate with the battalion intelligence cell for any IPB products or tools they may need.

2-14. Due to the lack of a staff and resources, as well as 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 the troop leading procedures.

Step 2—Issue a Warning Order

2-15. The battalion intelligence cell 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 AOIs.
- Commander’s critical information requirements and essential elements of friendly information.
- Risk guidance.
- Surveillance and reconnaissance to initiate.
- Security measures.
- Deception guidance.
- Mobility and countermobility.
- Guidance on rehearsals.

Step 3—Make a Tentative Plan

2-16. When developing a tentative plan, the company commander relies on the battalion intelligence cell to provide IPB tools as the leader conducts mission analysis, COA development, COA analysis, and COA comparison and selection.

Mission Analysis

2-17. The battalion intelligence cell provides IPB tools and products on mission analysis by evaluating enemy, terrain and weather, and civil considerations. This includes providing information and analysis on the terrain and friendly and enemy forces that most affect tactical operations.

Course of Action Development

2-18. IPB products assist the leader in constructing a solid COA. The purpose of COA development is determining 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.

Course of Action Analysis

2-19. The battalion intelligence cell provides IPB tools the leader can use to determine how the enemy will likely react during war gaming. War gaming assists the leader in synchronizing friendly actions while considering the enemy's likely reactions. COA analysis begins with both friendly and threat COAs and, using a method of action-reaction-counteraction war game, results in a synchronized friendly plan, identified strengths and vulnerabilities, and an updated risk assessment. After developing the COA, the leader analyzes it to determine its strengths and vulnerabilities and gains insights into actions at the decisive point of the mission. COA analysis (war game) unites friendly and enemy forces on the actual terrain to visualize how the operation will unfold.

Course of Action Comparison and Selection

2-20. The battalion intelligence cell provides products from IPB to leaders to determine PIRs, friendly force information requirements, and essential elements of friendly information. Although essential elements of friendly information are not part of the commander's critical information requirements, they still become priorities, and this information must be protected from enemy identification.

Step 4—Initiate Movement

2-21. The battalion intelligence cell 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

2-22. If time permits, leaders verify intelligence from higher headquarters by reconnoitering to seek to confirm PIRs that support their tentative plans. These PIRs usually consist of assumptions or critical facts about the enemy (including 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).

IPB AND DECISION MAKING

2-23. Decision making refers to selecting a COA as the one most favorable to accomplish the mission. Decision making is knowing whether to decide or not, then when and what to decide, and finally understanding the consequences. Commanders make decisions in part based on the intelligence developed during initial IPB and on the refinement of that intelligence throughout the operations process. (For more information on the operations process, see ADRP 5-0.)

2-24. Commanders require accurate and timely intelligence about the OE to make informed and good decisions. Through IPB, the staff aids the commander's understanding of how the mission variables of enemy, terrain and weather, and civil considerations influence the OE and affect operations. IPB also assists the commander in understanding how to influence, use, or employ these variables to achieve the desired conditions and end state. IPB is essential in assisting the commander to—

- Understand, visualize, and describe the OE:
  - **Understand.** Understanding involves analyzing the mission variables in a given OE. IPB defines and describes the mission variables of enemy, terrain and weather, and civil considerations but more importantly, concludes how the interrelationships, dynamics, and interactions of these variables cause changes in the OE.
  - **Visualize.** 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 assisting the commander to visualize the situation. These products must be produced on time and in accordance with unit standard operating procedures.
  - **Describe.** After commanders visualize an operation, they communicate their vision to the staffs and subordinate commands using staff products developed during IPB.
- Make and articulate decisions.
- Direct, lead, and assess military operations.

2-25. One technique commanders and staffs commonly use during execution is the rapid decision-making and synchronization process. Throughout mission execution, continuous information collection is conducted to answer information requirements and to close intelligence gaps. The process is usually conducted based on an existing operation order that includes the IPB products and estimates produced during the MDMP. The rapid decision-making and synchronization process has five steps:

- **Compare the current situation to the order.** During execution, the staff looks for indicators of change that may affect the overall operation. These changes must be identified for the commander to the make necessary modifications to the operation plan. The event template and event matrix (developed during step 4 of IPB) and the DST (a critical output of step 4 of the MDMP) are the primary staff tools used to identify variances and alert the commander to situations that require a decision. These products are updated as changes occur.
- **Determine the type of decision required.** When a variance is identified, the staff describes the variance and determines if it provides a significant opportunity to friendly forces or the enemy.
- **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.** The commander and staff conduct a mental war game of the new COA. At a minimum the enemy situation template and COA statement, along with the friendly operations graphics and COA statement, are required to focus the mental war game.
- **Implement.** The commander normally implements the new COA by issuing a fragmentary order. The following are issued as part of that fragmentary order:
  - IPB products, including the enemy situation template with COA statement and HPT list, and terrain, weather, and civil considerations products.
  - Updated PIRs.

2-26. See ADRP 5-0 for more information on the rapid decision-making and synchronization process.

PART TWO

Fundamental Task Techniques

Chapter 3

Step 1—Define the Operational Environment

WHAT IS IT?

3-1. During step 1 of the IPB process, the intelligence staff identifies for further analysis the significant characteristics of or activities within the OE that may influence friendly and threat COAs and command decisions, as well as the physical space the mission will occupy. Within an OE, Army forces may face large-scale combat operations, which simultaneously encompass multiple domains, military engagements, and populations. Examples 1 and 2 portray planning scenarios.

Example 1

During planning for a foreign humanitarian assistance mission, a brigade S-2 identifies five ethnic groups with armed militias that have attacked each other, as well as host-nation security forces, in the past 12 months. In the last month, a rocket-propelled grenade shot down a host-nation military helicopter. The militias have not attacked any of the nongovernmental aid organizations in the area. The brigade S-2 identifies each of these groups as a threat. There is no information about these groups in the command's intelligence data files nor in the higher headquarters' data files to assist the brigade S-2 in developing valid potential COAs these groups may adopt when U.S. forces enter their AOs.

The intelligence staff searches various organizations' data files within the intelligence community and discovers that, while little is known about the threat characteristics of these militias, some information is available. Each militia is a company-sized element with various types of small arms and crew-served weapons, mortars, demolitions, and antiarmor rockets. It is unknown whether these militias have any ADA.

The brigade S-2 initiates a request for collection on the current locations, dispositions, strengths, and capabilities of these militias. Since the information will not be available during IPB, the brigade S-2 determines possible threat COAs based on what the brigade S-2 knows and assumes about the threat, ensuring the commander and the rest of the staff understand what is known and assumed. As intelligence related to the request for collection arrives, the brigade S-2 updates threat COAs and informs the commander and the rest of the staff.

Example 2

During planning for an attack, a brigade S-2 identifies the enemy has an attack helicopter squadron that could threaten the friendly mission. When developing the threat situation template, the brigade 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 brigade S-2 also generates requests for collection to locate and track these assets to support the command's targeting operations.

SO WHAT?

3-2. The "so what" of step 1 is to clearly define for commanders the relevant characteristics of their AOIs:

- **Outcome of success:** Success results in time and effort saved by focusing only on those characteristics that 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 OE characteristics that do not influence the operation.
  - Staff failure to identify all significant characteristics in all domains relevant to the OE may lead to the command's surprise and unpreparedness when some overlooked feature of the OE affects the operation for which the commander did not plan.

HOW TO DO IT: THE PROCESS

3-3. Defining the OE consists of the substeps and outputs shown in figure 3-1.

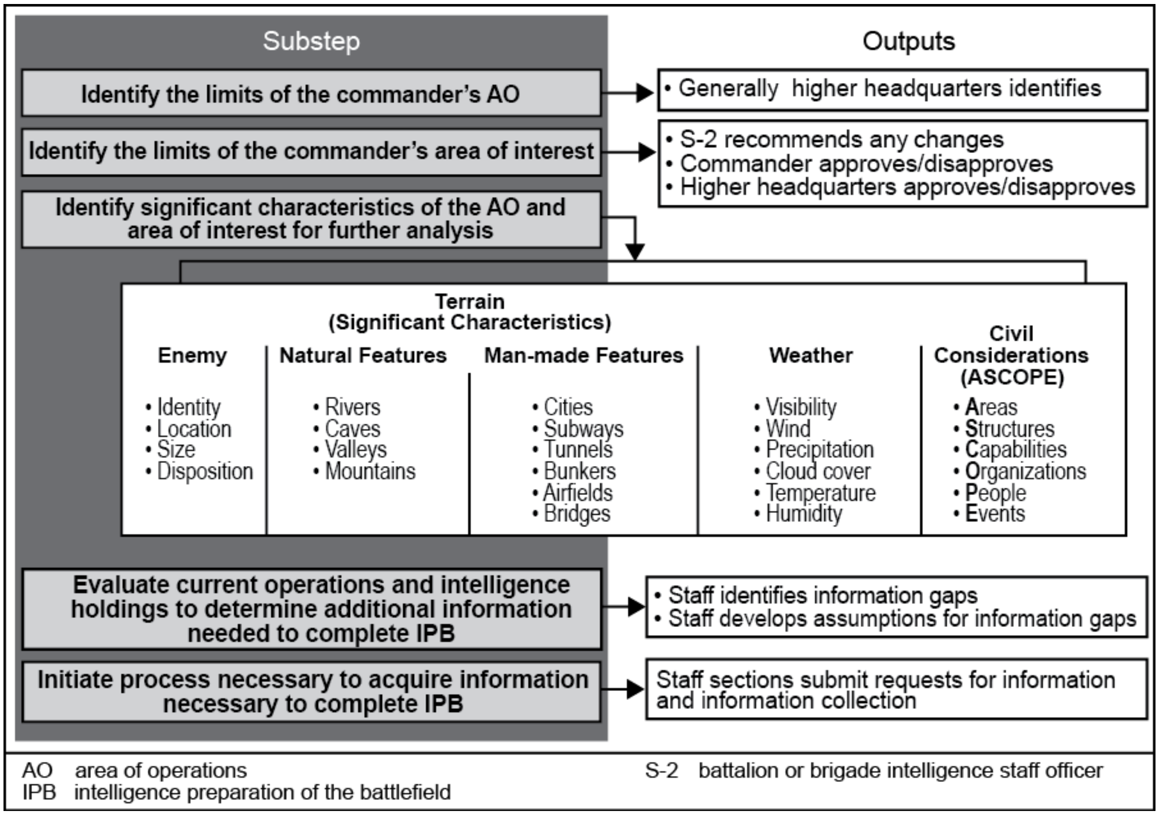

Substep
Outputs
Identify the limits of the commander's AO
• Generally higher headquarters identifies
Identify the limits of the commander's area of interest
• S-2 recommends any changes
• Commander approves/disapproves
• Higher headquarters approves/disapproves
Identify significant characteristics of the AO and area of interest for further analysis
Terrain (Significant Characteristics)
Enemy
• Identity
• Location
• Size
• Disposition
Natural Features
• Rivers
• Caves
• Valleys
• Mountains
Man-made Features
• Cities
• Subways
• Tunnels
• Bunkers
• Airfields
• Bridges
Weather
• Visibility
• Wind
• Precipitation
• Cloud cover
• Temperature
• Humidity
Civil Considerations (ASCOPE)
• Areas
• Structures
• Capabilities
• Organizations
• People
• Events
Evaluate current operations and intelligence holdings to determine additional information needed to complete IPB
• Staff identifies information gaps
• Staff develops assumptions for information gaps
Initiate process necessary to acquire information necessary to complete IPB
Staff sections submit requests for information and information collection
AO area of operations
IPB intelligence preparation of the battlefield
S-2 battalion or brigade intelligence staff officer

Figure 3-1. Substeps and outputs of step 1 of the IPB process

IDENTIFY THE LIMITS OF THE COMMANDER’S AREA OF OPERATIONS

3-4. *Area of operations* is an operational area defined by a commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces (JP 3-0). The AO comprises an external boundary that delineates adjacent units AOs and includes subordinate unit AOs. Subordinate unit AOs may be contiguous or noncontiguous.

3-5. Within an AO, commanders conduct decisive, shaping, and sustaining operations to articulate an operation in terms of purpose. Commanders designate main and supporting efforts to establish the shifting and prioritization of resources. 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 illustrates contiguous AOs. (See FM 3-0 for more information on AOs and decisive, shaping, and operational operations.)

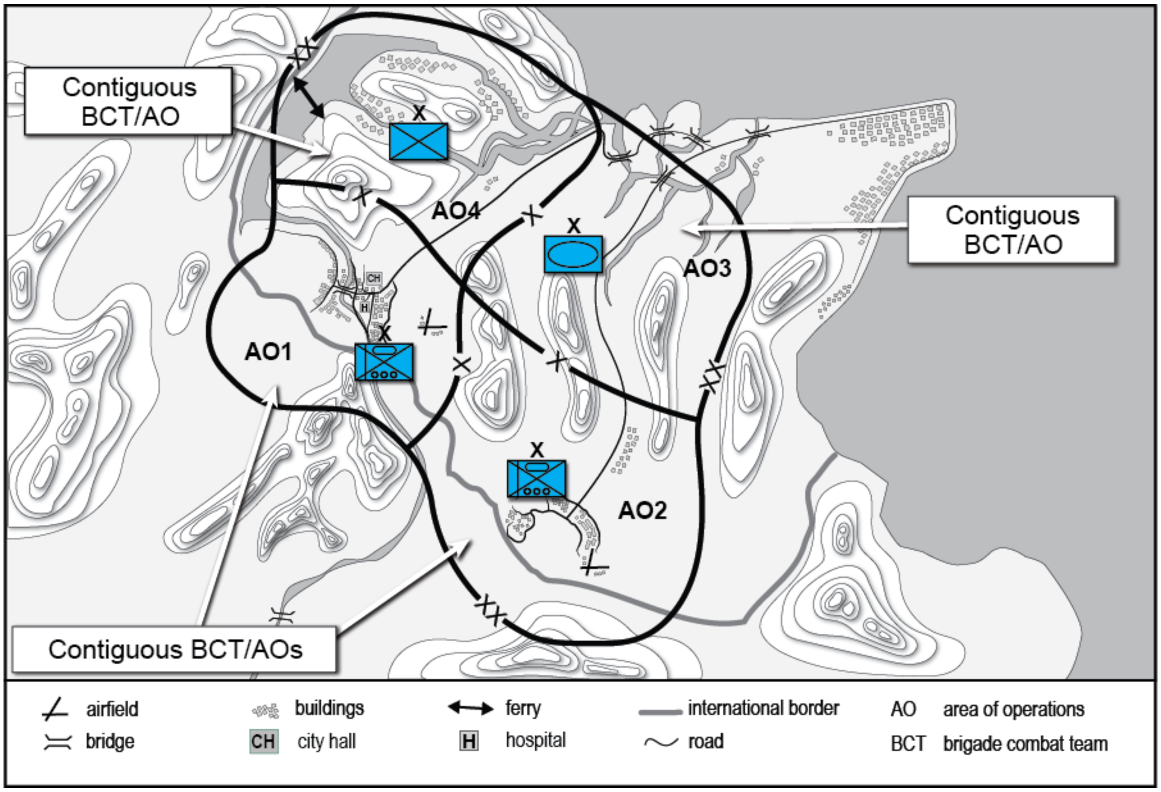


Figure 3-2. Area of operations examples

IDENTIFY THE LIMITS OF THE COMMANDER’S AREA OF INTEREST

3-6. 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 (JP 3-0). The AOI also includes areas occupied by threat forces who could jeopardize mission accomplishment. An *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 area of influence includes terrain inside and outside the AO and is determined by both the G-2/S-2 and G-3/S-3.

3-7. The AOI is—

- Established by the commander with input from the G-2/S-2 or G-3/S-3. The operational and mission variables must be considered.
- An area normally larger than or outside the area of influence that directly impacts the AO; therefore, possibly requiring more intelligence assets to monitor. It may include staging areas.
- An area that may be irregular in shape or noncontiguous and can overlap the areas of adjacent and subordinate unit AOs.
- An area that assists in determining NAIs during step 4 of the IPB process.

3-8. An AOI is the geographical area from which information is required to facilitate planning and the successful conduct of the command's operation. The area changes as the situation changes and as commanders determine new information requirements. It includes any threat forces or characteristics that significantly influence accomplishing the command's mission. In combat operations, the AOI extends into threat territory to the objectives of current or planned friendly operations if those objectives are located outside the assigned AO. In stability or defense support of civil authorities tasks, the AOI is typically much larger than that defined for combat operations.

3-9. In establishing the limits of an AOI, *time* is one of the primary considerations. Time limits should be based not only on the threat's mobility but also on the amount of time needed to accomplish the friendly mission. For example, if the command estimates that it will take two days to accomplish the friendly mission, the AOI must encompass all threat forces and activities that could influence accomplishing the command's mission within the two days. Additional considerations when establishing AOI limits include but are not limited to—

- **Dividing the AOI into several components** (for example, ground AOI, air AOI, subterranean AOI, and cyberspace AOI). Such a division accommodates the types of information relevant to each AOI as well as each AOI's different geographical limits. At some point, it may be necessary to integrate the various AOIs into a whole in order to present a holistic picture to the commander. One method of illustrating and articulating the AOI is the use of overlays to depict the relevant aspects of the AOI. For example, a threat force outside the AO may have capabilities that reside in or are employed in each of the domains. An overlay depicting this threat's capabilities (one relevant aspect of the AOI) can be layered with other relevant aspects to show a holistic view.
- **Threats to mission accomplishment that may also cross into neutral terrain countries.** For example, if political decisions in a neutral terrain country may influence the accomplishment of a unit's mission, include that country within the limits of the AOI. Likewise, if a segment of the population in a neutral terrain country provides a support base to forces that oppose the command's mission, include that country within the AOI.
- **Technological advances.** Due to technological advances in communications, such as social media and global media organizations, commanders are likely to witness increased visibility of friendly operations. This may lead to an increase in neutral and threat actions caused by friendly operations. Considering this, it is important to analyze how civil considerations and the dissemination of information may affect operations (see paragraphs 3-19 through 3-22).

Analyzing the AO Based on the AOI Effects

By analyzing the AO, as well as identifying and establishing an AOI, the commander and staff can determine how the relevant aspects of the AOI may impact the conduct of operations in the AO. This assists the commander in determining the required capabilities for mission accomplishment, identifying additional required capabilities, and requesting required capabilities in time to successfully impact operations. These required capabilities include the staff's ability to execute 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 area of influence encompasses the entire AO. The area of influence is useful to the commander to focus information collection operations, shape the battlefield, and facilitate future operations.

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

3-10. In order to focus IPB and what is important to the commander, the staff identifies and defines the characteristics of the enemy, terrain and weather, and civil considerations of the OE to determine the significance of each in relation to the mission—essentially building an environmental model as the framework for conducting and then presenting analysis to the commander. This prevents unnecessary analysis and allows the staff to dedicate and maximize resources in critical areas. The initial analysis that occurs in this substep determines the amount of time and resources the intelligence staff commits to the detailed analysis that occurs in step 2 of the IPB process.

3-11. When identifying significant characteristics of the OE, the staff may be faced with analyzing aspects that transcend the AO—for example, analyzing a threat located outside the AO (and potentially outside the geographic combatant commander's area of responsibility) who will likely use cyberspace capabilities to affect friendly operations in the AO across multiple domains. Accounting for these actors and their capabilities and determining their relationships and interdependencies with systems and other actors in the OE significantly increase the effectiveness of analysis in subsequent IPB steps and provide commanders with multiple options during the MDMP.

3-12. Additionally, the intelligence staff and other staff sections must consider threat forces and other aspects of the environment that may affect accomplishing the friendly mission. These include but are not limited to—

- The area's geography, terrain, and weather.
- Population demographics (ethnic groups, religious groups, age distribution, income groups).
- Political or socioeconomic factors, including the role of clans, tribes, religious organizations, criminal organizations, corruption, rule of law, gender, age, cultural groups, and ethnicity.
- Infrastructures such as transportation or telecommunications.
- Rules of engagement or legal restrictions such as international treaties, status of forces agreements, international sanctions, or United Nations charters.
- Threat force capabilities, including, military, other foreign security forces, as well as paramilitary forces, criminal and terrorist organizations (transnational and local), and antigovernment groups.

3-13. The intelligence staff should—

- Inspect each characteristic briefly to identify those of significance to the command and its mission.
- Further evaluate the effects of each characteristic in later steps of the IPB process.
- Analyze each characteristic that may impact decisive, shaping, and sustaining operations.
- Evaluate each threat's specific capabilities and determine probable COAs during later steps of the IPB process.

ENEMY

3-14. Analysis of the enemy includes not only the known enemy but also other threats to mission success, such as multiple threats posing with a wide array of political, economic, religious, and personal motivations. Additionally, threats may wear uniforms and be easily identifiable, blend into the population, and use either traditional threat capabilities (such as rifles or mortars) or nontraditional capabilities (such as computer networks and social media). To understand threat capabilities and vulnerabilities, commanders and staffs require detailed, timely, and accurate intelligence produced because of IPB.

TERRAIN AND WEATHER

3-15. It is important to identify the types of environments in which a unit will conduct operations. Terrain and weather are natural conditions of the environment that profoundly influence operations and the type of information collected. Terrain and weather favor neither the friendly nor the threat force, unless one is more familiar with or better prepared to operate in the physical environment.

Terrain

3-16. Terrain includes natural features (such as rivers, caves, valleys, and mountains) and man-made features (such as cities, subway tunnels, bunkers, 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.

3-17. The effective use of terrain reduces the effects of threat 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 and staffs analyze terrain using the five military aspects of terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment [OAKOC]), as performed during step 2 of the IPB process.

Weather

3-18. Climate refers to the average weather conditions of 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, threat TTP, and other capabilities based on specific weather sensitivity thresholds when operational planning occurs more than 10 days before 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. (See chapter 4 for more information on weather effects.)

CIVIL CONSIDERATIONS

3-19. *Civil considerations* is the influence of manmade infrastructure, civilian institutions, and activities of civilian leaders, populations, and organizations within an area of operations on the conduct of military operations (ADRP 5-0). Commanders and staffs analyze civil considerations in terms of these characteristics: areas, structures, capabilities, organizations, people, and events (ASCOPE). (See chapter 4.)

3-20. Civil considerations assist commanders in refining their understanding of the operational and mission variables within the AO and effects on the mission. Understanding the relationship between military operations and populations is critical in conducting operations and essential in developing effective plans. Operations often involve stabilizing the situation, securing the peace, building partner capacity, and transitioning authority to civilian control. Combat 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 the offensive and defensive operational design.

3-21. 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 an understanding to the level of cultural awareness. At this level, commanders can estimate the effects of friendly actions and direct subordinates with confidence. Cultural awareness improves how Soldiers interact with the populace and deters false or unrealistic expectations by both sides. Soldiers have more knowledge of the society’s common practices, perceptions, assumptions, customs, and values, giving better insight into the intent of individuals and groups. This allows staffs to better understand how friendly actions may affect the OE and assist in planning for possible branches and sequels.

3-22. To improve commanders’ sociocultural understanding, intelligence staffs can use sociocultural databases and repositories, when available, to aid the intelligence analysis conducted as part of assessing civil considerations. (See paragraphs 4-96 through 4-103.) Additionally, commanders and staffs should continually seek to improve cultural understanding to improve their roles in IPB.

SIGNIFICANT CHARACTERISTICS BRIEFING EXAMPLE

3-23. During step 1, the intelligence staff briefs the commander on the AO’s significant characteristics. This brief should be concise and provide all significant characteristics pertaining to step 1 only; it should not include specifics, such as the MCOO and threat template statements, which pertain to steps 2 and 3, respectively. The example provides a briefing used by intelligence analysts to inform the commander of the AO's significant characteristics.

Example Briefing: Identifying Significant Characteristics

Terrain:

- Wooded areas are primarily composed of pine trees.
- Most creeks require an armored vehicle-launched bridge to cross if there is no ford or road crossing.
- Major roadways can support four lanes of traffic.
- Marshes within the AO are restrictive most of the year; during heavy rains, they can become severely restrictive.
- The soil composition is loose dirt, and the water table is six to seven feet below ground except where the marshes are located.
- The highest point is located on the ridgeline in the northeastern sector of the AO.

Weather:

- The weather during this time of year consists of light rain with mild thunderstorms.
- The average rainfall is three to four inches.
- Precipitation affects potential river crossing sites.
- Strong gusts usually occur in early mornings and midafternoons, which can affect some aerial assets.
- Temperatures range from 65 to 80 degrees Fahrenheit. Fog occurs during the early morning hours and can last up to two hours after sunrise.

Civil considerations:

- Two major groups occupy the AO—the Regional Military Force and the National Liberation Group. A small group of the Russian-speaking population supports the National Liberation Group by providing sustainment and cache locations. The Russian-speaking population is sporadic through the AO and supported indirectly by the Regional Military Force.
- Apartments are usually several stories high and made of reinforced concrete; single-family homes are stone or brick with tile roofs.
- The population receives information primarily through television and social media sites.
- The major highway that runs through the AO is a hardball and all weather, but most of roads are dirt.
- The airfield is all weather and can support C-130 traffic.
- One potable water treatment plant operates in the AO and supports the whole region.
- The AO has two major cities where 40 percent of the population resides.

Enemy:

- Based on recent reporting and historical information, the staff expects to encounter a brigade- to division-sized element in the AO.
- The enemy likely has simple battle positions that are covered for dismounts and uncovered for vehicle fighting positions.
- Rudimentary tunnels link battle positions adjacent to mountainous terrain.
- Most simple battle positions have a tank ditch directly in front of them and a mine field about 50 to 100 meters in front of the tank ditch.
- C2 nodes consist of multiple hardened underground facilities.
- General support assets reside about 2 to 5 kilometers from the most forward battle positions.
- The staff expects to encounter ADA, artillery, T-90 tanks, and small arms weapons capabilities.

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

3-24. Not all information needed to complete IPB will be in the command's or higher headquarters' data files and databases. Information gaps should be identified early and prioritized based on the commander's initial guidance and intent for intelligence and information collection. The staff should ensure the commander is aware of any information gaps that cannot be answered within the time allotted for IPB, develop reasonable assumptions to use in place of these answers, and explain to the commander how it arrived at these assumptions.

INITIATE PROCESSES TO ACQUIRE THE INFORMATION NEEDED TO COMPLETE IPB

3-25. After determining that the information necessary to complete IPB is not contained within local and searchable external data files and databases, staff sections 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 eliminated. New intelligence gaps and information requirements may be developed as IPB continues. (See FM 3-55 for more information on information collection. See ATP 2-01 for more information on collection management.)

Chapter 4

Step 2—Describe Environmental Effects on Operations

WHAT IS IT?

4-1. Step 2 of the IPB process determines how significant characteristics of the OE can affect friendly and threat operations. The staff begins evaluation by analyzing existing and projected conditions in the AO and AOI, and then determining effects on both friendly and threat operations. The example shows how significant characteristics of the OE (specifically the terrain) impact friendly operations.

Example

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

SO WHAT?

4-2. The "so what" of step 2 is to identify how relevant characteristics of the AOI affect friendly and threat operations:

- **Outcome of success:** Success results in the commander being able to quickly choose and exploit terrain, weather, and civil considerations to best support the mission during decisive, shaping, and sustaining operations.
- **Consequences of failure:**
  - The commander may not have the information needed to exploit the opportunities the OE provides at a given time and place.
  - The threat commander may have the information needed to exploit the opportunities the OE provides in a way the friendly commander did not anticipate. For example, the threat commander may use subterranean terrain to maneuver against friendly forces. If the friendly commander is unaware of the advantage that this terrain provides to the threat, all threat COAs will not be considered during this step.

HOW TO DO IT: THE PROCESS

4-3. Describing environmental effects on operations consists of the substeps and outputs shown in figure 4-1.

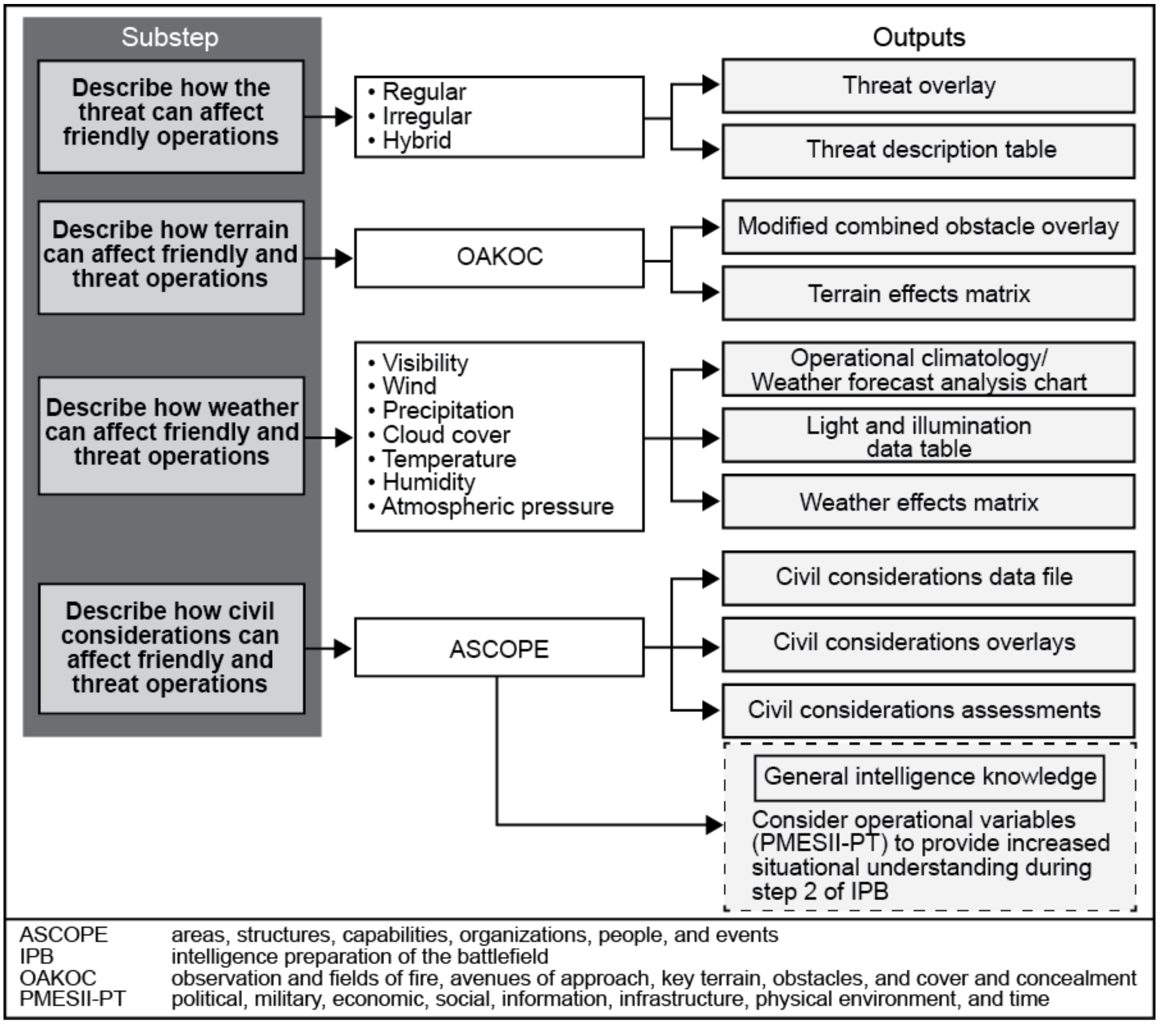

Substep
Outputs
Describe how the threat can affect friendly operations
• Regular
• Irregular
• Hybrid
Threat overlay
Threat description table
Describe how terrain can affect friendly and threat operations
OAKOC
Modified combined obstacle overlay
Terrain effects matrix
Describe how weather can affect friendly and threat operations
• Visibility
• Wind
• Precipitation
• Cloud cover
• Temperature
• Humidity
• Atmospheric pressure
Operational climatology/ Weather forecast analysis chart
Light and illumination data table
Weather effects matrix
Describe how civil considerations can affect friendly and threat operations
ASCOPE
Civil considerations data file
Civil considerations overlays
Civil considerations assessments
General intelligence knowledge
Consider operational variables (PMESII-PT) to provide increased situational understanding during step 2 of IPB
ASCOPE areas, structures, capabilities, organizations, people, and events
IPB intelligence preparation of the battlefield
OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment
PMESII-PT political, military, economic, social, information, infrastructure, physical environment, and time

Figure 4-1. Substeps and outputs of step 2 of the IPB process

DESCRIBE HOW THE THREAT CAN AFFECT FRIENDLY OPERATIONS

4-4. Threats are part of the OE; therefore, commanders need to understand all threats that can potentially affect operations within the AO and AOI. They may face one unified threat force or several disparate threat forces that must be engaged to accomplish the mission. Although detailed analysis of threat forces occurs during steps 3 and 4 of the IPB process, the type of threat force and its general capabilities must be defined during step 2. This places the threat force in context with other variables in order to understand its relative importance as a characteristic of the OE. For example—

- When facing a regular threat in combat operations, regardless of where the engagement occurs, that threat is likely the most important characteristic in that OE.
- When facing an irregular threat 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 posed by the irregular threat.

- When facing a hybrid threat in combat operations, the hybrid threat will likely be equipped with capabilities that can be used to exploit perceived friendly vulnerabilities. The mixture of regular and irregular threat capabilities expands threat COA possibilities and can create significant impacts outside friendly force decision cycles.

4-5. The threat overlay and the threat description table focus the analysis of the threat and assist in communicating that analysis to the commander. (See chapter 5 for descriptions of regular, irregular, and hybrid threats.)

THREAT OVERLAY

4-6. The threat overlay depicts the current physical location of all potential threats in the AO and the AOI. The overlay includes the identity, size, location, strength, and AO for each known threat location. The date-time group of the threat activity should be annotated on the threat overlay or maintained in intelligence reference files. Maintaining a threat overlay provides a reference to past threat activity and assists in determining patterns of threat movement and dispositions. During step 4 of the IPB process, this reference assists in determining threat COAs. Figure 4-2 illustrates an example of a threat overlay.

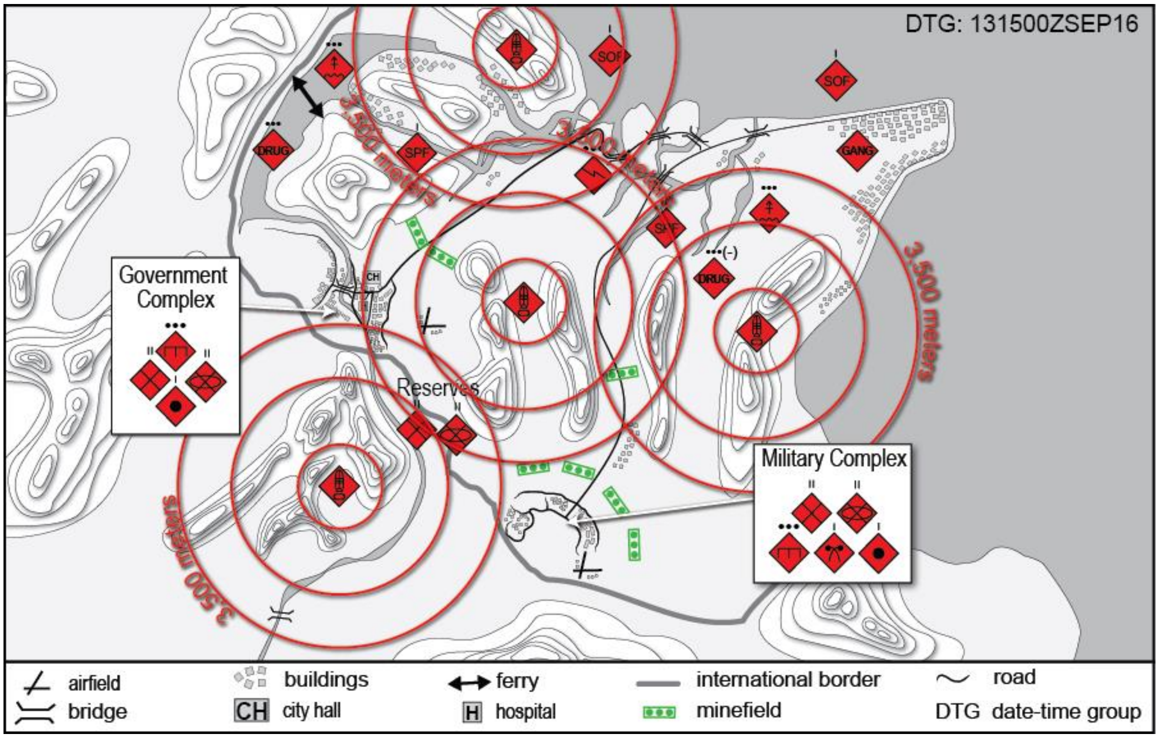


Figure 4-2. Threat overlay example

THREAT DESCRIPTION TABLE

4-7. The threat description table supports the threat overlay by classifying the types of threats identified on the overlay and describing the broad capabilities of each threat. Table 4-1 exemplifies a threat description table.

Table 4-1. Threat description table example

Identity	*Location*	*Disposition*	*Description*
2x special purpose forces companies	Northern coast	Companies are known to operate down to platoon and section echelons from sanctuary locations.	Companies conduct littoral reconnaissance to provide information on potential regional threat coastal invasion or border incursions.
Platoon(+) drug trafficking personnel	East and west international boundary	Platoons operate in 10-15 personnel teams.	• Platoons oversee smuggling of methamphetamines and their precursor chemicals out of the country. • Platoons are known to work with gangs for distribution of narcotics in urban areas.
2x platoons riverine infantry	Eastern and western marsh areas	Normally maintain platoon integrity while patrolling rivers and littoral areas.	Key forces prevent regional threats from using riverine network to move south toward key terrain.
Gang personnel (assessed to be approximately 100 personnel)	Northeast urban center	Normally operate in cells of 7-10 personnel.	• Gang personnel support the distribution of narcotics within urban areas. • Gang personnel provide information on regional threats operating near the coast.
2x special purpose forces companies	Vicinity main north-south highways	Companies operate down to section and team echelons from hasty defensive positions and hide sites.	• Companies overwatch main north-south highways and establish hasty checkpoints. • Companies use population centers to collect information on regional threats. • Companies also conduct counterreconnaissance of low-lying marsh areas.
Battery (-) air defense artillery	Coastal and inland regions usually masked by terrain	SA-13 systems are positioned to protect air avenues of approach vicinity, the coast, and inland key terrain.	Air defense artillery assets conduct area denial in air avenues of approach vicinity leading to the Government Complex and Military Complex.
72d Mechanized Battalion (BN)	Government Complex	• BN is manned at 90% strength. • Currently conducting training exercises for the next 15 days • BN leadership has changed within the last 30 days.	• Top tier BN. • Trained mostly in defensive tasks as regional threats have postured for attacks in the last five years. • Retention of Government Complex and support of regional military partners are key strategies to maintain control of country. • Nested with coastal special purpose forces to provide early warning of regional threat presence.
65th Mechanized BN	Military Complex	• BN is manned at 75% strength. • Will initiate training exercises in the next 30 days.	• Trained mostly in defensive tasks as regional threats have postured for attacks over the last five years. • Focuses on using obstacle belts and flanking maneuvers.
97th Mechanized BN and 10th Infantry BN (reserve forces)	Masked by terrain equidistant from Government Complex and Military Complex	• Both BNs are manned at 60% strength. • Both BNs completed training exercises within the last 90 days. • Last training exercise focused on occupation of urban areas.	• Trained in urban operations. • Well-versed in deception and information warfare.

DESCRIBE HOW TERRAIN CAN AFFECT FRIENDLY AND THREAT OPERATIONS

4-8. *Terrain analysis* is 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). It also involves the study and interpretation of natural and man-made features within an area, their effects on military operations, and the effects of weather and climate on these features. Terrain analysis is a continual process since changes in the OE may alter the analysis of terrain effects on operations.

4-9. A command may operate in two types of terrain—natural and complex—which are analyzed based on the military aspects of terrain (OAKOC) (see figure 4-3):

- **Natural terrain analysis** focuses on airspace and surface and subsurface areas.
- **Complex terrain analysis** also focuses on airspace, surface and subsurface areas, but it must also consider internal, external, and supersurface areas.

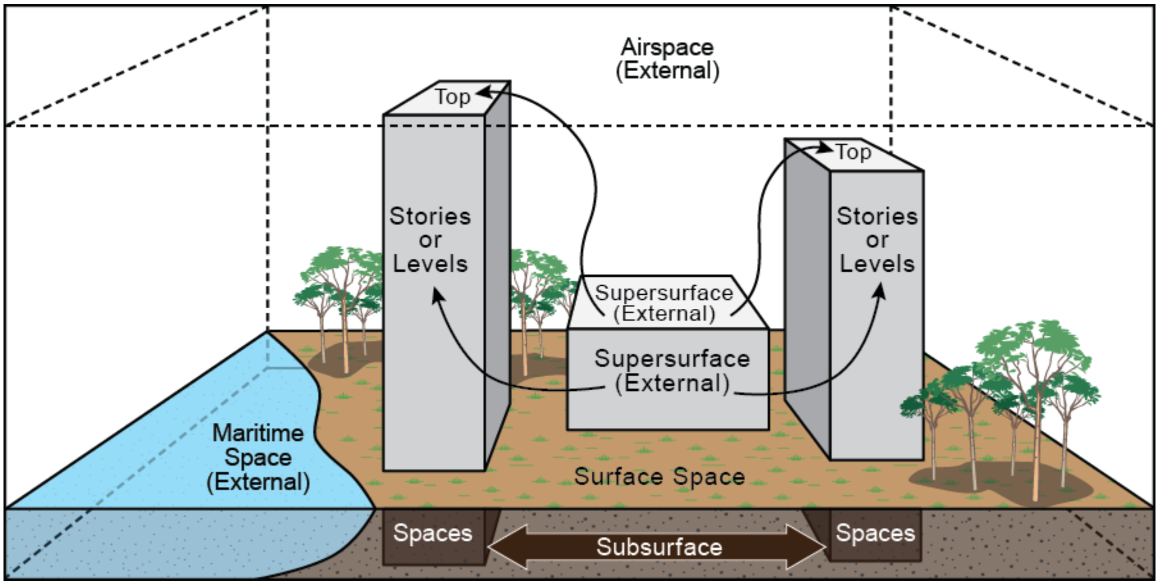


Figure 4-3. The focus of natural and complex terrain analysis

ANALYZE THE MILITARY ASPECTS OF TERRAIN

4-10. Geospatial intelligence cells generally conduct detailed terrain analysis. These cells are assigned to theater army, corps, and division headquarters and to brigade combat teams based on priorities established by the S-2. These cells have digital mapping tools and access to national-level support from agencies such as the National Geospatial-Intelligence Agency. The geospatial intelligence cell, along with the G-2/S-2, collaborates with an Air Force staff weather officer to leverage the appropriate weather capabilities in order to incorporate the effects of current and future weather conditions into terrain analysis. Terrain analysis results in the evaluation of the military aspects of terrain (OAKOC) on operations.

4-11. Staff collaboration during terrain analysis can assist in identifying and addressing factors such as—

- Cross-country mobility.
- Canalizing terrain.
- Line of sight (LOS) impacts on weapon use.
- Terrain impacts on CBRN weapon use.
- Communications dead space.
- Lines of communications (LOCs) (transportation, communications, and power).
- Vegetation types and distribution.

- Natural and man-made surface and subsurface areas and materials.
- Natural and man-made obstacles.
- Significant infrastructure.
- Flood zones.
- Aircraft and amphibious sites.

Note. The discussion in this section provides broad aspects of the terrain analysis essential to intelligence analysts conducting terrain analysis to support threat analysis. (For more information on the military aspects of terrain, see ATP 3-34.80 and JP 2-03.)

Observation and Fields of Fire

4-12. *Observation* is the condition of weather and terrain that permits a force to see the friendly, enemy, and neutral personnel and systems, and key aspects of the environment (ADP 1-02). Commanders evaluate their observation capabilities for electronic and optical LOS surveillance systems, as well as for unaided visual observation. The highest terrain normally provides the best observation. (For LOS distances in nautical miles [height of eye] versus statute miles [horizon range], see appendix B.)

4-13. 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. *Intervisibility* is the condition of being able to see one point from the other. Figure 4-4 shows how an observer at Position A can see up the slope to Position B, but the ridgeline prevents the observer from seeing Position D, and the valley prevents the observer from seeing Position C. Whatever the observer cannot see becomes a masked area. An observer at Position B can see Positions A, C, and D because this observer is on the intervisibility line.

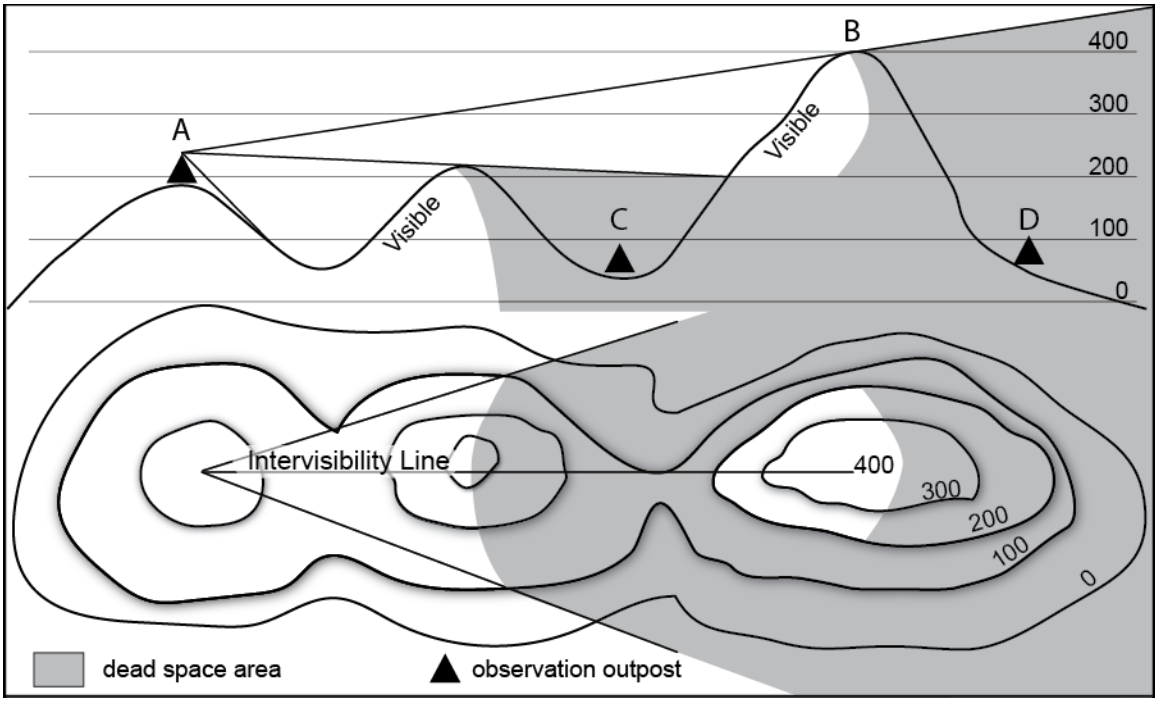


Figure 4-4. Intervisibility line example

4-14. Observation can also be limited by adverse weather, smoke, the time of day, and the amount of illumination at night. In urban areas, observation is limited primarily by man-made structures as well as the activity and debris associated with human activity. Analyzing observation and fields of fire in urban areas is more complicated than it is for natural terrain; analysts must also consider surface, subsurface, supersurface, external, and internal areas (see figure 4-3 on page 4-5).

> ***Note.*** Threat forces will seek to exploit observation advantages from areas that friendly forces may not consider. For example, threat forces may use a building protected under the rules of engagement (religious buildings, cultural monuments, places of worship, hospitals, medical clinics) to conduct observations on friendly forces. Threat forces may use subterranean terrain portals to identify friendly forces' movement routes. (See ATP 3-21.51.)

4-15. *Field of fire* is the area that a weapon or group of weapons may cover effectively from a given position (FM 3-90-1). 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, which offers good observation and fields of fire.
- Specific equipment or equipment positions.
- Areas where forces are most vulnerable to observation and fires.
- Visual dead space.

4-16. Analysis of fields of fire includes an evaluation of all direct and indirect fire weapon systems in a command's inventory. An ideal field of fire for direct fire weapon systems is an open area where the threat can be seen and has no protection out to the maximum effective range of that weapon.

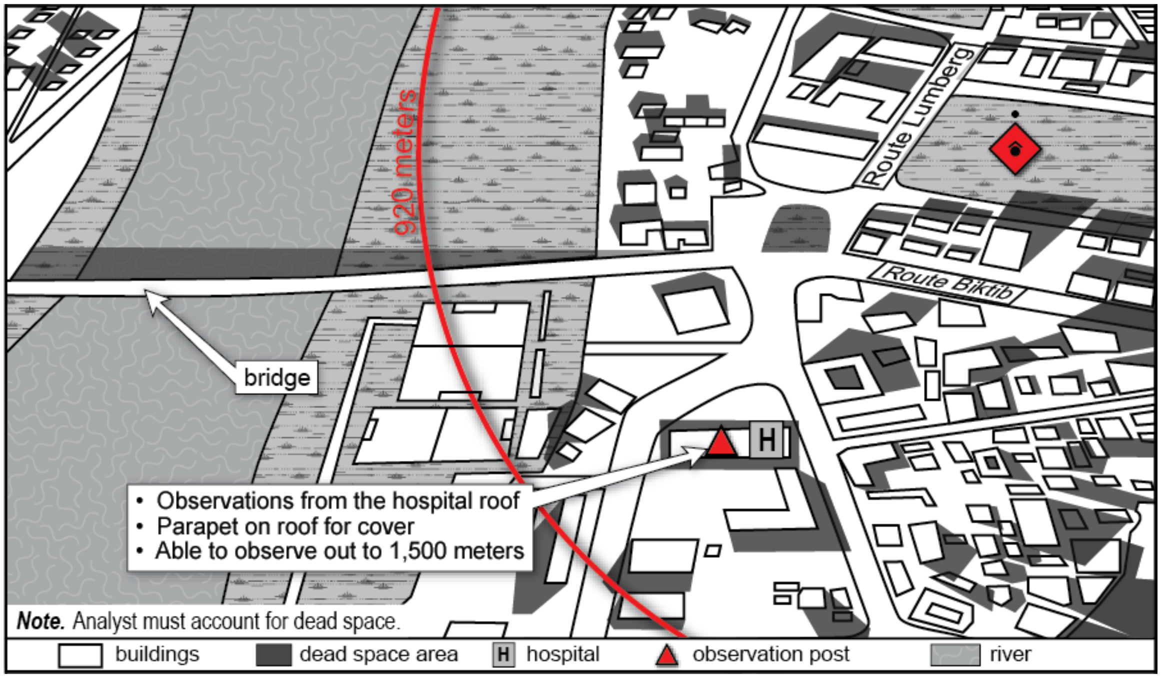
4-17. Both observation and fields of fire are based on LOSs. ***Line of sight*** **is the unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another**. In other words, a LOS is a straight line from one point to another.

4-18. There are two types of LOSs normally evaluated during terrain analysis:

- **Horizontal LOS** is an unobstructed path from a Soldier's weapon, weapon sight, laser designator, and electronic sending and receiving antennas.
- **Oblique (or vertical) LOS** assists in planning ADA system locations, selecting landing zones and drop zones, and selecting forward arming and refueling points.

4-19. Identifying areas vulnerable to threat aerial information collection systems assists in selecting friendly battle positions. Establishing LOSs and identifying intervisibility lines are critical to analyzing observation and fields of fire because they have a bearing on LOS direct fire weapons, antennas, reconnaissance, and some electro-optical systems. Essentially, identifying intervisibility lines can assist in identifying potential threat locations as well as those locations where friendly forces can evade detection from threat forces.

4-20. An effective technique for analyzing observation and fields of fire is the production of a map displaying observation and fields of fire. Computer-generated terrain applications can assist in producing observation and fields of fire graphics that depict expected ranges and locations of nonpresent, decreased, or increased observation and fields of fire. An ideal field of fire for direct fire weapons is an open field in which the threat 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. Figure 4-5 on page 4-8 shows LOS analysis used to depict observation and fields of fire from a point on, or above, the ground. This depiction accounts for natural and man-made obstacles to observation. Rings can be added to accommodate for weapons ranges.



- Observations from the hospital roof
- Parapet on roof for cover
- Able to observe out to 1,500 meters

Note. Analyst must account for dead space.

Figure 4-5. Observation and fields of fire (complex terrain) example

Avenues of Approach

4-21. *Avenue of approach* is a path used by an attacking force leading to its objective or to key terrain. Avenues of approach exist in all domains (ADP 3-90). Identifying AAs is important because all COAs that involve maneuver depend on available AAs. During offensive tasks, the evaluation of AAs leads to a recommendation of the best AAs to a command's objective and to the identification of AAs available to the threat for counterattack, withdrawal, or the movement of reinforcements or reserves. During defensive tasks, it is important to identify AAs that support threat offensive capabilities and AAs that support the movement and commitment of friendly reserves.

4-22. AAs consist of a series of mobility corridors through which a maneuvering force must pass to reach its objective. (See figure 4-6.) AAs must provide ease of movement and enough width for dispersion of a force large enough to affect the outcome of the operation significantly. AAs are developed by identifying, categorizing, and grouping mobility corridors and evaluating AAs.

4-23. Evaluating AAs is a combined effort by the entire staff to identify those AAs that best support threat or friendly capabilities. The AAs should be prioritized based on how well each supports the ability to meet the desired end state timely and efficiently. AAs are evaluated for suitability in terms of access to key terrain and adjacent AAs, degree of canalization and ease of movement, sustainability (LOC support), and access to the objective. Once evaluated for suitability, AAs are prioritized based on how well each supports maneuver.

4-24. *Mobility corridor* is 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). They use unrestricted terrain that provides enough space for a freedom of action by breaching or bypassing obstacles. The geospatial team provides terrain visualization products for mobility corridors. Identifying mobility corridors requires knowledge of friendly and threat forces and their preferred tactics. (For more information on terrain visualization products, see ATP 3-34.80.)

4-25. Mobility corridor requirements are directly proportional to the type and mobility of the force being evaluated. Military forces, such as mechanized infantry or armored units, have more freedom of movement and maneuver in open areas. Dismounted forces are less impacted in wooded areas, where mechanized units would be delayed. Geospatial teams can produce cross-country mobility-terrain visualization products corresponding with the type of element being employed in a specific area. Reconnaissance should be conducted to validate computer-generated products.

4-26. Mobility corridors are categorized based on the size or type of force they can accommodate, as well as by their 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 the rate of march and the lack of fire power, dismounted forces require a more covered and concealed route for survivability to reach their objective.

4-27. 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 and the typical widths of mobility corridors for a mechanized force.

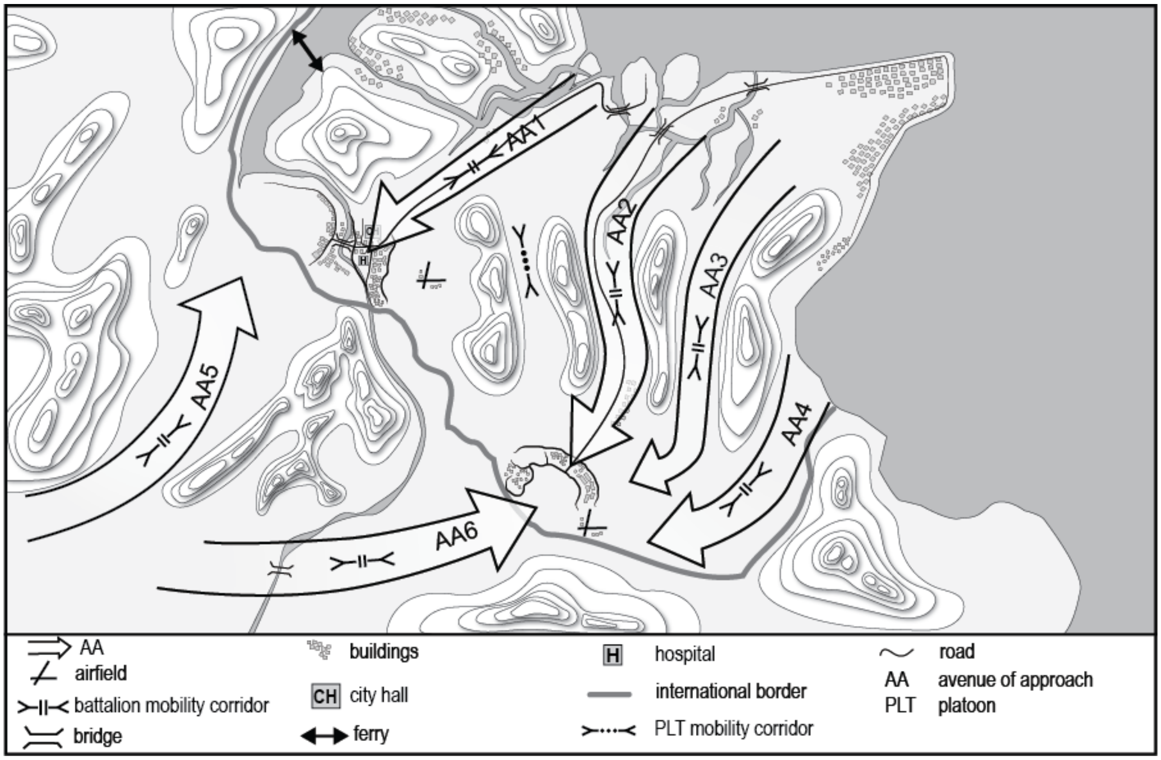


Figure 4-6. Avenues of approach with mobility corridors (natural terrain) example

Table 4-2. Maximum distances between and typical widths of mobility corridors

<table>
<tr><th colspan="3"><i>Maximum distances between mobility corridors</i></th></tr>
<tr><th><i>Avenue of approach</i></th><th><i>Cross-country mobility corridor classification</i></th><th><i>Approximate distance between terrain features</i></th></tr>
<tr><td>Division</td><td>Brigade</td><td>10 kilometers</td></tr>
<tr><td>Brigade</td><td>Battalion</td><td>6 kilometers</td></tr>
<tr><td>Battalion</td><td>Company</td><td>2 kilometers</td></tr>
<tr><th colspan="3"><i>Typical widths of mobility corridors</i></th></tr>
<tr><th><i>Unit</i></th><th colspan="2"><i>Width</i></th></tr>
<tr><td>Division</td><td colspan="2">6 kilometers</td></tr>
<tr><td>Brigade</td><td colspan="2">3 kilometers</td></tr>
<tr><td>Battalion</td><td colspan="2">1.5 kilometers</td></tr>
<tr><td>Company</td><td colspan="2">500 meters</td></tr>
</table>

Key Terrain

4-28. *Key terrain* is an identifiable characteristic whose seizure or retention affords a marked advantage to either combatant (ADP 3-90). In natural terrain environments dominated by restrictive terrain features, high ground can be key terrain because it dominates an area with good observation and fields of fire. (See figure 4-7.) In an open or arid environment, a dry riverbed, channel, or valley can be key terrain because it offers good cover and concealment.

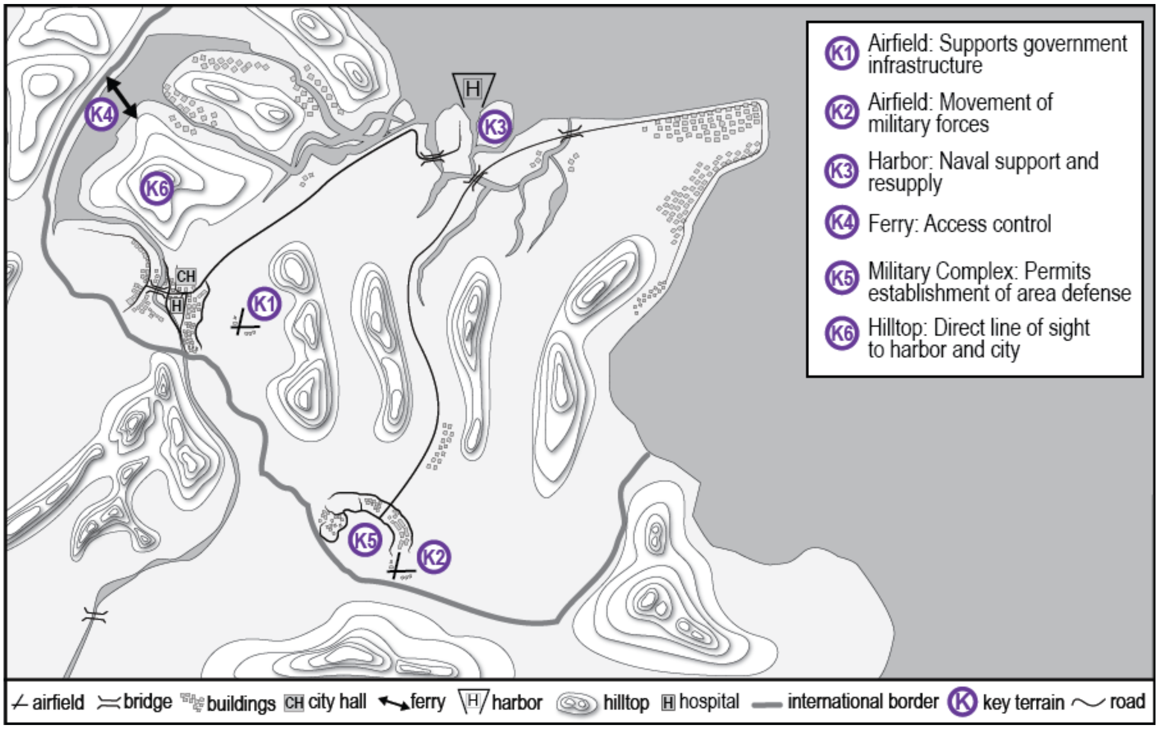

K1 Airfield: Supports government infrastructure
K2 Airfield: Movement of military forces
K3 Harbor: Naval support and resupply
K4 Ferry: Access control
K5 Military Complex: Permits establishment of area defense
K6 Hilltop: Direct line of sight to harbor and city
K1
K2
K3
K4
K5
K6
CH
H
H
airfield
bridge
buildings
CH city hall
ferry
H harbor
hilltop
H hospital
international border
K key terrain
road

Figure 4-7. Key terrain (natural terrain) example

4-29. In urban areas, infrastructure (such as bridges, medical facilities, choke points, intersections, industrial complexes, and economic, social, and government institutions) can be considered key terrain. 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.

Example Key Terrain Considerations for Urban Areas

- **Economic or social institution:** The main bazaar in a town is key terrain; whoever controls the bazaar controls the town. The economic health of the bazaar is crucial to the economic health of the area. If the threat can maneuver through and control the bazaar (key terrain), it can shut down the town and the economy.
- **Government institution:** As key terrain, the local police may exert a great deal of influence on the local population (elections, law enforcement, tribal politics). The tactical use of this key terrain is often directed at increasing the capability to apply combat power while simultaneously forcing threats 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 using the evaluation of the other four military aspects of terrain (observation and fields of fire, AAs, obstacles, and cover and concealment) 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.
- Areas along a LOC that affect the use of reserves or sustainment operations.

4-33. In stability tasks, key terrain may include portions of the population, such as—

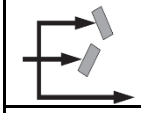
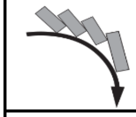
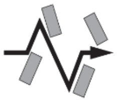
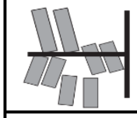
- Political, tribal, or religious groups or leaders.
- A local population.
- Governmental organizations.

4-34. *Decisive terrain* is key terrain whose seizure and retention is mandatory for successful mission accomplishment (ADP 3-90). 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 a threat force. Commanders designate decisive terrain to communicate to the staff and subordinate commanders about the importance of the terrain to the concept of operations.

Obstacles

4-35. 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). Table 4-3 depicts tactical effects associated with obstacles.

Table 4-3. Tactical obstacle effects

Obstacle effect	***Description***
Disrupt 	• The arrows indicate the direction of threat advance. • The length of the arrows indicates where the threat is slowed or allowed to pass.
Turn 	• The heel of the arrow is the anchor point. • The direction of the arrow indicates the desired direction of the turn.
Fix 	• The arrow indicates the direction of threat advance. • The irregular part of the arrow indicates where threat advance is slowed by obstacles.
Block 	• The vertical line indicates the limit of threat advance and where the obstacle ties into severely restricted terrain. • The horizontal line shows the depth of the obstacle effort.
Direction of threat attack ⟶	

4-36. The geospatial team can visually depict cross-country mobility based on obstacles, vehicle capabilities, and preferred movement formations. This product is used to identify AAs and to plan the size and/or echelon that supports movements, socioeconomic restrictive areas, as well as religious and cultural sites.

4-37. Obstacles affect certain types of mobility differently:

- **Mounted mobility.** 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 mobility than on dismounted mobility.
- **Dismounted mobility.** Antipersonnel minefields, concertina wire, or steep slopes may be more effective against dismounted mobility.

4-38. Obstacles to air mobility include terrain features that—

- Exceed the aircraft's service ceiling.
- Affect nap-of-the-earth flight.
- Impact aircraft lift capabilities.
- Force the aircraft to employ a particular flight profile. (Examples include 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 fixed-wing and rotary-wing aircraft lift capabilities.)

4-39. Obstacles may decrease the effectiveness of information-related capabilities to influence threat operations and activities, as well as friendly and neutral populations. For example, mountains may block terrestrial-based signals used to broadcast surrender appeals to a threat-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 local terrain effects. Obstacles may also decrease a commander's ability to communicate and influence the AO, whether that be with organic or attached communications capabilities or an attached psychological operations force.

Cover and Concealment

4-40. *Cover* is protection from the effects of fires (FM 3-96). 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 personnel survivability. (See appendix B for examples of cover; see ATP 3-37.34 for more information on hardening infrastructure and creating survivability positions.)

4-41. *Concealment* is protection from observation or surveillance (FM 3-96). It degrades the threat's ability to observe forces, equipment, or positions. Concealment can be provided by trees, underbrush, tall grass, cultivated vegetation, weather conditions (such as snow, fog, or rain), as well as man-made camouflage. Concealment does not necessarily provide cover.

4-42. LOS analysis determines the observation, fields of fire, and cover and concealment the terrain will provide to both friendly and threat forces. Together, the LOS example and figure 4-8 illustrate the concept of cover and concealment in natural terrain and LOS analysis.

LOS Example

The masked areas lie behind terrain that is level with or higher than the defensive position. One cannot see into the masked areas or fire direct weapons into them. One does not have observation or fields of fire behind the masking terrain. The masked areas provide the attacker cover from the defender's direct fire and concealment from the defender's observations. If the threat performs proper analysis, then the threat will select one or more of the approach routes.

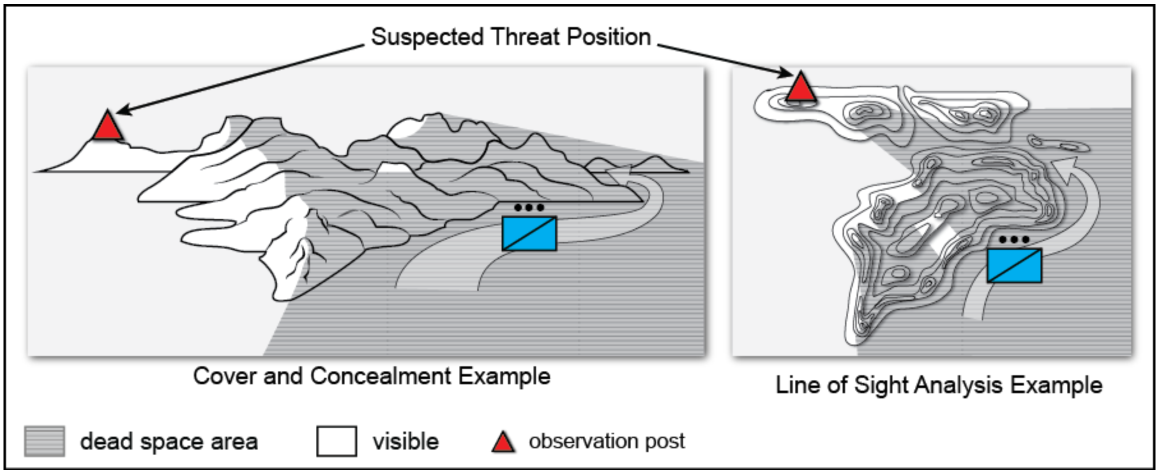

Suspected Threat Position
Cover and Concealment Example
Line of Sight Analysis Example
dead space area
visible
observation post

Figure 4-8. Cover and concealment (natural terrain) and line of sight analysis examples

EVALUATE TERRAIN EFFECTS ON MILITARY OPERATIONS

4-43. The staff determines terrain effects on friendly and threat operations. The MCOO and the terrain effects matrix are the primary analytic tools used to determine these effects.

Modified Combined Obstacle Overlay

4-44. 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 impediments to mobility, such as built-up areas, slope, soils, vegetation, and hydrology into one overlay. This overlay also allows the staff to visualize impediments to mobility for both friendly and threat forces. The overlay depicts areas that impede mobility (severely restricted and restricted areas) and areas where friendly and threat forces can move unimpeded (unrestricted areas).

4-45. The *modified combined obstacle overlay* is 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 (JP 2-01.3). The MCOO is tailored to the mission and is a collaborative effort involving input from the entire staff. The staff uses its warfighting function expertise to determine how the terrain will impact that function. For example, the S-6 provides input on how the terrain may affect LOS communications for friendly and threat forces. The nuclear, biological, chemical officer provides information on how terrain may affect the use of persistent and nonpersistent chemical agents.

4-46. Specific aspects of the MCOO include but are not limited to AAs, key terrain, mobility corridors, natural and man-made obstacles, and terrain mobility classifications. (See figure 4-9 and table 4-4 on page 4-14 for an example of and color control measures for MCOO overlays, respectively.) The MCOO depicts the terrain according to the 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, such as committing engineer assets to improving mobility or deviating from doctrinal tactics (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 dense obstacle compositions with few bypasses. A common technique to depict this type of terrain on overlays and sketches is marking the areas with green crosshatched diagonal lines. (See appendix B for information on severely restricted terrain for mechanize or armored forces.)
- **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-dense obstacle compositions, such as restrictive slopes or curves. 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 to depict restricted terrain on overlays and sketches is marking the areas with green diagonal lines. (See appendix B for information on restricted terrain for mechanize or armored forces.)

- **Unrestricted terrain** is free from any restriction to movement. Nothing is required to enhance mobility. Unrestricted terrain for armored or mechanized forces is typically flat to moderately sloping terrain with few obstacles such as limiting slopes or curves. This 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.

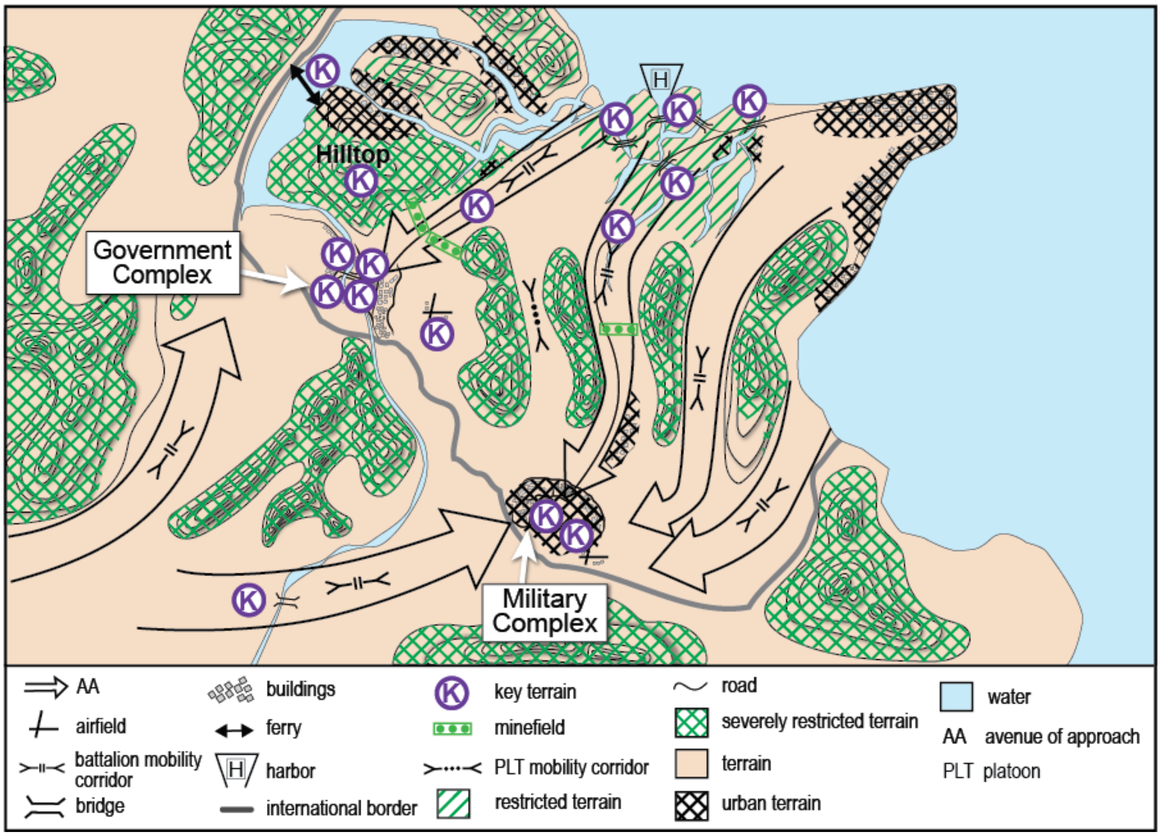


Figure 4-9. Modified combined obstacle overlay example

Table 4-4. Typical color control measures for modified combined obstacle overlays

Description	***Color***
Avenue of approach	Friendly = blue ⇒ neutral = black ⇒ threat = red ⇒
Built-up area (urban terrain)	Black ☒
Hydrology	Blue 🟦
Key terrain	Purple Ⓚ
Mobility corridor	Black
Natural and man-made obstacles	Black (See ADP 1-02 for exceptions.)
Restricted terrain	Green ▨
Severely restricted terrain	Green ☒

4-47. 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 force's ability to maneuver in combat formations or transition from one type of formation to another. The staff should consider the following:

- Obstacles are only effective if covered by observation and fields of fire. However, even undefended obstacles may canalize an attacker into concentrations, which are easier to detect and target or defend. Obstacles are green on map overlays.
- When evaluating the terrain's effects on more than one type of organization (for example, mounted or dismounted), obstacle overlays reflect an impact on mobility of a particular force.
- The cumulative effects of individual obstacles should be considered 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; together, the slope and dense forest may prove to be restrictive.
- The staff should 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.

4-48. For urban areas, graphics typically depict population status overlays (dense population centers, political boundaries), logistics sustainability overlays, LOCs, route overlays (street names, patterns, widths), bridges (underpass and overpass information), potential sniper and ambush locations (will likely be a separate overlay), and key navigational landmarks. (See figure 4-10.) In developing urban area and complex terrain overlays, the following should be depicted:

- **Natural terrain:** The underlying terrain on which man-made terrain is superimposed, such as rivers, streams, hills, valleys, forests, desert, bogs, swamps.
- **Man-made terrain:** Streets, bridges, buildings, railways, canals, sewer systems, subway systems, military bunkers, traffic control points; building density, construct, dimensions; functional zone disposition; street construct, materials, disposition, dimensions.
- **Key facilities, targets, and/or terrain:** Banks, hospitals, police stations, industrial plants and factories, media and information facilities, bridges, airports, seaports, electric power grids, oil facilities, military facilities, key residences and places of employment, waterways; tall structures (skyscrapers); choke points; street patterns, intersections; industrial complexes; other facilities; density of construction or population.
- **Obstacles:** Rubble and vehicles on the road; fixed barriers; masking of fires, burning of buildings, and other fire hazards; rivers and lakes; power lines and cell phone towers; population; trenches and minefields; certain religious or cultural sites; wire obstacles (concertina wire, barb wire).

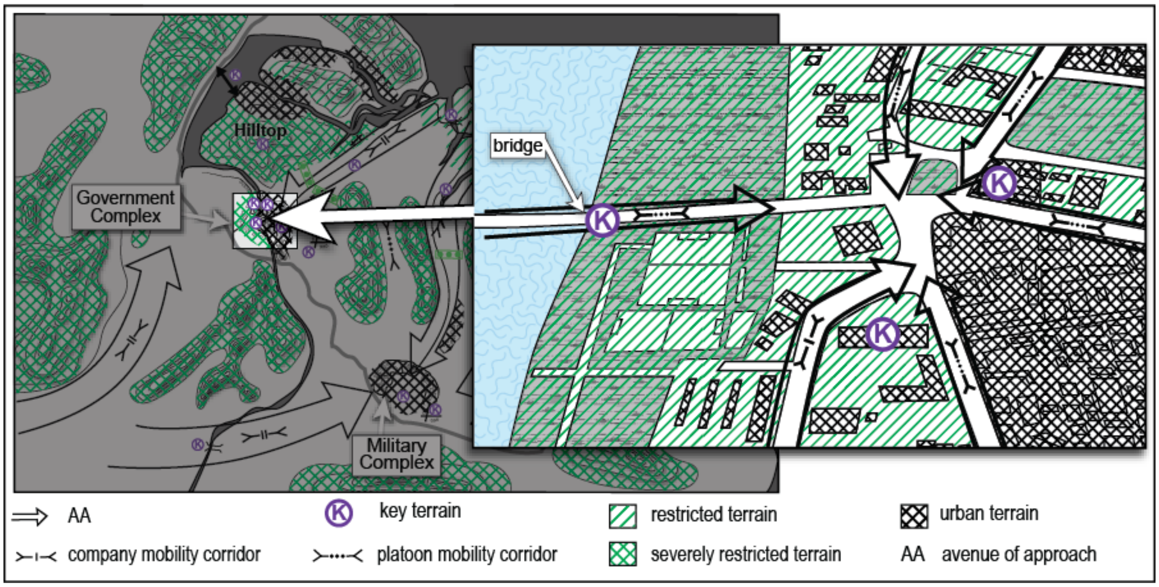


Figure 4-10. Modified combined obstacle overlay example for an urban area

> ***Note.*** In urban areas, the staff should depict storm and drainage systems and public transportation routes, which may function as mobility corridors for future friendly and threat actions. (See chapter 7 for more on urban areas.)

4-49. In developing urban area graphics, the staff should also consider—

- The street level necessary to support the smallest friendly or threat unit size, and the local street names whenever possible (official and unofficial).
- The width of routes in urban areas. The width may not facilitate military vehicle movement.
- The use of certain vehicle-mounted weapon systems. Buildings and other structures may degrade the use of certain vehicle-mounted weapon systems due to the lack of weapon traverse space or ability to aim above certain angles.
- 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, runways, inland-ports, and any known pipelines (with their status: active, inactive, dimensions).

Terrain Effects Matrix

4-50. Using the MCOO as a guide, a terrain effects matrix describes OAKOC factor effects on friendly and threat operations. (See table 4-5.)

Table 4-5. Terrain effects matrix example

OAKOC factors (military aspects of terrain)	*Terrain effects*
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. • Limited air support observation due to sparse terrain and the Earth's curvature. • Fields of fire for direct fire are 300 to 500 meters for small arms. • Intermediate breaks in observation and fields of fire due to runoffs and cuts. • Likely engagement area at Julian pass. • Likely engagement area 1000 meters north of the major city.
Avenues of approach (AAs)	• Primary and secondary road systems for high AAs. • Generally flat terrain with brigade-sized mobility corridors between small villages. • Railroad in the north running east to west. • AA2 is the recommended AA as it enables the placement of organic weapon systems in range before observation from the threat in the defense.
Key terrain	• Airfield used as resupply and troop movements. • Dam controls water flow on the river and is the primary objective of the threat.
Obstacles	• Restrictive runoffs and cuts run 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. • Aboveground oil and transport pipeline (which is severely restrictive terrain) that runs through the central width of the area of operations.
Cover and concealment	• Cover by direct fire systems is provided by intervisibility lines. • Concealment is limited by the open terrain and sparse vegetation.

Techniques for Evaluating Terrain Effects

4-51. Analysts must relate the evaluation of terrain effects on the COAs available to friendly and threat forces. This evaluation should include a detailed discussion of the military aspects of terrain (OAKOC). To evaluate terrain effects on COAs, analysts use four basic techniques:

- **Concentric ring.** The concentric ring technique establishes concentric rings around U.S. forces, starting from a unit's base of operations and working outward. Each ring is balanced and based on the threat's environment and the commander's need to develop knowledge of the tactical situation. Once a certain information collection ring is in place, it is not abandoned; however, the focus of the evaluation is expanding and establishing a second ring. (See figure 4-11.)
- **Belt.** The belt technique divides the AO into belts (areas) running the width of the AO. The shape of the belt is based on analysis of the mission variables (METT-TC). It is most effective when terrain is divided into well-defined cross-compartments during phased operations (such as river crossings, air assaults, or airborne operations), or when the threat is deployed in clearly defined belts. Belts can be adjacent to or overlap each other. (See figure 4-12 on page 4-18.)
- **Avenue in depth.** This technique focuses on one AA. It is good for offensive COAs or in the defense when canalized terrain inhibits mutual support. (See figure 4-13 on page 4-18.)
- **Box.** The box technique is a detailed analysis of a critical area, such as an engagement area, a river-crossing site, or a landing zone. It is most useful when time is constrained, and operations are conducted in a noncontiguous AO. (See figure 4-14 on page 4-19.)

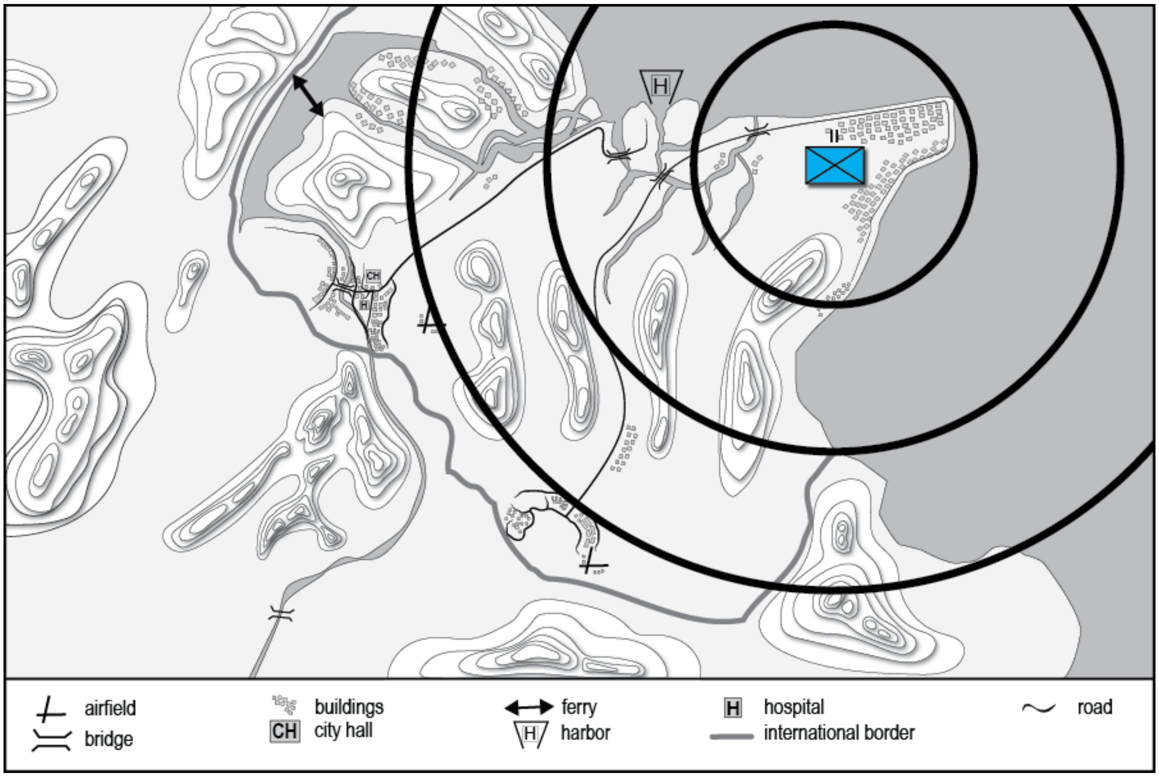


Figure 4-11. Concentric ring technique example

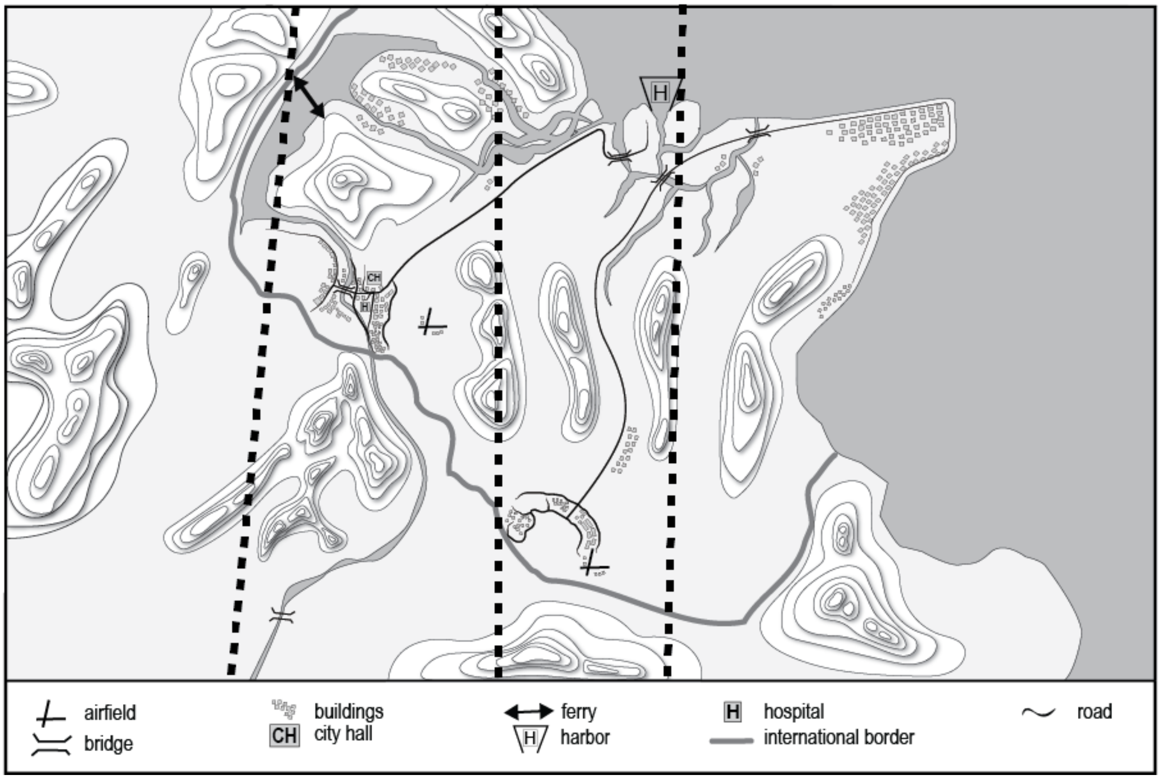


Figure 4-12. Belt technique example

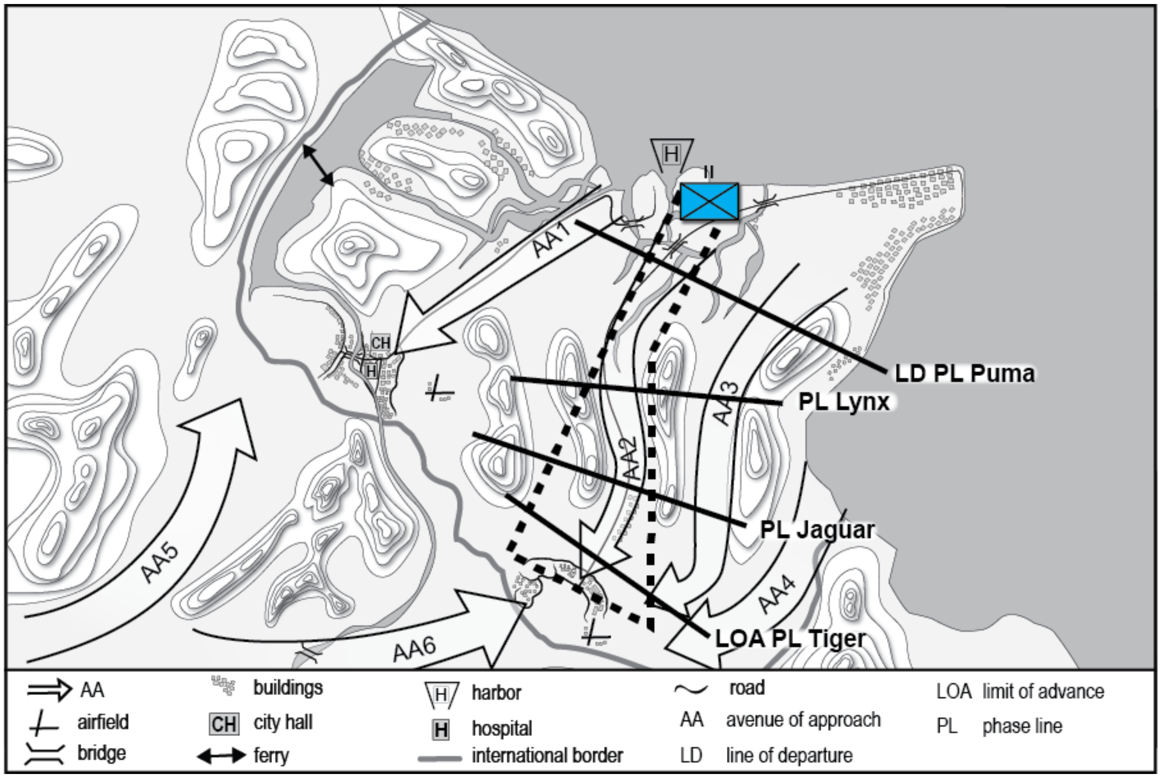


Figure 4-13. Avenue-in-depth technique example

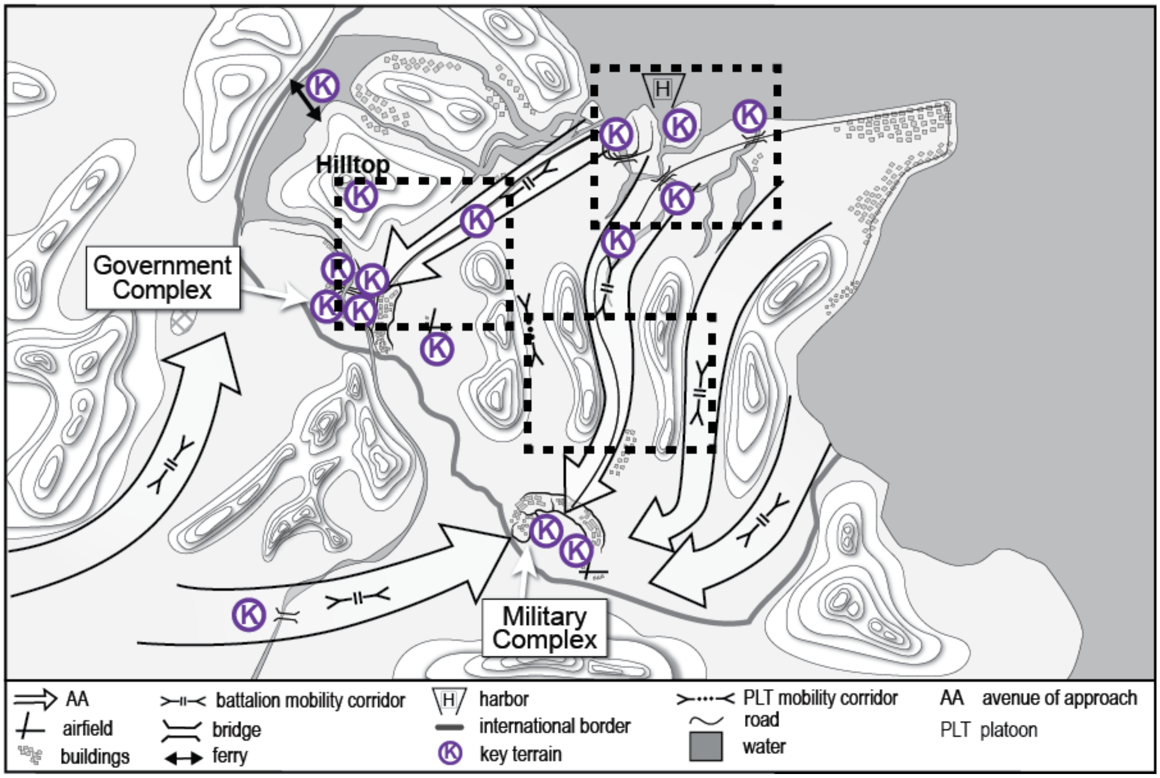


Figure 4-14. Box technique example

4-52. When properly applied, these four basic techniques assist in identifying areas for use as potential—

- **Engagement areas and ambush sites.** Using cover and concealment evaluation results, identify areas where the force is vulnerable to threat fires:
  - If the command is attacking, these are areas where friendly forces are vulnerable to threat fires.
  - If the command is defending, these are potential engagement areas.
- **Battle positions.** Identify covered and concealed positions that offer observation and fields of fire into potential engagement areas:
  - If the command is attacking, battle positions provide a start point for determining possible threat COAs.
  - If the command is defending, these positions are potential defensive positions. These battle positions might also be used by friendly attacking forces to block threat counterattacks.
- **Immediate or intermediate objectives.** Identify any areas or terrain features that dominate the AAs or assigned objective areas. These objectives usually correspond to areas already identified as key terrain.

4-53. The terrain rarely favors one type of operation throughout the width and breadth of the AO. Within a given area, certain subsectors affect various operations to varying degrees. Based on the location and nature of potential engagement areas, battle positions, and objectives, analysts must determine which areas of the AO favor each COA. The analysis of the AO, intelligence estimate, and MCOO are useful tools for disseminating the results of terrain analysis.

DESCRIBE HOW WEATHER CAN AFFECT FRIENDLY AND THREAT OPERATIONS

4-54. Weather analysis is the collection, processing, evaluation, and interpretation of relevant military aspects of weather. It is the evaluation of forecasted weather effects on operations. Analysts should evaluate the effects of each military aspect of weather. However, just as with terrain analysis, they should focus on the aspects that have the most bearing on operations and decision making. The evaluation of each aspect should begin with the local climatology, and the analysts should refine the evaluation with the most current forecasts available. There are two substeps in weather analysis:

- Analyze the military aspects (characteristics) of weather.
- Evaluate the weather's effects on military operations.

ANALYZE THE MILITARY ASPECTS OF WEATHER

4-55. The military aspects of weather are visibility, wind, precipitation, cloud cover, temperature, humidity, and atmospheric pressure (as required).

Visibility

4-56. Visibility refers to 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 following factors:

- *Begin morning nautical twilight* is 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 (JP 3-09.3). Light intensification devices are still effective and may enhance capabilities.
- *Begin morning civil twilight* 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). Currently, light intensification devices are no longer effective, and the Sun is 6 degrees below the eastern horizon.
- *Sunrise* is the apparent rising of the Sun above the horizon. Rising times depend on latitude.
- *Sunset* is the apparent descent of the Sun below the horizon. Setting times depend on latitude.
- *End evening civil twilight* 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* 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). There is no further sunlight available at end of evening nautical twilight.
- *Moonrise* is the time at which the moon first rises above the horizon. Rising times depend on latitude. *Moonset* is the time at which the moon sets below the horizon. Setting times depend on latitude. (See ATP 3-18.10 for information on how the moon phases affect illumination and when moonrise and moonlight will occur.)

4-57. 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 the 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

4-58. Wind of sufficient speed from any direction can reduce the combat effectiveness of a force due to 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 can also 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 friendly and threat detection systems such an aerostat or unmanned aircraft systems (UASs). Evaluation of weather to support operations requires information on the wind at the surface as well as at varying altitudes and elevations.

Precipitation

4-59. 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 needed for information collection. Heavy precipitation can affect sustainment, communications, personnel, military operations, information collection, and many civilian activities.

Cloud Cover

4-60. Cloud cover affects ground operations by limiting illumination and could affect the thermal signature of targets. Heavy cloud cover can degrade many intelligence sensors, 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.

4-61. A cloud cover means the height above the Earth's surface of the lowest layer of clouds or obscuring phenomena 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. Low cloud ceiling also reflects sound waves back to the ground, increasing noise level, making engine noises of mechanized formations and generators, as well as explosions, gunfire, and artillery more audibly detectable.

Temperature

4-62. Temperature extremes can reduce the effectiveness of troops and equipment capabilities. They may affect the timing of combat operations. For example, extremely high temperatures in a desert environment may require dismounted troops to operate at night. High temperatures can affect the lift capability of medium-rotary-lift assets in high altitudes and elevations. For example, during the summer months of Operation Enduring Freedom in Afghanistan, the UH 60 could not carry its full complement of passengers. High temperatures can also increase fuel consumption in vehicles, cause overheating, and affect the muzzle velocity of direct and indirect fire weapons (155-millimeter howitzers, sniper rifles, tanks).

4-63. *Thermal crossover* 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 (JP 3-09.3). In other words, 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. Because of this condition, thermal optics are unable to detect threat vehicles until a temperature disparity exists between the land and the vehicles.

Humidity

4-64. Humidity is the state of the atmosphere with respect to water vapor content. High humidity affects the human body's ability to cool itself. 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. High relative humidity (near or at 100 percent) or coincidence between the temperature and absolute humidity (dew point) create fog. When the air is saturated with moisture, clouds begin to form at ground level, creating additional visibility factors from humidity. Fog typically forms in the mornings when the temperature and dew point are closest to each other.

Atmospheric Pressure

4-65. 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 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 information on aircraft operations.)

EVALUATE THE WEATHER EFFECTS ON MILITARY OPERATIONS

4-66. 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 because 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, affect observation for both friendly and threat forces. Severe restrictions to visibility often restrict aviation operations.
- Hot, dry weather might force friendly and threat forces to consider water sources as key terrain.
- Dense, humid air limits the range of loudspeaker broadcasts, affecting sonic deception, surrender appeals to threat 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.

4-67. Weather and climate effects can impact seasonal outlooks, which affect seasonal decision making—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.

4-68. The G-2/S-2 coordinates with the Air Force staff weather officer to provide weather effects to support operations. The following work aids assist in analyzing and describing weather effects on operations:

- **Weather forecast charts** are guides for determining the weather information needed for planning and operations.
- **Light and illumination data tables** are guides for determining the light and illumination data needed for planning and operations.
- **Weather effects matrices** are guides for determining the weather effects on personnel, weapons, and equipment needed for planning and operations.

DESCRIBE HOW CIVIL CONSIDERATIONS CAN AFFECT FRIENDLY AND THREAT OPERATIONS

4-69. An understanding of civil considerations—the ability to analyze their impact on operations—enhances several aspects of operations, including 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. Generating intelligence knowledge is an opportunity to leverage nonorganic units, agencies, academia, other organizations, or other Services that are not deploying with the unit but have relevant regional knowledge. This is especially true when accounting for cyberspace considerations, which may not be an organic expertise at the G-2/S-2 levels.

4-70. Civil considerations assist commanders in understanding the social, political, and cultural variables within the AO and their effects on the mission. Tactical Army staffs use ASCOPE characteristics to analyze civil considerations that are essential in supporting the development of effective plans for operations. Table 4-6 presents one method by cross-walking civil considerations (including examples for each ASCOPE characteristic) with the operational variables (PMESII).

Table 4-6. Crosswalk of civil considerations (ASCOPE) with operational variables (PMESII)

	Areas	*Structures*	*Capabilities*	*Organizations*	*People*	*Events*
POLITICAL	• Enclaves • Municipalities • Provinces • Districts • Political districts • Voting • Party affiliation areas • Shadow government influence areas	• Courts (court house, mobile courts) • Government centers • Provincial/District centers • Meeting halls • Polling sites • Police stations • Prisons	• Public administration: ▪ Civil authority, practices, and rights ▪ Political system, stability, traditions ▪ Standards and effectiveness • Executive and 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 • Corrections	• Banks • Business organizations • Cooperatives • Economic nongovernment organizations • Guilds • Labor unions • Major illicit industries • Large landholders • Volunteer groups	• United Nations representatives • Political leaders • Governors • Councils • Elders • Community leaders • Paramilitary members • Judges • Prosecutors • Law enforcement officers • Corrections officers	• Elections • Council meetings • Speeches (significant) • Security and military training sessions • Significant trials • Political Motivation • Treaties • Will
MILITARY	• Areas of influence • Areas of interest • Areas of operations • Safe havens or sanctuaries • Multinational/local nation bases • Historic data on operations by the opposition	• 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 forces • Insurgent strength • Enemy recruiting	• Host-nation forces present • Insurgent groups present and networks • Multinational forces present • Paramilitary organizations • Fraternal organizations • Civic organizations	• Key leaders • Multinational, insurgent, military	• Combat • Historical • Noncombat • Kinetic events • Unit reliefs • Loss of leadership
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 • Can tolerate 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 • Police departments	• Bankers • Police • Employers/ Employees • Labor occupations • Consumption patterns • Unemployment rate (if exists) • Job lines • Landholders • Merchants • Money lenders • Black marketers • Gang members • Smuggling chain	• Drought, harvest, yield, domestic animals, livestock (cattle, sheep), market cycles • Labor migration events • Market days • Payday • Business openings • Loss of business

Table 4-6. Crosswalk of civil considerations (ASCOPE) with operational variables (PMESII) *(continued)*

	Areas	*Structures*	*Capabilities*	*Organizations*	*People*	*Events*
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 buildings • Schools/ Universities • Stadiums • Cemeteries • Bars and tea shops • Social gathering places (meeting places) • Restaurants • Police stations	• Medical: Traditional, modern • Social networks, including those on websites • Academic • Strength of tribal/ village traditional structures • Judicial • Police	• Clan • Community councils and organizations • School councils • Familial • Patriotic/Service organizations • Religious groups • Tribes • Police departments	• Community leaders, councils, and members • Education • Ethnicity/Racial: biases, dominant group, percentages, role in conflict • Key figures: criminals, entertainment, religious leaders, chiefs/elders • Languages/ Dialects • Vulnerable populations • Displaced persons • Sports • Influential families • Migration patterns • Culture: Artifacts, behaviors, customs, shared beliefs/value • Police	• Celebrations • Civil disturbance • National holidays • Religious holidays and observance days • Food lines • Weddings • Birthdays • Funerals • Sports events • Market days • Family gatherings • History: major wars/ conflicts • Police engagement
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 • Television stations • Radio stations	• Availability of electronic media • Local communications networks • Internet access • Intelligence services • Printed material: flyers, journals, newspapers • Propaganda • Radio • Television • Social media • Literacy rate • Word of mouth	• Media groups, news organizations • Religious groups • Insurgent inform and influence activity groups • Government groups • Public relations and advertising groups	• Decision makers • Media personalities • Media groups, news organizations • Community leaders • Elders • Heads of families	• Disruption of services • Censorship • Religious observance days • Publishing dates • Inform and influence activity 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 • Maintenance of roads, dams, irrigation, sewage systems • Environmental management	• Construction companies: government, contract	• Builders • Road contractors • Local development councils	• Scheduled maintenance (road/bridge construction) • Natural/Man-made disasters • Well digging • Community center construction • School construction

4-71. Due to the complexity and volume of data involving civil considerations, there is no simple model for presenting civil considerations analysis. The intelligence staff maintains this information in the civil considerations data file and constructs intelligence products comprising overlays and assessments areas overlay to assist in planning.

AREAS

4-72. Key civilian areas are localities or aspects of the terrain within an AO that often are not militarily significant. Key civilian area approaches terrain analysis (OAKOC) from a civilian perspective. The intelligence staff analyzes key civilian areas in terms of how these areas may affect the friendly force mission as well as how friendly military operations may affect these areas. Examples of key civilian areas include but are not limited to—

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

STRUCTURES

4-73. Existing structures can have various degrees of significance. Analyzing a structure 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 should carefully weigh the expected military benefits against costs to the community, which must be considered 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 to the community and should be maintained or restored quickly. (Appendix B provides examples of how to determine the importance of some structures in the OE.)

4-74. The possibility of repaying locals for using shared facilities or building more of the same facilities, time and cost permitting, should also be considered. Examples of structures include but are not limited to military bases; military underground facilities; 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; and universities and schools.

4-75. Other structures are cultural sites, generally protected by international law or other agreements. Examples include but are not limited to religious structures; national libraries and archives; hospitals and medical clinics; monuments; works of art; archaeological sites; scientific buildings, museums; crops, livestock, and irrigation works; and United Nations Educational, Scientific, and Cultural Organizations-designated World Heritage sites.

CAPABILITIES

4-76. 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, media outlets, technology, and necessities (food, water, medical availability).

4-77. Capabilities include those areas, such as public works and utilities, public health, economics, and commerce, in which the populace may require assistance after combat operations. Capabilities also include resources and services that can be contracted to support the military mission, such as interpreters, laundry services, construction materials, and equipment.

ORGANIZATIONS

4-78. IPB considers the organization dimension (such as nonmilitary groups or institutions), the political influence, and the impact of each on the AO. Organizations influence and interact with the populace, friendly forces, the threat, and each other. An important aspect of civil considerations is the political dimension of the local population and its expectations relative to friendly and threat operations.

4-79. Political structures and processes enjoy varying degrees of legitimacy with populations from local to 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.

4-80. Understanding the political circumstances assists commanders and staffs in recognizing key organizations and determining 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 nongovernmental organizations that provide humanitarian assistance.

4-81. Political analysis must include an assessment of varying political interests and the threat's political decisive point and will. Will is the primary intangible factor; it motivates participants to sacrifice in order to persevere against obstacles. Understanding what motivates key groups (for example, political, military, and insurgent) assists commanders in understanding those groups' goals and willingness to sacrifice to achieve their desired end state.

4-82. 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 logistical support. Some organizations may be indigenous to the area. These organizations include but are not limited to—

- Religious, fraternal, or patriotic/service organizations.
- Labor unions.
- Criminal organizations.
- Community watch groups.
- Political groups.
- Agencies, boards, committees, commissions (local and regional, councils).
- Multinational corporations.
- Other host-nation government agencies (such as the foreign version of the Department of Education, U.S. Agency for International Development). ***Note.*** These agencies are separate from organizations with the threat capability (military, intelligence, police, paramilitary), such as the Central Intelligence Agency.
- Nongovernmental organizations, such as the International Committee of the Red Cross.
- Media outlets.

4-83. To enhance situational awareness, commanders should remain familiar with organizations operating in their AOs, such as local organizations that 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 those organizations' activities. From this, commanders can determine how organizations and military forces can collaborate toward common goals when necessary.

4-84. In most instances, 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.

PEOPLE

4-85. The general use of the 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 forces work closely with civilians of all types. Therefore, understanding the sociocultural factors of the people in the AO is a critical component of understanding the OE. Commanders and staffs make decisions on which people to engage and how to engage them based not only on a comprehensive understanding of but also on the dynamics of the OE. (For a detailed discussion on network engagement, see ATP 3-55.4 and ATP 5-0.6.)

4-86. *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). Sociocultural factors must be analyzed closely during irregular warfare and hybrid conflicts. This cultural information, incorporated into the IPB process, provides the backdrop against which the analysis of social and political factors facilitates successful operations.

Language

4-87. Language is always a relevant aspect of the OE. The staff identifies the languages and dialects used within the AO and AOI. Language training, communications aids (digital translators and phrase cards), and required capabilities, such as translators and military intelligence language-specific assets, can be requested. Translators can be crucial for collecting intelligence, interacting with local citizens and community leaders, and developing products.

4-88. Another aspect of language involves the transliteration guide not written using the English alphabet. This impacts all intelligence operations, including collection, analysis, processing, exploitation, 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. Additionally, detainees may be released from custody, targets may be missed, and data on target sets will not be analyzed if names are misidentified. To overcome these problems, there must be one spelling standard for a theater. Because of the interagency nature of operations, the standard must be agreed upon by non-Department of Defense agencies. Intelligence staffs should also be aware of naming conventions that may differ across cultures and geographic regions.

Religion

4-89. Another major consideration when analyzing people is religion. Religion has shaped almost every past conflict, and there are indicators that its influence will only grow. Religion can shape the OE; add a higher intensity, severity, brutality, and lethality to conflicts than almost any other factor; and motivate and mobilize the masses quickly and inexpensively.

4-90. The staff must consider the following when incorporating religion into planning:

- 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 both negatively or positively.
- Attempt to understand all parties, no matter how violent or exclusive.

Culture

4-91. Part of the analysis of people is identifying cultural terms and conditions. Cultural terms and conditions describe both U.S. and foreign thoughts and behaviors. 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. Intelligence analysts must consider that threat motivations and intentions may outweigh cultural norms and practices. In stability tasks, supporting data may include cultural issues and their effects on the combat capabilities or limitations of the threat.

4-92. Understanding culture gives insight into motives and intent of nearly every person or group in the OE—friend, threat, or other. In turn, this insight 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 definitions. Additionally, U.S. forces must recognize they are at an immediate disadvantage in terms of cultural knowledge and understanding because they do not have the benefit of residing in the AO's proximity. Analysts must set aside personal bias and judgment and examine the cultural group dispassionately, basing their 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.

4-93. Culture is studied 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 to understand motivation and intent.

EVENTS

4-94. Events are routine, cyclical, planned, or spontaneous activities that significantly affect organizations, people, and military operations. Examples include but are not limited to—

- National and religious holidays.
- Internationally observed cultural and religious holidays.
- Agricultural crop or livestock and market cycles.
- Elections.
- Civil disturbances.
- Celebrations.
- Natural phenomenon (monsoons, seasonal floods and droughts, volcanic and seismic activity, natural disasters).
- Man-made disasters.

4-95. Examples of events precipitated by military forces include combat operations, congested road networks, security restrictions, and economic infrastructure disruption or stimulus. Once significant events are determined, it is important to template and analyze the events for political, economic, psychological, environmental, and legal implications. Events occurring in the AOI and area of influence may significantly impact the AO and lead to contingency operations.

CIVIL CONSIDERATIONS DATA FILES, OVERLAYS, AND ASSESSMENTS

4-96. The intelligence staff maintains a civil considerations data file that organizes 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.

Example

Under the "capabilities" characteristic, there may be a section for the subcharacteristic of "oil." This section may include—

- Information on the location of the infrastructure components associated with oil.
- How oil may impact other sectors such as financial institutions and regional partnerships.
- The biographical, contact, and location information for the personnel associated with this capability.
- Any intelligence assessments and recommendations associated with oil.
- Any outside countries or organizations contributing to the oil sector.
- Disputes regarding distribution of oil dividends.

4-97. One way of maintaining civil considerations data is in a data file and/or database; this contributes to the continual evaluation of civil considerations as part of the running estimate by organizing the vast amounts of information necessary to analyze civil considerations.

4-98. Civil considerations overlays are graphic depictions of the data file. They assist in planning throughout the MDMP, developing the situation during operations, and the intelligence staff in describing civil considerations effects, as assessed in the data file, to the commander and the rest of the staff. For example, the civil considerations overlay may assist in identifying areas or routes likely to be used if conflict creates conditions for refugees or displaced persons. This information can permit the prepositioning of capabilities, materials, and assets to mitigate impacts to ongoing friendly operations and to assist in humanitarian assistance efforts.

4-99. The civil considerations data file and associated overlays assist the commander and staff in identifying information and intelligence requirements not normally identified through the event templating process associated with determining threat COAs. In contingency operations, or when conducting stability tasks, these work aids assist the intelligence staff in determining and assessing threat COAs.

4-100. Civil considerations assessments are used throughout the MDMP. They use both the civil considerations data file and overlays to provide the supported commander with a detailed analysis of the civil component of the AOI in accordance with ASCOPE characteristics. Potential areas of investigation in the civil considerations assessment include mapping social and political patterns (formal and informal leadership and identifying key societal friction points.

4-101. Understanding the relationship between military operations and civilians, culture, and society is critical to operations and essential in developing effective plans. The development of the civil considerations data file, overlays, and assessments can be augmented by regional civil considerations data repositories maintained at national and theater levels. During—

- Predeployment, unit intelligence staffs should become familiar with the information available on assigned or contingency regions in military and other data repositories, websites, and portals.
- Operations, units use, update, and add to the information available to them and others.
- Relief in place and/or transfer of authority, it is critical for outgoing units to educate incoming units on the information sources available for the AO.

4-102. Civil and foreign affairs officers can also provide detailed information and analysis pertaining to sociocultural factors as aspects of civil considerations. The insights these personnel provide often fill multiple information gaps concerning those areas unfamiliar to both the intelligence and other staff sections.

4-103. There is no standard set of subcharacteristics and overlays produced by the intelligence staff. Determining what is needed is based on the intelligence staff's assessment of the situation and complexity of the AO. Each staff section may have pertinent information to add to the overlays.

This page intentionally left blank.

Chapter 5

Step 3—Evaluate the Threat

WHAT IS IT?

5-1. Step 3 of the IPB process determines threat force capabilities and the doctrinal principles and TTP threat forces prefer to employ. This may include threats that create multiple dilemmas for U.S. maneuver forces by simultaneously employing regular, irregular, and terrorist forces and criminal elements, using a variety of traditional and nontraditional tactics.

> **Example**
>
> While planning a contingency show-of-force operation, a G-2 requests the joint intelligence center study the recent decisions of the targeted country's dictator. Because of this research, the joint intelligence center produces a model of how the dictator makes decisions, emphasizing the dictator's tendencies during political crises. Meanwhile, the S-2 for the brigade conducting the operation evaluates the threat. Using the S-2's contingency area threat characteristics files, the S-2 determines that the two threat brigades within the target area are equipped, organized, and trained well enough for offensive and defensive tasks against the friendly brigade. The S-2 prepares threat models depicting normal offensive and defensive tasks in built-up areas, which lead to a show-of-force operation.

5-2. Over the past three decades, threats have studied the manner in which U.S. forces have deployed and conducted operations. Several have adapted, modernized, and developed capabilities to counter U.S. advantages in the air, land, maritime, space, and cyberspace domains. Military advances by Russia, China, North Korea, and Iran most clearly portray this changing threat. Therefore, understanding threat capabilities is critical to developing COAs.

5-3. Threats, large and small, increasingly operate in an indeterminate zone between peace and war. They seek to avoid U.S. strengths and, instead, take advantage of U.S. laws and policies regarding the use of information and cyberspace capabilities. Coupled with the Nation's initial reluctance to engage in major combat operations, threats achieve incremental gains that advance their agenda and narrative. They use a range of techniques, including nonattribution, innuendo, propaganda, disinformation, and misinformation, to sway global opinion favorable to their aims.

5-4. For the Army, threats are a fundamental part of an overall OE for any operation, but they 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 may include paramilitary or military forces, nation-states, national alliances, individuals, groups of individuals (organized or not organized), or conditions that can damage or destroy life, vital resources, or institutions. (See ADRP 3-0.)

5-5. While the Army must be manned, equipped, and trained to operate across the range of military operations, large-scale ground combat against a peer threat represents the most significant readiness requirement. FM 3-0 focuses on peer threats in large-scale combat operations. It describes peer threats as adversaries or enemies with capabilities and capacity to oppose U.S. forces across multiple domains worldwide or in a specific region where they enjoy a position of relative advantage. Peer threats possess roughly equal combat power in geographical proximity to a conflict area with U.S. forces. They may also have a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary. Peer threats generate tactical, operational, and strategic challenges of an order of magnitude more challenging militarily than those the Army has faced since the end of the Cold War.

5-6. Peer threats—

- Employ strategies that capitalize on their capabilities to achieve their objectives.
- Prefer to achieve their goals without directly engaging U.S. forces in combat.
- Often employ information warfare in combination with conventional and irregular military capabilities to achieve their goals.
- Will try to weaken the resolve of the United States and its partners to sustain conflict.
- Will exploit friendly sensitivity to world opinion and attempt to exploit American domestic opinion and sensitivity to friendly casualties.
- Believe they have a comparative advantage because of their willingness to endure greater hardship, casualties, and negative public opinion.

5-7. Peer threats employ their resources across multiple domains to attack U.S. vulnerabilities. They use their capabilities to create lethal and nonlethal effects throughout an OE. Peer threats will use various methods to employ their national elements of power to render U.S. power irrelevant. Five broad peer threat methods, often used in combination, include information warfare, preclusion, isolation, sanctuary, and systems warfare. During combat operations, threats seek to inflict significant damage across multiple domains in a short time. They seek to delay friendly forces long enough to achieve their goals and end hostilities before friendly forces reach culmination. (See FM 3-0.)

5-8. For this publication, the Army divides these threats into the following categories:

- Regular threats.
- Irregular threats.
- Hybrid threats.

REGULAR THREAT

5-9. Regular threats from peer competitors with significant ability to act in all domains are considered multi-domain threats. These peer threats are only peer in the military or economic elements of power. In the diplomacy and informational elements of power, multi-domain threats use their lack of democratic institutional constraints, realpolitik (practical politics) approaches, and cyberspace capabilities to overmatch U.S. forces. When analyzing the peer threat, it is important to understand the complexity of the OE, since all types of force structures, capabilities, and domains are available to use against U.S. forces to accomplish threat goals and objectives.

5-10. Peer threats seek to reduce the ability of the United States to achieve dominance in the air, land, maritime, space, and cyberspace domains. By using state and nonstate actors, peer threats attempt to apply technology across the domains to disrupt U.S. advantages in communications, long-range precision-guided munitions, movement and maneuver, and surveillance. Peer threats also seek to reduce the United States' ability to achieve dominance in those domains; therefore, Army forces cannot always depend on an advantage in technology, communications, and information collection.

5-11. To capitalize on the perceived vulnerabilities of the United States and its allies, peer threats may use nation-states to establish proxy forces. These forces may act on behalf of peer threats to achieve a desired end state in territories where peer threats do not want to disclose their involvement. Proxy force capabilities range from using insurgent tactics to technologically advanced capabilities. Historic conflicts that relied on proxy force capabilities include but are not limited to the Ukraine crisis (2014), the Syrian Civil War (2011), the Korean War (1950 to 1953), and the Nicaraguan Civil War (1979 to 1990).

IRREGULAR THREAT

5-12. Irregular threats are opponents employing unconventional, asymmetric methods and means to counter U.S. advantages, such as overwhelming firepower and technological overmatch. A weaker threat often uses unconventional methods to exhaust the U.S. collective will through protracted conflict. Unconventional methods include terrorism, insurgency, and guerrilla warfare. Economic, political, informational, and cultural initiatives usually accompany and may even be the chief means of irregular attacks on the U.S. influence. The Hamas and al-Qaida are examples of irregular threats.

5-13. Irregular threats have diverse capabilities that may change rapidly, outpacing what military personnel are accustomed to with the military acquisitions process. Analysis of threat capabilities must be continuous to keep abreast of changes in both equipment and techniques employed. This is particularly true with nonlethal capabilities.

5-14. Irregular threats can take advantage of commercially available technology and exploit cyberspace. For example, irregular threats can use cyberspace to influence global audiences, communicate with specific audiences, and impact U.S. capabilities using direct and indirect means.

5-15. Drug cartels; nationalist, antireligion, and political organizations; foreign terrorist organizations, transnational criminal organizations, and insurgencies; and militant activists may be classified as irregular threats. These groups may have vastly different capabilities and objectives. Some objectives may be rooted in financial gain, while others may be rooted in power, political change, or in governmental policy changes that exceed politics.

HYBRID THREAT

5-16. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting threat effects (ADRP 3-0). A hybrid threat also seeks to achieve shared or separate purposes, shared or separate objectives, or any combination of effects, purposes, or objectives.

Hybrid Threat Example

Country A may use Country B’s military force to achieve a political objective and maintain deniability of its involvement. Country A supports Country B’s military by using a smuggling network to transport weapons, supplies, and cash across international borders. Country A compensates Country B for its actions by lowering tariffs on imports. Despite their different objectives, these parties have a mutually beneficial relationship. Country A achieves a political objective without degrading its international image. Country B gains an economic boost and strengthens an international relationship. The professional smugglers have no interest in politics or national objectives; their only concern is financial.

5-17. From an IPB perspective, the term hybrid threat serves to capture the complexity of OEs, including the variety of actors involved and the blurring of traditional elements of conflict. It also adds another layer of complexity to the evaluation of irregular threats. For example, the involvement of the regular threat (nation-state) may not be overt; its entire purpose for using the irregular threat may be to achieve anonymity or to stay within those confines that will keep the competition below the state of armed conflict. Determining the motivation for the irregular threat’s actions will assist analysts in identifying the potential logic of other actor’s involvement even if that involvement is limited to influence.

SO WHAT?

5-18. The “so what” of step 3 is to enhance commanders’ understanding of the regular, irregular, and hybrid threats within their AOI:

- **Outcome of success:** Threat COAs developed in the next step of IPB reflect what the threat is capable of and trained to do in similar situations.
- **Consequences of failure:**
  - The staff may lack the intelligence needed for planning.
  - The threat may surprise the friendly force with capabilities not accounted for by the G-2/S-2.
  - The staff may waste time and effort planning against nonexistent threat capabilities.
  - The friendly force’s ability to exploit threat windows of vulnerability may be degraded.

HOW TO DO IT: THE PROCESS

5-19. Step 3 of the IPB process consists of the substeps and outputs shown in figure 5-1.

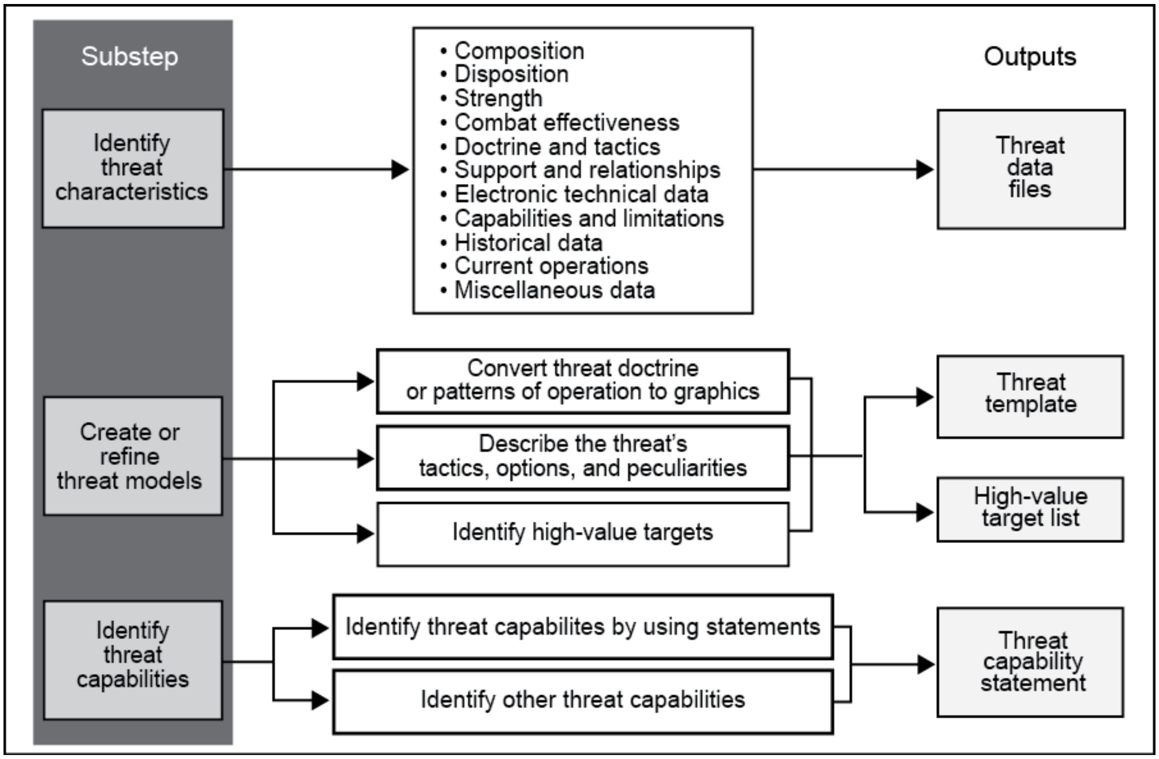

Substep
Outputs
Identify threat characteristics
• Composition
• Disposition
• Strength
• Combat effectiveness
• Doctrine and tactics
• Support and relationships
• Electronic technical data
• Capabilities and limitations
• Historical data
• Current operations
• Miscellaneous data
Threat data files
Create or refine threat models
Convert threat doctrine or patterns of operation to graphics
Describe the threat's tactics, options, and peculiarities
Identify high-value targets
Threat template
High-value target list
Identify threat capabilities
Identify threat capabilites by using statements
Identify other threat capabilities
Threat capability statement

Figure 5-1. Substeps and outputs of step 3 of the IPB process

5-20. Evaluating the threat should begin with identifying all threats based on their characteristics and ultimately creating the threat model (regular, irregular, or hybrid structure). At the tactical level, threat characteristics are often referred to as order of battle. The tactical-level evaluation of a military threat should concentrate on standard threat characteristics/order of battle factors, such as the composition, disposition, strength, TTP, and training status of specific tactical units or factional groups that could interfere with mission accomplishment. *Order of battle* is the identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force (JP 2-01.3).

> ***Note.*** When operating against a new or emerging threat not identified and described in the unit's threat data files, the intelligence staff must develop new data files for each of these threats. Other units' and organizations' data files may also assist in developing threat products.

5-21. A commander's understanding of the threat is based in part on the intelligence staff's research and analysis of the threat characteristics, as part of generating intelligence knowledge. The intelligence staff considers broad characteristics when analyzing the threat, such as composition, disposition, strength, combat effectiveness, doctrine and tactics, support and relationships, electronic technical data, capabilities and limitations, current operations, historical data, and miscellaneous data. To ensure this understanding is as complete as possible, the intelligence staff considers the following when assessing these characteristics:

- Threat characteristics form a framework for the consistent evaluation of any force.
- The threat characteristics evaluation framework should be adapted to the threat mission and the unit's needs.
- Properly maintained files at multiple echelons and organizations are sources of information on threat operations, capabilities, and vulnerabilities.
- Threat characteristics are analyzed as a whole.

5-22. Although threat forces may conform to some of the fundamental principles of warfare that guide Army operations, these forces have obvious and subtle differences in how they approach situations and problem solving. Understanding these differences is essential to understanding how a threat force reacts in a given situation.

IDENTIFY THREAT CHARACTERISTICS

5-23. During steps 1 and 2 of the IPB process, the intelligence staff identifies and defines each individual threat within the commander's AOI. During step 3, the intelligence staff analyzes the characteristics associated with each of these threats as well as develops threat models for each of these threats. (See appendix C for threat characteristics associated with regular, irregular, and hybrid threats.)

COMPOSITION

5-24. Composition is the identification and organization of a threat. It describes how an entity is organized and equipped—essentially the number and types of personnel, weapons, and equipment available for a given operation. Composition applies to specific units or commands as opposed to types of units. Understanding a threat's composition—

- Is essential in determining the threat's capabilities and limitations.
- To help construct threat models that assist in developing valid threat COAs and friendly counteractions.
- Assists in determining a threat's combat effectiveness and conducting combat assessment.

5-25. Regular threats are normally self-identified and organized similarly to friendly forces. Irregular threats may follow similar rules but are mostly organized mostly based on a cellular structure. The staff uses line and block chart products to depict the threat's composition. (See figure 5-2 and figure 5-3 on page 5-6.)

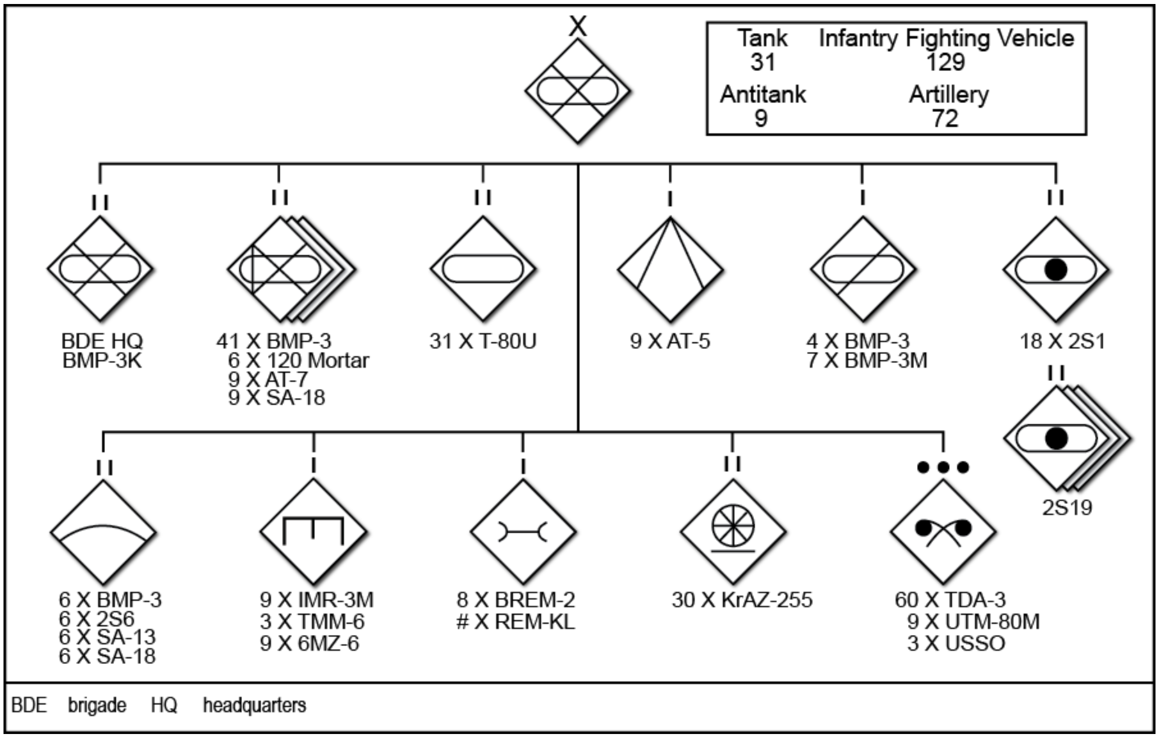


Figure 5-2. Regular threat organizational chart example

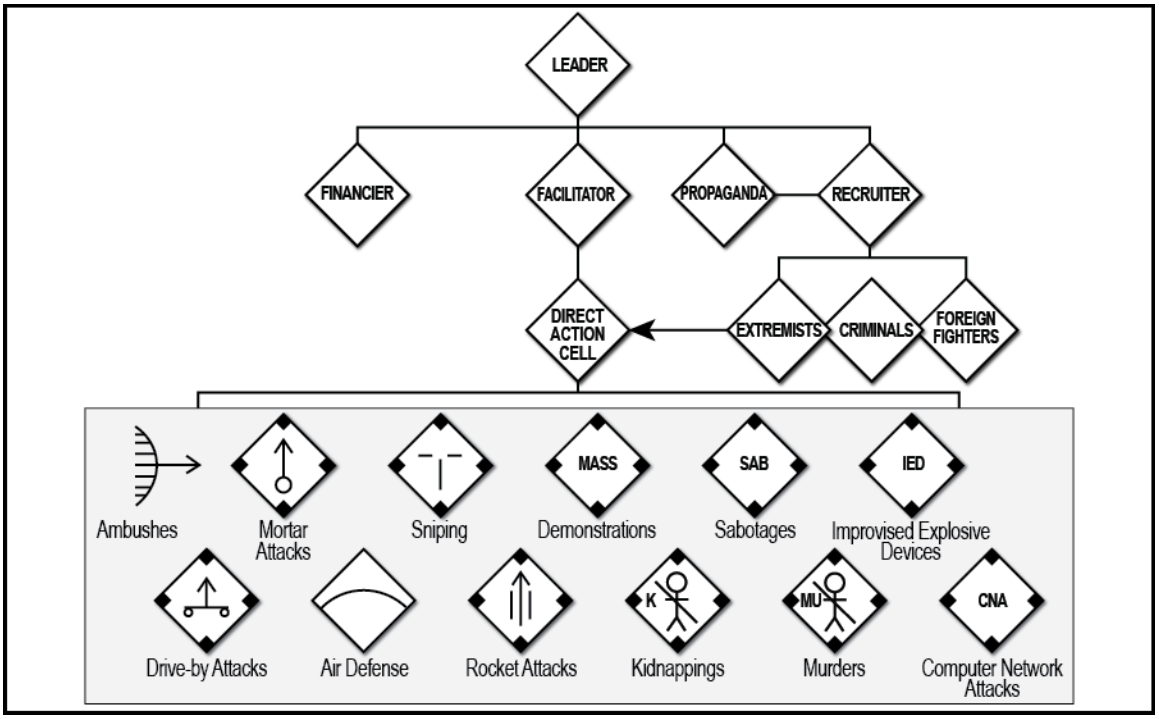


Figure 5-3. Irregular threat organizational chart example

Note. There is no standard organizational structure for hybrid threats.

5-26. 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. They 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 or conflict. Regardless of the threat type, knowing its structure assists in understanding its capabilities and limitations.

DISPOSITION

5-27. Disposition refers to how threat forces are arrayed on the battlefield. It includes the recent, current, and projected movements or locations of tactical forces. Regular threats generally conduct some form of offensive or defensive maneuver. Irregular threats are generally in part of the plan, prepare, execute, and assess activities of an operation, such as a raid or ambush. In a hybrid threat scenario, irregular threats may have the capability to mass and be the main effort or fixing force on the battlefield. Understanding how the threat doctrinally arrays on the battlefield is essential in developing threat models in step 3 of IPB and threat situation templates in step 4 of IPB. The intelligence staff becomes familiar with graphic training aids to illustrate range fans with weapon fire limits and direct and indirect weapon capabilities. This provides a better understanding of threat weapon systems.

STRENGTH

5-28. Strength describes a unit in terms of personnel, weapons, and equipment. Information concerning strength provides commanders with an indication of threat capabilities and assists in determining the probable COAs or options open to threat commanders. A lack of strength or a preponderance of strength has the effect lowering or raising the estimate of the threat’s capabilities. Likewise, a marked concentration or build-up of units in an area gives commanders certain indications of threat objectives and probable COAs. During peacetime, changes in the strength of potential threats are important factors as they may indicate changes in the threat’s intention. Strength is determined by comparing how a threat organization is doctrinally staffed and equipped with what the organization has on hand.

COMBAT EFFECTIVENESS

5-29. Combat effectiveness, the readiness of a military unit to engage in combat based on behavioral, operational, and leadership considerations. Combat effectiveness measures the ability of a military force to accomplish its objective—it describes a unit's abilities and fighting quality. Numerous tangible and intangible factors affect combat effectiveness, including but not limited to the number of personnel or equipment losses and replacements, reinforcements (tangibles), and operational experience and morale (intangibles). The simple fact that a military has large numbers does not ensure a unit is combat effective. In large-scale ground combat, it is important to determine the threat's response to personnel and equipment losses, if and how equipment is replaced, and how units are reinforced.

DOCTRINE AND TACTICS

5-30. Doctrine and tactics include tactical doctrine as well as tactics employed by specific units. While tactical doctrine refers to the threat's accepted organization and employment principles, tactics refer to the threat force's conduct of operations. Based on knowledge of a threat's tactical doctrine, the intelligence staff can determine how the threat may employ its forces in the offense and defense under various conditions. Analysts integrate tactics in threat templates and other intelligence products.

SUPPORT AND RELATIONSHIPS

5-31. The threat's adoption of a COA should depend on its support system's ability to support that action. However, depending on the threat'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's combat effectiveness, strength, and capabilities.

ELECTRONIC TECHNICAL DATA

5-32. Electronic technical data is required to conduct EW. For the Army, this data is also derived from cyberspace electromagnetic activities, signals intelligence (SIGINT), and measurement and signature intelligence. This data includes communications and noncommunications equipment parameters, such as emitter type and nomenclature, modulation, multiplex capability, pulse duration, pulse repetition frequency, bandwidth, associated weapon systems, and other technical characteristics of electronic emissions. This information can be developed into an overlay. To produce the overlay, SIGINT personnel require the targeting and EW staffs' assistance and input.

CAPABILITIES AND LIMITATIONS

5-33. Capabilities are the broad COAs and supporting operations that the threat can take to achieve its goals and objectives. The following tactical COAs are generally open to military forces in conventional operations: attack, defend, reinforce, and retrograde. Each of these broad COAs can be divided into specific COAs. For example, 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 capabilities include support to broad COAs or specific types of operations, such as—

- Information warfare—cyberwarfare, cyberspace operations, perception management, influence activities, information activities, deception, EW, and operations security.
- Intelligence operations.
- CBRN employment.
- Espionage, sabotage, and subversion.

CURRENT OPERATIONS

5-34. 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 other threat characteristics.

HISTORICAL DATA

5-35. Compiling the history of any threat organization involves conducting the research necessary to gather all relevant information regarding the threat 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. These methods support intelligence training, officer professional development, and noncommissioned officer professional development. The history component of the threat data file includes the original sources of information used to compile information briefings and papers. These sources form part of the professional readings required by the unit's intelligence personnel.

MISCELLANEOUS DATA

5-36. Intelligence staffs use supporting information to develop threat force characteristics and to construct comprehensive intelligence estimates. This information includes but is not limited to biographic and personality data, culture (see paragraphs 4-91 through 4-93), biometric and forensic data, as well as other information important to mission accomplishment.

Biographic and Personality Data

5-37. Biographic data contains information on characteristics and attributes of a threat force's members. Personality data is personality profiles; strategic personality assessments of leaders are valuable because the tactics and combat efficiency of particular units are directly related to the commander's character, schooling, and personality traits.

5-38. Personality is critical especially when combating irregular threats. Analysts focus on leaders and other important individuals. Personality files assist analysts in conducting 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.

5-39. Analysts use these personality files to conduct link analysis and build organizational diagrams to determine relationships between critical personalities and their associations to various groups or activities. When combating irregular threats, this analysis is often known as network analysis. This thorough analysis is critical in determining the roles and relationships of many different people and organizations and assessing their loyalties, political significance, and interests. (See ATP 2-33.4 and ATP 5-0.6 for more information on link and network analysis.)

Note. Any relationship or organization can span across illegal, terrorist, and other threat activities, as well as legitimate people, money, and activities.

Biometric and Forensic Data

5-40. Friendly forces have used biometric and forensic collection extensively during recent operations, specifically to support stability tasks by establishing the identity, affiliations, and authorizations of an individual; denying anonymity to a threat; and protecting friendly forces, facilities, and forces.

5-41. Valuable intelligence can and has been analyzed from identity activities—a collection of functions and actions that appropriately recognize and differentiate one person from another to support decision making. Identity activities include the production of identity intelligence. *Identity intelligence* is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (JP 2-0). Identity attributes and associated modalities are collected, analyzed, protected, exploited, and managed 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 that seeks to blend into a civilian populace.

Internal Organizational Processes

5-42. 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 members 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?
- What are the rewards and punishments? Are they consistently applied?
- Are internal rivalries complex, or does organizational discipline have primacy?
- How are policies adjusted and adjudicated, through violence or dialogue?
- What are potential divisions and policy fractures?
- Which leaders support specific positions, and why?
- Are leader motivations organizational, family, or personal?

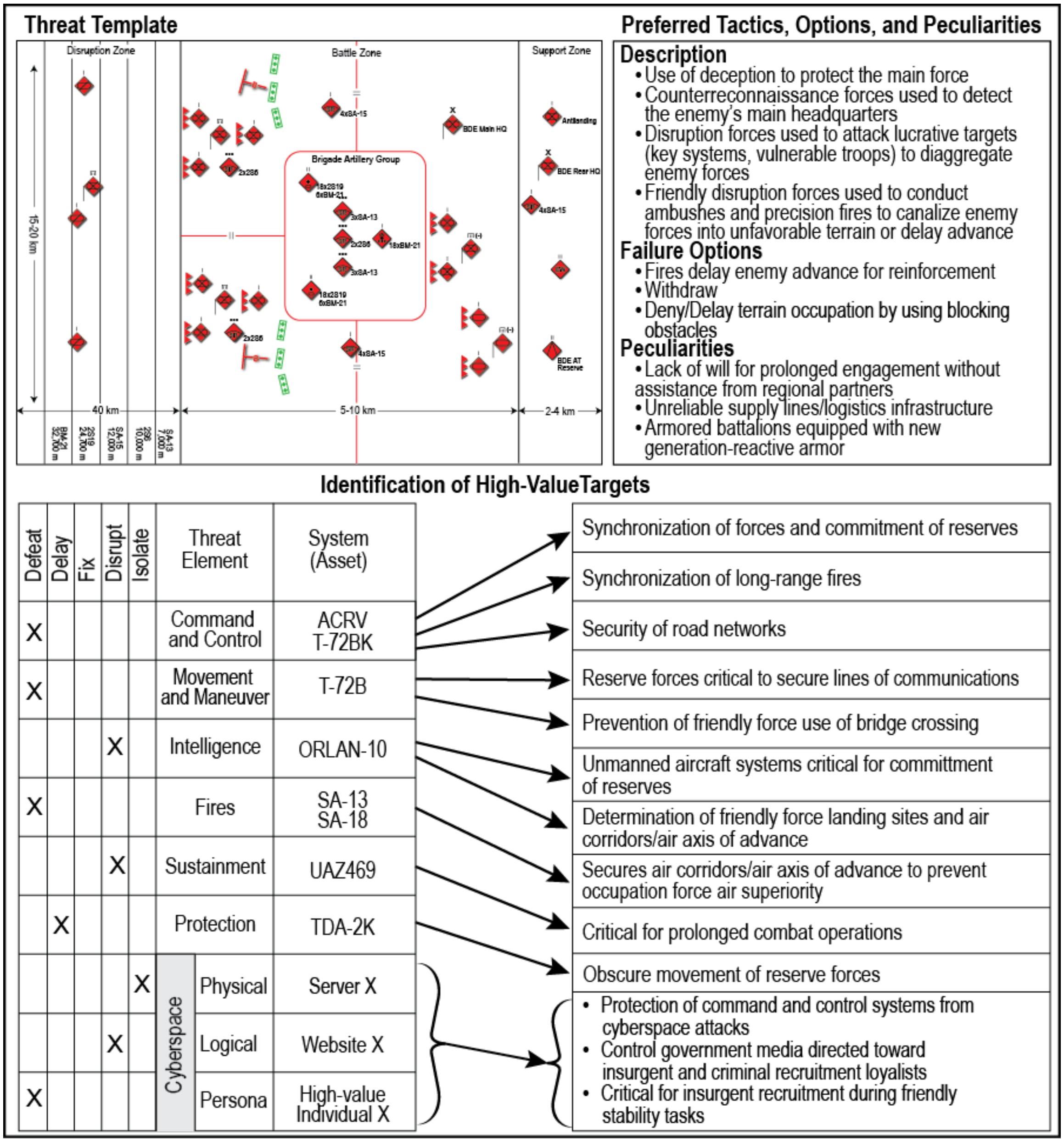
CREATE OR REFINE THREAT MODELS

5-43. Threat models accurately portray how threat forces normally execute operations and how they have reacted to similar situations in the past. This also includes knowledge of threat capabilities based on the current situation. Threat models are initially created by analyzing information in various databases concerning threat organizations, equipment, doctrine, and TTP. Higher agencies and organizations create some threat models; but in immature OEs or when a new threat emerges, analysts develop threat models.

5-44. Analysts must use all available sources to update and refine threat models. The most useful sources are threat characteristic files with information that assists analysts in making conclusions about threat operations, capabilities, and vulnerabilities. Staff integration during threat model development is essential in achieving the most accurate depiction of how the threat conducts operations in ideal situations with no terrain constraints.

5-45. A threat model is an analytical tool that assists analysts in developing situation templates during step 4 of the IPB process. Threat models consist of three activities (see figure 5-4 on page 5-10):

- Convert threat doctrine or patterns of operations to graphics (threat template).
- Describe the threat's preferred tactics, options, and peculiarities.
- Identify HVTs.



Preferred Tactics, Options, and Peculiarities

Description

- Use of deception to protect the main force
- Counterreconnaissance forces used to detect the enemy's main headquarters
- Disruption forces used to attack lucrative targets (key systems, vulnerable troops) to diaggregate enemy forces
- Friendly disruption forces used to conduct ambushes and precision fires to canalize enemy forces into unfavorable terrain or delay advance

Failure Options

- Fires delay enemy advance for reinforcement
- Withdraw
- Deny/Delay terrain occupation by using blocking obstacles

Peculiarities

- Lack of will for prolonged engagement without assistance from regional partners
- Unreliable supply lines/logistics infrastructure
- Armored battalions equipped with new generation-reactive armor

Identification of High-ValueTargets

Defeat	Delay	Fix	Disrupt	Isolate	Threat Element		System (Asset)
X					Command and Control		ACRV T-72BK
X					Movement and Maneuver		T-72B
			X		Intelligence		ORLAN-10
X					Fires		SA-13 SA-18
			X		Sustainment		UAZ469
	X				Protection		TDA-2K
				X	Cyberspace	Physical	Server X
			X			Logical	Website X
X						Persona	High-value Individual X

- Synchronization of forces and commitment of reserves
- Synchronization of long-range fires
- Security of road networks
- Reserve forces critical to secure lines of communications
- Prevention of friendly force use of bridge crossing
- Unmanned aircraft systems critical for committment of reserves
- Determination of friendly force landing sites and air corridors/air axis of advance
- Secures air corridors/air axis of advance to prevent occupation force air superiority
- Critical for prolonged combat operations
- Obscure movement of reserve forces
- Protection of command and control systems from cyberspace attacks
- Control government media directed toward insurgent and criminal recruitment loyalists
- Critical for insurgent recruitment during friendly stability tasks

Figure 5-4. Threat model example

CONVERT THREAT DOCTRINE OR PATTERNS OF OPERATIONS TO GRAPHICS

5-46. Threat templates graphically portray how the threat might use its capabilities to perform the functions required to accomplish its objectives when not constrained by the effects of the OE. Threat templates are scaled to depict the threat's disposition and actions for a type of operation (for example, offense, defense, ambush, personnel movement, clandestine sustainment operations or kidnapping). When possible, templates should be depicted graphically as an overlay, on a supporting system, or through some other means.

5-47. Threat templates are tailored to the needs of the unit or staff creating them. For example, a G-2 section's threat template differs in scope from a brigade S-2 section's template. Some threat templates consider threat forces, while others focus on a single warfighting function, such as intelligence or fire support. Other products depict pattern analysis, time event charts, and association matrices. Threat templates may depict, but are not limited to, unit frontages, unit depths, boundaries, engagement areas, and obstacles. (See ATP 2-33.4 for more on pattern analysis and association matrices.)

5-48. When constructing threat templates, analysts—

- Access and analyze information about the threat from intelligence databases.
- Evaluate the threat's past operations.
- Determine how the threat normally organizes for combat and how it deploys and employs its forces and assets.
- Look for patterns on how the threat organizes its forces, timing, distances, relative locations, groupings, or use of terrain and weather.

5-49. Templating requires continuous refinement to accurately portray threat patterns and practices. For example, while there may be no threat 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 evaluation of the implementation time to determine the likelihood of locations or participants.

Note. G-2/S-2s should allow the mission and threat types of to help drive their required templates.

DESCRIBE THE THREAT'S TACTICS, OPTIONS, AND PECULIARITIES

5-50. When creating the threat model, analysts describe the threat's tactics, options, and peculiarities.

Tactics

5-51. The threat model includes a description of the threat's preferred tactics (including but not limited to attack, defend, reinforce, and retrograde). A description is still required even if the preferred tactics are depicted in graphic form. This allows the template to become more than a "snapshot in time" of the operation being depicted. It assists in mentally war gaming the operation over its duration during the development of threat COAs and situation templates.

Options

5-52. Options are described by listing items such as identified threat capabilities and branches and sequels. Branches and sequels are used primarily for changing deployments or direction of movement and for accepting or declining combat. In accordance with joint doctrine, branches provide a range of alternatives often built into the basic plan. Sequels anticipate and plan for subsequent operations based on the possible outcomes of the current operation—victory, defeat, or stalemate. Analysts list branches and sequels available to the threat should the operation succeed or fail. For example, the threat might prefer to follow successful attacks with pursuit. Should an attack begin to fail, the preferred branches might include committing reserves or reinforcements or shifting the main effort. Should the attack fail, the preferred sequel might be a hasty defense.

5-53. Analysts also describe supporting warfighting-function relevant actions to identify and develop HVTs. They examine timelines and phases of operations because target values may change from phase to phase. Additionally, analysts describe and determine goals the threat is trying to achieve. Threat objectives are often what the unit's mission tries to prevent, and those actions the threat takes to prevent accomplishment of the unit's mission. Threat objectives are specific to the threat type, the AO, the unit's composition and mission, and other factors, such as when and where a unit transitions from one form of maneuver to the next. Analysts also describe threat objectives in terms of purpose and end state. Several different functions must be executed each time a threat force attempts to achieve a goal.

Peculiarities

5-54. Analysts research and annotate any threat peculiarities about the operation. Peculiarities can provide insights into threat strengths and vulnerabilities, as well as assist friendly forces in addressing them. For example, based on research, analysts noted that threat forces lack sufficient armor-piercing 120-millimeter tank rounds. This assists the friendly commander in formulating when and where to use armored assets. Other peculiarities include but are not limited to the following:

- Threat fuel shortages.
- Threat armored battalions have recently completed defensive training exercises.
- The threat has insufficient obstacles to protect defensive sites.
- The threat relies heavily on information warfare to control the local populace.
- The threat lacks information collection assets to collect on certain AAs.
- Threat special purpose forces are well-trained in conducting hasty ambushes to impede movements along AAs.
- The threat lacks the leadership and training to conduct simultaneous counterattacks in multiple locations.

IDENTIFY HIGH-VALUE TARGETS

5-55. Identifying HVTs assists the staff in creating HPTs during the COA development step of the MDMP. The following techniques may be useful in identifying and evaluating HVTs:

- Identify HVTs from existing intelligence studies; the evaluation of the databases; size, activity, location, unit, time, and equipment (also called SALUTE) reports; patrol debriefs; the threat template and its associated threat capability statement; and the use of tactical judgment.
- Review threat TTP and previous threat operations as well as understand the threat's task, purpose, method, and end state.
- Consider that HVTs usually fall within nonmaneuver elements (command and control [C2], intelligence, fires, sustainment, and protection).
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat might react to losing each identified HVT. Consider the threat's ability to substitute other assets as well as adopt branches or sequels.
- Conduct mental war gaming and think through the operation under consideration and how the threat will use assets from each of the elements (such as fire support, engineers).

5-56. As analysts identify key assets (see table 5-1), they group them into categories to assist in identifying threat objectives. Categories include but are not limited to C2, movement and maneuver, intelligence, fires, sustainment, protection, cyberspace.

Table 5-1. High-value targets by threat element and cyberspace

Threat element	*Systems (assets)*	*Capability*	*Strength*	*Weakness*	*Reaction to loss*
Command and control	Radios	• Range • Digital • Encryption • Frequency hop	• What makes it hardened against interception or jamming? • Strong range	• What makes it vulnerable to interception or jamming? • Does it have a weak range?	Only means of communications to leadership
	Runners	Are they present?	• What types of camouflage do they use? • Do they wear civilian attire?	Is this the only communications that they possess?	Only means of communications with priority messages (if loss of radio communications)
	Computer networks	• Fire control networks • Command and control networks (Blue Force Tracker) • Range • Satellite uplink • Network-based • Civilian infrastructure	What makes it more efficient than U.S. systems?	What makes it weaker than U.S. systems?	Only means of communications to leadership

Table 5-1. High-value targets by threat element and cyberspace (*continued*)

Threat element	*Systems (assets)*	*Capability*	*Strength*	*Weakness*	*Reaction to loss*
Movement and maneuver	Tanks/APCs/ IFVs	• Range of main gun • Types of ammunition (range can differ) • Rate of fire • Target acquisition (laser-range finder, wire-guided, basic optical magnification, fire on the move capability) • Armor • Range of system (How far system can travel before refuel?) • Can the commander fire the main gun? • Troop capacity, is it amphibious?	What makes it more efficient than U.S. systems?	What makes it weaker than U.S. systems?	• Strongest armored platform on the battlefield • Only armored personnel carrier • Primary mounted fighting platform
	Mobility and countermobility systems	• Unit basic load • Dig rate • Mine emplacement rate/size of minefield if scatterable mine layer • Bridge lay rate	What makes it more efficient than U.S. systems?	What makes it weaker than U.S. systems?	Only means of obstacle emplacement
	Crew served weapons	• Range of weapons • Types of ammunition (range can differ) • Rate of fire • Target acquisition (laser-range finders, basic optical magnification, fire on the move capability) • Portability (crew size)	What makes it more efficient than U.S. crew-served weapons	What makes it weaker than U.S. crew-served weapons	Primary support by fire platform, largest casualty producing weapons
Protection	Chemical protection	• What types of chemicals can the mask or system withstand? • What type of chemicals does the enemy employ?	What makes it effective against U.S. gas masks?	What MOPP level effectively withstands the chemical?	• Unable to protect against WMD • Unable to implement WMD
	Survivability	Personnel battle armor, what is the rating for (weapon size)?	What makes it more efficient against U.S. weapon systems?	What makes it ineffective against U.S. weapon systems?	Incapable of protecting against 5.56/7.62-caliber round
Fires	Artillery	• Type of ammunition • Range of ammunition • Rate of fire • Fire control system	What makes it more efficient than U.S. artillery/counter artillery?	What makes it weak against U.S. counter artillery?	Unable to implement artillery indirect fire or severely degraded
	Air defense	• Surface to air missile (range of missile • Altitude • Portability • Acquisition system (passive IR, laser) • Air defense guns (range, altitude, portability, acquisition system)	What makes it effective against U.S. airframes?	What are its inferiorities against U.S. airframes?	Unable to deny U.S. air superiority

Table 5-1. High-value targets by threat element and cyberspace (*continued*)

Threat element	*Systems (assets)*	*Capability*	*Strength*	*Weakness*	*Reaction to loss*
Intelligence	UASs	• Type of sensors carried (EO, IR) • Range and loiter time	System is undetectable against ADA radar	System is detectable against ADA radar and dismounts	Unable to implement aerial reconnaissance
	Ground surveillance radars	• Range of detection for vehicles • Range of detection for dismounts	Capable of detecting both mounted and dismounted with range	Incapable of detecting mounted or dismounted	Unable to detect ground forces
	Signals intelligence	• Frequency range • Range of system	What makes it effective against U.S. communications systems?	Not capable of intercepting encrypted messages	Unable to intercept and detect U.S. communications
	RECON vehicles	• Range of vehicles • Sensors carried (EO, IR, optics)	Sensors outrange U.S. RECON vehicles	Weaker range than U.S. RECON vehicles	Unable to effectively RECON U.S. forces from a mounted position
	Human intelligence	How many teams?	• Native to the area • Same cultural heritage	What makes it weaker than U.S. systems?	Unable to infiltrate the populace
	Counterbattery radars	• Range of mortars • Range for rockets and howitzers • Range of detection	Is the range of detection further than U.S. artillery range?	• Is it jammable? • Does the U.S. artillery out-range the range of detection? • Reaction time is slow	Unable to detect U.S. indirect fire point of origins
	ADA radars	Range	What makes it effective against U.S. airframes?	What makes it ineffective against U.S. airframes?	Unable to detect U.S. aerial assets
Sustainment	Sustainment vehicle types	• Carrying capacity • Range of vehicle • Level of medical care • Amphibious	What makes it more efficient than U.S. systems?	What makes it weaker than U.S. systems?	Unable to conduct ambulatory evacuations or to effectively resupply forward elements
Cyberspace	Physical	Interconnectivity in the network (able to reach local network or global)	Able to connect to government networks	Unable to connect to government networks	Unable to connect to government networks to infiltrate
	Logical	Skills available to infiltrate a network	Able to infiltrate government networks	Unable to infiltrate government networks	Loss of capability to infiltrate networks
	Persona	• Media access scrambler • Internet protocol obfuscation • Use of anonymous networks	Availability of persona obfuscation	• No use of persona obfuscation • Identity known	Identity will be known

ADA	air defense artillery	MOPP	mission-oriented protective posture
APC	armored personnel carrier	RECON	reconnaissance
EO	electro-optical	UAS	unmanned aircraft system
FMV	full motion video	U.S.	United States
IR	infrared	WMD	weapons of mass destruction

Time Event Chart

5-57. After identifying HVTs, analysts place them in order of their relative value (see table 5-2 on page 5-16) to the threat's operation and record them as part of the threat model. The value of the HVTs varies over the course of an operation. Analysts can use a time event chart (see figure 5-5) to assist in identifying HVTs over the course of an operation. A time event chart provides a method for visualizing individual or group actions chronologically. The chart can assist analysts in identifying which assets threat forces will need to conduct certain operations. Staffs should identify and annotate changes in the value of HVTs by each phase of an operation. (See ATP 2-33.4 for information on time event charts.)

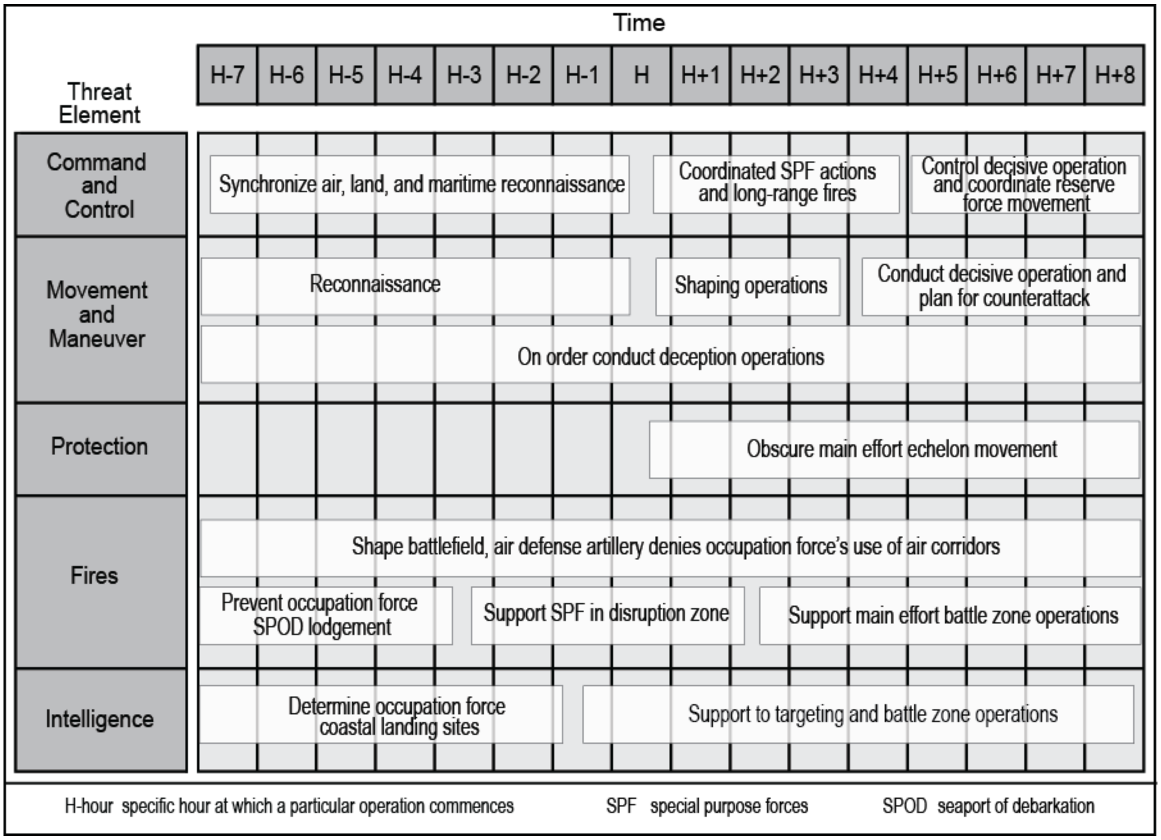

Time
H-7
H-6
H-5
H-4
H-3
H-2
H-1
H
H+1
H+2
H+3
H+4
H+5
H+6
H+7
H+8
Threat Element
Command and Control
Synchronize air, land, and maritime reconnaissance
Coordinated SPF actions and long-range fires
Control decisive operation and coordinate reserve force movement
Movement and Maneuver
Reconnaissance
Shaping operations
Conduct decisive operation and plan for counterattack
On order conduct deception operations
Protection
Obscure main effort echelon movement
Fires
Shape battlefield, air defense artillery denies occupation force's use of air corridors
Prevent occupation force SPOD lodgement
Support SPF in disruption zone
Support main effort battle zone operations
Intelligence
Determine occupation force coastal landing sites
Support to targeting and battle zone operations
H-hour specific hour at which a particular operation commences
SPF special purpose forces
SPOD seaport of debarkation

Figure 5-5. Time event chart example

Target Value Analysis

5-58. HVTs should be prioritized by their relative value to the threat's operation. Target value analysis assists in prioritizing HVTs. Target value analysis 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 threat operation. This analysis is based in part on the conclusions reached by the intelligence staff upon evaluating threat characteristics. The IPB products required to support target value analysis are the threat template, the HVT list, and the threat capability statement. These products assist 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 to facilitate the mission's success.
- Identifying effects criteria.

Note. While target value analysis is conducted initially during IPB, it is a separate process that is repeated throughout the operations process as part of targeting. To be effective, this analysis depends on the most current intelligence related to the threat. Initially, based on the threat template developed during step 3 of IPB, target value analysis should be refined based on the threat COAs developed during step 4 of IPB, and refined continually based on changes to the threat overlay during operations. Whenever conducted, the intelligence staff supports target value analysis with the most up-to-date threat-related intelligence. (See ATP 3-60 and JP 3-60 for more information on target value analysis.)

5-59. The CARVER matrix is a target value analysis tool used to identify and prioritize specific targets, so attack resources can be used efficiently. (See table 5-2.) CARVER stands for criticality, accessibility, recuperability, vulnerability, effect, and recognizability.

Table 5-2. CARVER matrix tool

Value	*Criticality*	*Accessibility*	*Recuperability*	*Vulnerability*	*Effect*	*Recognizability*
5	Loss would end the mission	Easily accessible; not in the vicinity of security	Extremely difficult to replace, long replacement time	Have the means and expertise to attack	Favorable impact on civilians	Easily recognized by information collection assets
4	Loss would reduce mission performance	Easily accessible	Difficult to replace with long down time (<1 year)	Probably have the means and expertise to attack	Favorable impact, no adverse impact on civilians	Easily recognized by information collection assets
3	Loss would reduce mission performance	Accessible	Can be replaced in relatively short time (months)	May have the means and expertise to attack	Favorable impact, some adverse impact on civilians	Recognized with some training
2	Loss may reduce mission performance	Difficult to gain access	Easily replaced in a short time (weeks)	Little capability to attack	No impact on forces, adverse impact on civilians	Hard to recognize, confusion probable
1	Loss would reduce mission performance	Very difficult to gain access	Easily replaced in a short time (days)	Very little capability to attack	Unfavorable impact, assured adverse impact on civilians	Extremely difficult to recognize without extensive orientation

IDENTIFY THREAT CAPABILITIES

5-60. Threat capabilities are broad options and supporting operations that the threat can take to influence accomplishing friendly missions. They provide the means for accomplishing goals, attacking friendly vulnerabilities, and degrading or neutralizing strengths. (See ADP 2-0 and FM 2-0 for additional information on threat capabilities.) Threat actors employ a combination of four major capabilities:

- **Conventional capabilities** are those military assets employed by states in identifiable formations. International law, military tradition, and custom govern conventional capabilities. Nearly every recognized nation-state maintains some conventional forces.
- **Irregular capabilities** are those means of employing unconventional methods, including asymmetric ways to counter U.S. advantages. Irregular capabilities are unregulated; they can act without legal restrictions on the use of violence. Additionally, they are used to create conditions for a protracted conflict in order to exhaust U.S. political will. Targeting economic or political centers with irregular capabilities or exacerbating cultural differences to promote instability are often the preferred means of attack on the U.S. influence.
- **Disruptive capabilities** involve the use of technologies to reduce friendly advantages. Disruptive capabilities use technology to provide the threat with an advantage over similar technology used by friendly forces.
- **Weapons of mass destruction (WMD) capabilities** involve the acquisition, possession, and use of CBRN weapons—also referred to as WMD. The likelihood of the threat's use of WMD increases during large-scale combat operations. The proliferation of these weapons provides potential threats the capability to inflict sudden and catastrophic effects likely to have significant military and political impact today more so than in the past.

IDENTIFY THREAT CAPABILITIES BY USING STATEMENTS

5-61. Analysts identify threat capabilities by using statements such as the following:

- "The threat has the capability to attack with up to eight divisions supported by 150 daily sorties of fixed-wing aircraft."
- "The criminal organization has the ability to pay off local law enforcement agencies."
- "The terrorists have the capability to send destructive viruses over the internet that can destroy computer files and archives."
- "The threat has ADA capabilities to counter rotary-wing support during infiltration operations."
- "The threat can establish a prepared defense by 14 May."
- "The terrorists have the capability of using CBRN weapons."
- "The threat has the capability to conduct information warfare from Site X."
- "The drug smugglers have the ability to conduct three drug-smuggling operations simultaneously."
- "The terrorists have the ability to conduct multiple car bombings simultaneously."
- "The threat has the ability to target friendly convoys along main supply routes using remotely detonated improvised explosive devices (IEDs)."
- "The threat has the ability to counter friendly UASs before crossing Phase Line Green."

IDENTIFY OTHER THREAT CAPABILITIES

5-62. Other threat capabilities include support to COAs, which may include attack, defend, reinforce, retrograde, or specific types of operations, as well as operations that would allow threat forces 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.
- EW operations.
- Use of air assets (fixed-wing and rotary-wing).
- Engineering operations.
- Air assault or airborne operations.
- Amphibious operations.
- River operations.
- Propaganda.
- Recruitment.
- Deception operations.
- Car bombings, bomb scares, and suicide bombers.
- Raids on weapons storage facilities.
- Carjacking or hijacking of vehicles used in transporting personnel, weapons, or drugs.
- Theft of chemicals related to drug manufacturing.
- Counter-UAS assets.
- Offensive cyberspace operations.
- Antiaccess and area denial assets.
- Social media exploitation.

5-63. When identifying threat capabilities and COAs, analysts start with a full set of threat models and consider the threat's ability to conduct each operation based on the current situation and the threat's METT-TC conditions. Most situations do not present the threat with ideal conditions envisioned by its doctrine. Therefore, the threat's actual capabilities usually do not mirror the ideal capabilities represented by the complete set of threat models. This, in turn, causes the threat to use certain capabilities during friendly windows of vulnerability.

5-64. The threat could be under strength in personnel and equipment or may be lacking in logistical support, or threat personnel may be inexperienced or poorly trained. For example, a terrorist group's normal tactics may call for the use of car bombs as a diversionary tactic to conduct other operations elsewhere. The evaluation of the threat's logistics might indicate a critical shortage of explosives. Analysts should consider the following:

- Avoid limiting threat models and capabilities strictly to the threat's conventional forces. For example, student rioters during a noncombatant evacuation operation may be or may become a threat during the operation. By not limiting threat capabilities, intelligence staffs have a more holistic view of all possible COAs when conducting step 4 of the IPB process.
- Avoid overstating threat models and capabilities. The proper use of findings and recommendations developed from threat assessments develops realistic threat models and reserves valuable time and resources for the commander and staff.
- During any discussion of the threat, be culturally aware; this 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, somewhere in between, or both.

OUTPUTS FROM STEP 3 OF THE IPB PROCESS

5-65. The following IPB products are developed based on outcomes from step 3 of the IPB process:

- Threat template.
- HVT list.
- Threat capability statement.

THREAT TEMPLATE

5-66. As operations begin, it is imperative to develop foundationally sound and accurate threat models through careful analysis. The analyst analyzes a threat's capabilities, vulnerabilities, doctrinal principles, and preferred TTP. It is from the threat's doctrine, training practices, and observed patterns and activities that analysts construct threat templates. (See figure 5-6.)

5-67. Threat templates graphically portray how the threat prefers to use its capabilities to perform the functions required to accomplish its objectives. They are scaled depictions of threat deployment patterns and dispositions for a particular operation (for example, offense, defense, ambush, or terrorist kidnapping operation) when not constrained by OE effects. Depending on the mission variables, developing templates can be time intensive.

> ***Note.*** Analysts should create as many threat templates as time allows. This assists in creating situation templates during step 4 of the IPB process.

5-68. Threat templates are tailored to the needs of the unit or staff creating them. When possible, they should be depicted graphically as an overlay, on a supporting system, or through some other means. Threat templates do not include environmental effects, such as terrain and weather. They include—

- The location of all threat 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 threat forces conducting a specific operation or activity.
- Graphic control measures associated with the operation, including but not limited to unit frontages, unit depths, boundaries, engagement areas, and obstacles.

5-69. Threat templates allow analysts and the staff to—

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

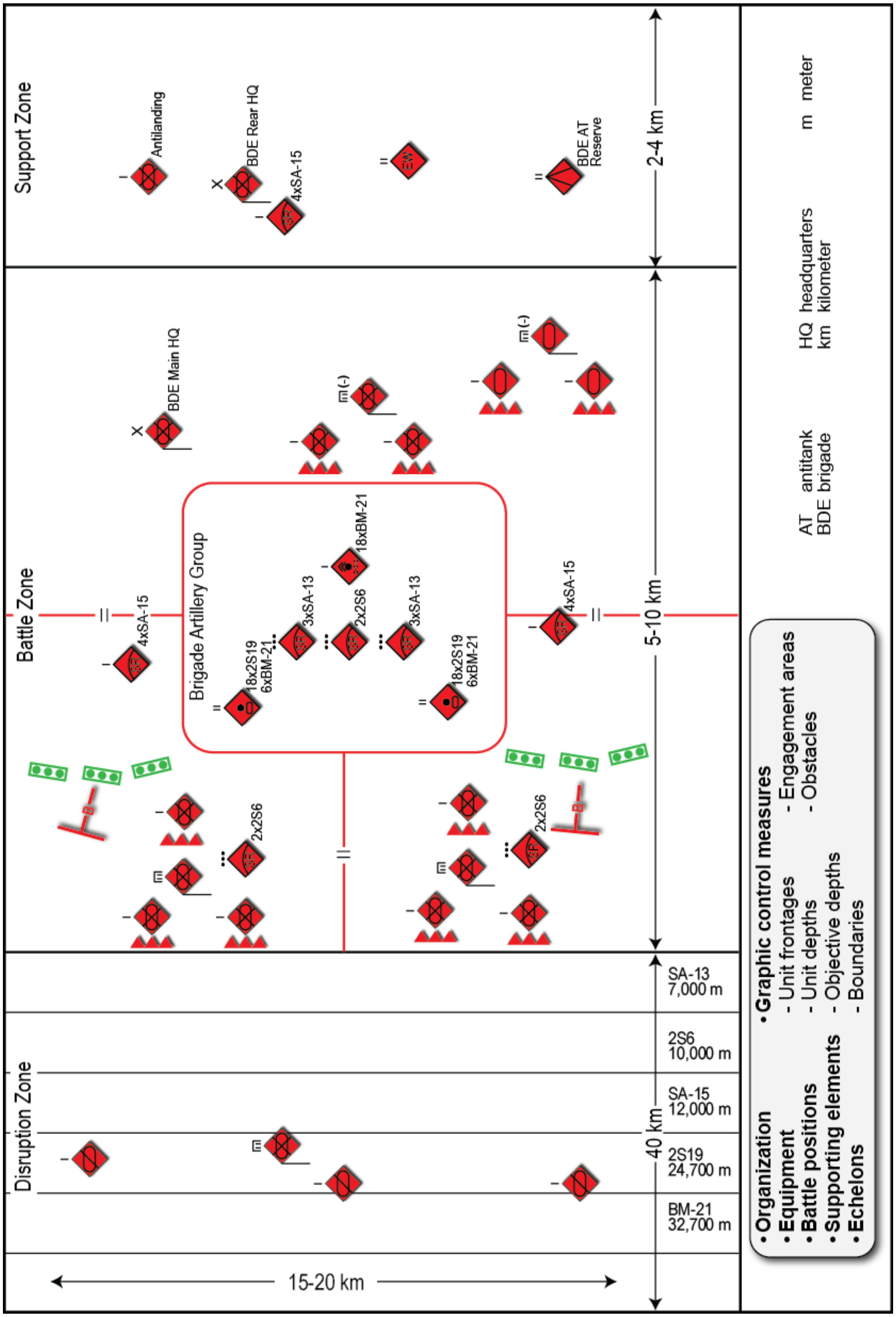


Figure 5-6. Threat template example

HIGH-VALUE TARGET LIST

5-70. The HVTs identified during step 3 of IPB are initially refined during step 4 of IPB. They are refined again during the COA analysis step of the MDMP. The HVT list is developed based on identified HVTs. (See figure 5-7.)

Threat element	***High-value targets***	
Command and control	• Commander's variant main battle tank (T-72 BK) • Command and staff vehicle (BMP-1KShM) • SAM system fire control (SA-15b)	• Artillery command and reconnaissance vehicle (1V14-3) • Command infantry fighting vehicle (BMP-3K)
Movement and maneuver	• Main battle tank (T-72B) • Excavating vehicle (MDK-3) • Tracked minelaying vehicle (GMZ-3) • Infantry fighting vehicle (BMP-3)	• Towed mechanical minelayer (PMZ-4) • Mine-clearing plow attached (KMT-8) • Armored personnel carrier (BTR-80)
Protection	• NBC reconnaissance vehicle (RKhm-4-01)	• NBC reconnaissance vehicle (BRDM-2RKh)
Fires	• 122-mm multiple rocket launcher (BM-21) • 30-mm self-propelled antiarcraft gun/missile system (2S6M1) • 152-mm self-propelled howitzer (2S19M1)	• 120-mm self-propelled mortar (2S12) • Man-portable SAM system (SA-18) • SAM system (SA-15b) • SAM system (SA-13b)
Intelligence	• Signal van (GAZ-66) • Battlefield surveillance radar (SNAR-10) • Armored scout car (BRDM)	• Short range drone (ORLAN-10) • SAM system radar system (SA-15b) • Artillery locating radar (ARK-1M)
Sustainment	• Tactical utility vehicle (UAZ-469) • 2-mT 4x4 cargo truck (GAZ-66)	• 4.5-mT 6x6 cargo truck (URAL-4320)
mm millimeter mT metric ton		NBC nuclear, biological, chemical SAM surface-to-air missile

Figure 5-7. High-value target list developed during step 3 of IPB (example)

THREAT CAPABILITY STATEMENT

5-71. A threat capability statement can be a narrative, table, or visual representation of the data. It identifies a particular action the threat has the capability to complete, and the tactics the threat prefers to accomplish its objectives. It addresses a major unit's operations portrayed on the threat template and the activities of each threat capability. Figures 5-8 and 5-9 show threat capability statements using different formats.

Threat element	***Statement***
Command and control	The threat can establish commands across the country based on communications capabilities. The threat has constant communications to maintain control of subordinate units from corps down to team echelons.
Movement and maneuver	Corps can provide defensive positions for the forward line of own troops, as well as necessary reinforcement operations to the forward division tactical groups via blocking and ambush operations. The groups will delay United States (U.S.) operations to the eastern border.
Protection	Corps will maintain constant communications to establish air corridor denial of U.S. forces within their respective areas of operations: coordinate with the 9th Corps to ensure successful capture of the capital while denying U.S. forces control of airspace and delaying U.S. forces arrival.
Fires	Division tactical groups will use SS26s and 2S19s to delay U.S. force advancements to the country capital while canalizing U.S. forces through constant fires operations. Division tactical groups will only retaliate with CBRN capability when U.S. forces first use CBRN or U.S. forces approach the capital before division tactical group control is imminent.
Intelligence	The threat uses special purpose forces for early warning systems and can establish terror organizations. It uses guerilla warfare and insurgency tactics against U.S. forces to delay advancement.
Sustainment	Protection and fires will ensure routes are established for resupply opportunities and will establish consolidation areas for refit of forward elements.
CBRN chemical, biological, radiological, and nuclear	

Figure 5-8. Threat capability statement example (narrative format)

Threat element	***Zones***		
	Disruption zone	**Battle zone**	**Support zone**
Command and control	1x reconnaissance BN HQ with: • 2x BTR-80K • 1x BMP-1KSh with line of sight communications, high frequency communications, and satellite communications capabilities	3x MECH INF BN HQ with: • 1x BMP-3K • 2x self-propelled artillery BN HQ with 8x ACRV • 1x tank BN HQ with 2x BTR-80AK • 1x MRL BN HQ with 8x ACRV • 1x BDE main command post	• 1x BDE rear command post • 1x signal BN HQ with 11x BMP-1KSh • 1x antitank BN HHQ with 4x BMP-1KSh • 1x MECH INF CO HQ with 1x BMP-3K
Movement and maneuver	• 3x CSOP • 2x BMP-2 • 26x RPG-27 • 4x AT-14 ***Note.*** Capability to ambush with antitank capabilities and to overwatch obstacles.	• 8x MECH INF CO with 13x BMP-3, 10x RPG-29, 3x AT-14, 1x AGS-30 • 3x tank CO with 12x T-90 • 1x engineer BN with 3x BMZ-3, 3x PMZ-4, 3x KMT-7, 4x MDK-3, 4x TMM, 2x IMR-2M, 1x GAT-2, 1x MTU-80 ***Note.*** Each minefield supports simple battle positions consisting of 10-meter intervals, 200 to 300 meters wide and three to four rows deep, and a 400-meter wide antitank ditch 3 meters deep.	1x MECH INF CO—antilanding reserve with: • 13x BMP-3 • 10x RPG-29 • 3x AT-14 • 1x AGS-30 ***Note.*** Able to interdict airborne operations within the area of operations in a maximum of 45 and a minimum of 15 minutes.
Protection	1x chemical defense CO with 2x ARS-14K and 3x BRDM-2RKh ***Note.*** Capability to detect airborne and ground contaminations.		
Fires		• 8x MECH INF CO with 3x SA-18 and 6x 2S12 • 3x tank CO with 2x SA-18 • 2x self-propelled artillery BN with 18x 2S19 and 6x BM-21 • 1x MRL BN with 18x BM-21 • 1x ADA BN with 8x SA-15 provide security for BNs • 6x 2S6 provide security for BNs • 6x SA-13 provide security for BDEs ***Note.*** Artillery in the battle zone can affect targets out to 37 kilometers from the BDE artillery group; ADA can protect out to 25 kilometers from the BDE artillery group.	1x ADA CO with 4x SA-15
Intelligence	• 1x BRM-3 • 4x BRDM-2 • 3x ORLAN-10 • 8x signal CO with 12x signal vans, 1x URAL-4320, 8x BMP-1KSh	• 2x self-propelled artillery BN with 1x SNAR-10 and 1x ARK-1M • 1x MRL BN with 1x SNAR-10 and 1x ARK-1M ***Note.*** Can detect points of origin of artillery operations and air platforms out to 40 kilometers for tanks, 30 kilometers for rotary assets, and 15 kilometers for dismounts.	1x signal BN HQ with: • 12x signal vans • 1x URAL-4320 • 11x BMP-1KSh

Figure 5-9. Threat capability statement example (table format)

Threat element	***Zones***		
	Disruption zone	**Battle zone**	**Support zone**
Sustainment	8x signal CO with 3x motorcycles	• 8x MECH INF CO with 5x GAZ-66 • 2x self-propelled artillery BN with 20x URAL-4320 • 1x MRL BN with 8x URAL-4320	• 1x medical BN with 8x UAZ-469 and 3x URAL-4320 • 1x material support BN with 43x URAL-375D, 2x URAL-4320 (water), 4x URAL-4320 (POL) • 1x maintenance BN with 3x motorcycles, 31x UAZ-469, 22x light trucks, 45x medium trucks, 2x water trucks, 4x light vans ***Note.*** Can provide refuel, resupply, and medical services throughout the BDE; medical facility is Role 3 capable.

ADA	air defense artillery
BDE	brigade
BN	battalion
CO	company
HHQ	higher headquarters
HQ	headquarters
INF	infantry
MECH	mechanized
MRL	multiple rocket launcher
POL	petroleum, oils, and lubricants

Figure 5-9. Threat capability statement example (table format) (*continued*)

Chapter 6

Step 4—Determine Threat Courses of Action

WHAT IS IT?

6-1. Step 4 of the IPB process identifies and describes threat 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

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."

6-2. When evaluating the threat, the intelligence staff should consider—

- How the operational variables (PMESII-PT) and civil considerations (ASCOPE) may impact how the threat operates.
- How friendly actions may impact threat operations and threat COAs.

SO WHAT?

6-3. The "so what" is to determine the threat COAs necessary to aid the development of friendly COAs:

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

HOW TO DO IT: THE PROCESS

6-4. Determining threat COAs is a two-step process consisting of the substeps and its outputs shown in figure 6-1.

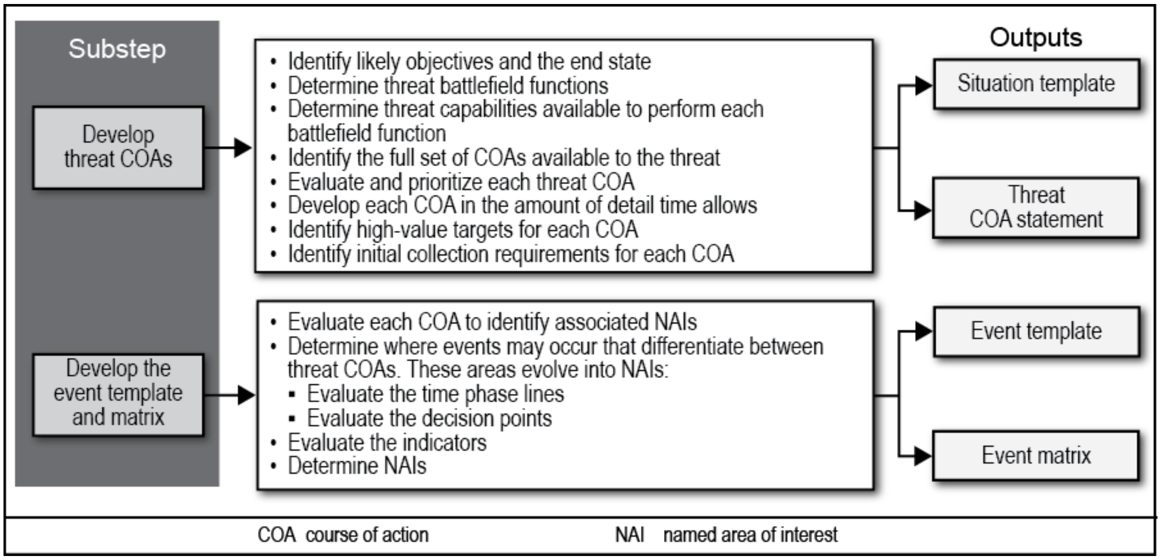

Substep
Develop threat COAs
Develop the event template and matrix
• Identify likely objectives and the end state
• Determine threat battlefield functions
• Determine threat capabilities available to perform each battlefield function
• Identify the full set of COAs available to the threat
• Evaluate and prioritize each threat COA
• Develop each COA in the amount of detail time allows
• Identify high-value targets for each COA
• Identify initial collection requirements for each COA
• Evaluate each COA to identify associated NAIs
• Determine where events may occur that differentiate between threat COAs. These areas evolve into NAIs:
▪ Evaluate the time phase lines
▪ Evaluate the decision points
• Evaluate the indicators
• Determine NAIs
Outputs
Situation template
Threat COA statement
Event template
Event matrix
COA course of action
NAI named area of interest

Figure 6-1. Substeps and outputs of step 4 of the IPB process

DEVELOP THREAT COURSES OF ACTION

6-5. Developing a threat COA requires an understanding of the threat characteristics discussed in chapter 5, as well as the effects of terrain, weather, and civil considerations on operations as discussed in chapter 4. Population effects on operations must be clearly annotated with full details. This ensures population effects and threat actions are portrayed during the war game.

6-6. The most important element in determining threat COAs is understanding threat operational art and tactics. U.S. forces may encounter regular, irregular, and hybrid threats. The process for determining the COAs these threat forces may employ mirrors friendly COA development and consists of the following:

- Identify likely objectives and the end state.
- Determine threat battlefield functions.
- Determine threat capabilities available to perform each battlefield function.
- Identify the full set of COAs available to the threat.
- Evaluate and prioritize each threat COA.
- Develop each COA in the amount of detail time allows.
- Identify HVTs for each COA.
- Identify initial collection requirements for each COA.

IDENTIFY LIKELY OBJECTIVES AND THE END STATE

6-7. Based on the results of the mission variables analysis conducted earlier in the IPB process, the staff now identifies the threat's likely immediate and subsequent objectives and desired end state. These elements are included in the threat COA statement developed for each COA.

6-8. An *objective* is the clearly defined, decisive, and attainable goal toward which an operation is directed (JP 5-0). Threat 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.

6-9. The *end state* is the set of required conditions that defines achievement of the commander's objectives (JP 3-0). The end state, if achieved, meets 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 the platoon level and friendly forces incapable of conducting a coordinated defense.

6-10. For regular threats, 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 performing an attack is to neutralize defending forces. The brigade's end state is to prevent defending forces from affecting the movement of second echelon forces. Additionally, the brigade's operations are synchronized in time with higher headquarters operations to ensure combat power is applied where and when needed to ensure success.

6-11. For irregular threats, while the end state is based on effect, objectives are not always linear or time-based. Often, the objectives for irregular threats are event- rather than time-driven. For example, the objective of a 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 is to convince the population to rely on security provided by the group rather than by 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.

6-12. For hybrid threats, objectives may be terrain- or force-oriented; the end state may be based on effect and time. Alternatively, for regular and irregular threats, the objectives may be disparate based on their unique capabilities. For example, the objective of an insurgent cell performing an IED attack may be to disrupt attacking forces. The mechanized infantry unit echeloned with the insurgent cell may have an end state of preventing attacking forces from increasing an occupation force's sphere of influence. Additional hybrid threat objectives may include but are not limited to preserving power, degrading the threat's will and capacity to fight, and gaining time for aggressive strategic operations to succeed.

DETERMINE THREAT BATTLEFIELD FUNCTIONS

6-13. The threat executes several different battlefield functions each time a threat attempts to accomplish a mission. Threat commanders identify the specific functions they intend their various subordinate forces or elements to perform. The functions do not change, regardless of the forces' or elements' location on the battlefield. While the various functions required to accomplish any given mission can be quite diverse, they can be divided into two very broad categories: action and enabling.

Action Function

6-14. The action function (also known as the exploitation, decision, or mission function) is performed by the set of capabilities accomplishing a given mission. If the threat objective is to destroy a city with a WMD, then the WMD is performing the action function. If the threat objective is to seize a friendly capital city, and the threat employs a WMD in another area to force a response by friendly forces that leaves the capital exposed, then the force used to seize the capital is performing the action function and the WMD is performing a different function.

6-15. One part of the unit or group of units conducting a particular action normally perform the primary function or task that accomplishes the objective or goal of that action. Therefore, that part of the unit can be called the action force or action element. However, in most cases, the higher commander gives the action force or element a more specific designation that identifies the specific function it is intended to perform. This equates to achieving the objective of the higher command's mission. For example—

- If the objective of the action conducts an assault, the assault element completes that action.
- In larger offensive actions, the exploitation force is the action force that completes the primary offensive mission by exploiting a window of opportunity created by another force.
- In defensive actions, the main defense force or element is the unit or group of units that performs the main defensive mission in the battle zone. However, in a maneuver defense, the main defensive action is executed by a combination of the contact force and the shielding force.

Enabling Function

6-16. The enabling function (also known as the assault function), designated as disruption, fixing, or security, is performed by a set of capabilities that acts to assist those capabilities in performing the action function. For example, 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. In relation to the forces or elements conducting the action function, all other organization parts or groupings conducting an action provide enabling functions of various kinds. Therefore, each of these parts can be called an enabling force or element. However, each subordinate force or element with an enabling function can be more clearly identified by the specific function it performs. For example—

- A force that enables by fixing threats so the threats cannot interfere with the primary action is a fixing force.
- An element that creates a breach to enable an assault element to assault threats on the far side of an obstacle is a breach element.

6-17. 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 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. 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 enabling forces or elements may not need to make contact with the threat. In the defense, an enabling function might be to counterattack to restore a portion of the area of responsibility to threat control.

Disruption

6-18. Disruption forces or elements operate to prevent U.S. forces from executing friendly COAs the way they want, and to prevent U.S. forces from interfering with threat COAs. U.S. forces can—

- Disrupt threat preparations or actions.
- Destroy or deceive threat reconnaissance.
- Begin reducing the effectiveness of key components of the threat's combat system.

Fixing

6-19. 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. Fixing is accomplished when a part of the threat force does not participate in actions that could lead to the failure of threat COAs. This includes but is not limited to—

- Suppressing a force with fires.
- Deceiving a force.
- Diverting a force by creating other priorities.
- Involving a force in a firefight away from the main action.
- Restricting a force's movement with countermobility effects.
- Depriving a force of logistics resources.

Security

6-20. 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 from threat elements that could alter the outcome. This can be accomplished by providing early warning and reaction time or actively delaying or destroying arriving threat forces.

Other Functions

6-21. The threat commander may designate a subordinate unit or grouping to conduct a deception action (such as a demonstration or feint). Therefore, this unit or grouping is a deception force or deception element. Its function is to lead the threat to act in ways prejudicial to threat interests or favoring the success of a threat action force or element.

6-22. A threat commander may also designate some subordinates to perform various support functions. These support elements can provide the following types of support:

- Perform support by fires (in which case, it can be called more specifically a support by fires element).
- Provide support or sustainment (combat or combat service support).
- Provide C2 functions.

6-23. At a commander's discretion, some forces or elements may be held out of the initial action, in reserve, pending determination of their specific function. Then, 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 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 task might become the counterattack force.

DETERMINE THREAT CAPABILITIES AVAILABLE TO PERFORM EACH BATTLEFIELD FUNCTION

6-24. Upon determining which battlefield functions the threat needs to perform and what objective or goal the threat commander seeks to accomplish through the performance of those functions, analysts must then determine what capabilities the threat has in order to execute each function.

6-25. While the functions required for a high chance of success in achieving a military objective or goal are universal, the means to accomplish them depend on the location, threat, and environment. For example, in one battlefield, the threat may employ an infantry platoon equipped with infantry-fighting vehicles and sophisticated thermal sensors to execute the security function. In another example, a civilian in a third-floor apartment window using a cellular phone may perform the same function.

6-26. Functional analysis is an analytical technique that depicts graphically how the threat might use its capabilities to perform the functions required to accomplish its objectives. It is based on the concept—while every action or battle is unique, certain functions are performed to bring about mission accomplishment. When analysts apply their knowledge of common and necessary military functions to specific threat capabilities, they are performing functional analysis. (See ATP 2-33.4 for more information about functional analysis.) Functional analysis—

- Forces analysts and the staff to learn and understand tactics instead of rote memorizations.
- Reduces the ability of the threat to deceive analysts and the staff.
- Applies across all theaters and works all along the range of military operations.

IDENTIFY THE FULL SET OF COURSES OF ACTION AVAILABLE TO THE THREAT

6-27. Each threat capability has unique COAs available at any given time. Regardless of the threat category and the capability employed, the threat plans the employment of specific capabilities based on a task, purpose, method, and end state. The intelligence staff identifies the task, purpose, method, and end state for each potential COA developed by the threat for each threat capability. By identifying these for each COA, the intelligence staff can better determine the chosen threat COA during the conduct of operations.

6-28. For regular threats, the analysis conducted by the intelligence staff to identify threat COAs is familiar as it largely mirrors the methodology used to identify COAs for friendly capabilities. (See FM 6-0 for further discussion on developing friendly COAs.)

6-29. When determining a threat COA, the intelligence staff accounts for all relevant threat activity, including but not limited to the analysis of the following:

- Current threat situation.
- Mission (includes task and purpose).
- Threat objectives, methods and functions, and end state.
- Commander's intent, purpose, and end state.
- Task organization.
- Capabilities.
- Vulnerabilities.
- HVTs.
- Decision points (essential in determining branches and sequels).
- Decisive points (source of strength, power, and resistance).
- Critical events.
- Branches and sequels.
- Intent for (includes task, purpose, method, and end state)—
  - Movement and maneuver.
  - Reconnaissance and surveillance.
  - Fires support.
  - Logistics.
  - Threat C2.
  - Protection.
  - Information activities.
  - Denial and deception.
- How terrain and weather affect threat operations.
- How civil considerations affect threat operations.
- How displaced civilians and displaced persons affect threat operations.
- How the presence and actions of U.S. forces affect threat operations (reverse IPB).

6-30. For threat offensive tasks, the staff focuses on determining the main, supporting, and reinforcing efforts; use of reserves; use of special munitions; use of air support; and use of UASs to support fires. For threat defensive tasks, the staff focuses on determining the location of engagement areas and obstacles; the location, type, and size of security zone forces and counterattack forces; and the use of special munitions, air support, UASs, and antiaccess and area denial systems.

6-31. The analysis of potential COAs for irregular threat capabilities is less familiar to the intelligence staff and other staff sections, mainly because those capabilities are not in current operational doctrine such as counterinsurgency. Irregular threats encompass a broad range of capabilities. Within a single AO there may be many irregular threats that compete with each other, are in conflict with each other, are in partnerships or alliances with each other, or simply operate unilaterally within established or accepted geographic, financial, or commodity limits to avoid conflict with others.

6-32. Using doctrinal military terms to analyze irregular threat potential COAs may invoke cognitive limitations and biases on analyses. The staff may have to set aside familiar terms (such as reconnaissance and surveillance, commander, deception, HVT, mission, and end state) and develop a new set of analytical criteria for each unique irregular threat capability. Invoking a systems perspective and integrating network engagement may facilitate developing these criteria as well as shifting the mental paradigm from armed combatants to the broad array of threats in the AO. (See ATP 5-0.6 for information on network engagement.)

6-33. When determining COAs for regular and hybrid threats, and the hybrid threat operates under the C2 of a unified command structure, the staff develops COAs focused on the objectives and end state of that command structure. However, when faced with multiple threats with varied and competing objectives, such as those encountered during stability task, the staff develops COAs for each of these threats.

EVALUATE AND PRIORITIZE EACH THREAT COURSE OF ACTION

6-34. To plan for all possible contingencies, the commander understands all COAs a threat commander can use to accomplish objectives. The staff assists in this understanding by determining all valid threat COAs and prioritizing them from most likely to least likely. The staff also determines which threat COA is the most dangerous to friendly forces. To be valid, threat COAs should be feasible, acceptable, suitable, distinguishable, and complete—the same criteria used to validate friendly COAs.

6-35. The commander approves a plan optimized to counter the most likely threat COA, while allowing for contingency options should the threat choose another COA. Therefore, the staff evaluates each threat and prioritizes it according to how likely it is that the threat will adopt that option. Generally, threat 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 may choose to accept risk to achieve a desired end state. It is impossible to predict what COA the threat will choose. Therefore, the staff develops and prioritizes as many valid threat COAs as time allows but, at a minimum, develops the most likely and most dangerous COAs.

6-36. Upon identifying all valid threat COAs, the staff compares each COA to the others and prioritizes them by number. For example, if four COAs have been developed, COA 1 is the threat's most likely COA, and COA 4 is the least likely. Additionally, the staff determines which COA is the most dangerous; however, the designation of the most dangerous COA largely depends on how much each threat COA threatens the selected friendly COA. 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 organization, including external organizations providing support)?
- **What** (type of tactical mission task such as defeat, destroy, seize)?
- **When** (the earliest time the action can begin)?
- **Where** (the battlefield geometry that frames the COA [boundaries, objectives, routes, other])?
- **How** (the threat attacks, defends)?
- **Why** (the threat's objectives)?

DEVELOP EACH COURSE OF ACTION IN THE AMOUNT OF DETAIL TIME ALLOWS

6-37. A threat COA consists of the following products:

- Situation template for the threat COA.
- Threat COA statement.

Situation Template for the Threat Course of Action

6-38. A *situation template* is 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). A situation template graphic depicts a potential threat COA as part of a particular threat operation. It usually depicts the most critical point in the operation as agreed upon by the commander, the operations officer, and the intelligence officer. However, the operation may require the preparation of several templates as overlays representing different "snapshots in time," starting with the threat's initial array of forces. These snapshots in time are useful in depicting—

- Points where the threat might adopt branches or sequels to the main COA.
- Places where the threat is especially vulnerable.
- Other key points in the battle, such as initial contact with friendly forces.

6-39. Situation templates are developed using the threat's current situation, based on threat doctrine and the effects of terrain, weather, and civil considerations. The situation template may include—

- Doctrinal rates of march. (See appendix B and ATP 3-34.80 for examples.)
- Time phase lines.

- Graphic control measures, including but not limited to—
  - Obstacles (natural and reinforcing). (See ATP 3-34.80 for examples.)
  - Engagement areas.
- Threat composition, disposition, and strength.
- Task, purpose, method, and end state.
- Key threat weapon systems range fans.
- AAs.
- NAIs.

6-40. The basis for modifying a threat situation template is the significant effects the OE may have on the threat COA. For example, the threat may prefer to establish battle positions 1 to 1.5 kilometers apart. However, the terrain may force it to increase this distance to protect its flanks. As another example, the threat 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 to use a suboptimal approach.

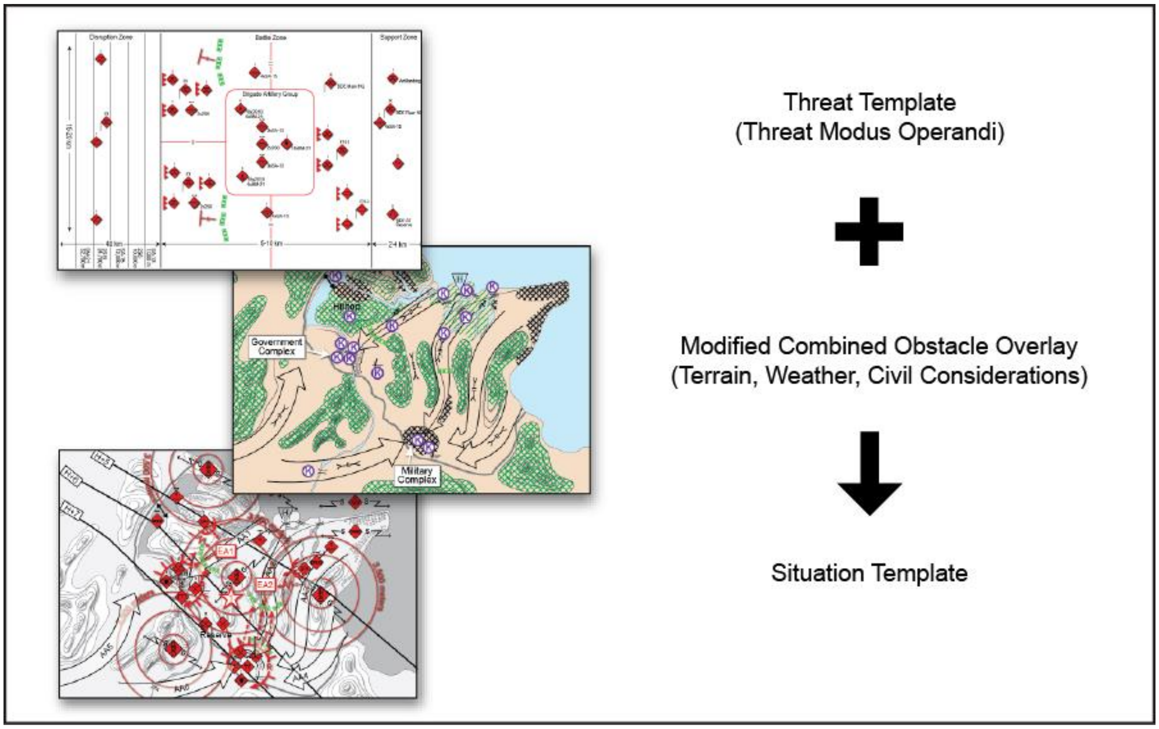
6-41. To develop a situation template, analysts can use the following process:

- Begin with the threat template developed as part of the threat model during step 3 of the IPB process. Overlay the threat template on those products that depict OE effects on operations (typically, the MCOO, but this may vary depending on the operation and situation). (See figure 6-2.)
- Adjust the dispositions portrayed on the threat template to account for OE effects:
  - Since there are many options available, use judgment and knowledge of the threat's preferred tactics and doctrine as depicted in the threat model.
  - Attempt to view the situation from the point of view of the threat commander when selecting from the threat templates.
  - Consider the OE, including but not limited to terrain, weather, and civil considerations (ASCOPE).
- Check the situation template. Account for all threat major assets, ensuring no inadvertent duplications. (See figure 6-3 on page 6-10.)
- Ensure the template reflects the main effort identified for the COA:
  - Compare the depicted dispositions to the threat's known doctrine and check for consistency.
  - Consider the threat's capability to present an ambiguous situation in order to achieve surprise.
- Include as much detail on the situation template as the time and situation warrant. For example, if the threat is defending—
  - Identify the likely engagement areas, reinforcing obstacle systems, and counterattack objectives that form part of his defensive COA.
  - Depict the locations and activities of the HVTs listed in the threat model.
- Use the description of preferred tactics that accompanies the threat model as a guide:
  - Think through the COA scheme of maneuver.
  - Visualize how the threat may transition from its current positions to those depicted on the template.
- Mentally war-game the scheme of maneuver from the positions depicted on the template through to the COA's success or failure:
  - Identify points where forces may transition from one formation to another.
  - Identify how each threat characteristics fits in and supports the operation.
- Evaluate time and space factors to develop time phase lines depicting threat movement. Draw time phase lines on the template to depict the expected progress of attacking forces and the movement of forces in the deep and rear battle areas.

- Base time phase lines on the threat's doctrinal rates of movement, with some modification:
  - Evaluate actual movement rates, as captured in the database, against threat doctrinal rates. ***Note.*** Analysts may need to reach out to outside organizations, such as the National Ground Intelligence Center, to attain accurate and up-to-date doctrinal rates. (See appendix B for examples.)
  - Consider OE effects on mobility.
  - If contact with friendly forces is expected, mentally war-game the effects this may have on the threat's speed as well. Further consideration includes the threat's logistics and maintenance capabilities.
- When placing time phase lines, consider only the time (assuming that time-consuming planning, issuance of orders, reconnaissance, and logistical preparations may occur during movement)—
  - It may take to adopt movement formations.
  - To conduct movement to the selected location.
  - For the unit to close after arrival.
- During staff war gaming of the situation templates against potential friendly COAs, update time phase lines to consider when threat movement may be triggered or how the threat might be influenced by friendly actions.

6-42. Analysts can prepare as many graphics as necessary to depict the COA in enough detail to support staff war gaming and collection planning. For example, a COA may begin as a movement to contact, transition to a hasty attack, followed by pursuit operations that include a river crossing. Each of these phases may require a separate template.

6-43. Analysts should tailor situation templates to their needs by focusing on factors important to the commander or mission area. For example, the situation might focus only on the threat's reconnaissance assets when determining and developing threat COAs. Situation templates produced might show only the location and movement routes of these assets, their likely employment areas, and their likely NAIs. An aviation unit, for example, might develop situation templates that depict details such as specific radar and ADA weapon locations and their range fans or areas of coverage.



Threat Template
(Threat Modus Operandi)

+

Modified Combined Obstacle Overlay
(Terrain, Weather, Civil Considerations)

↓

Situation Template

Figure 6-2. Developing a situation template

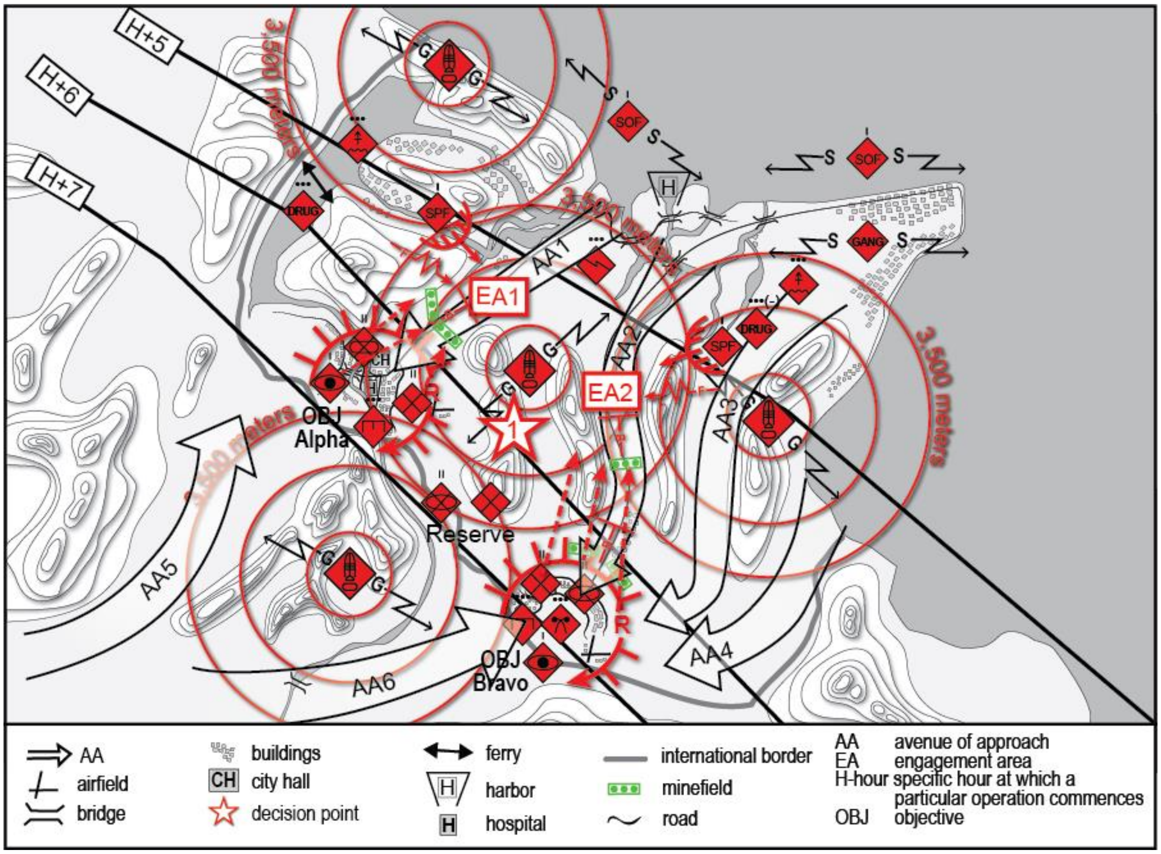


Figure 6-3. Completed situation template example

6-44. At higher echelons, situation templates usually focus on culminating points and installations or activities associated with decisive points rather than specific military units. Some situation templates are better presented in a matrix format. Figure 6-4 illustrates a situation template in a matrix format that shows one threat COA for area defense. The timeline indicates when the threat is most likely to use assets to reach a desired end state, as well as the time threat assets or effects are expected within each NAI.

NAI/Time (H-hour)	*H+5*	*H+6*
NAI1	**Task:** Disrupt forces in vicinity EA1. **Purpose:** Delay movement along western avenue of approach. **Method:** Special purpose forces conduct ambushes. **End State:** Threat forces able to maneuver into secondary defensive positions if needed.	**Task:** Destroy aviation assets in vicinity EA1. **Purpose:** Prevent seizure of airfield in vicinity Objective Alpha. **Method:** SA-13 and SA-18. **End State:** Retain capability to use airfield to conduct operations.
NAI2	**Task:** Destroy forces in vicinity EA2. **Purpose:** Prevent seizure of the Military Complex. **Method:** Coordinated long-range fires. **End State:** Retention of military mission command networks.	**Task:** Block maneuver forces from moving south of EA2. **Purpose:** Provide targets for long-range fires. **Method:** Deliberate obstacle belts in vicinity EA2. **End State:** Maneuver forces not able to exfiltrate kill sacks.
EA engagement area H-hour specific hour at which a particular operation commences		NAI named area of interest OBJ objective

Figure 6-4. Situation template in a matrix format example

6-45. Generally, there is not enough time during the MDMP to develop threat situation templates for all COAs. A good technique is to develop alternate or secondary COAs, write a COA statement, and produce an HVT list to use during the mission analysis briefing and COA development. Once these tools and products are complete, the staff constructs as many overlays as needed or possible depicting threat COAs. At a minimum, the staff may develop overlays for the threat's most likely and most dangerous COAs. The overlays are used during friendly COA analysis.

> ***Note.*** Sometimes, situation templates are replaced by other products, such as a key facilities and targets overlay. Analysts should use whatever technique best graphically depicts the threat's COAs.

6-46. There are three primary types of enemy situation templates the staff may need to develop as overlays:

- Enemy in the offense.
- Enemy in the defense.
- Irregular forces.

6-47. 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 terrorist activities. Because the enemy is more static in defensive tasks, the staff may have information related to enemy locations that may assist in developing the overlay.

6-48. When developing an overlay depicting regular forces conducting offensive or defensive tasks, the staff should depict enemy locations and activities two levels down. For example, a friendly brigade combat team would construct an overlay showing maneuver companies and specialty platoons. One of the brigade's battalions would refine that overlay for its zone or sector showing maneuver platoons and specialty teams.

6-49. When developing an overlay depicting irregular enemies, the staff at every echelon depicts enemy locations and activities at the cellular level. For example, whether at corps, division, brigade, or battalion 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.

Overlay Depicting the Enemy in Offensive Tasks

6-50. The staff constructs an enemy offensive task overlay using a five-step process that includes the following steps:

- Step 1—Determine the enemy's end state to make U.S. forces combat ineffective. Visualize enemy success and how the enemy force achieved those objectives given the forces available. Most enemy offensive objectives are force-orientated.
  - Step 1A: Review the U.S. forces' defensive plan. Even if the commander has not have approved the plan, the planning staff should have a rough idea of the friendly force defense based on the IPB process thus far.
  - Step 1B: Identify the U.S. forces' key targets on the battlefield that the enemy commander would attack (enemy commander HPTs).
  - Step 1C (brigade and above): Determine the vulnerability of this operation based on the operational variables gathered from previous IPB process steps.
  - Step 1D: Review the enemy commander's purpose for the offense: gain freedom of movement; restrict freedom of movement; gain control of key terrain, personnel, or equipment; gain information; dislocate; and disrupt.
- Step 2—Identify the functions used by the enemy to reach the end state:
  - Step 2A: Determine the action element (what the enemy uses to accomplish the mission).
  - Step 2B: Determine the enabling elements (what makes it possible for the action element to accomplish the mission).
  - Step 2C: Display the action form, task, and purpose for each element (for example, action form: enabling element, task: fix U.S. battalion, purpose: prevent U.S. forces from maneuvering).

- Step 3—Allocate the enemy's resources:
  - Step 3A: How many enemy units are required to accomplish the mission?
  - Step3B: What types of capabilities are required to support the enemy's mission?
    - Step 3B1: Determine locations of enemy reconnaissance assets needed to support the offensive mission. This is normally associated with the enemy commander's decision points and locations where reconnaissance assets can provide observation to support targeting.
    - Step 3B2: Determine initial and subsequent artillery and air defense firing positions and display the range fans for each type of enemy direct fire system and indirect fire system required to support the mission.
    - Step 3B3: Determine potential locations where the enemy may employ special munitions to isolate part of the friendly defense.
    - Step 3B4: Determine enemy air AAs that enable the enemy's use of close air support (CAS) to support the mission.
- Step 4—Synchronize the enemy mission:
  - Step 4A: Determine enemy attack sequence and movement formations.
  - Step 4B: Determine the enemy commander's decision points.
- Step 5—Continue refining the enemy COA; collaborating with staff sections, review staff estimates and changes to the U.S. forces' array.

6-51. Figure 6-5 illustrates an enemy situation template as an overlay depicting a mechanized infantry brigade in the attack.

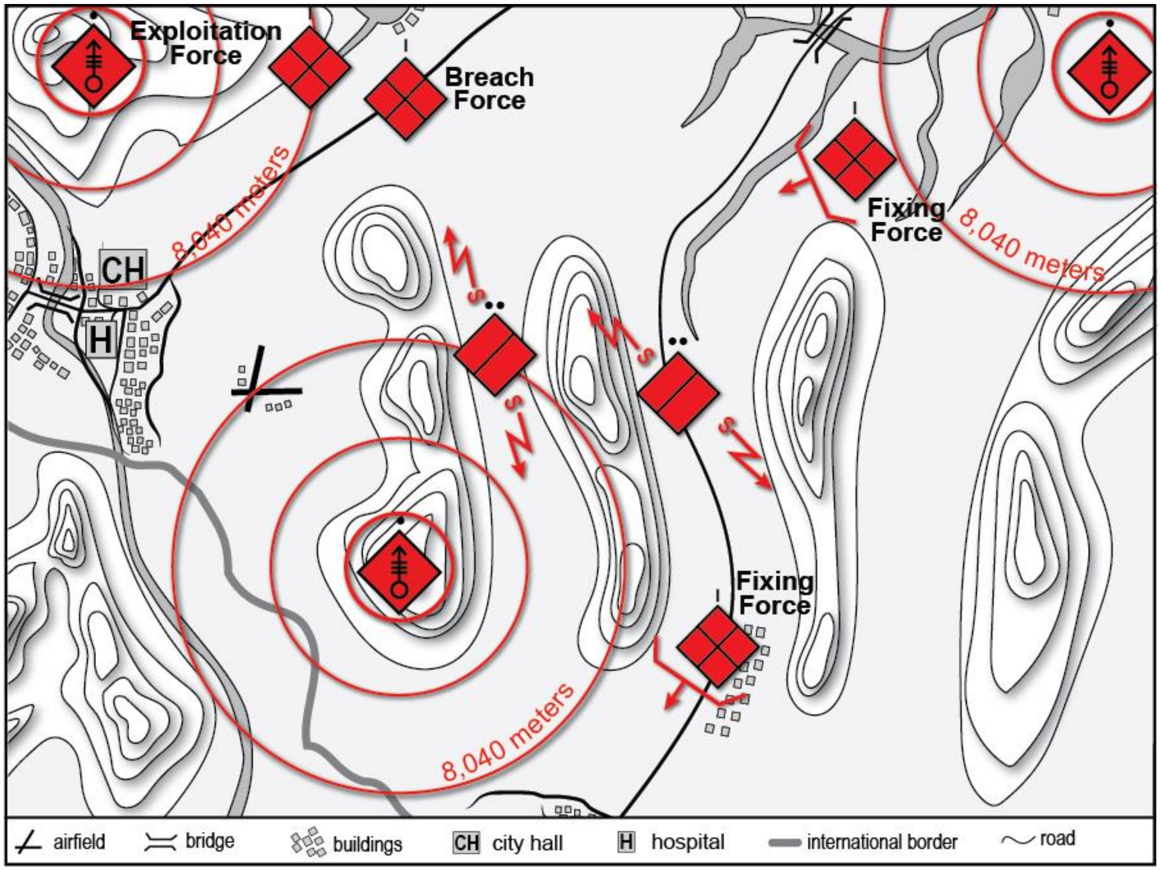


Figure 6-5. Situation template as an overlay depicting the enemy in offensive tasks

Overlays Depicting the Enemy in Defensive Tasks

6-52. The staff constructs an enemy defensive overlay using a five-step process that includes the following steps:

- Step 1—Determine the enemy's end state to make U.S. forces combat ineffective. Visualize enemy success and how the enemy force achieved those objectives given the forces available.
  - Step 1A: Review the U.S. forces' offensive plan. Although the commander may not have approved the plan, the planning staff should already have a rough idea of the friendly force plan for an attack based on the IPB process thus far.
  - Step 1B: Identify the U.S. forces' key targets on the battlefield that the enemy commander would attack (enemy commander HPTs).
  - Step 1C: (brigade and above) Determine the vulnerability of this operation based on the operational variables gathered from previous IPB process steps.
  - Step 1D: Review the enemy commander's purpose for the defense:
    - Protect personnel and equipment.
    - Restrict freedom of movement.
    - Control key terrain.
    - Gain time.
- Step 2—Identify the functions used by the enemy to reach the end state:
  - Step 2A: Determine the action element (what the enemy uses to accomplish the mission).
  - Step 2B: Determine the enabling elements (what makes it possible for the action element to accomplish the mission).
  - Step 2C: Display the action form, task, and purpose for each element (for example: action form: enabling element, task: fix U.S. battalion, purpose: prevent U.S. forces from maneuvering).
- Step 3—Allocate the enemy's resources:
  - Step 3A: How many enemy units are required to accomplish the mission?
  - Step 3B: What types of capabilities are required to support the enemy's mission?
    - Step 3B1: Determine locations of enemy reconnaissance assets needed to support the defensive mission. This is normally associated with the enemy commander's decision points and locations where reconnaissance assets can provide observation to support targeting.
    - Step 3B2: Determine initial and subsequent artillery and air defense firing positions and display the range fans for each type of enemy direct fire system and indirect fire system required to support the mission.
    - Step 3B3: Determine potential locations where the enemy may employ special munitions to isolate part of the friendly offense.
    - Step 3B4: Determine enemy air AAs that enable the enemy's use of CAS to support the mission.
    - Step 3B5: Determine the locations of enemy disruption zones, battle zones, and support zones with suspected unit boundaries. Add time phase lines, supplementary and primary simple battle positions, ambush locations, and observation posts.
    - Step 3B6: Determine enemy obstacle locations and intents for each obstacle.
- Step 4—Synchronize the enemy mission:
  - Step 4A: Determine enemy attack sequence and movement formations.
  - Step 4B: Determine the enemy commander's decision points.
- Step 5—Continue refining the enemy COA; collaborating with staff sections, review staff estimates and changes to the U.S. forces' array.

6-53. Figure 6-6 illustrates a situation template as an overlay depicting an enemy defense.

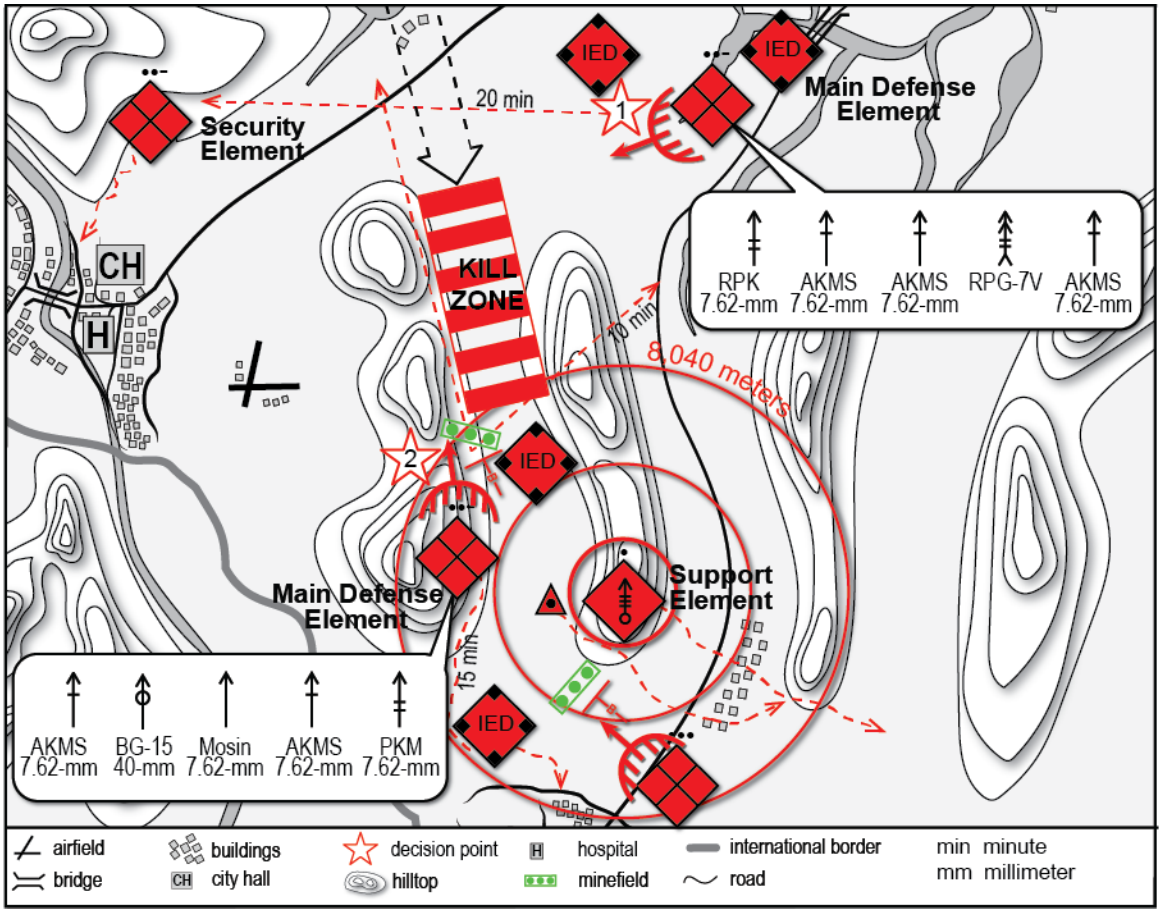


Figure 6-6. Situation template as an overlay depicting the enemy defense

Overlays Depicting Irregular Forces

6-54. Overlays depicting irregular forces (see figure 6-7) conducting operations typically focus on armed forces in a tactical array. The staff should consider whether to create overlays that depict the enemy's less visible elements, such as leadership, enemy external relationships, support networks, as well as the activities in which the enemy engages. Additionally, the staff should capture the process used to template the overlay, so the staff and subordinate staffs can replicate the process as required. The techniques in ATP 5-0.6 can facilitate this analysis.

6-55. The staff constructs an irregular force overlay using a 10-step process that includes the following steps:

- Step 1—Template the physical objectives irregular forces may attack. These objectives typically include friendly unit locations and movement routes; elements or individuals associated with host-nation political, civil, and security organizations; critical infrastructure; and 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. Analysis is based on the ranges of enemy indirect fire and air defense systems.
- Step 4—Template potential locations of reconnaissance and surveillance assets. Analysis includes consideration of the physical areas of observation around and on the objective. It also focuses on identifying TTP used by the enemy to conduct reconnaissance.

- Step 5—Template potential ambush sites along movement routes and near objectives. 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. 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. Analysis is based on pattern and predictive analysis, as well as on analysis of friendly activities and movement.
- Step 8—Template potential cache sites. 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 individuals. Analysis is based on pattern and predictive analysis.
- Step 10—Draw the AO for each direct action cell. Analysis is based on pattern and predictive analysis.

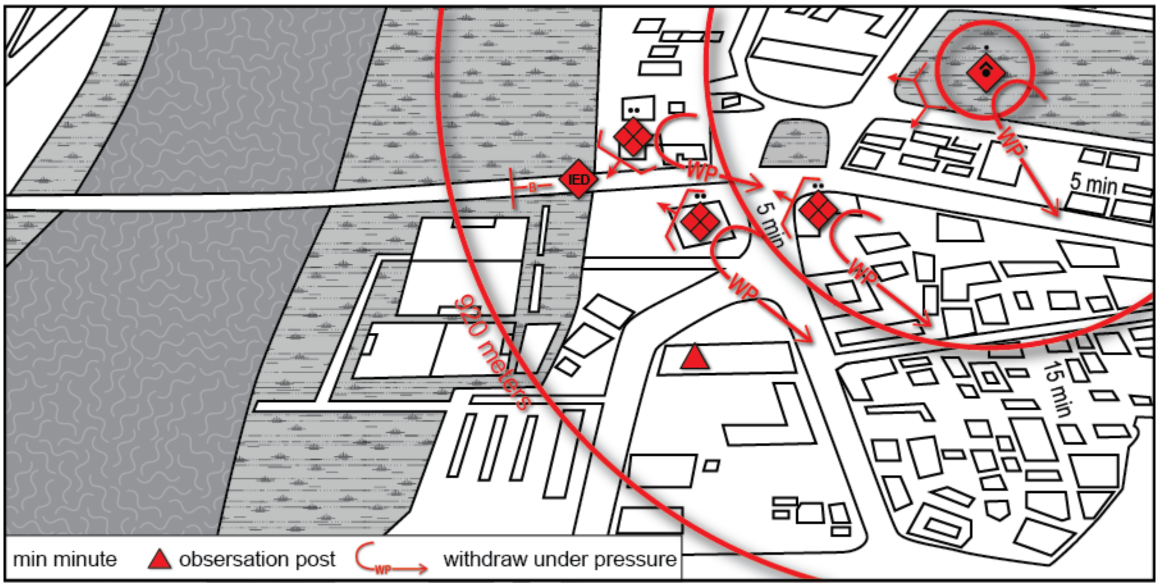


Figure 6-7. Situation template as an overlay depicting irregular forces

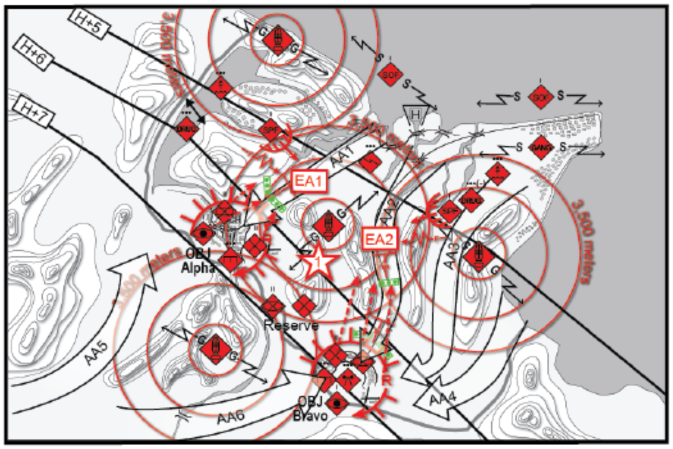
Threat Course of Action Statement

6-56. Every threat COA includes a threat COA statement, which is a narrative that describes the situation template as an overlay. Figure 6-8 illustrates a threat COA statement.

Mission: The 375th Brigade Tactical Group conducts an area defense at OBJ Alpha and OBJ Bravo no later than 110900ZNOV16 to prevent occupation force seizure of government and military infrastructure.

Enemy Commander's Intent: Retain control of OBJ Alpha and OBJ Bravo with minimal key infrastructure losses.

End State:
Enemy: Occupation force denied seizure of OBJ Alpha and OBJ Bravo.
Friendly: Maintain combat effectiveness of 75% until negotiations or regional partner assistance obtained.
Terrain: Key coastal and inland infrastructure remain intact.



Decisive Operations: The 65th and 72d Mechanized BNs conduct area defense no later than 110900ZNOV16 to deny occupation force seizure of OBJ Alpha and OBJ Bravo.

Shaping Operations:
Shaping Operation 1: Special purpose forces conduct ambushes along high-speed AAs to disrupt occupation force freedom of movement toward southern infrastructure.
Shaping Operation 2: Engineer emplacement of minefields along high-speed AAs to block occupation force.

Movement and Maneuver
Disruption Zone:
85th Special Purpose Force
Task: Disrupt occupation force in vicinity EA1 and EA2.
Purpose: Delay occupation force movement to the south.
Method: Conduct ambushes on occupation force using complex terrain features and hasty defensive positions.
End State: Occupation force ground movement is delayed in vicinity EA1 and EA2.

Battle Zone:
65th Mechanized BN
Task: Prevent western movement of occupation force.
Purpose: Protect southern flank of the 72d Mechanized BN.
Method: Use of obstacle belts and attack by fire positions.
End State: Occupation force is unable to turn west to OBJ Alpha.

72d Mechanized BN
Task: Prevent occupation of OBJ Alpha.
Purpose: Retain control of government.
Method: Use of obstacle belts and attack by fire position.
End State: Government status quo is maintained.

Support Zone:
97th Mechanized BN and 10th Infantry BN (Reserve)
Task: Reinforce the 65th and 72d Mechanized BNs.
Purpose: Prevent occupation force flanking of the 65th and 72d Mechanized BNs.
Method: Conduct a counterattack.
End State: Occupation force is prevented from seizing OBJ Alpha and OBJ Bravo.

AA	avenue of approach	EA	engagement area
BN	battalion	OBJ	objective
C2	command and control		

Fires
Disruption Zone:
Task: Disrupt occupation force coastal lodgement.
Purpose: Delay movement to the south.
Method: Long-range precision fires.
End State: The 65th and 72d Mechanized BNs are afforded additional time to prepare defenses.

Battle Zone:
Task: Disrupt air AAs.
Purpose: Prevent light infantry air assault in vicinity OBJ Alpha and OBJ Bravo.
Method: Use SA-13s to close air corridors.
End State: Occupation force unable to control friendly rear.

Sustainment:
Task: Conduct resupply operations across all zones.
Purpose: Maintain the initiative.
Method: Support echelons aligned to support main and supporting efforts.
End State: Friendly forces are able to maintain momentum of the battle to repel occupation force.

Reconnaissance
Disruption Zone:
Task: Identify coastal landing areas.
Purpose: Direct long-range precision fires.
Method: Special purpose forces.
End State: Occupation force lodgement is contested and delayed.

Battle Zone:
Task: Identify occupation force AAs.
Purpose: Direct long-range precision fires.
Method: Special purpose forces.
End State: C2 elements are able to direct the main effort.

Figure 6-8. Threat course of action statement example

IDENTIFY HIGH-VALUE TARGETS FOR EACH COURSE OF ACTION

6-57. Identifying HVTs involves mentally war gaming a threat COA to determine the assets required to complete the mission. This process involves using as a guide the HVT list developed based on HVTs identified as part of the threat model in step 3 of the IPB process, determining the effect on the threat COA if the target is lost, and identifying possible threat responses if the target is lost.

6-58. Based on the situation, one or more of the targets from the threat model may be validated as HVTs. Additionally, targets that were not identified in the threat model may be HVTs. During planning, the staff uses the HVT list (see figure 6-9) developed for each threat COA to develop the HPT list during the COA development step of the MDMP.

Threat element	***High-value targets***	
Command and control	• SAM system fire control (SA-15b) • Government Complex	• Military Complex • Artillery command and reconnaissance vehicle (1V14-3)
Movement and maneuver	• Main battle tank (T-72B) • Tracked minelaying vehicle (GMZ-3)	• Towed mechanical minelayer (PMZ-4) • Special purpose forces
Protection	• Nuclear, biological, chemical reconnaissance vehicle (BRDM-2RKh)	
Fires	• 152-mm self-propelled howitzer (2S19M1) • TDA-2K smoke generator	• Man-portable SAM system (SA-18) • SAM system (SA-13b)
Intelligence	• Battlefield surveillance radar (SNAR-10) • Short-range drone (ORLAN-10)	• SAM system radar system (SA-15b)
Sustainment	• Two-metric ton 4x4 cargo truck (GAZ-66)	
mm millimeter		SAM surface-to-air missile

Figure 6-9. High-value target list developed during step 4 of IPB (example)

6-59. Once identified and nominated, HPTs are grouped into a list—identified for a specific time and space in the battle and prioritized based on the commander's approval for formal targeting. The HPT list (see figure 6-10) is continually refined during execution by targeting groups. HPTs can include various threat considerations potentially detrimental to the success of friendly missions. HPTs are incorporated into the scheme of fires and used to create target selection standards and attack guidance matrices. (For a detailed discussion on targeting, see ATP 3-60.)

Threat element	***Time (H-hour)***	***Priority***	***Targets***	***Desired effect***
Intelligence	H-24-H+10	1	• Air defense radar	Destroy
Fires		2	• Air missile defense (SA-13, SA-18)	
Intelligence		3	• Artillery locating radar (ARK-1M)	
Fires	H-H+10	4	• Field artillery companies (2S1)	
Command and control	H-H+10	4	• Control node/Government Complex • Threat communications networks	Neutralize
H-hour specific hour at which a particular operation commences				

Figure 6-10. High-payoff target list developed during step 3 of the MDMP (example)

IDENTIFY INITIAL COLLECTION REQUIREMENTS FOR EACH COURSE OF ACTION

6-60. After identifying the full set of potential threat COAs, the staff develops the tools necessary to determine which COA the threat may implement. Because the threat 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 the information collection plan that can provide the information necessary to confirm or deny threat COAs and locate threat targets.

6-61. *Information requirements* are, in intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander (JP 2-0). An *indicator* is, in intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action (JP 2-0). Identifying and monitoring indicators are fundamental tasks of intelligence analysis, as they are the principal means of avoiding surprise. Indicators are often described as forward looking of predictive indicators.

6-62. Tables 6-1 and 6-2 list offensive and defensive indicators, respectively.

Table 6-1. Offensive indicators

Activity	*Explanation*
Massing of maneuver elements, armor, artillery, and logistic support	May indicate the main effort by weakening areas of secondary importance
Deployment of combat elements on relatively narrow frontage (not forced by terrain)	• May provide maximum combat power at attacking point by reducing frontages • Likely threat decisive effort
Massing of indirect fire support assets	May indicate initiation of main effort
Extensive artillery preparation of up to 10 minutes in duration or longer	Initiates preparation preceding an attack
Dispersal of tanks and self-propelled artillery to forward units	Can indicate formation of combined arms assault formations with tanks accompanying the leading maneuver elements and artillery following in bounds
Surface-to-surface missile units located forward	• Provides depth to threat offensive tasks • Places friendly support and unassigned areas in range • May also indicate, when employed alone, harassing or special weapons (chemical) delivery
Antiaircraft artillery and mobile surface-to-surface missiles located well forward with maneuver elements	• Provides increased protection to massed forces before attack • Extends air defense umbrella forward as units advance
Demonstrations and feints	• May precede an attack • May deceive actual point of attack
Establishment and strengthening of counterreconnaissance screen	• Protects assembly areas and forces as they prepare for attack • May be effort to prevent friendly forces from seeing attack preparations
Concentration of mass toward one or both flanks within the forward area	May indicate intent for single or double envelopment, particularly if massing units are armor heavy
Increased patrolling or ground reconnaissance	May indicate efforts to gather detailed intelligence regarding friendly dispositions before attack
Command posts located well forward; mobile command posts identified	Indicates preparation to command an offensive task from as far forward as possible
Movement of noncombatants from the area of operations	Indicates preparation for rapid forward advance of troops and follow-on forces
Extensive conduct of drills and rehearsals in unassigned areas	Often indicates major attacks, particularly against fortified positions or strongly defended natural or man-made barriers, which require rehearsal of specialized tactics and skills
Cessation of drills and rehearsals	• Unit completes rehearsals • Unit prepares for offensive tasks
Increased activity in supply, maintenance, and motor transport areas	• May indicate movement of additional forces to the front to sustain a major attack • Stocking of sustainment items, such as ammunition and medical supplies, before an attack
Increased aerial reconnaissance (including unmanned aircraft systems)	Threat effort to collect further intelligence on friendly dispositions or defensive positions
Establishment of forward arming and refueling points, auxiliary airfields, or activation of inactive airfields	• Indicates preparation for increased sorties for aircraft and faster turnaround time and aviation sustainment • Indicates preparation to support offensive tasks with aircraft as far forward as possible
Clearing lanes through own obstacles	Facilitates forward movement and grouping of assault units, particularly at night, and usually immediately precedes an attack
Reconnaissance, marking, and destruction of defending force's obstacles	Indicates where assaults will occur
Gap-crossing equipment (swimming vehicles, bridging, ferries, assault boats) located in forward areas (provides large water obstacle or gap)	Expect a substantial effort to cross a water obstacle during a main attack
Electronic warfare activity observed (inability to communicate with some units, artillery or air defense radars suppressed	• May indicate intent to isolate and destroy jammed unit or unit supported by jammed unit • Radar suppression may indicate impending artillery or aviation strike.

Table 6-1. Offensive indicators (*continued*)

Activity	*Explanation*
Staging of airborne, air assault, or special forces with transportation assets such as transport aircraft or helicopters	• Airborne or air assault operations likely indicates efforts to attack friendly commands, communications, or sustainment nodes • May indicate a main effort in which airborne forces will link with ground maneuver forces
Increased signals traffic or radio silence	• May indicate intent to conduct offensive tasks; however, increased traffic may be an attempt to deceive • Radio silence denies information derived from signals intelligence
Signals intelligence and electronic warfare assets located forward	Provides electronic attack and surveillance support for the attack

Table 6-2. Defensive indicators

Activity	*Explanation*
Preparation of battalion and company defensive areas consisting of company and platoon strong points	Indicates intent for holding terrain with defense in-depth, normally supported by armored counterattack forces
Extensive preparation of field fortifications, obstacles, and minefields	Indicates strong positional defense
Attachment of additional antitank assets to frontline defensive positions	• Indicates intent to contest friendly armor in forward positions • Attempts to attrite and channel friendly armor into engagement areas for armor counterattack forces
Formation of antitank strong points in depth along avenues of approach	• May allow penetration of friendly armor into engagement areas • May engage armor in depth
Preparation of alternate artillery positions	• Increases survivability of artillery in the defense • Indicates great effort to support main defensive area with artillery—no withdrawal of maneuver forces from main defense unless defeated
Concentration of armor units in assembly areas in the rear of the main defensive area	Indicates holding armor units in reserve for possible counterattack or counteroffensive tasks
Presence of concentrated antitank reserves	Provides quick reaction capability against armor penetrations of the main defense
Displacement of sustainment and medical units toward the rear area	Facilitates defensive repositioning, maneuver, and counterattacks (support units are not "in the way")
Pre-stocking of ammunition, supplies, and engineer or pioneer equipment in forward positions	• Reduces the burden on sustainment support during the battle • Reduces vulnerability of interdiction of supplies • Ensures strong points can survive for reasonable periods if bypassed or cut off by advancing forces
Withdrawal from defensive positions before becoming heavily engaged	Indicates delaying action to avoid decisive engagements
Numerous local counterattacks with limited objectives; counterattacks broken off before position is restored	Assists disengaging units in contact, rather than an attack to restore position
Units bounding rearward to new defensive positions, while another force begins or continues to engage	• Indicates units conducting local withdrawals to new positions • Usually an effort to preserve the defending force and trade space for time
Maximum firepower located forward, firing initiated at long ranges	• Intent to inflict casualties thus slowing advance of attacking force and provide sufficient volume of fire to avoid decisive engagements • Allows for time to disengage and reposition defending forces
Extremely large unit frontages compared to usual defensive positions	Indicates delaying action to economize force, allowing larger formations to withdraw
Chemical or biological weapons in forward areas. Reports of threat in chemical protective clothing while handling munitions	• Indicates possible chemical munitions use • Chemically contaminated areas cause significant delays to attacking forces
Identification of dummy positions and minefields	• Indicates defending force using economy of force • Causes advancing force to determine if mines are live or inert

6-63. Chapter 7 discusses the types of information needed to support offensive, defensive, and stability tasks. Generally, these requirements are related to confirming or denying a threat COA and locating threat HVTs.

DEVELOP THE EVENT TEMPLATE AND MATRIX

6-64. Intelligence analysts develop event templates and event matrices as analytical planning tools. The initial event template and event matrix are normally developed before 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 assist in developing subordinate unit information collection plans.

EVENT TEMPLATE

6-65. An *event template* is a guide for collection planning that depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted (JP 2-01.3). It is a graphic overlay used during the COA analysis step of the MDMP to confirm or deny threat COAs throughout war gaming. Additionally, the event template is used to develop the information collection overlay (see FM 3-55) and/or matrix and the DST during COA analysis. The event template is used during the execution activity of the operations process to assist in determining which COA the threat has adopted. An event template is accompanied by an event matrix.

6-66. The event template comprises—

- **Time phase lines.** These lines are linear geographic areas that depict when threat activity may occur.
- **NAIs.** Although NAIs are usually selected to capture indications of threat COAs, they may also be related to OE conditions. NAIs may be in the AO or in the AOI. NAIs in an AOI may be in another commander's AO and require coordination for collection and cueing.
- **Decision points.** A *decision point* is a point in space and time when the commander or staff anticipates making a key decision concerning a specific course of action (JP 5-0). The threat decision point is the point where the commander or staff anticipates the threat having to make a key decision. Predicting threat decision points also facilitates developing COAs that allow friendly forces to drive when and where the threat has to make decisions, thus limiting the threat's COAs.

6-67. Constructing an event template is an analytical process that involves comparing the multiple threat COAs developed earlier in step 4 of the IPB process to determine the time or event and the place or condition where the threat commander must decide on a particular COA. To create an event template—

- Begin with the situation template.
- Evaluate each COA to identify associated NAIs.
- Determine where events may occur that differentiate between threat COAs. These areas evolve into NAIs; evaluate both the time phase lines and decision points.
- Determine what action confirms or denies a particular threat COA (indicators).
- Determine the specific hour at which a particular event occurs.
- Compare the NAIs and indicators associated with each COA against the others and identify differences.
- Focus on the differences that may provide the most reliable indications of the adoption of each unique COA.
- Mark the selected NAIs on the event template.
- Upon refining, overlay the threat COAs with decision points and NAIs.

6-68. Figure 6-11 illustrates the basic mechanics of this process. The figure displays minimal information for what is included on the event template.

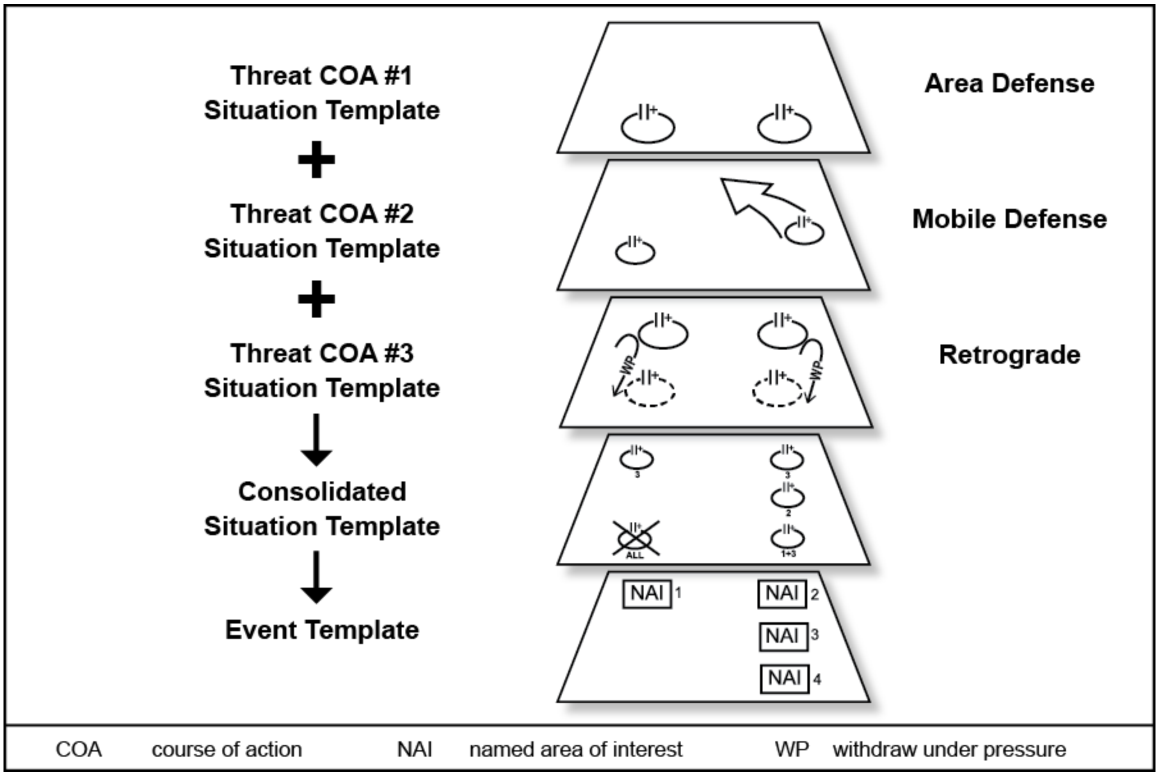


Figure 6-11. Developing an event template

6-69. Figure 6-12 illustrates a completed event template based on the consolidation of the area, mobile, and retrograde defensive tasks. In threat doctrine, these types of defensive tasks are tactical methods and guides for designing operational COAs. (See chapter 7 for more on defensive tasks.)

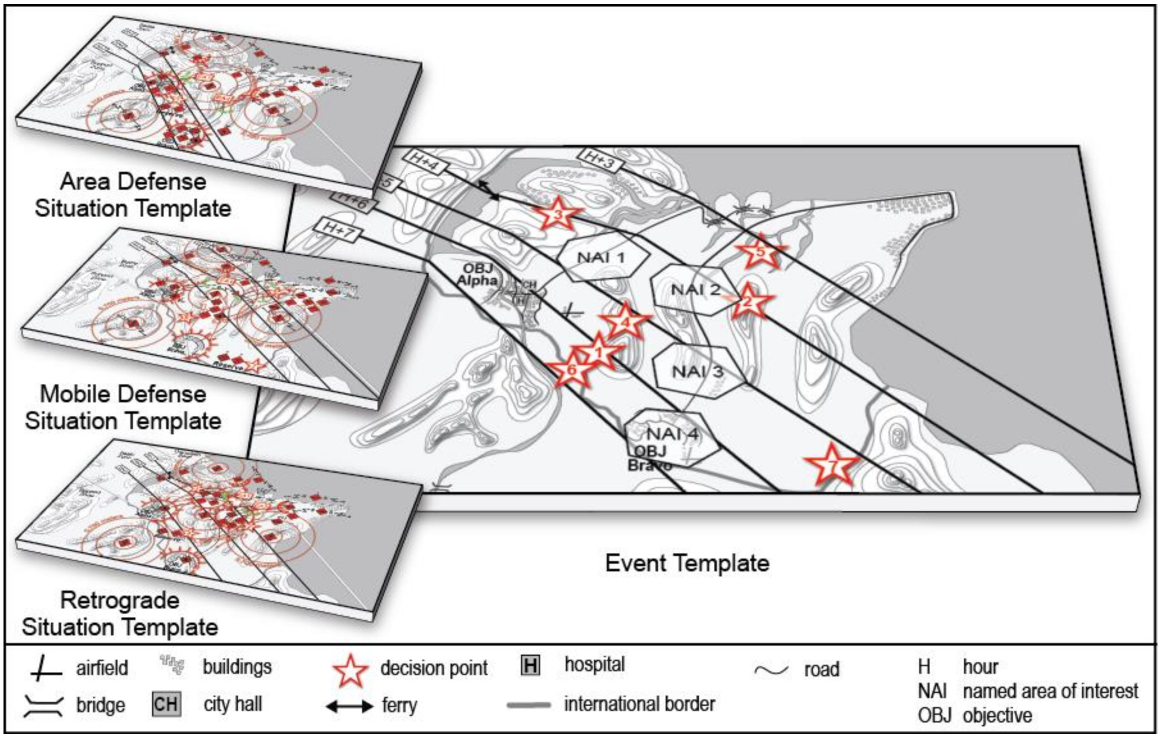
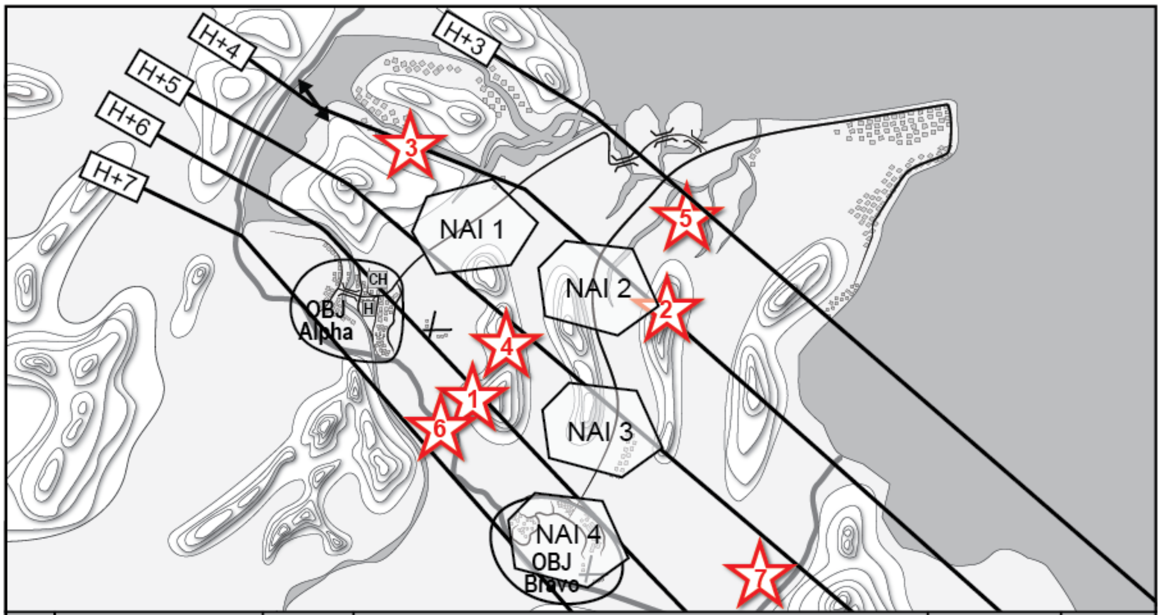


Figure 6-12. Completed event template example

EVENT MATRIX

6-70. An *event matrix* is a cross-referenced description of the indicators and activity expected to occur in each named area of interest (JP 2-01.3). Constructing an event matrix table is an analytical process that involves associating NAIs and threat decision points identified on the event template with indicators to assist in determining which COA the threat commander is implementing. (See figure 6-13.) To create an event matrix—

- Using the event template, examine the events associated with each NAI and restate the events as indicators.
- Enter the indicators into the event matrix along with the associated times they are likely to occur. Use the time phase lines from the event template to establish the expected times in the event matrix.
- Take the threat decision points from the event template and list them in the event matrix.



NAI	Grid Locations	Enemy COA	Indicators	HVT	NET/NLT
1	10A BC 12345 67891	COA1	1. SPF in hasty defensive positions in vicinity EA1 2. Blocking obstacles on southern portion of AA1	BMP-1KshM T-72B SPF SA-18	H+4/H+5
2	10A BC 23456 78910	COA2	1. SPF in hasty defensive positions in vicinity EA2 2. Blocking obstacles on southern portion of AA2	BMP-1KshM T-72B SPF SA-18	H+4/H+5
3	10A BC 21223 24252	COA3	1. Staging of the 65th Mechanized Battalion north of OBJ Bravo 2. The72d Mechanized Battalion positioned as fixing force in vicinity minefields on AA1 3. Presence of turning obstacles on northern portion of AA2	BMP-1KshM T-72B SPF SA-18	H+3/H+4
4	10T BC 23456 78910	COA4	1. Presence of the 72d and 65th Mechanized Battalions in forward defensive positions 2. The 2S191s remain in southern urban areas	BMP-1KshM T-72B SA-18 TDA-2K UMZ-K 2ST91	H-3/H+7

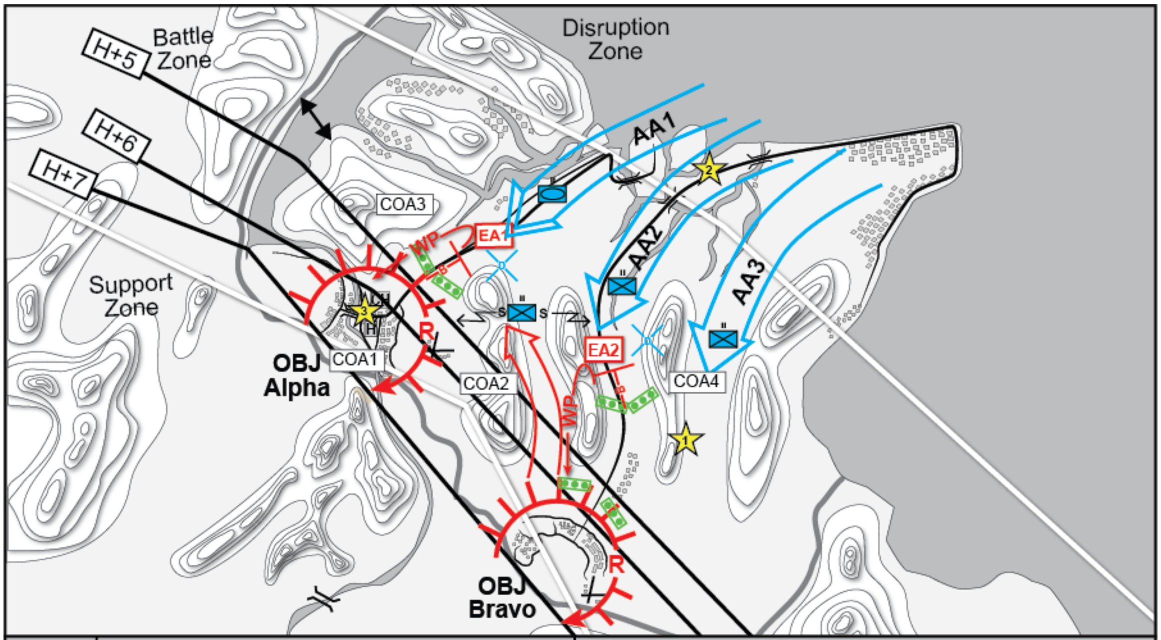
AA avenue of approach
COA course of action
EA engagement area
H-hour specific hour at which a particular operation commences
HVT high-value target
NAI named area of interest
NET no earlier than
NLT no later than
OBJ objective
SPF special purpose forces

Figure 6-13. Completed event template and its associated event matrix example

DECISION SUPPORT TEMPLATE AND INFORMATION COLLECTION MATRIX

6-71. The completed event template and event matrix form the basis for planning collection strategies, synchronizing intelligence with friendly operations, and developing the DST and matrix and information collection matrix (see figure 6-14 and figure 6-15 on page 6-24). In some instances, the staff might disseminate the event template as a collection graphic to support intelligence planning and collection by other units.

6-72. The DST provides the commander with a structured basis for deploying fires, maneuver, and jamming assets and for reducing the enemy's defensive capability with these assets. Simply stated, it provides commanders with the specific points on the battlefield where they will be required to make decisions regarding the employment of assets. These decisions can be keyed to phase lines, events on the ground, or to specific enemy actions.



Decision Point	Event	Decision
1	The 85th Special Purpose Force commits to disrupt occupation force movement along AA1 and AA2.	Use AA3 to conduct attacks on OBJ Alpha and OBJ Bravo. The 1/33 BCT remains in the northern consolidation area to ensure the 85th Special Purpose Force is unable to conduct counterattacks.
2	The 85th Special Purpose Force destroys bridges across the northern portion of AA2.	Initiate gap crossing.
3	The 375th BTG commits SA-18 batteries to OBJ Alpha.	Delay air assault until air defense artillerycoverage is degraded to 15%.

⊥	airfield	★	decision point	H	hospital	AA	avenue of approach
⌣	bridge	⇨	enemy AA	—	international border	BCT	brigade combat team
	buildings	↔	ferry	🟩	minefield	BTG	brigade tactical group
CH	city hall	⇨	friendly AA	∼	road	EA	engagement area
						H-hour	specific hour at which a particular operation commences
						OBJ	objective

Figure 6-14. Decision support template and matrix example

Priority Intelligence Requirement	Indicators	Specific Information Requirement	NAI	Start	Stop	Assets													Decision Point	Target Area of Interest
						Brigade							EAB							
						1st BN	2d BN	3d BN	3/67 CAV REG	Shadow	Prophet/LLVI	HCT	COMINT	ELINT	HUMINT	GEOINT	CI	MASINT		
1. Where along AA1 will the 375th BTG initiate shaping operations for an area defense?	1. Special purpose forces in hasty battle positions in vicinity EA1 and EA2	1.1.1 Report communications coordinating enemy movement	1,2	H-48	H+2	C	C	C	C	NT	TA	NT	R	R					1	1
		1.1.2 Report movement of fighters into defensive positions	1,2	H-48	H+2	C	C	C	TP	TA	TA	NT	R			R		R	1	1
		1.1.3 Report communications of reconnaissance assets	1,2	H-48	H+2	C	TA	C	TP	TA	TP	NT	R	R					1	1
	2. Blocking obstacles on AA1 and AA2	1.2.1 Report location of engineer assets	1,2,3	H-48	H+2	C	C	C	TP	TA	TA	NT	R	R		R		R	1	2
		1.2.2 Report location of deliberate obstacle belts	1,2	H-48	H+2	C	C	C	TP	TA	TA	NT		R		R		R	1	2

AA	avenue of approach	HCT	human intelligence collection team
BN	battalion	HUMINT	human intelligence
BTG	brigade tactical group	LLVI	low-level voice intercept
C	capable	MASINT	measurement and signature intelligence
CAV	cavalry	NAI	named area of interest
CI	counterintelligence	NT	not tasked
COMINT	communications intelligence	R	requested
EA	engagement area	REG	regiment
EAB	echelons above brigade	TA	tasked as alternate
GEOINT	geospatial intelligence	TP	tasked as primary
H	hour		

Figure 6-15. Information collection matrix example

PART THREE

Considerations for Operations and Environments

Chapter 7

IPB for Unified Action and Unique Environments

SECTION I – UNIFIED ACTION

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, nongovernment organizations, unified action partners, and the private sector.

7-2. The Army's contribution to unified action, as well as its operational concept, is unified land operations. *Unified land operations* are simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part of unified action (ADRP 3-0). This chapter discusses specific considerations for IPB conducted to support unified land operations. (For further discussion on unified land operations, see ADP 3-0.) Army forces conduct decisive and sustainable land operations through the simultaneous combination of offensive, defensive, and stability operations appropriate to the mission and environment.

OFFENSIVE TASKS

7-3. *Offensive task* is a task conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers (ADRP 3-0). 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 the enemy's attack, and to set the conditions for future successful operations. Intelligence requirements generally associated with offensive tasks include the following:

- Determine what type of defense the enemy is employing area defense, maneuver defense, and 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.
  - CAS and other aviation supporting the defense.
  - Other assets supporting the defense.
- Determine the enemy commander's end state, objectives, decision points, decisive point, critical event, and win, lose, and tie options.
- Determine enemy commander's intent for denial and deception operations, information activities, reconnaissance and surveillance, and 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 (CAS, 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, air defense, signal, and reconnaissance).
  - Prevailing winds, temperature inversion, humidity, illumination, and other weather elements.
- Determine the impact of civil considerations on friendly and enemy operations:
  - Rural communities.
  - Refugee camps.
  - Displaced persons.
  - Refugee movement.
  - Aid organizations located in the AO.

7-4. Forces may engage in four types of offensive tasks: movement to contact, attack, exploitation, and pursuit. In addition to the intelligence requirements listed in paragraph 7-3, each type of offensive tasks has its own unique requirements. (See ADP 3-90 for additional information on offensive tasks.)

MOVEMENT TO CONTACT

7-5. *Movement to contact* is an offensive task designed to develop the situation and to establish or regain contact (ADP 3-90). It may also include preliminary diversionary actions and preparation fires. The extent and nature of the movement to contact depends on whether threat 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. 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 man-made 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

7-6. An *attack* is an offensive task that destroys or defeats enemy forces, seizes and secures terrain, or both (ADP 3-90). 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. 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 that friendly forces can use to support flanking fire and maneuver, such as support by fire and attack by fire positions.
- Template positions of known enemy forces and obstacles (combat surveillance and observation posts, observation posts, simple battle positions, tank ditches, minefields).

EXPLOITATION

7-7. *Exploitation* is an offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth (JP 2-01.3). The objective of exploitation is to complete the enemy's disintegration. Exploitation takes advantage of previous successes and friendly force continuing activities. 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 before 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

7-8. *Pursuit* is an offensive task designed to catch or cut off a hostile force attempting to escape, with the aim of destroying it (ADP 3-90). 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 the enemy can be destroyed by conventional means or by WMD). 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.
- Indications of increased resistance.

DEFENSIVE TASKS

7-9. 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 3-0). Intelligence requirements generally associated with defensive tasks include the following:

- 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 the enemy's use of special munitions (chemical, biological, radiological, nuclear, and high-yield explosives [also called CBRNE]); artillery; scatterable mines).
- Locate and/or track enemy CAS.
- Locate enemy information capabilities.
- Locate enemy sustainment assets.
- Determine enemy offensive sustainment needs based on size and type of enemy force.
- Determine enemy offensive endurance/culmination point without sustainment reinforcement.
- Identify enemy deception operations.
- Determine the enemy commander's end state.
- Determine the enemy commander's objectives.
- Determine the enemy commander's decision points.
- Determine enemy decisive points.
- Determine the enemy's critical events.
- Determine the 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 CAS.
- Determine the effect of civil considerations on friendly and enemy operations for—
  - Rural communities.
  - Urban areas.
  - Displaced persons.
  - Refugee camps.
  - Refugee movement.
  - Aid organizations located in the AO.
- Threat forces using the civilian populace to cover movement.

7-10. Forces may engage in three types of defensive tasks: area defense, mobile defense, and retrograde. In addition to the intelligence requirements listed in paragraph 7-9, each type of defensive task has its own unique requirements. (See ADP 3-90 for additional information on defensive tasks.)

AREA DEFENSE

7-11. *Area defense* is a defensive task that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright (ADP 3-90). 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. Commanders use their reserves to—

- Reinforce fires.
- Add depth, block, or restore the position by counterattack.
- Seize the initiative.
- Destroy enemy forces.

7-12. Conducting an area defense includes considering the following intelligence requirements during IPB:

- Location of natural lines of resistance, well-defined AAs, intervisibility lines, 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 defensive task that concentrates on the destruction or defeat of the enemy through a decisive attack by a striking force (ADP 3-90). A mobile defense focuses on defeating or destroying the enemy by allowing enemy forces to advance to a point where they are exposed to a decisive counterattack by the striking force. *Striking force* is a dedicated counterattack force in a mobile defense constituted with the bulk of available combat power (ADP 3-90). A fixing force supplements the striking force. Commanders use their fixing force to—

- Hold attacking enemy forces in position.
- Help channel attacking enemy forces into ambush areas.
- Retain areas from which to launch the striking force.

7-14. Conducting a mobile defense 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

7-15. *Retrograde* is a defensive task that involves organized movement away from the enemy (ADP 3-90). The enemy may force these operations, or a commander may execute them voluntarily. In either case, the higher commander of the force executing the retrograde must approve the retrograde operation before its initiation. 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. Conducting a retrograde 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 by using obstacles, indirect fire, and CAS.

7-16. As in supporting planning for offensive tasks, the primary intelligence products and work aids necessary to support planning for defensive tasks include the following:

- MCOO.
- Weather effects matrix.
- Threat organizational chart.
- Threat capability statement.
- Threat situation templates, including those depicted as overlays with COA statements.
- Event template and event matrix.
- Relative target value matrix.
- HVT lists.
- Intelligence requirements specific to the enemy operation.

STABILITY TASKS

7-17. *Stability tasks* are tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADRP 3-07).

7-18. Stabilization actions are conducted across the conflict continuum from peace to war and can be conducted by military forces before, during, and after conflict. These actions may be conducted to support other U.S. Government departments and agencies as part of an integrated country strategy. Commanders appropriately combine stability actions with offensive actions and defensive actions to achieve objectives.

7-19. The purpose of stability tasks is to provide a secure environment, gain support for the host-nation government, meet the critical needs of the populace, build support for host-nation governments and institutions, and shape the environment for interagency and host-nation success.

7-20. IPB aids commanders in gaining the situational understanding needed to accomplish these tasks by—

- Understanding the root causes of the insurgency.
- Identifying external and internal support for the insurgency.
- Understanding how 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 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/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.

7-21. The purpose of IPB in stability tasks is the same as in offensive and defensive tasks. However, the nature of these tasks 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, an environment dominated by offensive and defensive tasks directed against an enemy force and stability tasks encompasses various military missions, tasks, and activities that are not enemy-centric.

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

7-23. Stability tasks promote and protect U.S. national interests by influencing the threat, political, and information aspects of OE 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 balancing the analytical effort in the same manner. Commanders and staffs should be wary of becoming too focused on enemy forces and not conducting the necessary analysis on civil considerations. A greater emphasis may need to be placed on civil considerations than on the enemy during stability tasks.

7-24. The primary stability tasks, as discussed in FM 3-07 are—

- Establish civil security.
- Establish civil control.
- Restore essential services.
- Support governance.
- Support economic and infrastructure development.
- Conduct security cooperation. (FM 3-0 added this as a stability task.)

7-25. A consistent observation 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 is required, so is the analysis related to all lines of operations identified by the commander as important. This means that the analysis of civil considerations may have equal or greater importance to the analysis of enemy forces.

7-26. In addition to providing intelligence about these lines of operations, IPB provides intelligence about people. U.S. forces must understand the people of the nations where they operate in order to accomplish their missions. Commanders and planners require accurate intelligence assessments into the culture, perceptions, values, beliefs, interests, and decision-making processes of the individual and groups that comprise the various social networks of the population.

ESTABLISH CIVIL SECURITY

7-27. Establishing civil security is the first responsibility of military forces stability tasks 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, and separate insurgents from the general population. Table 7-1 identifies intelligence requirements that may be associated with each of these subtasks.

Table 7-1. Civil security intelligence requirements

Protect external borders	*Combat internal threats*	*Separate insurgents from the general population*
• Identify all external state and nonstate actors attempting to influence United States (U.S.) operations. • Identify the objectives of these groups/individuals. • Identify the tactics, techniques, and procedures these groups/individuals use to accomplish their objectives. • Identify the physical locations these groups/individuals use 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 for each threat group. • Develop templates for each threat group. • Develop a situation template overlay for each threat group. • Identify high-value targets. • Identify and verify individuals as insurgents, known or suspected terrorists, and/or criminals. • Identify actors in the population providing support to the enemy. • Identify external actors providing support to the enemy. • Identify groups and populations 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.

Protect External Borders

7-28. When conducting stability tasks, U.S. forces generally do not have to prepare for an attack by a regional power across an international border. The primary cross-border threats U.S. forces encounter are foreign nation special forces, terrorist organizations, regionally based irregular forces, and criminal organizations.

> ***Note.*** Nation-states may use proxy forces to conduct cross-border operations to subvert friendly operations. (See paragraph 5-11 for more information on proxy forces.)

7-29. The primary threat activity U.S. forces 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.

7-30. 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 provides methods for evaluating external threat organizations and for presenting this information.

Table 7-2. Evaluating external threat organizations

Step	*Requirement*	*Tactics, techniques, and procedures (TTP)*
1	Identify all external state and nonstate actors attempting to influence United States operations and their objectives, including— • Identity. • Location. • Objectives. • Operations. • Methods. • Defeat mechanisms.	• Identify all organizations and their objectives during mission analysis. • Develop organizational charts for each of these groups during mission analysis. • Present this information during the mission analysis 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 use to transport weapons, equipment, personnel, money, media, and ideas across the border.	• Develop a situation template (digital overlay) that depicts 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. • Present this information during the mission analysis briefing. • Include this information as part of the intelligence estimate. • Maintain the situation template as part of the joint common database.
3	Identify TTP these groups or individuals use to accomplish their objectives.	• Identify these methods during mission analysis. • Develop special assessments (text and graphics) that describe TTP in detail. • Present this information during the mission analysis 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 that describes these locations. • Present this information during the mission analysis briefing. • Include this information as part of the intelligence estimate. • Maintain digital terrain overlays as part of the joint common database.

Combat Internal Threats

7-31. When engaged in stability tasks, 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 may 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 achieving their goals through violence. Beyond that, these groups can generally be characterized as follows:

- Neither locatable nor easily detected by U.S. information collection assets.
- Often unidentified early in an operation.
- Usually operate under a decentralized chain of command.
- Organized under a cellular, militia, or special forces structure.
- Operate in complex terrain usually within urban centers or severely restricted natural terrain.
- An enemy that thinks, adapts, and modifies TTP, as needed, to operate against conventional forces.
- Target four general groups: host-nation political and civil authorities, host-nation military and police forces, general population, and U.S. armed forces and other international military and civilian agencies.
- Sustain themselves through external and/or internal support mechanisms (usually differs by function—for example, weapons, equipment, and finances from external support, but recruiting, replacements, and information-related capabilities from internal support).
- Establish sanctuary in complex terrain or among civilian populations.
- Avoid massing forces.
- Employ—
  - Commercial-off-the-shelf communications technology (telephone, cell phone, internet).
  - Tactical radios.
  - Nonelectronic methods of C2.
  - Civilian transportation (public transportation, privately owned vehicles).
  - Small arms and crew-served weapons.
  - IEDs.
  - Mortars.
  - Shoulder-fired antiaircraft weapons.
- Capable of conducting operations directed against U.S. forces, such as—
  - IED attacks.
  - Mortar attacks.
  - Complex attacks.
  - Sniper attacks.
  - Drive-by shootings.
  - Infiltration.
  - Ambushes.
  - Raids.
  - Sabotages.
  - Suicide bombings.
  - Information activities.
  - Information for effect.
  - Misinformation.
  - Propaganda.
  - Reconnaissance and surveillance.
- Can also conduct operations directed against host-nation political, civil, and security targets, and the general population. These operations include but are not limited to assassination and murder, kidnapping, coercion, intimidation, and recruitment.

7-32. The commander needs detailed intelligence on all insurgent organizations in the AOs 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, the intelligence staff maintains up-to-date data files relating to the threat characteristics and historical and current reporting to produce the predictive assessments required by the commander to plan operation. Table 7-3 on page 7-10 provides TTP for evaluating internal threat organizations.

Table 7-3. Evaluating internal threat organizations

Step	*Requirement*	*Tactics, techniques, and procedures (TTP)*
1	Identify all regular and irregular forces that pose a military threat to United States and host-nation security forces.	• Identify all organizations and their objectives during mission analysis. • Develop organizational charts for each of these groups during mission analysis. • Present this information during the mission analysis 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 use 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. • Present this information during the mission analysis 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 use to accomplish their objectives.	• Identify these methods during mission analysis. • Develop special assessments (text and graphics) that describe TTP in detail. • Present this information during the mission analysis 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 that describes these locations. • Present this information during the mission analysis briefing. • Include this information as part of the intelligence estimate. • Maintain digital terrain overlays as part of the joint common database.

Separate Insurgents from the General Population

7-33. 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.
- Use civilian transportation, communications, and financial and general services to sustain operations.
- Receive funding by winning the approval of segments of the population or by extortion.
- Use segments of the population to provide indications of U.S. operations.
- Conduct information activities targeting the population.
- Use the threat of violence or specific actions to coerce the population.

7-34. To separate these forces from the population, commanders need to understand how and why the population supports these forces. Many factors, such as the following, may influence a local population's perspective and sway its support: safety from the violence of war and crime, economic viability, religious freedom, view toward government, and view toward U.S. presence.

7-35. The intelligence staff continually reevaluates the population's role in the conflict and provides the information commanders need to conduct operations that can influence the population to support their programs. Steps 1 and 2 in table 7-4 provide TTP for presenting this information.

Table 7-4. 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.	• Begin this assessment during predeployment, since it can be a long and difficult process. • Integrate civil affairs personnel and assessments in the intelligence preparation of the battlefield process. • Consider how successful insurgent groups have conducted population surveys to determine how they 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 assist in combating enemy forces. • Determine how the enemy uses 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 assists civil reconnaissance as well as information collection operations.
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 assessment in targeting and information collection working groups.

ESTABLISH CIVIL CONTROL

7-36. 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 and military and police forces.
  - Civil affairs teams/Civil-military operations center.
  - Department of State provincial reconstruction teams.
- Leaders of host-nation religious and ethnic groups.
- U.S., host-nation, and international aid organizations.
- Host-nation judicial bodies.
- Local populations.

7-37. Establishing civil control occurs in conjunction with establishing civil security and involves developing interim mechanisms for establishing the 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.

7-38. 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.
- The civilian police functions that need to be performed by U.S. military forces.
- Major crime issues.
- Critical infrastructure related to criminal justice and security institutions that require protection.

7-39. The civil affairs staff, military police, staff judge advocate office, and other information sources, including local nationals, local government officials, and nongovernmental organizations, 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

7-40. 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 from which military forces build on the unified action partner capacity to operate and maintain essential civil services.

7-41. During IPB, the commander and staff should determine the nature and scope of the humanitarian crisis as well as the following for essential services:

- 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 the 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 nongovernmental organizations.
- 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.
  - Identify nongovernment relief organizations in the area and their current progress.

7-42. The civil affairs staff, military police, staff judge advocate office, and other sources of information, including local nationals, local government officials, and nongovernmental organizations, can provide Department of State information about those programs and initiatives.

SUPPORT GOVERNANCE

7-43. When a legitimate and functional host-nation government is present, military forces operating to support 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 requiring possible analysis during IPB.

7-44. During IPB, the commander and staff assess whether the indigenous government is performing its basic civil functions adequately; otherwise, the commander and staff will—

- Identify founding documents that establish the nature of the host-nation government (for example, United Nations mandate, declarations of independence, constitutions, or bylaws).
- Implement representative facets to government (councils, elections).
- Support civil administration and unified action partners by assisting in the development of 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 and humanitarian civil assistance programs to support the internal defense and development plan.

7-45. The G-3/S-3 and other sources of information, including local nationals and government officials and nongovernmental organizations, can provide Department of State information on support to governance for transitional administrations, local governments, anticorruption initiatives, and elections.

SUPPORT ECONOMIC AND INFRASTRUCTURE DEVELOPMENT

7-46. 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, including economic development, of its citizens. 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 are critical to a commander’s ability to plan and conduct operations that improve economic conditions.

7-47. 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 briefing and included as part of the intelligence estimate issued with the operation plan and/or order. Additionally, to support continued operations, this analysis is continually updated to ensure planning teams and assessment working groups have the most current data.

Economic Development

7-48. When assessing economic conditions, the commander and staff consider the following (not all-inclusive):

- 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 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 earn their living (agriculture, trade, industry).
- From where do the most important items come that the population consumes.
- 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.
- The 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 or similar programs, allowing the commander to allocate funds and resources to civilian infrastructure or relief projects.
- Status of dislocated civilian population and ongoing relief efforts.
- Measures of effectiveness that can be used for assistance programs and civic action programs.

7-49. 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 provides the intelligence staff with information sources for answering these questions. Additional sources include local nationals and government officials and nongovernmental organizations.

Table 7-5. Information sources for supporting economic developments

Economic categories	*Staff proponent*	*Information sources*
Economic generation and enterprise creation, monetary programs, and national treasury operation	Civil affairs	Department of Treasury
Natural resource protection	Civil affairs	Department of Interior
Agricultural development	Civil affairs	Department of Agriculture
Public sector investment programs, private sector development, transportation infrastructure programs, telecommunications infrastructure programs, and general infrastructure programs	Civil affairs	Department of Commerce

Infrastructure Development

7-50. 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.

7-51. These considerations may assist the commander in prioritizing infrastructure development projects, maximizing existing resources, and potentially leveraging external resources. Data collected during infrastructure reconnaissance can assist with these considerations. *Infrastructure reconnaissance* is a multidisciplinary reconnaissance focused on gathering technical information on the condition and capacity of existing public systems, municipal services, and facilities within an assigned area of operations (ATP 3-34.81). Infrastructure reconnaissance results assist in developing situational understanding of the local capability to support the infrastructure requirements of the local populace within a specific area.

CONDUCT SECURITY COOPERATION

7-52. Security cooperation, as part of consolidation of gains, enhances military engagement and builds the security capacity of partner states. Security cooperation comprises multiple activities, programs, and missions; it is functionally and conceptually related to security assistance, security force assistance, internal defense and development, foreign internal defense, and security sector reform. As an example, security sector reform involves disarming, demobilizing, and reintegrating former warring factions in the aftermath of an insurgency, assists the host-nation reform its security forces (for example, military and police), bolsters rule of law through constitutional reform, and conducts advisory missions. Army forces may be granted special authorities and called upon to execute tasks to support these programs, which build partner capacity to support broader national security interests. Security cooperation activities can be executed discretely or in concert with each other across the range of military operations, consolidating many requirements, authorities, and force structures. (See FM 6-22 for more information on security cooperation activities.)

SECTION II – UNIQUE ENVIRONMENTS

7-53. This section discusses IPB considerations for littoral, urban, and subterranean environments.

LITTORAL ENVIRONMENTS

7-54. The *littoral* comprises two segments of operational environment: 1. Seaward: the area from the open ocean to the shore, which must be controlled to support operations ashore. 2. Landward: the area inland from the shore that can be supported and defended directly from the sea (JP 2-01.3). Due to globalization, and subsequently to world trade and access to global markets (including those that use them), the importance of littoral zones to friendly and threat forces has increased. Securing littorals from threat forces, as well as using them as places from which to project forces further inland, may increase opportunities for threats to affect regions worldwide.

UNIQUE CHARACTERISTICS OF LITTORAL ENVIRONMENTS

7-55. Work performed by the staff during generate intelligence knowledge is critical to understanding littoral areas and zones in the OE. Integrating the staff into IPB and using outside resources (such as Service-level intelligence centers, relevant geographic combatant command intelligence operation centers, and intelligence community agencies that may operate in and/or maintain databases on these areas more frequently) can be useful to formulate assessments.

7-56. As with IPB products for other environments, littoral products should address the relevant aspects that may affect friendly and threat operations. Characteristics to consider include but are not limited to—

- Coastal terrain and composition.
- Commerce and trade.
- Infrastructure development.
- Navigable bodies of water (rivers, lakes, bays, estuaries).
- Population density.
- Threat groups.
- Tidal and current information.
- Transportation networks.

7-57. IPB products for littoral operations stem from identifying relevant characteristics of the OE and determining how to best portray those characteristics. Intelligence staffs must also consider using additional tools (such as riverine and coastal navigational charts) that may offer more detail than standard military maps. Table 7-6 depicts one method of determining relevant aspects of littoral environments.

Table 7-6. Framework for determining relevant aspects of littoral environments

Step	*Relevant aspects of littoral environments*
Step 1	**Hydrography:** Tidal flow rate and current direction, high and low tide (times), gradient and slope of beach, water depth, surf and wind effects
Step 2	**Beach type:** Shape, delta, cliffs, levies
Step 3	**Soil consistency:** Trafficability concerns
Step 4	**Beach landing site criteria:** Size of force involved
Step 5	**Mobility corridors and avenues of approach**
Step 6	**Lines of communications:** Roads, rivers/canals, railways, subways, lines of sight, rubble effects, beach exits
Step 7	**Obstacle types:** Sandbars and shoals, rocks, mud flats, dunes, man-made obstacles such as mines and abatises
Step 8	**OAKOC factors:** Imagery overlays, navigation charts, riverine charts
Step 9	**Threat:** Coastal defense batteries (antiship and air), minefields, enemy shipping trenches, bunkers, piracy, criminal networks, antiaccess and antiarea defense systems, trafficking (narcotics, human, black-market goods), antiaccess threats (submarines, fast surface craft, mines)
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment

7-58. Determining the type of littoral terrain on which friendly and threat operations may occur assists in identifying relevant aspects to mission accomplishment. Each type of littoral environment has different characteristics that may affect those operations. Factors to consider include but are not limited to—

- Status of treaties and other agreements among regional territories that may potentially create conflict.
- Boundaries of international and territorial waters.
- Contested waterways and their proximity to land.
- Status of and access to waterways.
- Types of commercial and military watercraft in the area and their ranges.
- Regional trade patterns, including legal and illicit trade.

7-59. When identifying littoral areas, it is important to determine if the areas are encompassed by either open or marginal seas, enclosed or semienclosed seas, or archipelagos, or (see figure 7-1):

- **Open seas** are unenclosed oceans or seas usually outside of territorial waters.
- **Marginal seas** are parts of open seas or oceans that bound land masses such as peninsulas, archipelagos, and islands.
- **Enclosed and semienclosed seas** are bodies of water surrounded by a land mass and connected to either an ocean or another enclosed sea by a connecting body of water such as a straight.
- **Archipelagos** are groups of islands.

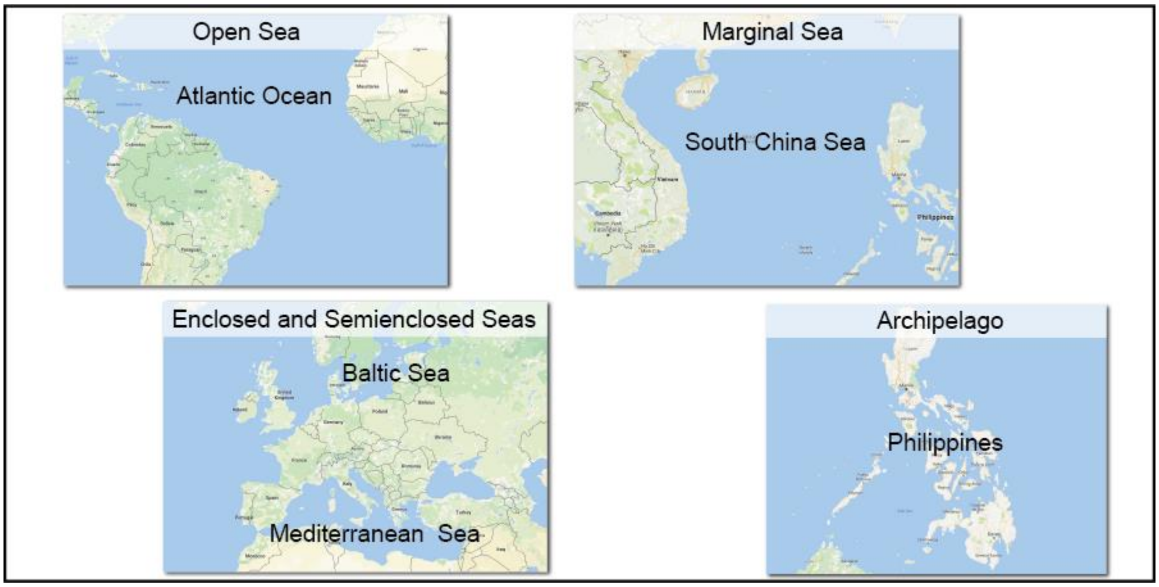


Figure 7-1. Types of seas and land masses encompassing littoral areas

Evaluating the Military Aspects of Terrain in Littoral Environments

7-60. The analysis of the military aspects of terrain (OAKOC) also applies to the littorals. Terrain variances in littoral environments are very diverse due to season, weather, and intended use, or are often abrupt, ranging from coastal regions with large populations to inland marshes and swamps with smaller populations.

7-61. Analysis of the relationships between varying littoral environments is necessary to understand how these environments may affect different phases of an operation. For example, phase 2 operations may focus on the establishment of a seaport of debarkation on the coast, while phase 4 operations may focus on humanitarian assistance inland. Analysts must be able to determine the effects of varying terrain on friendly threat forces over time and distance.

Observation and Fields of Fire

7-62. Littorals are one of the most diverse environments worldwide. This diversity often creates significant changes in observation and fields of fire over short distances. For example, many littoral areas in Central and South America contain large urban areas, but they also contain dense jungle environments in close proximity. In instances like these, detailed MCOOs are needed to ensure accurate depiction of impacts, including but not limited to areas where vegetation hinders observation; coastal weather phenomena, such as sea fog, that may impact observation; and terrain transitions (jungle to urban) that may impact fields of fire.

Avenues of Approach

7-63. The seaward and landward portions of littoral areas may provide different accessibility for operations:

- **Seaward portions** are generally more accessible to large vessels and typically offer unimpeded travel to ports.
- **Landward portions** are typically more canalizing with chokepoints as they move inland into rivers and estuaries.

7-64. Littorals are often centers for trade and have the requisite networks to facilitate movement by land and waterways. AAs vary by location and consist of but are not limited to open seas leading to ports and harbors; shipping lanes; river, marsh, estuary, and delta networks; road and rail networks; and highways leading from coastal areas inland, facilitating trade and transportation.

Key Terrain

7-65. Littoral regions are often important parts of a country’s or region’s economic infrastructure. Often, they include key financial and trade hubs, and are used by military forces for projection of power and to secure borders. For these reasons, littorals often contain key terrain essential to the success of the friendly mission. When considering the aspects of key terrain in relation to littorals, analysts should consider the following aspects:

- Ports, harbors, and anchorages.
- Military infrastructure, including coastal defenses and antiaccess and area denial systems.
- Canalizing terrain.
- Terrain supporting weapon and radar emplacements.
- Shipping lanes.

Obstacles

7-66. Obstacles in littoral terrain are often used to prevent an opposing force from encroaching closer to shores and inland terrain. Obstacles may vary from offshore mines and abatises to waterways bordering population centers. Coastal terrain, wave and tidal surges, reefs, shoals, and levies are other obstacle considerations.

Cover and Concealment

7-67. Cover and concealment vary by location. Littoral environments range from urban areas providing substantial cover and concealment to rural areas where cover and concealment may be limited.

Evaluating Aspects of the Threat in Littoral Environments

7-68. Littorals are often complex and multilayered environments. The ability to understand a holistic littoral OE, including threats, can be difficult. Friendly forces operating in littoral areas may encounter a multitude of threat forces across multiple domains.

7-69. Threat forces may use a multitude of COAs to counter friendly operations in littoral zones. It is important to leverage all Service intelligence organizations to determine which threat forces are present within the OE. Depending on a unit’s mission and location, threat forces in littoral zones may range from conventional military forces, paramilitary forces, insurgents or guerillas, terrorists, common criminals, drug traffickers, and street gangs. These forces may work together or separately.

URBAN ENVIRONMENTS

7-70. The effective conduct of urban operations requires a basic understanding of urban environments. Currently more than 50 percent of the world population lives in urban areas and is likely to increase to 70 percent by 2050, making military operations in cities both inevitable and the norm. An urban environment is a physical urban area—the terrain (natural and man-made), population, and infrastructure. The complex and dynamic interactions among those key components create an overlapping and interdependent system of systems (see figure 7-2). As witnessed during the 2014 operations in Raqqa, Syria, and the 2016 operations in Mosul, Iraq, urban environments can be resource-intensive, require significant planning and coordination, create security challenges, and often draw international media attention. (See ATP 3-06.)

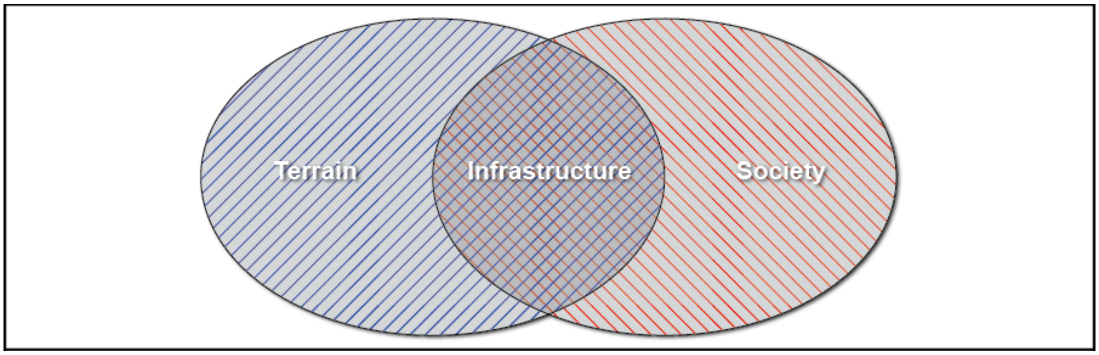


Figure 7-2. Interaction among key components of the urban environment

7-71. Urban environments may vary in size—from small villages with as little as 500 inhabitants living in one-story homes, to megacities with more than 10 million inhabitants—and consist of buildings that range from high-rise apartment complexes to single-story homes and commercial areas. Currently, there are more than 20 megacities worldwide. This number is expected to increase to 40 megacities by 2035. In some areas, population increases have occurred more quickly than the local and national governments' ability to provide adequate governance, infrastructure, security, and basic services. These shortfalls can contribute to political instability, increase the likelihood of man-made crises, and compound the adverse effects of natural disasters within cities. (See ATP 3-06.)

7-72. Critical elements of the infrastructure within an urban environment may be located beyond the physical confines of the urban area. For example, power stations and communications hubs may be located outside the physical urban area in rural or neighboring urban areas. This is critical in understanding the totality and scope of urban dynamics and the various locations that may affect urban environments.

7-73. An urban area is a topographical complex where man-made construction or high-population density is the dominant feature. The evaluation of urban areas during IPB is most effective when the staff views the environment as a triad consisting of man-made physical terrain, a population of significant size and density and varying sociocultural groupings, and an infrastructure. The staff must consider the effects of the natural terrain, sea, air, and weather on each portion of the triad during its analysis. Chapters 3 and 4 provide a discussion on terrain analysis for natural terrain and urban areas. (See JP 3-06.)

7-74. The evaluation of urban areas during IPB is directed at 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. When it is a factor, there are several considerations when performing IPB, including the area's homogeneity and social divisions (physical, ideological, economical). Treating an urban population as a completely homogenous entity leads to false assumptions, cultural misunderstandings, and poor situational understanding. Whether an urban area is the AO or a relevant aspect of a larger AO, the intelligence staff and the rest of the staff must consider the importance of the population. (See ATP 3-06.)

URBAN OPERATIONS

7-75. The Army defines *urban operations* as operations across the range of military operations planned and conducted on, or against objectives on a topographical complex and its adjacent natural terrain, where man-made construction or the density of population are the dominant features (ATP 3-06). During urban operations, the primary terrain effect in an urban environment is the multidimensional nature of the environment. Urban areas comprise horizontal, vertical, interior, exterior, and subterranean forms superimposed on the natural relief, drainage, and vegetation. Special considerations for urban operations extend beyond the uniqueness of urban areas. The characteristics of the urban environment affect friendly and threat forces based on their doctrine and tactics. When performing IPB for urban operations, the staff evaluates the effects of those characteristics on friendly, neutral, and threat forces. This section discusses IPB considerations normally associated with planning requirements for urban operations.

7-76. The vast number of urban areas worldwide makes urban operations across the conflict continuum highly likely even in areas where governance or infrastructure are not the underlying causes of conflict. (See ATP 3-06.) The following includes but is not limited to reasons military forces operate in urban areas:

- The urban environment offers defensive advantages.
- The urban area harbors threats that can attack friendly forces at other locations.
- The urban area's infrastructure (ports, airports, railroad hubs, financial, media, electrical, water, health) can influence the local population as well as populations in distant areas.
- The urban area's capabilities and resources have operational and/or strategic value.
- The urban area's geographical location dominates a region or AA.

7-77. Threat forces strive to achieve several key objectives in urban areas:

- Use the population to their advantage.
- Control information as a commodity.
- Manipulate key facilities.
- Engage the entire enemy force.
- Focus attacks on support areas, isolated groups, and individuals.

7-78. Military operations in urban environments are—

- Often high in risk. (See ATP 3-06 for associated risks.)
- Often part of a larger campaign.
- Force tailored to include a larger infantry component.
- More likely to have casualties than in operations in other environments.
- Often intensive in resources.

7-79. Urban operations significantly increase the demands on the IPB process. The scale of large urban environments presents more data points for analysts to identify, analyze, and monitor; while the complexity of an urban environment requires more specifically focused intelligence resources than other environments. Urban operations require intelligence with greater targeting precision and combatant/noncombatant discrimination than operations in other environments. Commanders and staffs broaden their awareness in this environment to extend beyond threat forces and effects of terrain, including how the environment is affected by friendly, neutral, and threat operations. The volume of information produced by an urban environment can overwhelm the ability to operationalize it all. Urban offensive doctrine implies an increased troop density; likewise, a commander should consider additional capacity for all aspects of intelligence operations of urban environments in order to meet the increased demands.

7-80. Offensive, defensive, and stability tasks are the three types of operations conducted by the Army in urban environments. (See section I of this chapter). IPB considerations for stability tasks include a more detailed focus on the population as the decisive point for operations.

7-81. Traditional IPB for combat operations and stability tasks limits the AOI to geographical areas from which the threat can jeopardize mission accomplishment. AOIs for urban operations should also include nodes that are noncontiguous to the AO, from which information and intelligence are required to plan and execute urban operations.

7-82. In addition to detailed discussions on urban operations, the listed publications provide the following information:

- ATP 3-06 provides a detailed discussion of IPB considerations for urban operations. IPB for urban operations includes specific products that may be useful to commanders and staffs.
- JP 3-06 provides an extensive discussion and appendix on joint intelligence preparation of the OE in urban areas.
- TC 2-91.4, ATTP 3-06.11, and JP 3-06 provide urban intelligence tools and products that may be employed in addition to traditional IPB products to assess the urban environment. Developing the necessary intelligence products should be a cross functional effort driven by the intelligence staff that also includes the expertise of the other staff and supporting elements, such as civil affairs, engineers, and military information support.

UNIQUE CHARACTERISTICS OF URBAN ENVIRONMENTS

7-83. Successful IPB of urban areas depends on generating intelligence knowledge sufficiently during precombat phases. Staffs require access to data files and intelligence products generated to aid the planning and execution of combat operations. Table 7-7 depicts one method of identifying relevant aspects of urban environments. (See ATP 3-06 for more information on relevant aspects of urban environments.)

Table 7-7. Example framework for identifying relevant aspects of urban environments

Step	*Relevant aspects of urban environments*
Step 1	**Key terrain:** Critical element of OAKOC factors
Step 2	**General urban description:** Megacity, large or small city, town, village, strip area
Step 3	**Population:** Composition, size, and density; location and proximity; beliefs; needs; agendas; leadership; and organizations, interaction, influence, control
Step 4	**Functional areas:** Core, outlying high-rise, military, commercial-ribbon, industrial, residential
Step 5	**Infrastructure categories:** Economics and commerce, administration and human services, energy, cultural, communications and information, and transportation and distribution
Step 6	**Lines of communications:** Roads, rivers/canals, railways, subway, lines of sight, rubble effects
Step 7	**Urban patterns:** Hub, satellite pattern, network pattern, linear pattern, segments/pie slices
Step 8	**Street patterns:** Grid, radial, irregular
Step 9	**Pattern effects:** Blocking effect, funnel effect, funnel-fan effect
Step 10	**Structural types:** Type of building
Step 11	**Mobility corridors:** Air, building, intrabuilding street, subterranean, maritime
Step 12	**Other significant characteristics:** Geo-political issues, history, demographics, politics, religion
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment

7-84. Due to the Army's expeditionary nature and ability to project forces quickly, it is often necessary to gain access to and maintain seaports and aerial ports of debarkation located near urban areas. Threats will attempt to capitalize on friendly vulnerabilities during the projection of force operations. For example, threat forces may conduct raids and ambushes from bases of operations in the vicinity of friendly seaports of debarkation in order to delay friendly follow-on operations. Threat forces may also conduct attacks in the vicinity of aerial ports of debarkation to prevent friendly airfield seizure operations.

7-85. In urban areas, tactical-level detail often has operational or strategic significance. Therefore, IPB must provide a higher level of detail than would be required for operations in a broader, less complex operational area. Effective IPB of an urban environment must include the integration of information from nontraditional intelligence sources. Staffs rely heavily on the voluminous data produced by large urban environments, much of which can be accessed through open sources. During planning, commanders and staffs should consider translation capabilities and the integration of unclassified sources with classified sources of information to build the common operational picture. Open-source intelligence may provide the critical information needed to gain situational understanding of an urban environment.

7-86. In addition to the general intelligence requirements associated with IPB and urban environments, analysts should consider effects of the following during IPB in urban environments:

- Threat forces will seek to achieve several key objectives.
- Threat forces can operate in multiple domains using the depth, breadth, and height of the OE.
- Threat forces will have the means to counter technological overmatch, mitigate numerical deficiencies, and forestall fighting on open terrain.
- During the conduct of urban operations, threat forces can gain time and space in other locations to facilitate a larger campaign plan or decisive battle.
- Urban areas often harbor critical resources or features such as air and port facilities.

7-87. The complexity of urban environments requires an understanding of the various aspects that comprise these environments. Intelligence staffs must analyze natural and man-made terrain, as well as analyze how the society interacts within and is impacted by the terrain. There are countless ways these factors can come together to affect friendly and enemy forces. Building the requisite knowledge of urban operations assists in determining which aspects of the environment intelligence staffs must focus on while performing IPB.

7-88. Staff elements conducting urban area analysis must broaden their scope, looking not only at the air and ground but also at threats that may appear from an urban structure's top, interior, exterior, maritime, and subsurface areas. Subsurface features and interior structures present unique challenges in mapping and monitoring threat forces. Open-source intelligence and information may assist the intelligence staff in mapping and monitoring threat forces in these areas.

7-89. An urban environment's horizontal, vertical, exterior, interior, and subsurface areas offer threat forces many advantages in conducting operations. The combination of these spaces is often equal to or larger in size than undeveloped terrain or bare ground. For example, a multilevel parking garage may have the same surface area as a soccer field, but the layers of the parking garage account for five times as much surface area as the soccer field (see figure 7-3). Analysts must consider and account for these aspects when determining threat uses of urban areas and how they may affect friendly and threat TTP and capabilities.

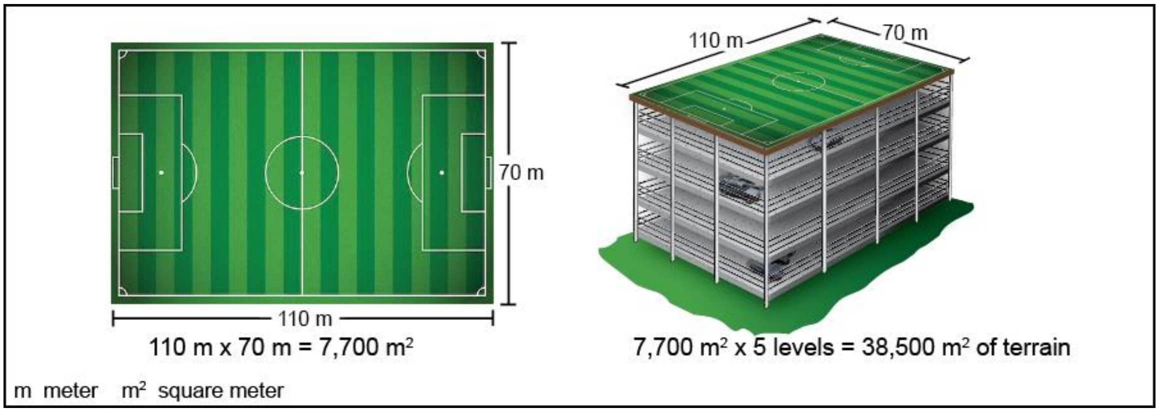


Figure 7-3. Urban environment surface area example

EVALUATING THE MILITARY ASPECTS OF TERRAIN IN URBAN ENVIRONMENTS

7-90. Evaluating the effects of terrain in an urban environment differs from evaluating the effects of open terrain. The analysis of the military aspects of terrain (OAKOC) still applies. However, this analysis must be in the context of urban battlefield characteristics. Chapter 4 fully discusses the evaluation of terrain effects on operations (See ATP 3-06 and TC 2-91.4 for detailed urban area considerations.)

7-91. When developing a MCOO for urban environments, analysts should take a holistic approach. Urban environment airspace and surface, subsurface, supersurface, maritime, internal, and external areas (see figure 4-3 on page 4-5) are all considerations—important to either the success or failure of a mission as well as to contingencies that may arise. A MCOO should include all relevant aspects for the commander's situational awareness and assist the staff in further planning and Army forces in better understanding the terrain associated with a given mission.

7-92. A standard MCOO developed from a military map is not very useful to leaders at the company level and below. Standard military maps do not have the detail required for a thorough analysis of urban areas. Many standard military maps are old and do not reflect the more recent buildings, streets, and significant urban growth. Additionally, standard maps do not show the subsurface aspects of an urban area: 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 identify water facilities, communications facilities, fuel supply, storage facilities, and temporary conditions (for example, construction sites) clearly. Having and providing the most recent information available lessens uncertainty. Figure 7-4 depicts an urban area-based MCOO, which can also depict the six categories of an urban infrastructure:

- Economics and commerce.
- Administration and human services.
- Energy.
- Cultural.
- Communications and information.
- Transportation and distribution.

7-93. This information assists the staff in planning and the commander in decision making. For example, annotating the communications and information sectors on the MCOO assists the staff in determining where to focus efforts to degrade a threat's ability to communicate with the local population.

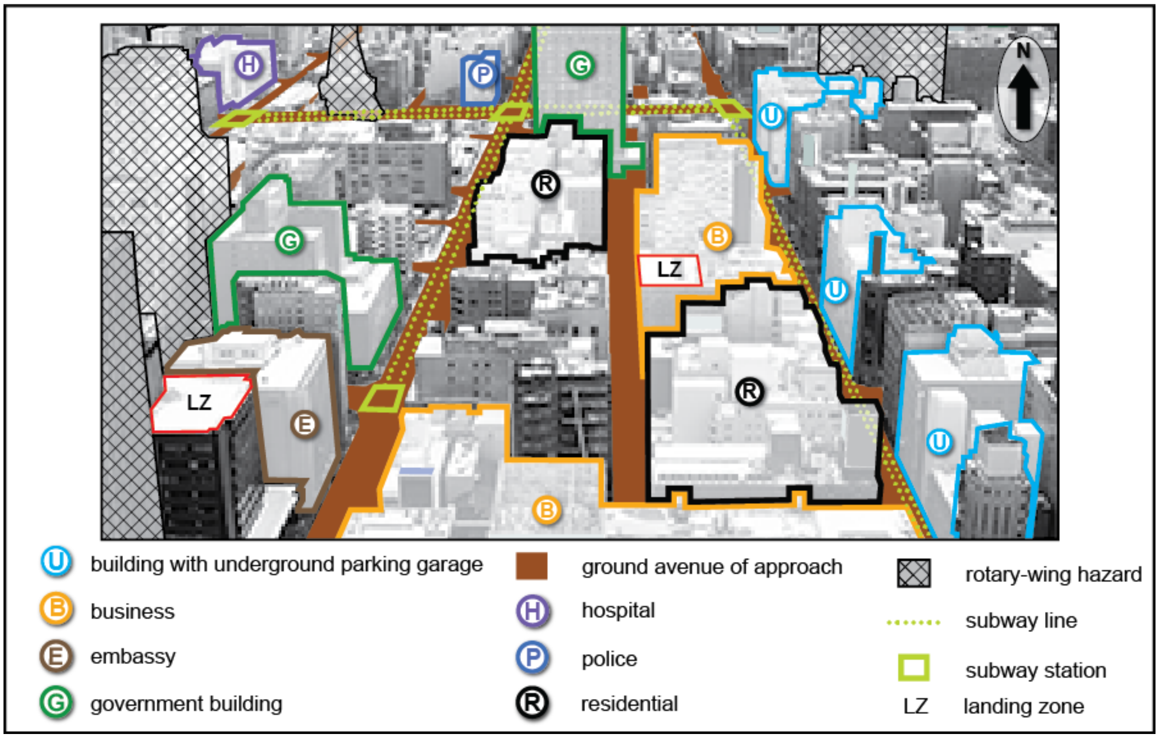


Figure 7-4. Urban area modified combined obstacle overlay example

7-94. Gridded reference graphics offer one method of using the most recent imagery to provide situational awareness to Army forces in an urban environment. (See figure 7-5 on page 7-24.) Analysts can use these graphics to annotate the location of hazards, obstacles, and other information pertinent to forces conducting operations. Staffs can use them during operations to ensure staff members, including commanders, have the latest information on unit locations and areas where contingencies may occur.

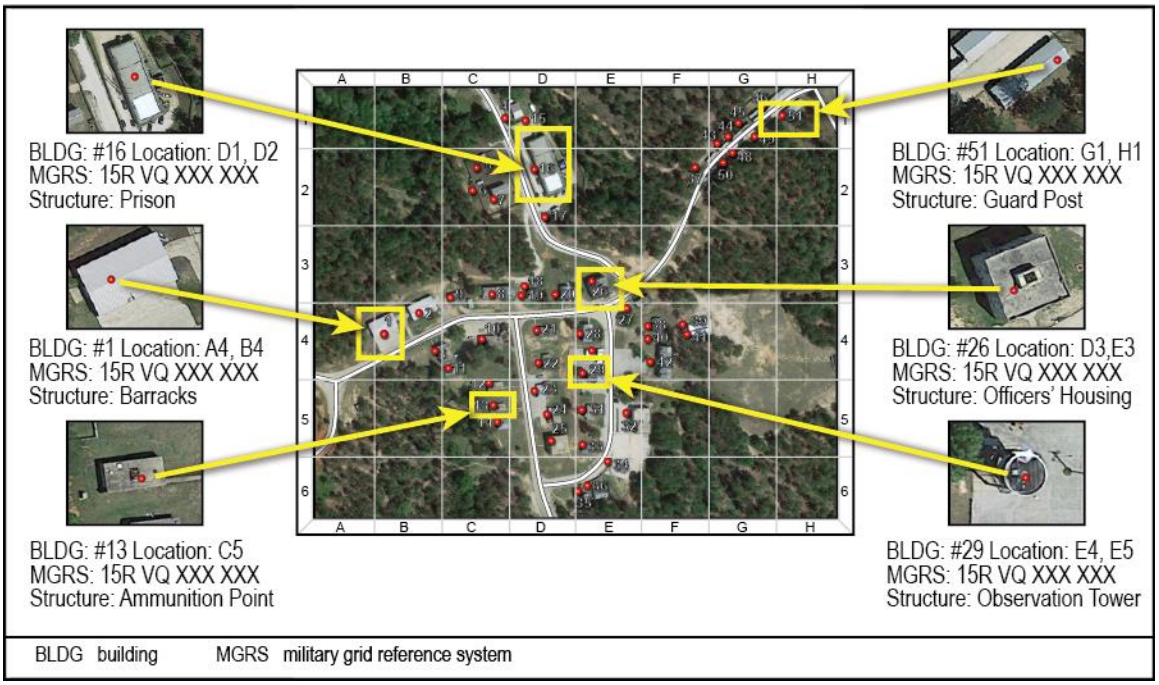

BLDG: #16 Location: D1, D2
MGRS: 15R VQ XXX XXX
Structure: Prison
BLDG: #1 Location: A4, B4
MGRS: 15R VQ XXX XXX
Structure: Barracks
BLDG: #13 Location: C5
MGRS: 15R VQ XXX XXX
Structure: Ammunition Point
BLDG: #51 Location: G1, H1
MGRS: 15R VQ XXX XXX
Structure: Guard Post
BLDG: #26 Location: D3,E3
MGRS: 15R VQ XXX XXX
Structure: Officers' Housing
BLDG: #29 Location: E4, E5
MGRS: 15R VQ XXX XXX
Structure: Observation Tower
A
B
C
D
E
F
G
H
1
2
3
4
5
6
BLDG building
MGRS military grid reference system

Figure 7-5. Gridded reference graphic example

7-95. Analysts conduct terrain analysis using maps or other imagery. While conducting terrain analysis for an entire city may be effective for planning at upper echelons, it lacks the necessary detail for the types of operations and requirements of small units (squads, platoons, and companies). Small units may request detailed terrain analysis at smaller scales to support operations such as raids and ambushes. The Center for Army Lessons Learned (also called CALL) has documented more than 10 years of terrain analysis techniques based on products developed from several urban operations campaigns such as Operation Iraqi Freedom, Operation Enduring Freedom–Horn of Africa, and the Philippines, as well as from responses to acts of nature such as hurricane. (See ATP 3-34.81 for more information on geospatial engineering and urban considerations.)

7-96. Another aspect of urban areas that may require extensive analysis is the presence of microclimates. Dust, smog, wind channeling, night illumination, and sun reflection from buildings are atmospheric effects unique to urban areas. Before Soldiers deploy to an urban area, especially those with urban centers comprising mostly large structures, staff planners must have a good understanding of the unique weather effects in the urban environment. Chapter 4 discusses weather effects on operations. (See TC 2-91.4 for detailed urban weather considerations.)

Observation and Fields of Fire

7-97. Limitations on observation and fields of fire in urban areas are less subtle than in natural terrain where the landscape often varies predictably. The man-made terrain of urban environments presents multiple complex issues to maneuver forces. Due to the built-up nature of urban environments, the best observation and clear LOSs are often from the air, on the streets or roads, or from roofs or supersurfaces.

7-98. Although roofs and supersurfaces enhance observation and fields of fire, they are limited by the angle at which an observer can see to the ground. This is important when considering the placement of observation posts and weapon systems because, unless friendly forces cover ground entrances, an opposing force may have the capability to move undetected within the look-down angle. (See figure 7-6.)

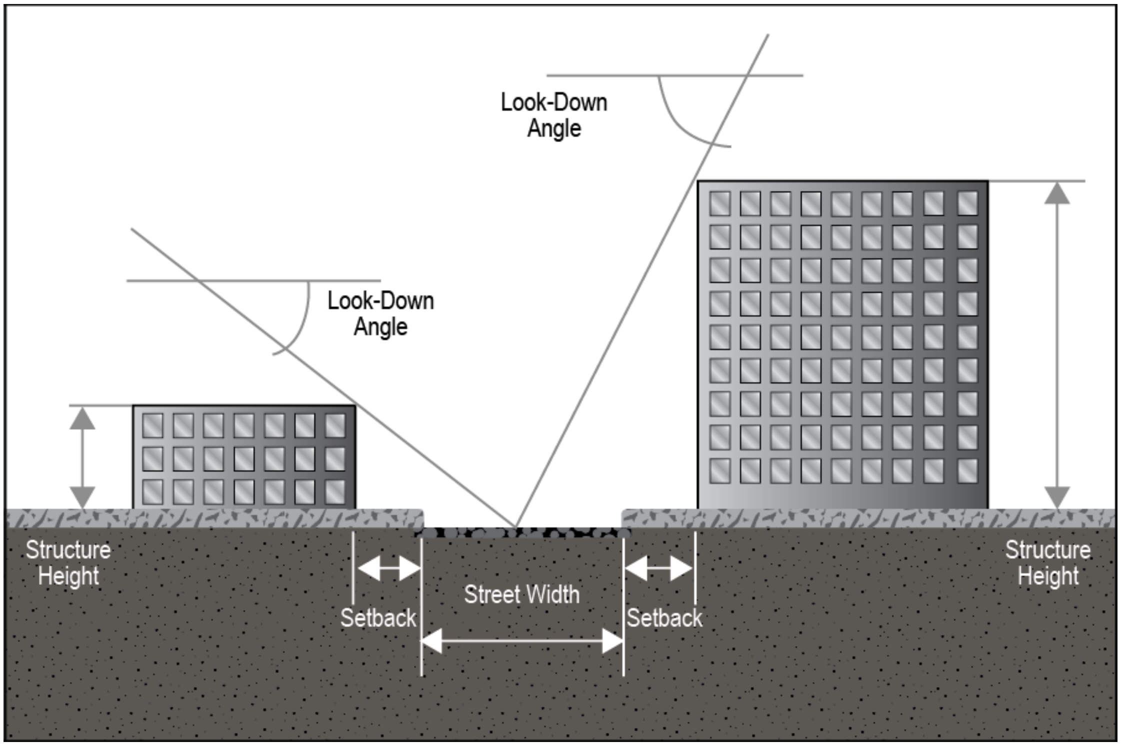


Figure 7-6. Urban look-down angle example

7-99. The physical aspects of the urban environment, such as the heights and concentration of buildings, may cause significant masking and dead space:

- **Masking** in an urban environment refers to using the terrain (or buildings) to avoid radar detection. Tall buildings can mask several blocks of area along the gun-target line.
- **Dead space** is an area that artillery fires cannot hit directly.

7-100. Intervening buildings that stand three or more stories tall hinder close indirect fire support. Target attack dead space behind a building is about five times the height of the building for low-angle fire; the trajectory of high-angle fire reduces the dead space to about half the height of the building. (See ATP 3-06.)

Avenues of Approach

7-101. The availability of AAs in urban areas is essential to accomplishing a maneuver element's mission. When identifying AAs in urban areas, staff integration and collaboration are essential as they assist in—

- Determining vehicle size limitations on road and bridge networks.
- Determining weapon limitations (traverse and elevation, LOS, cover and concealment) on roads bounded by man-made structures.
- Identifying air AAs to facilitate ground maneuver.
- Identifying subterranean networks that can be used for counterattacks and to disrupt friendly advance.
- Identifying areas where signal communications will be masked, intermittent, or experience interference due to natural and man-made structures.
- Identifying observation dead space caused by natural and man-made terrain.

7-102. During mission planning, it may be determined that road networks are heavily trafficked by civilians, do not support the movement of military vehicles, or are heavily defended and covered by enemy fires. Depending on the mission, air and maritime AAs may be options that lead to both surprise and speed (see figure 7-7 on page 7-26).

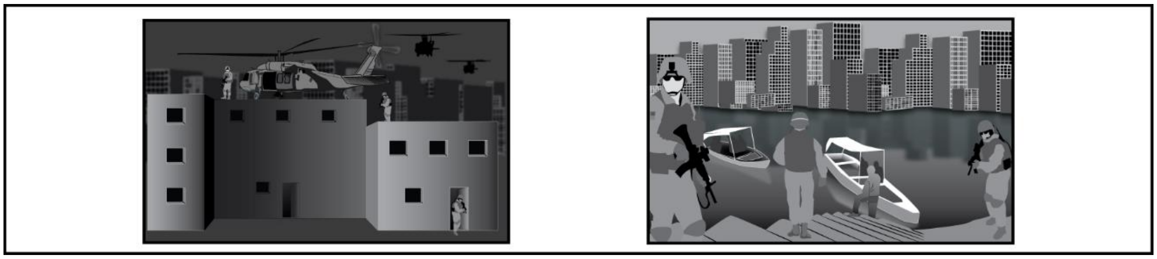


Figure 7-7. Urban environment air and maritime avenues of approach

7-103. Identifying how streets are arrayed in an urban environment provides direct support to OAKOC factors. Most of the world's greatest cities were founded as river or ocean port cities. As these cities grew, their streets were hardened, broadened, or lengthened. Additionally, streets were adjusted based on natural features such as swamps, lakes, and hills. However, not all such modifications were associated with natural constraints. Some cities were designed to foster defense while others were designed to foster trade. Understanding these aspects can assist analysts in determining how threat forces will interact with the terrain during combat operations. For example, after conducting research, analysts determine a city has multiple large boulevards to facilitate the movement of people and goods to and from port cities. Analysts determine these boulevards are likely AAs threat forces will use in their defensive plan to prevent friendly forces from seizing key terrain.

7-104. Pattern effects are a simple form of obstacle and trafficability analysis. Pattern effects analysis of an urban area in an AO and AOI is based on a particular type of urban and/or street pattern. This analysis has less relevance when the entire AO is an urban area; AA analysis is more important. Pattern effects analysis gains more relevance when the AO has many urban areas due to the impact they may have on mobility corridors throughout the urban areas. The following includes types of pattern effects:

- **Blocking:** Often the shape and density of the hub, as well as the width of major streets and proximity of side streets, have the effect of almost completely blocking an operation.
- **Funnel:** The concentration and canalization of forces may occur without immediate fanning. This occurs most frequently when a linear pattern is encountered. This pattern limits the number of maneuver units that may be applied against a series of hubs that must be confronted in succession, and it forces a greater reliance on long-range and indirect fire weapons.
- **Funnel fan:** This effect normally occurs when the hub is located between terrain features unsuitable for mounted operations. Movement of units into the area results in the concentration of forces, loss of offensive momentum, and canalization. Beyond the hub, forces are required to spread or fan out before full combat power can be developed. This favors the defense because it creates an accordion effect in units moving through the hub, reducing C2 and operating effectiveness.

7-105. Urban patterns influence the conduct of operations in urban environments. (See figure 7-8.) During step 2 of the IPB process, analysts should consider how urban patterns shape the OE, including but not limited to how they—

- Impact AAs and mobility corridors.
- Create obstacles (how the layout of buildings and other man-made structures impede movement).
- May assist in determining locations of key terrain (principal urban areas and hubs).
- Facilitate or impede cover and concealment.
- Impact the use of weapon systems.
- Impact rules of engagement.

7-106. Street patterns and urban layouts are designed for ease of mobility. (See figure 7-9.) During military operations, both friendly and threat forces use inherent mobility aspects such as streets, bridges, tunnels, and rail systems. Analysis of these mobility aspects assists in determining optimal approaches to and in cities and where opposing forces are likely to observe and attack friendly forces.

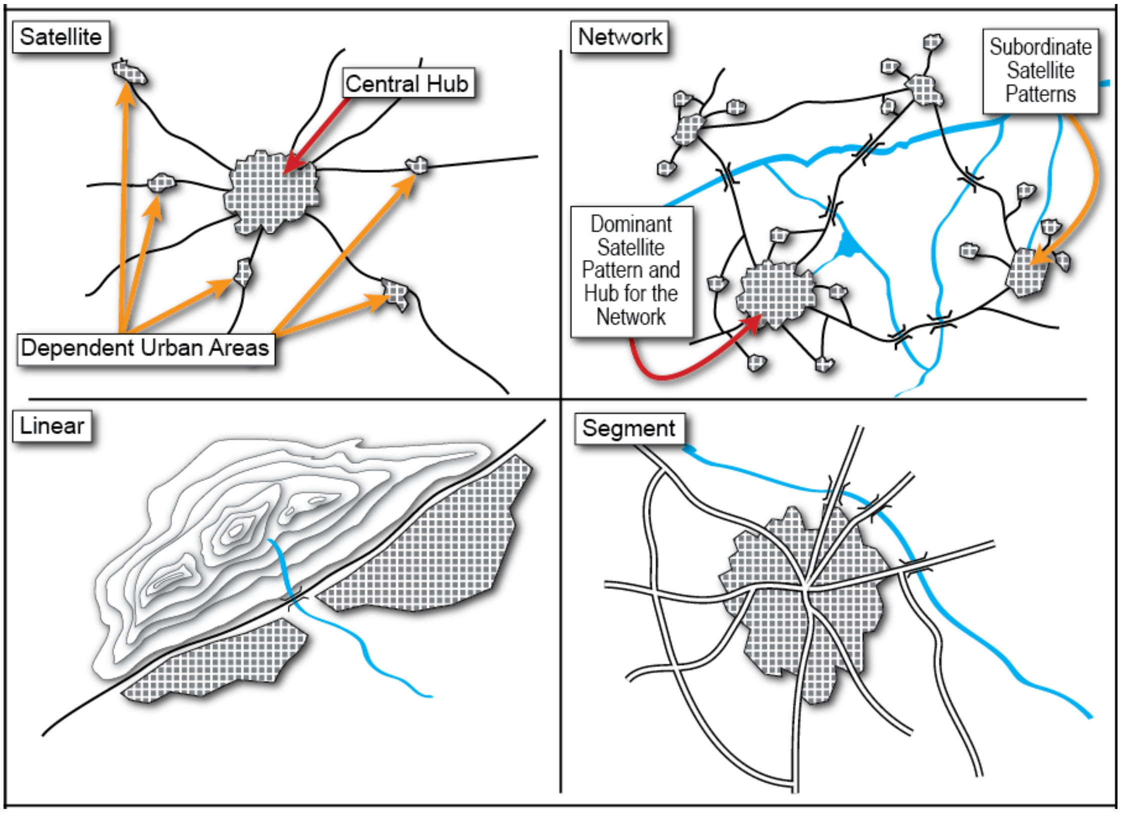

Satellite
Central Hub
Dependent Urban Areas
Network
Subordinate Satellite Patterns
Dominant Satellite Pattern and Hub for the Network
Linear
Segment

Figure 7-8. Urban pattern examples

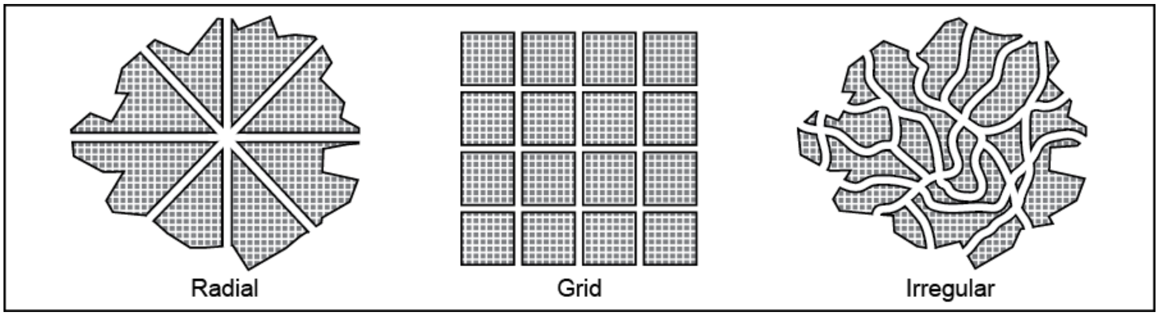


Figure 7-9. Street pattern and urban layout examples

7-107. For urban underground systems, AA or mobility corridor overlays should be prepared when appropriate. This is required where the underground systems (sewer, water, subway, gas, steam, or telephone) have pipes, tunnels, or culverts large enough to facilitate foot or vehicular movement. The overlay should show the size of the tunnels, pipes, and culverts and their approximate orientation. Color coding assists in distinguishing systems types and sizes. When possible, subsurface AAs or mobility corridors should be prioritized based on the likelihood of their use.

Key Terrain

7-108. Key terrain varies based on the composition of the urban area and the nature of the threat. For example, if an opposing force prefers indirect fire using observation posts, tall buildings could be considered key terrain. Key terrain also varies based on the infrastructure of the urban area. Because infrastructure serves as the link between the physical terrain and the urban society, often infrastructure can be considered key terrain for a given operation. For example, TV communications may serve as the main means for communicating with and influencing a population; therefore, the infrastructure associated with TV communications could be considered key terrain.

7-109. Terrain that offers a marked advantage to either combatants in urban environments varies by intended use. An urban environment's man-made and natural terrain, municipal sites, and population centers may all have significant bearings on a unit's mission. It is important to analyze the mission and determine which aspects of the urban area may affect accomplishing the friendly and threat mission.

7-110. Key terrain may include but is not limited to—

- Bridges.
- Government buildings.
- Economic sectors.
- Street intersections.
- Media (television, internet, radio).
- Public utilities.
- Transportation nodes.
- Subterranean networks (subways, sewers, disaster shelters).
- Cell phone networks.
- Buildings that provide good LOSs.

Obstacles

7-111. Depending on a unit's mission, urban areas could be considered as obstacles. Due to potential collateral damage, civilians on the battlefield, and canalizing terrain, commanders may decide to bypass urban areas during the MDMP. When considering that obstacles are used to disrupt, fix, turn, or block, it is understandable that an urban environment's built-up terrain can be used to achieve these effects on air and ground mobility. Urban environment populations could also be considered as obstacles as they have the potential to restrict movement and freedom of action.

7-112. Urban environment interior and exterior spaces can present challenges to ground forces as well as to forces using the air domain. These spaces are often canalizing, making direction of movement predictable to opposing forces. City layouts, street patterns, and buildings are designed with ease of mobility in mind. These considerations direct movement and can make the direction of travel predictable during conflicts. They also provide threats likely areas where friendly force movement will likely terminate. For example, if friendly forces are conducting operations in a city with a radial layout, threat forces will more than likely know where to plan ambushes.

7-113. Urban environments may contain multiple obstacles to air and ground mobility, including but not limited to areas of civilian concentration, barriers, bridges and overpasses, buildings and streets, built-up areas masked to fires, doorways and hallways, stairways and staircases, subterranean terrain, towers, walls, windows, and wires. For example, figure 7-10 illustrates how a staircase can minimize lateral movement and optimize fields of fire for forces in the defense, and how a street can focus movement and lend to predictability.

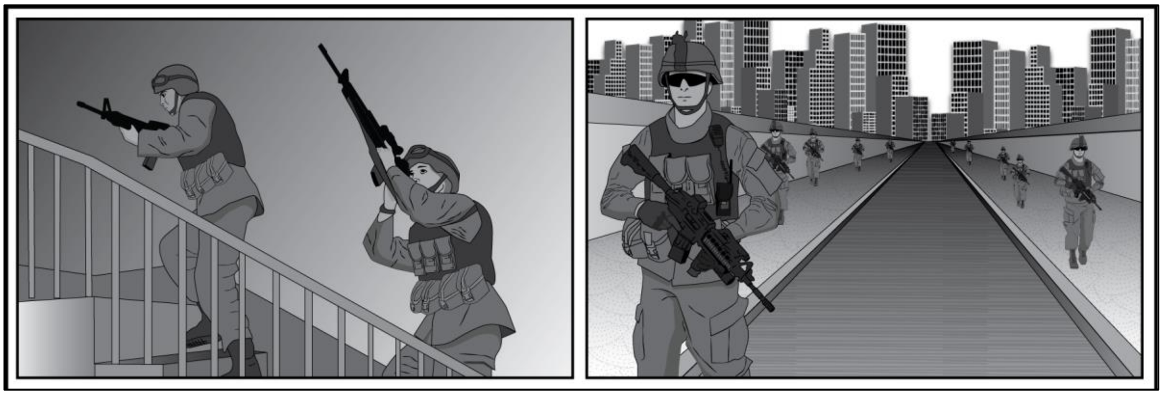


Figure 7-10. Urban environment obstacles to ground mobility

Cover and Concealment

7-114. Sources of cover in urban environments include but are not limited to walls, vehicles, ditches, and tunnels. Depending on their composition and structure, buildings in urban environments may also provide cover. During generate intelligence knowledge, analysts must seek relevant information about the composition of buildings to assist them in determining—

- Friendly and threat weapon effectiveness.
- Possible collateral damage.
- Locations for establishing friendly bases of operations.

Note. Infrastructure analysis can assist in determining the composition of structures within urban environments.

7-115. An urban environment's complex nature and the multitude of surface and subsurface terrain present an array of concealment opportunities, including but not limited to—

- Barriers.
- Buildings.
- Canal systems and aqueducts.
- Internal and external walls.
- Stadiums.
- Pockets of natural terrain (parks, greenways, forests, hedgerows).
- Subterranean terrain (sewers, subway tunnels, parking garages, utility tunnels).
- Vehicles.

7-116. Threat groups may use civilian crowds as concealment or even as cover in the form of hostages—a technique often referred to as using a human shield. Compromised rules of engagement or areas that threats perceive friendly forces will not violate may be used as cover and concealment. Figure 7-11 depicts cover and concealment use in urban environments.

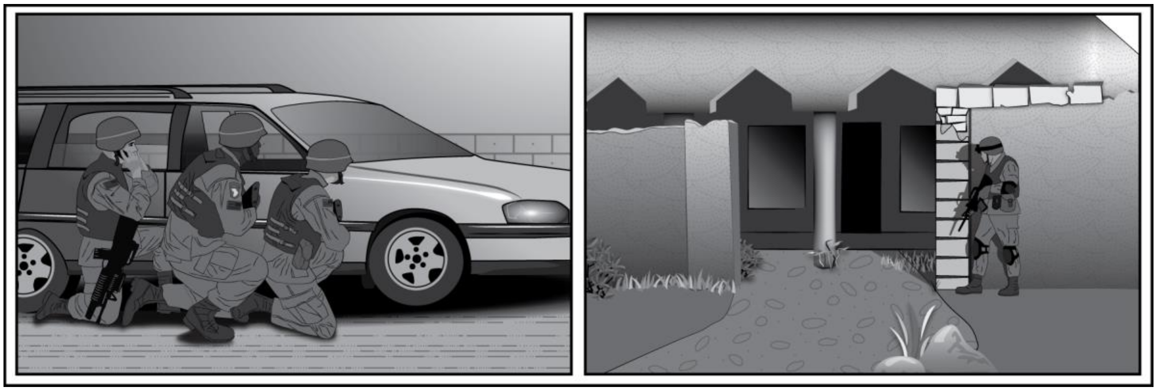


Figure 7-11. Urban environment cover and concealment examples

EVALUATING ASPECTS OF THE THREAT IN URBAN ENVIRONMENTS

7-117. Specific threats in urban environments can be difficult to identify. Urban environments may have a variety of elements, including but not limited to conventional and special operations forces, paramilitary forces, elements of resistance groups, corrupt public officials, activist groups, nongovernmental organizations, proxy forces, elements of terrorist organizations, common criminals, and organized criminal organizations.

7-118. Analysts must provide adequate information that enables leaders to distinguish threats from nonthreats and combatants from noncombatants. This legal requirement of distinction is the initial obligation of decision makers that rely primarily on the intelligence they are provided. The ability to distinguish threats from nonthreats often requires extensive cultural and regional expertise as well as thorough knowledge and understanding of the current problem or conflict. This can be complicated by the multiplicity of indigenous and international demographic factions, state and nonstate actors, and the use of proxy forces representing forces vying for a given outcome. Chapter 4 discusses threat effects on operations. (See TC 2-91.4 for detailed urban threat considerations.)

7-119. In urban areas, threats use the physical characteristics of the terrain to their advantage—operating from any side, above, below, or from within the feature. Threats may have unrestricted access to the cyberspace domain and an urban environment's infrastructure to achieve tactical and strategic objectives.

EVALUATING ASPECTS OF THE POPULATION IN URBAN ENVIRONMENTS

7-120. While an urban area describes the physical nature of the environment, perhaps the most important mission variable to consider is the people within cities and their surroundings. Urban operations often require Army forces to operate in proximity to a high density of civilians. Even evacuated areas can have a stay-behind population measured in the tens of thousands. This population's presence, attitudes, actions, communications with the media, and needs may affect the conduct of operations. Homogeneity decreases drastically as the size of the urban area increases. (See ATP 3-06.)

7-121. Compared to other types of operations, urban operations are largely influenced by civil considerations. The decisive point for operations in urban environments is often human. To effectively operate amid an urban population, it is important to develop a thorough understanding of the society and its culture, including values, needs, history, religion, customs, and social structure. Chapter 4 discusses civil considerations effects on operations. (See TC 2-91.4.)

7-122. Civilian populations pose a special challenge to commanders conducting urban operations. Civilians react to, interact with, and influence Army forces throughout an urban area. Commanders know and account for the potential influence these populations have on all phases of an operation. The intelligence warfighting function monitors and predicts the reactions of the civil population. Accurate predictive analysis of a large population during all phases of an operations requires extensive cultural and regional expertise not normally resident in Army formations.

7-123. Analysis of civil considerations is further complicated by the presence of nonmilitary government departments and agencies, other specialized entities or religious/social influencers, and cultural norms or expectations. Alternative governance structures may emerge in sectors where a population is disenfranchised or beyond the reach of a central government's control. The following includes some of the competing power structures analysts may find within an urban environment:

- Insurgencies.
- Religious organizations.
- Criminal organizations.
- Armed factions.
- Clans or tribes.
- Merchant classes or the economic elite.

EVALUATING ASPECTS OF THE INFRASTRUCTURE IN URBAN ENVIRONMENTS

7-124. An urban infrastructure consists of six categories (see paragraph 7-92). Hundreds of systems exist within an urban infrastructure's categories. Each system has a critical role in the smooth functioning of the urban area. Determining the interdependence of these systems aids decision making and mitigates risk when determining how best to affect the OE. For example, to prevent unintentional harm to an AO's population, the staff maps out all systems linked to a country's hydroelectric dam. By doing this, the staff can avoid damaging periphery infrastructure that may affect the dam's ability to provide electricity.

7-125. Each category of the infrastructure consists of both a physical (terrain) component and human component. For example, the physical component of the electrical segment of the energy infrastructure consists of power stations, substations, a distribution network of lines and wires, and necessary vehicles, repair supplies, and equipment. The human component of this electrical segment consists of the supervisors, engineers, linemen, electricians, and others who operate the system, as well as the end users who rely on it. Commanders understand and recognize both physical and human components in their assessments.

7-126. The key elements that allow an urban area to function are also significant to operations, especially stability tasks. The force that controls the water, electricity, telecommunications, natural gas, food production and distribution, and medical facilities virtually controls the urban area. Chapter 4 discusses infrastructure effects on operations. (See TC 2-91.4 for detailed urban infrastructure considerations.)

7-127. Urban infrastructure is often saturated with sensors for commercial and security purposes, such as traffic cameras, closed-captioned television and smart meters in buildings. Accessing the data feeds from these sensors enables staffs to monitor specific locations within an urban environment in real time.

7-128. The ability to control elements of an urban environment's physical infrastructure can have tactical advantages. The ability to regulate the flow of power and water into sections under threat control can degrade combat effectiveness and present dilemmas.

ADDITIONAL CONSIDERATIONS FOR URBAN ENVIRONMENTS

7-129. Additional considerations for an urban environment include but are not limited to surface, supersurface, subsurface, airspace, maritime, infrastructure analysis, threat forces, threat COAs.

Surface Considerations

7-130. Surface areas consist of ground-level areas, including but not limited to streets, sidewalks, greenways, fields, and plazas. These are the primary movement routes or AAs when considering ground movement. Often in urban environments, ground movement becomes canalized due to the amount of man-made terrain (such as traffic patterns formed by street arrays, bridges, and tunnels). Threat forces may attempt to mitigate the canalization of ground movement by bypassing or modifying man-made terrain. For example, figure 7-12 illustrates how threat forces modified urban infrastructure to create spaces for mobility. Insurgents placed holes in the walls of a building to permit lateral movement and the use of surprise on unsuspecting forces.

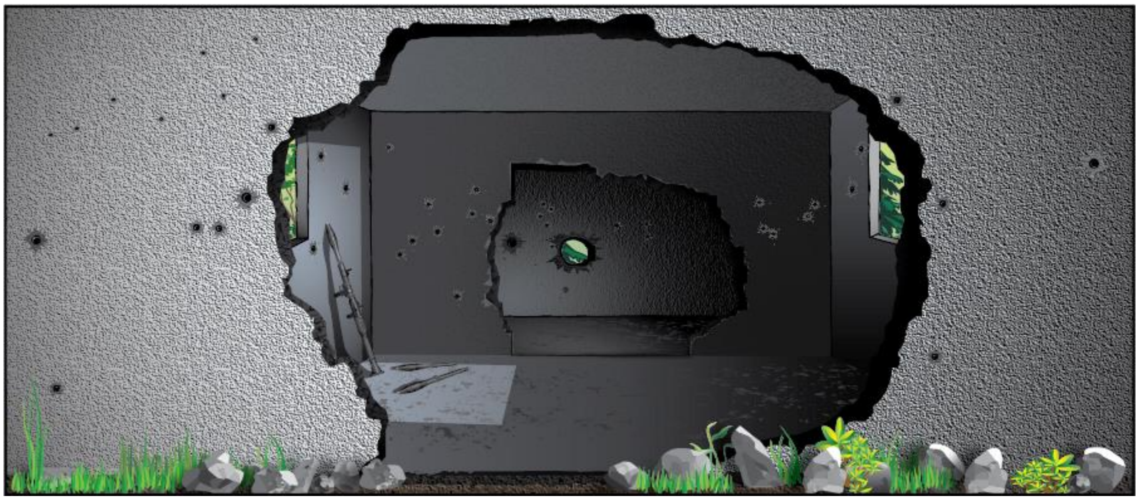


Figure 7-12. Modification of urban infrastructure to permit ground mobility

Supersurface Considerations

7-131. Supersurface areas include the internal floors or levels (intrasurface areas) and external roofs or tops of buildings, stadiums, towers, and other vertical structures. These areas provide cover and concealment; limit or enhance observation and fields of fire; and restrict, canalize, or block movement. The uses of supersurfaces in urban areas can be likened to raised surface terrain, mainly because raised surfaces can be used to mitigate obstacles and a lack of unimpeded mobility. Figure 7-13 on page 7-32 shows examples of how supersurfaces can be used in urban environments. The forces depicted use unimpeded LOSs and fields of fire provided by the supersurfaces. (See ATP 3-06 for more information on supersurface areas.)

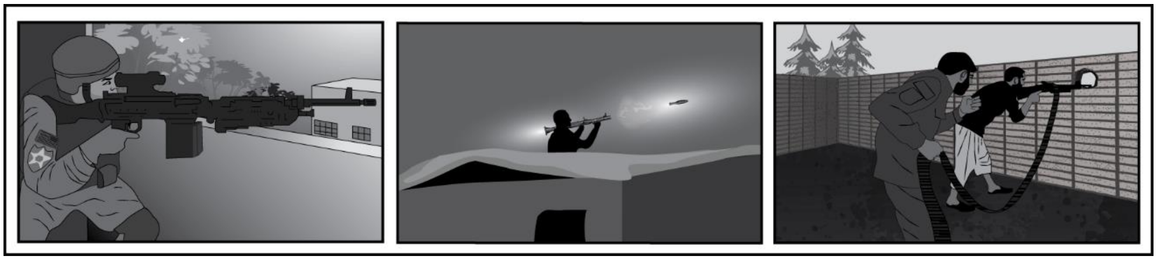


Figure 7-13. Use of supersurfaces for weapons employment

Subsurface Considerations

7-132. Subsurface areas consist of areas below the surface area. These areas present significant challenges to fires, control, and protection that commanders must mitigate. Populations use natural and man-made subsurface terrain for many reasons, including movement of people and materials, storage, water preservation, and living quarters. In modern OEs, subsurface areas provide a means of protecting forces, supplies, and capabilities where they would likely be observed at surface levels. Subsurface areas include but are not limited to—

- Tunnels.
- Subway and drainage systems.
- Sewers.
- Basements.
- Civil defense shelters.
- Mines (such as coal mines).
- Cellars.
- Wells.
- Underground irrigation systems.
- Other underground dwellings or utility systems.

7-133. Underground routes are a primary concern when considering how effective they can be as AAs and LOCs. Sewers, subways, tunnels, and basements provide mobility, cover, concealment, and storage sites for threat forces.

7-134. Key to analyzing subsurface areas and understanding their effects on friendly and threat operations is determining, during step 1 of IPB, if they are present in the AO, how they have been used in the past, and what capabilities they facilitate. Both attacker and defender use subsurface areas to gain surprise and maneuver against the rear and flanks of a threat and conduct ambushes. These areas are the most restrictive and easiest to defend or block. (See ATP 3-06 for more information on subsurface areas.)

Airspace Considerations

7-135. The importance of airspace to Army operations is based on the use of aviation for observation and information collection, air delivery of munitions, aerial attack, and transporting forces and materials. In urban environments, airspace considerations mostly pertain to the mobility of aircraft and the effects the terrain has on observation and fields of fire.

7-136. Because of buildings and other man-made structures (such as power lines, towers, and bridges), analysts must consider obstacles and their impact on friendly and threat air operations. Analysts must consider obstacles to flight and the trajectory of many air-launched munitions because they may limit friendly reactions to threat COAs and threat capabilities to conduct threat COAs.

Maritime Considerations

7-137. Many cities are bounded by the maritime domain, including Lagos, Nigeria, and Aden, Yemen. Therefore, the maritime domain is as critical to urban areas as roads, bridges, and airports. Not only do they support a country's/region's economy, but they are often woven into the cultural structure. Understanding the maritime domain's interdependence with other portions of the urban environment assists in conducting analysis of friendly, neutral, and threat forces' potential impacts within a given OE. For example, understanding the importance the Niger Delta has on transportation and Nigeria's economy, intelligence analysts may determine how threat forces may attempt to leverage their capabilities in the maritime domain to influence their information campaign.

Infrastructure Analysis

7-138. Analyzing an urban area's infrastructure is important in understanding the complexity of the terrain and the society. The infrastructure of an urban environment consists of the basic resources, communications, and industries on which the population depends. The key elements allowing an urban area to function are also among the most important from a military perspective. The force that controls the water, electricity, telecommunications, natural gas, food production and process, and medical facilities may control the urban area. These facilities may not be located within the city's boundaries but, if they are not, they are not far away. The infrastructure upon which the urban area depends may also provide human services and cultural and political structure beyond that urban area, perhaps the entire nation.

7-139. A city's infrastructure is its foundation. It includes buildings, bridges, roads, airfields, ports, subways, sewers, power plants, industrial sectors, and similar physical structures. Electrical, sewage, and water elements should be identified as critical infrastructure. Other important infrastructure elements, such as media outlets, financial institutions, and the location of government entities (police, fire, seats of government), should also be identified.

7-140. Infrastructure varies from city to city. In developed countries, the infrastructure and service sectors are highly sophisticated and well-integrated. In developing cities, often the basic infrastructure is lacking. To understand how the infrastructure of a city supports the population, it needs to be viewed as a system of systems—each component affects the population, the normal operation of the city, and the potential long-term success of military operations conducted there.

7-141. Military planners must understand the functions and interrelationships of these components to assess how disruption of the infrastructure affects the population and ultimately the mission. By determining the critical nodes and vulnerabilities of a city, allied forces can delineate locations where threat forces may attack vulnerable elements within the city infrastructure to disrupt or complicate the urban mission. A city's infrastructure can also support the mission. Local airfields or ports are vital for sustained operations. Host-nation medical facilities become vital when allied casualties are greater than what organic medical capabilities can handle, as well as in maintaining good will with the local population.

Threat Forces

7-142. The decision for threat forces to attack an urban area may be based on tactical, operational, or political considerations. The following include reasons for threats to attack or occupy an urban environment:

- Destroy defending forces within a built-up area.
- Achieve political, strategic, economic, logistics, or military goals.
- Gain time to achieve objectives at other locations.
- Occupy urban areas, which is significant to the threat information campaign.
- Prolong a battle or campaign.

Threat Courses of Action

7-143. When developing situation templates for threats conducting operations in an urban environment, consider that threats may conduct multiple operations simultaneously within a given area. Some of these operations may be diversionary, designed to detract attention away from primary objectives. More often, they are designed to force friendly forces and local authorities to focus on several incidents simultaneously, creating the illusion that they cannot handle the situation.

7-144. Event templates for urban operations focus mainly on terrain since focusing NAIs to events has limited utility in a slow-moving urban battle. Because NAIs may be individual buildings, they may be closer together than in nonurban areas. However, they perform the same functions of confirming or denying threat COAs and serve as the basis for directing the information collection effort.

7-145. DSTs for urban operations must result directly from war gaming. As with situation and event templates, DSTs normally cover areas less than 1,000 square meters and exceptionally slow-paced operations—rarely relying on time phase lines to key decisions. However, cross streets that run perpendicular to the axis of advance may replace time phase lines. Street intersections, open areas, or individual buildings may also serve as decision points, especially when street patterns are not rectangular. Decision points must consider the slower pace of urban operations, and not be placed too far in advance or too close to the TAIs to which they are keyed.

7-146. It is exceptionally critical to prepare threat DSTs for urban operations. The restrictive nature of the terrain limits freedom of action to such an extent that the commander must be able to determine threat options at a glance. When possible, the threat DST should be developed on, or as an overlay to the friendly DST. It is also possible to develop a combined friendly and threat DST with decisions or counterdecisions keyed to points, events, or time phase lines. Since emphasis is placed on night operations for achieving surprise in urban warfare, analysts may consider developing separate DSTs for day and night operations. Consideration factors for developing night DSTs include but are not limited to—

- Infiltration.
- Increased reconnaissance.
- A more rapid pace of operations.
- A reliance on stealth and illumination.

SUBTERRANEAN ENVIRONMENTS

7-147. The use of subterranean spaces and structures can be a means of covertly maintaining the initiative against an opponent. Such spaces and structures can be used for C2, defensive networks, operations, storage, production, or protection. Continued improvements in the construction of subterranean environments have increased their usefulness and proliferations. (See ATP 3-21.51.)

7-148. Although not a new tactic, using subterranean systems (any space or structure located below ground) allows for the surreptitious use of terrain to gain advantages that are often applied above ground. Threats lacking either troop strength or technical or tactical advantages use these systems to gain freedom of action at a time and place of their choosing.

7-149. Subterranean systems can be used in offensive and defensive tasks. Throughout history, friendly and threat forces have noted the tactical value provided by subterranean systems. Not only do they mask movement across an OE, but subterranean systems are also essential to logistics operations. Tables 7-8 and 7-9 depict subterranean environment categories and subterranean terrain features, respectively.

Table 7-8. Subterranean environment categories

Categories	**Category 1:** Tunnels, natural cavities, and caves		**Category 2:** Urban subsurface systems		**Category 3:** Underground facilities (military-purposed)	
Subcategories	**Rudimentary:** Lack of shoring	**Sophisticated:** Shoring, basic amenities	**Substructure:** Basements, parking garages	**Civil works:** Subways, sewers, aqueducts	**Shallow:** Silos, bunkers (< 20 meters)	**Deep:** Military bases (> 20 meters)
Functions	**Civil:** Commercial operations, transportation, storage **Enemy:** Command and control, operations, storage, production, protection				Command and control, operations, storage, production, protection	
Supporting amenities/ infrastructure	Power cords, small generators, lights, ventilation shafts, small pumps		Electrical power, transportation corridors, life support systems, environmental controls, communications lines ***Note.*** Internal redundancies may exist allowing the facility to operate for extended periods, independent from external support.			
Common threats	Personnel, improvised explosive devices, traps, direct fire methods				Military offensive and defensive measures	
Common hazards	Environmental (poor air quality, dangerous gases, wildlife), materiel (munitions, fuels), structural integrity					

Table 7-9. Subterranean terrain features

Feature	*Description*
Adit	An entrance to an underground mine which is horizontal or nearly horizontal; or an opening into a mountain with only one entrance.
Alcove	A limited and localized enlargement of a tunnel to accommodate equipment.
Barrier	Doors, gates, hatches and framing, as well as the presence of any reinforcement to hinges, locking mechanisms, or the barrier itself to control entry and exit.
Blast door	A door designed to withstand blast effects, sometimes up to the nuclear detonation level.
Blast berm	A wall or mound of earth directly in front of a portal used to deny or minimize kinetic weapon effects.
Blast valve	A valve, normally open, to facilitate ventilation that closes automatically when exposed to high-blast pressures. May be closed manually for chemical, biological, radiological, and nuclear protection.
Bomb trap	A space designed to contain or divert blast effects.
Confined space	An enclosed or narrow space not meant for continuous human inhabitance.
Deep	A facility with more than 20 meters overburden.
Fall	A mass of roof rock or coal that has fallen in any part of a mine.
Footprint	The surface area that incorporates all components of a subterranean system.
Gallery	A large horizontal or a nearly horizontal underground passage, either natural or artificial.
Hard structure	Structures resistant to kinetic weapon effects; highways, railroad tunnels, some bridges, and airfields may be considered hard structure because of their design.
Hardened structure	A structure intentionally strengthened for protection from kinetic weapon effects.
Mission space	The space where facility functions occur (also known as the functional area).
Overburden	The amount of earthen material above the ceiling of the subterranean system.
Portal	The structure surrounding the immediate entrance to a mine; the mouth of a cave or tunnel.
Shallow	A facility with 20 meters or less overburden.
Silo	A vertical, cylindrical structure extending from the surface into the ground used to protect a missile.
Shaft	An opening from a subterranean space used for ventilation, drainage, or hoisting of personnel or materials. Connects the surface with underground workings.
Tunnel	A horizontal, or near-horizontal, underground passage, that is open to the surface at both ends.
Umbilicals	Supporting infrastructure that allows a system to function.

UNIQUE CHARACTERISTICS OF SUBTERRANEAN ENVIRONMENTS

7-150. Knowledge of the types of natural (category 1) and man-made (category 2) subterranean environments within an OE offers a significant advantage when performing IPB and subsequent planning. Identifying subterranean environments assists intelligence staffs in developing threat COAs that may impact friendly operations and lessen the threat’s use of surprise to gain relative positions of advantage. Advantages that must be addressed when conducting IPB include but are not limited to—

- Providing a concealed method of infiltrating forces.
- Allowing for the disruption of defenses.
- Providing covered and concealed routes to move reinforcements or to launch counterattacks.
- Using LOCs for the movement of supplies and evacuation of casualties.
- Providing space to cache supplies and equipment.
- Providing concealed locations to conduct C2 operations.
- Providing protection from forces with technical advantages.

Category 1: Natural Subterranean Environments

7-151. Caves and natural cavities are primarily formed by the erosion or dissolving of limestone over time. Examples include Carlsbad Caverns in New Mexico or the Lascaux Cave in France. Tunnels are natural or often linear caves, but they can also be man-made structures, such as railway tunnels or the Channel Tunnel that links the United Kingdom to France.

7-152. Depending on their intended use, category 1 subterranean environments can be—

- **Rudimentary systems**, which have no means of support, for example, wooden bracing.
- **Sophisticated systems**, which usually contain some form of bracing material, for example, wood or concrete.

Category 2: Man-Made Subterranean Environments

7-153. Urban subsurface systems include civil works and substructures. Civil works include aqueducts, sewers, subways, transportation, and utility tunnels. Substructures include basements, shelters, and parking garages, which may appear similar to sophisticated tunnels or may be more robust with complex supporting infrastructure.

7-154. Urban subsurface systems are key aspects when considering dense urban area operations. Threats may repurpose these systems due to the advantages they may provide against an opposing force. For example, subway systems may be used to protect civilian populations, military forces, and equipment from airstrikes, as witnessed in the German Blitzkrieg of London during World War II. These systems have also been used to shelter military forces and permit surreptitious movement, as witnessed during the conflict in Grozny, Chechnya, during the First Chechen War, 1994-1996. The following includes but is not limited to other reasons for repurposing urban subsurface systems:

- Lack of secure aboveground terrain to maneuver.
- Lack of aboveground protection from air strikes.
- Providing a method of communications.
- Providing a method to evacuate casualties.
- Protection and sanctuary C2 nodes.

The Maginot Line

One of the most extensive uses of man-made subterranean terrain is the French-built Maginot Line. The French built this series of fortifications to deter German aggression along the France-German border post World War I. This fortified line consisted of fortresses, bunkers, outposts, and tunnels used in the defense but unable to support counterattacks. The subterranean portions of the line, some of which included railway tracks, allowed French forces to move undetected, store and provide logistics to support combat operations, and conduct reconnaissance operations. Although the Maginot Line did not prevent Germany from successfully conducting operations in France, it was tantamount in recognizing the importance subterranean terrain can have on the scope of combat operations.

Evaluating Subterranean Environments Using the Military Aspects of Terrain

7-155. Using subterranean environments provides a means of expanding the physical battlefield and cover and concealment along routes of movement. Historically, threat forces have used subterranean terrain as a means to counter friendly overwhelming manpower, technology, and firepower.

7-156. When viewing the OE holistically, determining whether subterranean environments are relative to a unit's mission is critical to understanding the full scope of available friendly and threat COAs. Regardless of the type of environment an operation is conducted, opportunities for friendly and threat forces to use subterranean environments must not be overlooked. For tactical operations, analysis of the subterranean environment uses the military aspects of terrain (OAKOC). Table 7-10 shows a terrain effects matrix that describes OAKOC factor effects on friendly and threat operations in a subterranean environment.

Table 7-10. Terrain effects matrix for a subterranean environment example

OAKOC factors (military aspects of terrain)	*Terrain effects*
Observation and fields of fire	• Use of night vision devices limited to sophisticated sections of the tunnel complex. • Observation limited to less than 10 meters with thermal devices. • Fields of fire for direct fire weapons less than 20 meters for small arms. • Over pressure due to weapon discharge will impact audible observation.
Avenues of approach (AAs)	• Primary and secondary road systems for high AAs. • Generally flat terrain with brigade-sized mobility corridors between small villages. • Railroad in the north running east to west. • Significant funneling of forces expected until bunker facility is reached.
Key terrain	• Command and control (C2) bunker. • Barriers blocking C2 bunker will impede attacking forces significantly. • Tunnel connected to C2 bunker likely has multiple exits.
Obstacles	• Booby traps likely at entrances to tunnels and at transitions from tunnels to bunker complexes. • One known tunnel entrance focuses defensive forces to attacking forces.
Cover and concealment	• Cover and concealment are limited corners and barriers near C2 bunker. • Ricochets likely due to reinforced concrete structure. • No ambient light favors defensive forces.

Observation and Fields of Fire

7-157. Observation in subterranean terrain varies based on the type of terrain. In urban subterranean environments, such as subway tunnels, observation may be good; however, in sewer systems, observation is limited due to lack of light. Since subterranean terrain is typically more confining than aboveground terrain, observation may also be limited to short distances. Fields of fire are limited due to confined spaces and favor forces in the defense.

Avenues of Approach

7-158. Maneuverability is one of the critical factors for using subterranean terrain. Forces using subterranean terrain as AAs have an advantage because their movement may be undetected. This increases forces' possible COAs. When developing threat COAs, analysts must consider counterattacks from subterranean terrain since it can potentially extend the battlefield. When layering surface terrain on top of subterranean terrain in overlays, analysts can see how forces using subterranean terrain can maneuver against surface forces effectively.

Key Terrain

7-159. When analyzing subterranean terrain and possible key terrain, it is important to note the relationship between surface terrain and subterranean terrain because exploiting subterranean terrain assists in gaining advantages on surface terrain. Possible key terrain in subterranean environments include but is not limited to access points to surface terrain and subterranean terrain (surface subway and sewer entrances), subsurfaces, bunkers tied to terrain that provides a tactical advantage, and tunnels providing maneuver advantage.

Obstacles

7-160. Subterranean environments affect friendly and threat COAs; therefore, they must be considered during planning. Depending on the mission and mission location, subterranean terrain can be the most significant obstacle in the OE. The importance of subterranean terrain to threats often requires additional focus by friendly forces and added resources such as engineers for clearing operations.

7-161. Subterranean terrain is often classified as an obstacle because it can impede friendly operations. Obstacles at intersections in tunnels and other subterranean terrain set up excellent ambush sites and turn subterranean passages into deadly mazes. Subterranean terrain can also be used to ambush forces. Booby traps or IEDs are easily hidden inside tunnels and culverts and can be effective methods of preventing or impeding enemy movement.

Cover and Concealment

7-162. The lack of cover and concealment in subterranean terrain favors forces in the defense, depending on the type of structure, its composition, and purpose:

- **Tunnels.** The inside of a tunnel provides minimal to no cover and concealment. Depending on the complexity, structure, and composition of the tunnel, internal structures, such as walls, barriers, and stairwells can be used for cover and concealment. Though darkness can be used is some tunnels, other more complex tunnels with internal and sometimes rudimentary lighting limit concealment.
- **Bunkers.** The structure of barriers varies depending on their purpose. Bunkers used for C2 are often very complex with much of the same infrastructure as aboveground structures. Bunkers may offer cover and concealment through internal walls, barriers, stairwells, and elevators. Other, less complex bunkers may only offer cover and concealment for forces using them in the defense.
- **Subways.** Subways and their associated infrastructure (subsurface stations and tunnels) offer cover and concealment in a variety of forms, including but not limited to internal walls, stairwells, escalators, and security barriers.
- **Caves and caverns.** These natural forms of subterranean terrain mainly provide cover and concealment for forces in the defense. The natural walls of caves and caverns provide significant cover as they are often used as bunkers to avoid aerial and indirect fire attacks. Darkness is the main form of concealment in caves and caverns, though rudimentary lighting systems may be used within.
- **Sewers.** Although sewers provide substantial cover and concealment from surface fires and observation, inside they offer minimal cover and concealment to forces in the offense or defense. Like surface streets, sewers are not straight. The angles they create as they follow surface infrastructure permit their use for cover and concealment.

Chapter 8

Additional Considerations for Operational Environments

THE OPERATIONAL ENVIRONMENT

8-1. During step 1 of the IPB process, the OE is defined. An OE encompasses the domains, the information environment, the EMS, and other factors. IPB applies across the range of Army operations. Therefore, when defining the OE, all domains in which Army and threat operations occur must be considered.

AIR DOMAIN

8-2. The *air domain* is the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible (JP 3-30). The air domain is the operating medium for fixed-wing and rotary-wing aircraft; air defense systems; UASs; cruise missiles; and some ballistic and antiballistic missile systems. Air AAs are different from maritime and ground AAs. Analysis of the air domain is critical in identifying air AAs, which are also associated with terrain restrictions of the land domain. (See JP 2-01.3.)

8-3. As with IPB conducted for land-based operations, IPB performed for air-based operations focuses on determining air domain characteristics that influence friendly and threat operations. Analysts should consider that IPB for the different domains is conducted using the same process; it is the characteristics of differing domains that are determined and incorporated into the overall IPB product. (For more on IPB considerations for the air domain, see FM 3-01.)

8-4. To determine the relevant aspects of the air domain, it may be useful to—

- **View it as a medium for using capabilities.** For example, how does or will the air domain affect the use of civilian and military aircraft, civilian and military UASs and drones, weather monitoring systems, air corridors, fly over rights, and broadcasting rights?
- **Think about relationships.** For example, what is the air domain's relationship to weather, the EMS and communications, and effects on performance (considering altitude, barometric pressure, and humidity)?

8-5. The air domain has potential relevant effects on maneuver units, signal units, psychological operations units, and artillery units just as it has on Army rotary-wing aircraft units.

LAND DOMAIN

8-6. The *land domain* is the area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals (JP 3-31). These areas also include subsurface and supersurface areas. Army operations are conducted primarily in the land domain. Analyzing the military aspects of terrain (OAKOC) of the land domain's natural and man-made features assists in determining the domain's effects on friendly and threat operations. In turn, this analysis assists in determining how terrain supports friendly and threat COAs.

8-7. Analysis of the OE's land domain covers natural and man-made features as well as populations, transportation systems (roads, bridges, railways, airports, seaports, inland waterways, tunnels), surface materials (including the density of buildings, building construction framework and material, building height, cultural or historic significance), ground water, cities, towns, villages, multistory buildings, skyscrapers, natural obstacles such as large bodies of water and mountains, the types and distribution of vegetation, and the configuration of surface drainage and other subsurface structures, such as subways, basements, bunkers. Understanding the relevant aspects of the land domain is essential in all steps of the IPB process.

MARITIME DOMAIN

8-8. The *maritime domain* is the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals (JP 3-32). The maritime domain's vastness and proximity to the land masses make this domain critical for force projection and the application of weapons and sensors that support Army operations. (See JP 2-01.3.)

8-9. The maritime domain is a vast maneuver space that allows for tactical maneuver in the air, on the surface, and beneath the surface of the water. Although the Navy is the primary Service responsible for security in the maritime domain, Army forces use this domain for all aspects of operations, including but not limited to joint forcible entry, multinational exercises, information collection, sustainment, aviation sea basing, protection, humanitarian assistance, and noncombatant evacuation.

8-10. The maritime domain facilitates most of the world's trade and is essential in maintaining a global economy. The interdependence of global economics and maritime security requires continuous monitoring of the maritime domain and the regions bordering its waters. Therefore, Army operations in this domain may likely continue to increase.

RELEVANT ASPECTS OF THE MARITIME DOMAIN

8-11. Because most Army operations occur in the land domain, intelligence staffs must maintain situational awareness of possible contingencies for which the maritime domain may become relevant to mission success. The following includes considerations when researching significant aspects of the maritime domain:

- Sea LOCs and sea ports of debarkation, including—
  - Chokepoints (straights, shipping lanes, and canals).
  - Naval bases.
  - Coastal defenses (antiaccess and area denial, coastal mines, and coastal long-range fires).
- Threat vessels, including but not limited to—
  - Civilian: Pirate, narcotics, and human-trafficking vessels.
  - Military: Destroyers, cruisers, carriers, frigates, and submarines.
- Natural harbors and anchorages.
- Infrastructure, including ports, shipping yards, and dry-docks.
- Friendly forces, including host-nation forces and other Services that may be able to provide OE information.
- Threat forces in the OE.
- Surface and subsurface effects.
- Weather effects.
- Tidal and current impacts.
- Transportation networks.

8-12. During generate intelligence knowledge, intelligence staffs should reach out to outside organizations and agencies as well as other Services to increase their knowledge base on the maritime domain. Many missions using this domain, especially missions in the littorals, are conducted with joint forces.

TRADE

8-13. Approximately 80 percent of global trade is conducted using the maritime domain. The importance of this domain on the global economy is significant mostly due to the low cost of shipping via water (ship) instead of air. Items such as finished products, raw materials, as well as components to finish products are shipped via the maritime domain. When considering global trade agreements and the impacts they have on billions of people, it is understandable why threat groups see maritime routes as potential avenues to leverage power and control.

8-14. Not all maritime trade is legal. Items, such as narcotics, weapons, money, people, and black-market and counterfeit goods, are trafficked using the maritime domain. In many OEs, illicit trade conducted using the maritime domain can be linked to threat groups that intelligence staffs evaluate.

THREAT FORCES

8-15. Threat forces in the maritime domain range from conventional naval forces conducting missions in open seas to criminal groups, including pirates, operating in the littorals. Based on the mission, intelligence staffs determine which threat groups have the capability to impact operations. Often, the OE determines what type of threat forces are present. Intelligence staffs must view the OE holistically to determine why threats are present. For example, oftentimes, isolated and poorly patrolled littoral waters along the coasts of Colombia, Central America, and Mexico offer drug trafficking organizations an adequate environment to smuggle narcotics in semisubmersible watercrafts. Another example is the isolated coast of Somalia, which offers pirates a good environment for using small, relatively fast watercraft to target international shipping lanes. Their presence could be rooted in many objectives such as the control of waterways for financial gain or the enforcement of legitimate or illegitimate coastal borders. The full range of maritime domain threat forces varies by location and threat objectives.

SPACE DOMAIN

8-16. The *space domain* is the area above the altitude where atmospheric effects on airborne objects become negligible (JP 3-14). The space domain is essential to information collection, missile tracking, launch detection, environmental monitoring, communications, navigation, global positioning, and timing. It is also essential to multiple systems and subsystems necessary for the conduct of military operations across the warfighting functions. Analysis of threat capabilities that can affect the space domain as well as the effects a degraded space domain can have on friendly operations must be considered as threat exploitation of friendly technology may be used. (See FM 3-14 and JP 3-14.)

8-17. Space is considered as the region around the Earth with little atmosphere, where satellites are placed in orbit. Increased access to information capabilities that leverage the cyberspace and space domains to disseminate information, demonstrates the importance of analyzing the space domain to identify its relevant aspects.

8-18. The U.S. military, including all Army warfighting functions as well as civil and commercial sectors, rely on the space domain to employ capabilities for daily operations. Use of the space domain facilitates military communications, navigation, environmental monitoring, information collection, and warning intelligence. Space-based resources provide freedom of action, global reach, responsiveness, and insights into an OE that might otherwise be a denied area. These resources are not constrained by the geographic borders of otherwise geographically denied regions.

8-19. Whether for commercial or military use, all countries have access to the space domain and its satellite capabilities. State and nonstate actors use these capabilities to shape the OE to achieve parity or overmatch. Army forces have freedom of action in the space domain. This has made threat forces aware that they must contest the U.S. presence in the space domain to achieve relative advantages in other domains, such as cyberspace where information campaigns can be used to level effects at a time and place of the threat's choosing. (See ATP 3-14.3 for more on space domain capabilities.)

8-20. Military, civil, and commercial sectors of the United States and its allies increasingly rely on space capabilities to create targets of opportunity. Threats often view these opportunities as exploitable vulnerabilities. The increasing reliance of the United States on space capabilities has created a valuable target for threats to exploit and attack. U.S. space-related centers of gravity are potential targets, especially ground space assets, including the supporting infrastructure of systems. To the threat, this vulnerability translates into an HVT. Conversely, a potential threat who relies even minimally on space systems will have space centers of gravity as potential, lucrative HPTs for friendly forces to engage.

8-21. The staff and commander need to consider space capabilities and vulnerabilities during IPB, ultimately leading to COAs that will synchronize space aspects into the operation. The use of space systems significantly affects operations involving communications, navigation, weather support, and surveillance. This protects force capabilities and intelligence information collected across the battlefield. Across the range of military operations—from predeployment to mission completion—space effects on operations are ongoing assets that the commander must plan for, can influence, and will rely on for the MDMP. The G-2 and space staff officer must ensure an effective space IPB effort is performed and incorporated into the overall IPB staff effort.

8-22. Intelligence staff coordination with the space support element (at corps, divisions, fires brigades, special forces groups, and other organizations with emerging requirements) is critical to understanding what space domain systems may influence an AO. To determine how those space domain systems will impact an operation from a friendly and threat perspective, the intelligence staff applies the IPB process.

RELEVANT ASPECTS OF THE SPACE DOMAIN

8-23. Relevant aspects of the space domain within the IPB process are the—

- Space environment.
- Space weather.
- Space weather phenomena.

Space Environment

8-24. *Space environment* is the environment corresponding to the space domain, where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences, and that encompasses the Earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere (JP 3-59). In addition to the emission of electromagnetic radiation, the space environment also consists of a continuous outflow of energetic charged particles from the Sun called solar wind. Solar wind is ionized gas composed of ions, electrons, and charged particles that continuously erupt from the solar corona at more than 400 kilometers per second. Several types of solar activity can cause energetic particle streams to enhance normal or background levels of solar wind. These enhancements and discontinuities in solar wind speed or density can cause solar storms, which impact the EMS.

8-25. The disturbance of ions, atoms, and electrons as they move through space accounts for either the degradation or improvement of radio wave propagation in the space domain. Environmental impacts, such as cosmic rays, solar storms, temperature fluctuations, and radiation commonly affect wave propagation. The layers of the Earth's atmosphere, through which radio waves travel, also affect propagation. (For more information on radio wave propagation, see ATP 2-22.6-2.)

8-26. To understand how the space domain may be impacted during operations, intelligence officers must engage Army space support teams and Air Force staff weather officers to understand and articulate the impact of three of the various layers of the Earth's atmosphere—ionosphere, stratosphere, and troposphere—that may affect the EMS and space-based capabilities (see figure 8-1). (See ATP 2-22.6-2 for a detailed explanation of those layers of the Earth's atmosphere.)

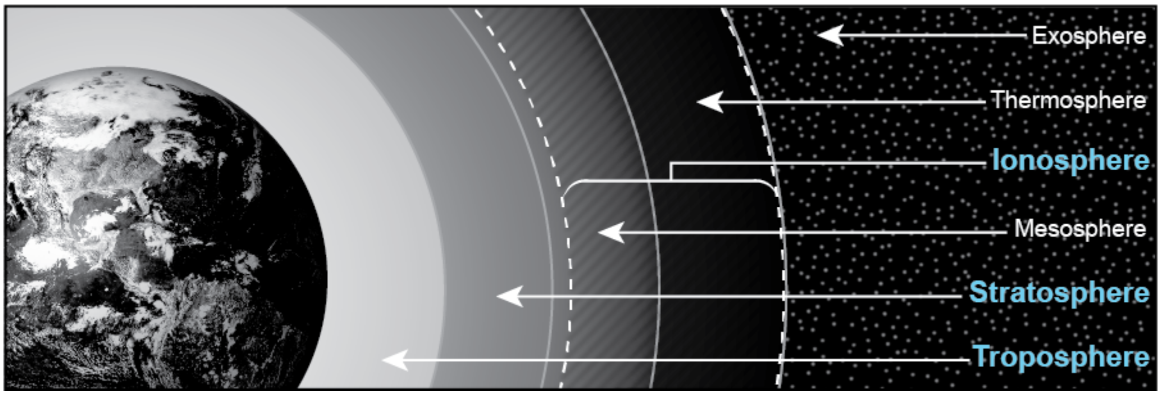


Figure 8-1. Layers of the Earth's atmosphere

Space Weather

8-27. *Space weather* is the conditions and phenomena in space and specifically in the near-Earth environment that may affect space assets or space operations (JP 3-59). Space weather is the variation in the space environment driven primarily by changes in the solar emissions of the Sun. As the understanding of space weather has increased, military considerations for space weather conditions and the implications on operations have increased as well. Intelligence officers must understand the possible or probable effects of space weather in a given timeframe to identify when mitigation strategies are needed. This becomes more evident when understanding the interdependence of domains and how space-based capabilities support operations across multiple domains. Although space support elements may not reside at all echelons, it is important to consider relevant information they must provide during IPB.

8-28. Space weather information should be integrated into the planning process to enable commanders to anticipate space weather impacts to friendly and threat systems and to exploit this information to optimize current and future operations. In coordination with the G-2/S-2 and the Air Force staff weather officer, the Army space support team provides space situational awareness to the commander and staff through the daily space brief. Changes in the status of space assets that yield operational implications according to the commander's critical information requirements are reported immediately.

8-29. The G-2/S-2, in coordination with the Army space support team and the Air Force staff weather officer, provides tailored weather effects from the surface to space on both space assets and Army operations, and integrates this information into the IPB process, mission command, MDMP, and risk management to enable situational understanding and decision making. The G-2/S-2 provides situational awareness on the weather effects from the surface to space, include but not limited to—

- Determining how weather effects could impact the supported unit, threat systems, operations, plans, and anticipated COAs.
- Identifying space-based alternatives and coordinating their usage with the appropriate staff.
- Monitoring the health and status of the Global Positioning System constellation, and potential effects of space weather.
- Providing updates on scintillation for ultrahigh frequency and high frequency propagation.

Space Weather Effects

8-30. Space weather phenomena are disturbances that can significantly degrade or effectively eliminate—for relatively short timeframes (several minutes to a few hours)—military space-based capabilities. Sources of space weather effects include but are not limited to the following space weather phenomena:

- **X-rays, electronic ultraviolet radiation, and radio bursts** from the Sun arrive at the Earth in approximately eight minutes, normally last one to two hours, and may result in the following effects: satellite communications interference, radar interference, high frequency radio blackout, geolocation errors, and satellite orbit decay.
- **Energetic particle events** arrive at the Earth from the Sun in 15 minutes to a period of hours, last days, and may result in the following effects: high altitude radiation hazards, spacecraft damage, satellite disorientation, launch payload failure, false sensor readings, and degraded high frequency communications (high latitudes).
- **Scintillation** occurs daily, lasts four to six hours following sunset and may result in the following: degraded satellite communications and Global Positioning System errors (position, navigation, and timing).
- **Geomagnetic storms** on the Sun arrive at the Earth in one to three days, last days, and may result in the following: spacecraft charging and drag, geolocation errors, space track errors, launch trajectory errors, radar interference, radio propagation anomalies, and power grid failures.

DETERMINING RELEVANT ASPECTS OF THE SPACE DOMAIN

8-31. During step 1 of the IPB process, intelligence staffs determine if there are relevant aspects of the space domain—ranging from environmental impacts on space platforms needed to provide information collection capabilities, to threat capabilities directed against friendly space systems—that must be considered for the mission. To determine relevant aspects that can affect capabilities provided through the space domain, intelligence staffs must understand the following space domain-related terms:

- **Orbital mechanics** describes the orbit a satellite moves in space.
- **Propagation** is the spread of radio signals through the EMS to and from the Earth to orbiting satellites.
- **Orbital density and debris** pertain to the number of satellites and amount of space debris in the same orbital path.
- **Solar and geomagnetic activity** pertains to atmospheric activity that has the ability to impact radio wave propagation.
- **EMS dependency** describes radio wave frequency and amplitude as it moves within through space and the characteristics that determine radio wave propagation.

8-32. See ATP 2-22.6-2 for detailed information on these space domain-related terms.

CYBERSPACE DOMAIN

8-33. *Cyberspace* is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12). The cyberspace domain is an essential part of the information environment. It can be used by nation-states and a variety of actors unable or unwilling to commit to military confrontation. Since multiple entities (military, government, economic sectors) worldwide depend on the cyberspace domain for information exchange, this domain must be considered during IPB.

Note. The IPB process remains unchanged in its framework when analyzing any of the domains of the OE. However, there are unique aspects that should be considered when analyzing the cyberspace domain. (For considerations unique to the cyberspace domain, see appendix D.)

THE INFORMATION ENVIRONMENT

8-34. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). Although defined separately, the information environment and OE are interdependent and integral to each other. A unit’s information operations officer or designated representative supports IPB with a specific focus on the information environment. (See FM 3-13 and ATP 3-13.1 for a detailed discussion on information operations considerations for IPB.)

8-35. The information environment consists of three interrelated dimensions—physical, informational, and cognitive. Cyberspace, a significant component of the information environment, overlaps the physical and informational dimensions. The IPB process must determine a threat’s capabilities to operate in each of these dimensions of the command’s battlefield:

- **Physical dimension** comprises C2 systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It includes but is not limited to people, computers, smart phones, and newspapers.
- **Informational dimension** encompasses where and how information is collected, processed, stored, disseminated, and protected. It includes but is not limited to C2 systems, knowledge management TTP, and physical and operational security policies. A key aspect of this dimension is determining where, how, and when friendly, neutral, and threat information and information systems will be vulnerable to exploitation and attack.

- **Cognitive dimension** encompasses the minds of those who transmit, receive, and respond to or act on information. It includes but is not limited to cultural norms, perspectives, beliefs, and ideologies.

8-36. Table 8-1 provides IPB considerations for the information environment. It assists in organizing where and how information and information capabilities reside, are employed, and disseminated.

Table 8-1. IPB considerations for the information environment

Informational aspects relevant to friendly forces
• Those that enable friendly capabilities, including each warfighting function. • Where, how, and when information can be employed to support operations. ***Note.*** This is not just outward application of capabilities; it includes knowledge management, information assurance, information security, operations security, as well as how the command leverages information to enable the staff and maneuver units to achieve the mission. • Where, how, and when friendly information and information systems will be vulnerable to exploitation and attack by others. • Identifying components of information infrastructure or nodes of information systems that must be destroyed, disabled, or left in place.
Informational aspects relevant to neutral forces
• Where, how, and when information can be employed to support operations. • Those that enable neutral capabilities, including each warfighting function or system. ***Note.*** Analysts should avoid putting U.S. architectures (warfighting functions) on other force's constructs as this may create a gap in analysis. • Where, how, and when neutral information and information systems will be vulnerable to exploitation and attack by others. • Identifying components of information infrastructure or nodes of information systems that neutral forces will consider for destruction and disablement, or will leave in place.
Informational aspects relevant to threat forces
• Where, how, and when information can be employed to support threat operations. • Those that enable threat capabilities, including each warfighting function or system. • Where, how, and when threat information and information systems will be vulnerable to exploitation and attack by others. • Identifying components of information infrastructure or nodes of information systems that threat forces will consider for destruction and/or disablement, or will leave in place.
Informational aspects relevant to populations
• Information capabilities that enable population support systems. • Sources of information that inform and influence decisions.

THE ELECTROMAGNETIC SPECTRUM

8-37. The *electromagnetic spectrum* is the entire range of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (JP 3-13.1). The EMS is a continuum of all electromagnetic waves arranged according to frequency and wavelength. The frequency range suitable for radio transmission (the radio spectrum) extends from 10 kilohertz to 300,000 megahertz, which is divided into a number of bands. Below the radio frequency spectrum, and overlapping it, is the audio frequency band, extending from 20 to 20,000 hertz. Above the radio frequency spectrum are heat and infrared, the optical (visible) spectrum (light in its various colors), ultra-violet rays, x-rays, and gamma rays. Within the radio frequency range, from 1 to 40 gigahertz (1,000 to 40,000 megahertz), between the ultrahigh frequency and extremely high frequency are additional bands, defined as follows:

- L band: 1 to 2 gigahertz.
- S band: 2 to 4 gigahertz.
- C band: 4 to 8 gigahertz.
- X band: 8 to 12 gigahertz.
- Ku band: 12 to 18 gigahertz.
- K band: 18 to 27 gigahertz.
- Ka band: 27 to 40 gigahertz.

8-38. Maritime radar systems commonly operate in the S and X bands, while satellite navigation system signals are found in the L band. The break of the K band into lower and upper ranges is necessary because the resonant frequency of water vapor occurs in the middle region of this band, and severe absorption of radio waves occurs in this part of the spectrum.

8-39. EMS-based operations must be understood to accurately depict possible threat COAs and how these COAs may impact friendly operations. EMS effects and the systems that use the EMS are critical IPB considerations that highlight the multi-domain nature of friendly and threat operations. Although interrelated by the EMS, each domain has different functions and objectives.

8-40. SIGINT, cyberspace operations, EW, and spectrum management operations all operate within the EMS. When performing IPB, considering the EMS maximizes the employment of friendly SIGINT and EW assets by providing direction to the collection management effort, electronic node analysis, and decision making, as well as a thorough understanding of the threat's communications and SIGINT and EW asset noncommunications, electronic surveillance, and electronic countermeasure capabilities.

8-41. SIGINT is the interception and collection of signals in the EMS. *Electronic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). SIGINT and EW information is integrated into the threat, situation, and event templates developed during the IPB process and the DST developed during the MDMP. These templates graphically portray threat dispositions, vulnerabilities, and capabilities, including capabilities to employ electronic systems throughout the AO for electronic countermeasures, C2, target acquisition, maneuver, and CAS and airspace management. (See ATP 2-22.6-2 and ATP 3-36 for more in SIGINT and EW, respectively.)

8-42. EMS considerations are integrated into DSTs during the MDMP to assist commanders and staffs in the decision-making process by depicting critical points on the battlefield and identifying HPTs, which, when exploited, provide friendly forces with an advantage. The intelligence staff integrates electronic data into the IPB process to verify threat unit identification, locations, and types and sizes.

8-43. The intelligence staff conducts the initial electronic data assessment, to include developing the intelligence portion of the DST. The EW officer integrates SIGINT and EW information into the DST with enough detail to satisfy targeting priorities and determine the effectiveness of threat EW systems. The DST, together with the MCOO, is forwarded to subordinate elements, where they are further refined to meet functional mission requirements.

Appendix A

Intelligence Staff Officer IPB Checklist

A-1. Each step of the IPB process consists of several principal judgment decisions and evaluations that together form the basic *how to* of IPB. Table A-1 outlines the *how to* of IPB as a checklist for the S-2.

Table A-1. Intelligence staff officer IPB checklist

Step 1—Define the operational environment
□ Identify the limits of the commander's area of operations □ Generally identified by higher headquarters
□ Identify the limits of the commander's area of interest: □ S-2 recommends any changes □ Commander approves/disapproves □ higher headquarters approves/disapproves
□ Identify significant characteristics within the area of operations and area of interest for further analysis: □ Enemy □ Terrain □ Weather □ Civil considerations
□ Evaluate current operations and intelligence holdings to determine additional information needed to complete IPB: □ Staff identifies information gaps □ Staff develops assumptions for information gaps
□ Initiate process necessary to acquire the information needed to complete IPB: □ Staff sections submit requests for information and information collection.
Note. An operational environment encompasses the air, land, maritime, space, and cyberspace domains, the information environment (which includes cyberspace), the electromagnetic spectrum, and other factors. IPB applies to the full range of Army operations. When defining the operational environment, it is important to consider all domains in which Army and threat operations occur.
Step 2—Describe environmental effects on operations
□ Describe how the threat can affect friendly operations (IPB products—threat overlay, threat description table): □ Regular □ Irregular □ Hybrid
□ Describe how terrain (OAKOC) can affect friendly and threat operations (IPB products—MCOO, terrain effects matrix) □ Observation and fields of fire □ Avenue of approach □ Key terrain □ Obstacles □ Cover and concealment
□ Describe how weather can affect friendly and threat operations (IPB products—operational climatology, light and illumination data table, weather effects matrix): □ Visibility □ Precipitation □ Temperature □ Atmospheric pressure □ Wind □ Cloud cover □ Humidity
□ Describe how civil considerations (ASCOPE and PMESII-PT) can affect friendly and threat operations (IPB products—civil considerations data file, civil considerations overlay, civil considerations assessment): □ Areas □ Structures □ Capabilities □ Organizations □ People □ Events □ Political □ Military □ Economic □ Social □ Information □ Infrastructure □ Physical environment □ Time
Step 3—Evaluate the threat
□ Identify threat characteristics (IPB products—threat characteristics files)
□ Create or refine threat models (IPB products—threat template, high-value target list): □ Convert threat doctrine or patterns of operation to graphics □ Describe the threat's tactics, options, and peculiarities □ Identify high-value targets
□ Identify threat capabilities (IPB products—threat capability statement): □ Identify threat capabilities by using statements □ Identify other threat capabilities
Step 4—Determine threat COAs
□ Develop threat COAs (IPB products—situation template, threat COA statement)
□ Develop the event template and matrix (IPB products—event template, event matrix)
COA course of action G-3 assistant chief of staff, operations IPB intelligence preparation of the battlefield MCOO modified combined obstacle overlay S-2 battalion or brigade intelligence staff officer S-3 battalion or brigade operations staff officer

This page intentionally left blank.

Appendix B

Tools for Use During IPB

B-1. When conducting IPB, analysts should strive to collect the most accurate and current information on the OE. This requires extensive research and analysis. If the data is unavailable, tables B-1 through B-11 should provide analysts a firm starting point for creating an IPB product.

> ***Note.*** These tables should be used as a last resort, and only when better and timely information is not available.

Table B-1. Height of eye versus horizon range

Height (feet)	*Nautical miles*	*Statute miles*	*Height (feet)*	*Nautical miles*	*Statute miles*	*Height (feet)*	*Nautical miles*	*Statute miles*
1	1.1	1.3	120	12.5	14.4	940	35.1	40.4
2	1.6	1.9	125	12.8	14.7	960	35.4	40.8
3	2.0	2.3	130	13.0	15.0	980	35.8	41.8
4	2.0	2.6	135	13.3	15.3	1000	36.2	42.8
5	2.6	2.9	140	13.6	15.6	1100	37.9	43.7
6	2.8	3.2	145	13.8	15.9	1200	39.6	45.6
7	3.0	3.5	150	14.0	16.1	1300	41.2	47.8
8	3.2	3.4	160	14.5	16.7	1400	43.8	49.8
9	3.4	4.0	170	14.9	17.2	1500	44.8	52.0
10	3.6	4.2	180	15.3	17.7	1600	45.8	52.8
11	3.8	4.4	190	15.8	18.2	1700	47.2	54.8
12	4.0	4.6	200	16.2	18.6	1800	48.5	55.9
13	4.1	4.7	210	16.6	19.1	1900	49.9	57.8
14	4.9	4.9	220	17.0	19.5	2000	51.2	58.9
15	5.1	5.1	230	17.3	20.0	2100	52.4	60.4
16	4.6	5.3	240	17.7	20.4	2200	53.7	61.8
17	4.7	5.4	250	18.1	20.8	2300	54.9	63.2
18	4.9	5.6	260	18.4	21.2	2400	56.0	54.8
19	5.0	5.7	270	18.8	21.6	2500	57.2	65.8
20	5.1	5.9	280	19.1	22.0	2600	58.3	57.2
21	5.2	6.0	290	19.5	22.4	2700	59.4	68.4
22	5.4	6.2	300	19.8	22.8	2800	60.5	69.7
23	5.5	6.3	310	20.1	23.2	2900	61.6	70.9
24	5.6	6.5	320	20.5	23.6	3000	62.7	72.1
25	5.7	6.6	330	20.8	23.9	3100	63.7	73.3
26	5.8	6.7	340	21.1	24.3	3200	34.7	74.5
27	5.9	6.8	350	21.4	24.6	3300	65.7	75.7
28	6.1	7.0	360	21.7	25.0	3400	66.7	76.8
29	6.2	7.1	370	22.0	25.3	3500	67.7	77.8
30	6.3	7.2	380	22.3	25.7	3600	68.6	79.0

Table B-1. Height of eye versus horizon range (*continued*)

Height (feet)	*Nautical miles*	*Statute miles*	*Height (feet)*	*Nautical miles*	*Statute miles*	*Height (feet)*	*Nautical miles*	*Statute miles*
31	6.4	7.3	390	22.6	26.0	3700	69.6	80.1
32	6.5	7.5	400	22.9	26.3	3800	70.5	81.3
33	6.6	7.6	410	23.2	26.7	3900	71.4	82.3
34	6.7	7.7	420	23.4	27.0	4000	72.4	83.3
35	6.8	7.8	430	23.7	27.3	4100	73.3	84.3
36	6.9	7.9	440	24.0	27.6	4200	74.1	85.4
37	7.0	8.0	450	24.3	27.9	4300	75.0	86.4
38	7.1	8.1	460	24.5	28.2	4400	75.9	87.4
39	7.1	8.2	470	24.8	28.6	4500	76.7	88.4
40	7.2	8.3	480	25.1	28.9	4600	77.6	89.3
41	7.3	8.4	490	25.3	29.2	4700	78.4	90.3
42	7.4	8.5	500	25.6	29.4	4800	49.3	91.2
43	7.5	8.6	520	26.1	30.0	4900	80.1	92.2
44	7.6	8.7	540	26.6	30.6	5000	80.9	93.1
45	7.7	8.8	560	27.1	31.2	6000	88.6	102.0
46	7.8	8.9	580	27.6	31.7	7000	95.7	110.9
47	7.8	9.0	600	28.0	32.3	8000	102.3	117.8
48	7.9	9.1	620	28.5	32.8	9000	108.5	124.8
49	8.0	9.2	640	28.9	33.3	10000	114.4	131.7
50	8.1	9.3	660	29.4	33.8	15000	140.0	161.3
55	8.5	9.8	680	29.8	34.3	20000	161.8	186.3
60	8.9	10.2	700	30.1	34.8	25000	180.9	208.2
65	9.2	10.6	720	30.7	35.3	30000	198.1	228.1
70	9.6	11.0	740	31.1	35.8	35000	210.0	246.4
75	9.9	11.4	760	31.5	36.3	40000	228.8	263.8
80	10.2	11.8	780	31.9	36.8	45000	242.7	279.4
85	10.5	12.1	800	32.4	37.3	50000	255.8	294.5
90	10.9	12.5	820	32.8	37.7	60000	280.2	322.8
95	11.2	12.8	840	33.2	38.2	70000	302.7	345.4
100	11.4	13.2	860	33.5	38.6	80000	322.6	372.5
105	11.7	13.5	880	33.9	39.1	90000	342.2	395.1
110	12.0	13.8	900	34.3	39.5	100000	361.8	416.5
115	12.3	14.1	920	34.7	39.9	200000	511.6	560.0

Table B-2. Terrain types for mechanized or armored forces

Terrain type	*Slope (%)*	*Streams*			*Vegetation*			*Typical seeds (unopposed) (km/hour)*
		Depth (feet)	*Current (feet/sec)*	*Width (feet)*	*Spacing (feet)*	*Trunk diameter (inches)*	*Roads/ Trails (per km)*	
Unrestricted	< 30	< 2	-----	< 5	> 20	< 2	2/4	24
Restricted	30 to 45	2 to 4	< 5	< AVLB length	< 20	2 to 6	1/2	16 (8 at night)
Severely restricted	> 45	> 4	> 5	> AVLB length	< 20	> 6	0/< 2	1 (.4 at night)

AVLB armored vehicle-launched bridge
km kilometer
sec second

Table B-3. Cover from flat trajectory weapons

Parameter	*Factor*	*Criteria (percent)*
Good	Slope	> 30
	Canopy closure	> 50*
	Roof coverage	> 40
Fair	Slope	10 to 30
	Canopy closure	< 50
	Roof coverage**	20 to 40
Poor	Slope	< 10
	Nonforested	
	Roof coverage**	< 20

* Or stem spacing 5 meters
** If evaluated

Table B-4. Concealment from aerial detection and percentage of roof coverage

Roof coverage (percentage)	*Category*	*Concealment*
75 to 100	Congested	Excellent
50 to 75	Dense	Good
25 to 50	Moderate	Fair
5 to 25	Sparse	Poor
0 to 5	Open	None

Table B-5. Port categories

Category	*Vessel*	*Water depth (meters)*	*Other (meters)*
Deep draft*	Naval	10	
	Container	10 to 15	
	Bulk carrier	12 to 18	
	Tankers	10 to 28	
Shallow draft**	Lash	2	3
	Seabee	3.4	31
	Barge	38	38

* Each vessel hatch requires 30 meters of wharf space, with the wharf at least 30-meters wide.
** The wharf length must be 12 meters.

Table B-6. Minimum helipad and heliport requirements

Landing pad					*Runway***		
Helipad or heliport type	*Length (feet)*	*Width (feet)*	*Shoulder width (feet)*	*Taxi/ Hover lane* width (feet)*	*Length (feet)*	*Width (feet)*	*Shoulder width (feet)*
Close battle area							
OH-6A	12	12	N/A	75	N/A	N/A	N/A
OH-58	12	12	N/A	75	N/A	N/A	N/A
AH-64	20	20	N/A	140	N/A	N/A	N/A
UH-1H	20	20	N/A	140	N/A	N/A	N/A
UH-60	20	20	N/A	140	N/A	N/A	N/A
CH-47	50	25	N/A	180	N/A	N/A	N/A
CH-54	50	50	N/A	200	N/A	N/A	N/A

Table B-6. Minimum helipad and heliport requirements (*continued*)

Landing pad					*Runway***		
Helipad or heliport type	***Length (feet)***	***Width (feet)***	***Shoulder width (feet)***	***Taxi/ Hover lane* width (feet)***	***Length (feet)***	***Width (feet)***	***Shoulder width (feet)***
Support area							
OH-6A	12	12	10	100	N/A	N/A	N/A
OH-58	12	12	10	100	N/A	N/A	N/A
AH-64	20	20	10	200	N/A	N/A	N/A
UH-1H	20	20	10	200	N/A	N/A	N/A
UH-60	20	20	10	200	N/A	N/A	N/A
CH-47	50	25	10	240	450	25	10
CH-54	50	50	10	250	450	50	10
Rear area							
OH-6A	25	25	25	100	N/A	N/A	N/A
OH-58	25	25	25	100	N/A	N/A	N/A
AH-64	40	40	25	200	N/A	N/A	N/A
UH-1H	40	40	25	200	N/A	N/A	N/A
UH-60	40	40	25	200	N/A	N/A	N/A
CH-47	100	50	25	240	450	40	25
CH-54	100	100	25	250	450	60	25

* Taxi/Hover lane is used for takeoff and landing where provided; length is variable.
** Where runway is not shown, takeoff and landing are on taxi/hover lane.

N/A not applicable

Table B-7. Factors of foot marches for typical dismounted units

Basic data table, foot marches				
Terrain	**Visibility**	**Rate of march* (kilometers/hour)**	**Normal march (8 hours) (kilometers)**	**Forced march (12 hours) (kilometers)**
Roads	Day	4	32	48
	Night	3	24	36
Cross-country	Day	2	16	24
	Night	1	8	12

* Computed on a 50-minute hour, allowing for a 10-minute halt each hour.

Length of column, factor table, foot marches*		
Formation**	**2 meters/person distance**	**5 meters/person distance**
Single file	2.4	5.4
Column of twos	1.2	2.7

* To determine the length of a column occupied by a dismounted unit, multiply the estimated or known number of personnel by the applicable factor.
** Foot marches vary with the tactical situation; normal formation is a column of twos with a file on either side of the road and staggered, much like U.S. forces. However, columns of threes and fours may be employed where conditions permit.

Pass time factors, foot marches*	
Rate (kilometer/hour)	**Factor**
4	0.015
3	0.018
2	0.020
1	0.023

*To determine the pass time in minutes for a dismounted unit, multiply the length of the column by the appropriate factor for the estimated or known rate of march.

Table B-8. Unopposed movement planning speeds for U.S. and opposition forces

A. United States movement speeds	
1. Maximum road speeds (day):	
• M1/M2/M3 = 70 kilometers/hour • M113/M901 = 40 kilometers/hour • Wheeled vehicle on road = 80 kilometers/hour	• Wheeled vehicle off road = 10 kilometers/hour • Cross-country movement speed = 30 kilometers/hour
2. Maximum road speeds (night):	
• M1A1/M1A2/M3 = 45 kilometers/hour • M113/M901 = 30 kilometers/hour • Wheeled vehicle on road = 10 kilometers/hour	• Wheeled vehicle off road = 6 kilometers/hour • Cross-country movement speed = 18 to 20 kilometers/hour
B. Opposition forces movement speeds	
1. Day:	
• Maximum speed = 30 kilometers/hour	• Average speed off road = 20 kilometers/hour
2. Night:	
• Maximum speed = 20 kilometers/hour	• Average speed off road = 10 kilometers/hour
C. Aircraft movement speeds	
• Rotary-wing flight speed = 150 kilometers/hour	• Fixed-wing = 500 knots
D. Dismounted movement speeds	
Dismounted rate = 3 kilometers/hour	

Table B-9. Movement conversion

Movement rates										
Time (minutes)										
Rate of march (kilometers/hour)	**Distance (meters)**									
	1,000	**2,000**	**3,000**	**4,000**	**5,000**	**6,000**	**7,000**	**8,000**	**9,000**	**10,000**
60	1	2	3	4	5	6	7	8	9	10
50	1.2	2.4	3.6	4.8	6	7.2	8.4	9.6	10.8	12
40	1.5	3	4.5	6	7.5	9	10.5	12	13.5	15
30	2	4	6	8	10	12	14	16	18	20
25	2.4	4.8	7.2	9.6	12	14.4	16.8	19.2	21.6	24
20	3	6	9	12	15	18	21	24	27	30
15	4	8	12	16	20	24	28	32	36	40
10	6	12	18	24	30	36	42	48	54	60
5	12	24	36	48	60	72	84	96	108	120

Movement rates reduced to minutes				
(kilometers/hour)	**(meters/minute)**	**(miles/hour)**	**(knots)**	**(feet/second)**
60	1000	37	32	55
50	833	31	27	46
40	667	25	22	36
30	500	19	16	27
25	417	16	13	23
20	333	12	11	18
15	250	9	8	14
10	167	6	5	9
5	83	3	3	5
1	17	0.6	0.5	0.9

Note. Tables B-10 and B-11 are examples; they should only be used when more accurate information is not available.

Table B-10. Example of typical Soviet style frontages and depths for units (defense)

	Division (kilometers)	*Brigade/Regiment (kilometers)*	*Battalion (kilometers)*	*Company/Team (kilometers)*
Frontage	20 to 30	10 to 15	3 to 5	0.5 to 1
Depth	15 to 20	7 to 10	2 to 3	0.5
Gaps between units			0.5 to 2	0.5 to 1.5
Note. Tanks may deploy 200 to 300 meters apart and armored personnel carriers up to 200 meters apart. Antitank obstacles are placed so that they are covered by direct fire.				

Table B-11. Example of typical Soviet style frontages and depths of objectives (offense)

	Army (kilometers)	*Division (kilometers)*	*Brigade/Regiment (kilometers)*	*Battalion (kilometers)*
Zone of attack	60 to 100	15 to 25	8 to 15	2 to 3
Main attack axis	35 to 45	6 to 10	3 to 5	1 to 2
Immediate objective depth	100 to 150	20 to 30	8 to 15	2 to 4
Subsequent objective depth	250 to 350	50 to 70	20 to 30	8 to 15
Note. These figures will vary with the tactical situation and terrain.				

B-2. Analyzing weather data is an important aspect of the IPB process. Table B-12 provides an example of weather data information and how it can affect operation systems on the battlefield.

Note. Table B-12 is an example; it should only be used when more accurate information is not available.

Table B-12. Environmental mission-limiting thresholds

Operation/System	*Favorable (no degradation)*	*Marginal (some degradation)*	*Unfavorable (significant degradation)*
Rotary wing (helicopter)			
Ceiling/Visibility	≥ 1000 feet and/or 2 SM (400 m)		≤ 500 feet and/or ½ SM (800 m)
Weather/Precipitation	None	Blowing sand	Thunderstorms or freezing precipitation
Wind speed	< 35 knots		≥ 45 knots
Density altitude	< 5000 feet		≥ 6000 knots
Turbulence	None to light (category II)	Moderate (category II)	Severe (category II)
Icing	None – light	Moderate	Severe
Unmanned aircraft systems			
Ceiling/Visibility	≥ 3000 feet and/or 3 SM (4800 m)		< 3000 feet and/or 3 SM (4800 m)
Weather/Precipitation	None	Light to moderate	Heavy precipitation, thunderstorms, or freezing precipitation
Wind speed	< 25 knots		≥ 45 knots
Turbulence	None to light (category I)	Moderate (category I)	Severe (category I)
Icing	None		Any

Table B-12. Environmental mission-limiting thresholds (*continued*)

Operation/System	*Favorable (no degradation)*	*Marginal (some degradation)*	*Unfavorable (significant degradation)*
Close air support			
Ceiling/Visibility	≥ 10000 feet and/or 3 SM (4800 m)		≤ 5000 feet and/or 3 SM (4800 m)
Weather/Precipitation		Thunderstorms/blowing sand	
Air interdiction			
Ceiling/Visibility	≥ 300 feet and/or ¼ SM (400 m)		≤ 300 feet and/or ¼ SM (400 m)
Aerial reconnaissance			
Ceiling/Visibility	≥ 5000 feet and/or 3 SM (4800 m)		≤ 1000 feet and/or 1600 m
Weather/Precipitation	None	Blowing sand	Thunderstorms
Wind speed	< 60 knots		≥ 60 knots
Icing	None	Trace	Light to severe
Night vision goggles			
Cloud cover or ceiling	< 50% or ≥ 300 feet	≥ 50% or < 3000 feet	
Visibility	≥ ½ SM (800 m)	< ½ SM (800 m)	
Precipitation	Light to moderate	Heavy	
Temperature	33°F to 124°F	≥ 125°F to < 33°F	
Smoke			
Precipitation	None	Light to moderate	Severe
Temperature	< 80°F		> 120°F
Nuclear, biological, chemical			
Ceiling and/or temperature	> 600 feet and/or 86°F to 32°F	< 600 feet and/or > 86°F	< -15°F
Precipitation	None	Light	Moderate
Low-level inversion and/or stability	Yes or stable	No or unstable	
Wind speed	0 to 9 knots		> 20 knots
Personnel			
Temperature or heat index	84°F to 33°F	> 85°F or < 33°F	> 95°F or < -40°F
Wind chill	> 15°F		< -25°F
Weather/precipitation	Light liquid or snow	Moderate or freezing drizzle	Heavy or freezing rain
Vehicles			
Snow depth	< 6 inches	< 12 inches	12 inches
Weather/precipitation	None or light	Moderate or light freezing rain	Heavy or moderate to heavy freezing rain
Temperature	104°F to 1°F	> 105°F or < 1°F	-53°F
Air defense artillery			
Ceiling and/or visibility	> 5000 feet and/or 1 SM (1600 m)		< 2500 feet and/or ½ SM (800 m)
Wind	< 35 knots		> 50 knots
Weather/precipitation	None to light	Blowing sand or dust	Heavy

Table B-12. Environmental mission-limiting thresholds (*continued*)

Operation/System	*Favorable (no degradation)*	*Marginal (some degradation)*	*Unfavorable (significant degradation)*
Visual systems			
Visibility and/or weather	> 2 SM (3200 m) and/or light precipitation		> 5/8 SM (1000 m) and/or heavy precipitation
Temperature or relative humidity (RH)	< 100°F or RH < 80%	≥ 100°F or < -25°F or RH ≥ 80%	
Infrared sensors			
Visibility and/or weather/precipitation	≥ 2 SM (3200 m) and/or light precipitation	< 2 SM (3200 m) and/or moderate precipitation	Heavy precipitation and/or fog and/or blowing sand and/or snow
Temperature or RH	125°F to 20°F or RH < 80%		> 125°F or < -25°F or RH > 85%
°F degrees Fahrenheit	m meter	SM statute mile	

B-3. Tables B-13 through B-17 provide additional tools that can be useful when completing the IPB process.

Table B-13. Maximum ranges for the identification of select targets

Targets	*Meters*	
	Naked eye	**Magnification power of 7.8x**
Tank crew members, troops, machine guns, mortars, antitank guns, antitank missile launchers	500	2000
Tank, armored personnel carriers, truck (by model)	1000	4000
Tank, howitzer, armored personnel carriers, rucks	1500	5000
Armored vehicles, wheeled vehicles	2000	6000

Table B-14. Minimum airfield requirements

Airfield type	*Runway length (feet)*	*Runway width (feet)*	*Runway shoulder width (feet)*	*Total aircraft traffic area* (1,000 square feet)*
Battle area				
Light lift and medium lift	2000	60	10	223
Forward area				
Liaison	1000	50	N/A	37.5
Surveillance	2500	60	10	337
Light lift and medium lift	2500	60	10	358
Support area				
Liaison	1000	50	N/A	50
Surveillance	3000	60	10	490
Light lift and medium lift	3500	60	10	753.5
Heavy lift	6000	100	10	1421
Tactical	5000	60	4	1071
Rear area				
Army	3000	72	10	882
Medium lift	6000	72	10	2362
Heavy lift	10000	156	10	3926
Tactical	8000	108	20	1989
* This area includes parking, runway, taxiway, and warm-up apron.				

Table B-15. Typical planning force ratios

Force ratio (friendly:enemy)	*Typical mission*
1:7	Delay
1:3	Defend (prepared)
1:2.5	Defend (hasty)
2.5:1	Attack (hasty positions)
3:1	Attack (prepared position)
1:1	Counterattack (flank)

Table B-16. Traffic flow capability based on route width

	Limited access	*Single lane*	*Single flow*	*Double flow*
Wheeled	At least 3.5 meters	3.5 to 5.5 meters	5.5 to 7.3 meters	Over 7.3 meters
Tracked or a combination of vehicles	At least 4.0 meters	4.0 t o6.0 meters	6.0 to 8.0 meters	Over 8 meters
Note. See ATP 3-34.81 for more on traffic flow capability.				

B-4. AR 25-30 states that weights, distances, quantities, and measurements in Army publications must be expressed in both U.S. standard and metric units. Table B-17 is a metric conversion chart for the measurements in this publication.

Table B-17. Metric conversion chart

U.S. units	*Multiplied by*	*Equals metric units*
Feet	0.30480	Meters
Feet per second	18.2880	Meters per second
Inches	2.54000	Centimeters
Inches	0.02540	Meters
Inches	25.40010	Millimeters
Miles (statute)	1.60930	Kilometers
Pounds	453.59000	Grams
Pounds	0.45360	Kilograms
Pounds per square inch	6.9000	Kilopascal
Short tons	0.90700	Metric (long) tons
Square feet	0.09290	Square meters
Square inches	6.45160	Square centimeters
Square yards	0.83610	Square meters
Yards	0.91400	Meters
Centimeters	0.39370	Inches
Kilograms	2.20460	Pounds
Grams	0.0022046	Pounds
Kilometers	0.62137	Miles (statute)
Kilopascal	0.14493	Pounds per square inch
Meters	3.28080	Feet
Meters	39.37000	Inches
Meters	1.09360	Yards
Meters per second	3.28080	Feet per second
Metric (long) tons	1.10200	Short tons
Millimeters	0.03937	Inches
Square centimeters	0.15500	Square inches
Square meters	1.19600	Square yards
Square meters	10.76400	Square feet
U.S. United States		

This page intentionally left blank.

Appendix C

Threat Characteristics for Regular, Irregular, and Hybrid Threats

COMPOSITION

C-1. **Regular threat.** The identity and organization of 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 threat is organized around a central command structure, illustrated via organizational charts (see figures 5-2 and 5-3 on pages 5-5 and 5-6 respectively) that depict the number and types of units as well as the number and types of personnel, weapon systems, and equipment associated with these units.

C-2. **Irregular threat.** Determining the composition for irregular threats 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 military units).
- Echelons.
- Staff elements.
- Political, religious, ideological, and military aims.
- Internal and external C2.
- Operational organizations.
- Internal and external support structure.
- External ties.
- Assassination squads.
- Bomb and demolition squads.
- Attack or hit squads.

C-3. Irregular threats are usually armed military organizations or terrorist groups that have bypassed legitimate political authority and have taken up arms to pursue a common cause. Table C-1 lists and describes potential irregular threats. This table is not all-inclusive.

Table C-1. Description of potential irregular threats

Type	*Description*
Revolutionaries	Organizations involved in a revolution. These forces almost always have a political component that established its goals and objectives.
Guerrillas	Organizations that use unconventional tactics to combat regular forces that have an advantage in size, capability, and support.
Militia	Generally, a militia comprises ordinary citizens who have been organized for a specific purpose. This can include foreign nationals.
Partisans	General unconventional forces that oppose control of an area by a foreign power or by an army of occupation by insurgent activity.
Paramilitaries	Usually elements of a regular force using unconventional tactics to combat an occupying regular Army.
Terrorist groups	Organizations that target civilians and/or regular forces in order to gain political leverage and legitimacy.

Table C-1. Description of potential irregular threats (*continued*)

Type	*Description*
Insurgent organizations	Organizations that 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 may provide 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	Organizations that are 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. Through 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.

Note. To capitalize on perceived U.S. forces' vulnerabilities, nation-state actors can use proxy forces with an array of capabilities. (See paragraph 5-11 for more on proxy forces.)

C-4. **Hybrid threat.** A hybrid threat comprises two or more of the following entities that combine, associate, or affiliate to achieve mutually beneficial goals and objectives:

- A nation-state regular threat.
- A nation-state irregular threat.
- Insurgent organizations. (See table C-1)
- Guerilla units. (See table C-1.)
- Criminal organizations. (See table C-1.)

DISPOSITION

C-5. **Regular threat.** Disposition consists of the location of threat units and the way these units are tactically (or administratively in times of peace) deployed. Additionally, disposition includes recent, current, and proposed (or probable) movements of threat units. When evaluating a regular threat, disposition refers to—

- **Geographical location.** Location refers to a geographical area or position occupied by a unit or units. Knowledge of the strength and location of a threat assists the intelligence staff in determining the threat's capabilities and its effect on accomplishing the friendly mission. This type of data is collected during peacetime and forms the basis for accessing capabilities during the initial period of hostilities.
- **Tactical deployment.** Tactical deployment is the relative position of units—
    - **With respect to one another:** Tactical formations are designed for executing the various tactical maneuvers. If this deployment can be predetermined, it may lead to an accurate appraisal of intentions. The knowledge of how threat units are echeloned may indicate (if the threat assumes the offensive) which units will be used in the main attack and which units will be used in supporting reserve roles.
    - **With respect to terrain:** A study of dispositions and an analysis of the terrain assist in developing conclusions concerning threat capabilities, vulnerabilities, and intentions.

- **Movement of formations.** 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 threat. When a threat unit has moved, is moving, or will be moving, there are several actions that may affect the situation; for example, a unit may be moving into an attack position, or moving to reinforce or replace a unit, or performing other missions unknown to friendly forces. Considering these possibilities, the movement of threat units becomes important and units are monitored at all times so analysts can provide correct and detailed data on threat dispositions.

C-6. When evaluating a regular threat at any point before receipt of mission, intelligence staffs do not know the terrain on which the threat or friendly force operates. Therefore, arraying the threat on the battlefield as commonly seen on a situation template is not possible. However, it is possible to portray doctrinally how the threat arrays itself on the battlefield to conduct specific operations. This process is called threat templating, which is part of the threat model process. This ongoing process is part of garrison intelligence operations. Intelligence staffs at any echelon develop threat templates, which are reexamined and refined during IPB.

C-7. **Irregular threat.** For these threats, disposition includes recent, current, and projected movements or locations of tactical forces. Disposition consists of but is not limited to the geographic location of the following elements: safe houses, movement routes, training camps, base camps, logistics bases, and resupply points.

C-8. **Hybrid threat.** Currently, there are no threat models or templates developed for specific hybrid threats. However, TC 7-100.3 includes some basic attack and/or defense hybrid threat scenarios designed to support exercise design. These scenarios, along with focused research of real-world threat activity, can assist in developing threat templates.

STRENGTH

C-9. **Regular threat.** Strength for regular threats is described in terms of personnel, weapons, and equipment. The most important aspect of strength when evaluating a regular threat is determining whether the threat may conduct specific operations. For example, a unit may have adequate weapon systems to conduct an operation, but it may not have enough trained personnel or crews to man the systems or provide leadership to conduct certain operations.

C-10. **Irregular threat.** For irregular threats, strength is the capability of direct-action teams, political cadre or cells, and, most importantly, popular support. Popular support can range from but is not limited to—

- Storage or movement of combat equipment.
- Assistance in conducting operations.
- Logistics.
- Sympathizers.
- Providing or withholding information.

C-11. **Hybrid threat.** The strength of a hybrid threat is determined by understanding the synergy of regular and irregular threats. The hybrid threat understands that the environment that produces the most challenges to U.S. forces is one in which conventional military operations occur in concert with unconventional warfare. The hybrid threat concept is not one of only managing with what is available, but it is primarily one of deliberately created complexity.

C-12. Each component of the hybrid threat brings a capability to bear. The synergy of these capabilities is not to be understated. OEs by their very nature provide a myriad of complexities based on their characteristics and reliance on multiple domains. The hybrid threat seeks to introduce additional complexity by using an ever-shifting array of forces, technologies, domains, and techniques. A hybrid threat can switch the main effort (action element) between regular and irregular threats.

COMBAT EFFECTIVENESS

C-13. **Regular threat.** Assessing the following factors determines the combat effectiveness of regular threats:

- 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 logistics support of the unit.
- Adequacy of military schooling at all levels.
- National characteristics of the people.

C-14. **Irregular threat.** Combat effectiveness for irregular threats is measured differently from combat effectiveness for regular threats. The threat is motivated by many factors, including but not limited to a goal of independence, equality, religion, ideology, occupation by a foreign nation, or economics. Combat effectiveness is determined by, but not limited to—

- **External support (financial, physical, moral, information).** Often threats are interconnected to other transnational groups, organizations, or governments. Irregular threats may depend on this external support, which can noticeably increase their significance. External support can establish materiel (weapons and weapons technology) and financial resources (cash, commodities, services of value legally or illegally) to fund operations. The intended use of these resources is of greater significance than their inherent value.
- **Governance.** Threats may govern or contest for governance in areas where the legitimate government fails to or is failing to govern. Irregular threats may appeal to legitimate grievances against the government and use information to influence the population and international public opinion. These activities may enhance the threat's legitimacy and undermine the legitimacy of the legitimate government.
- **Popular support.** Threats rely on the population's support. This support can be tactic or explicit and can be produced through coercion or given freely. Resistance movements, undergrounds, and insurgencies are fairly well understood to require the support of the population to achieve their goals. Other irregular threats rely on the population's support as well. Sometimes this support stems from the population's culture or specific population segment. For example, criminal organizations (such as cartels, gangs, mobs, mafias, as well as related activities like trafficking, smuggling, racketeering) rely on the support of the local population to conduct operations.

C-15. **Hybrid threat.** The intelligence staff and other staff determine the combat effectiveness for hybrid threats by considering tangible and intangible factors associated with determining the combat effectiveness for regular and irregular threats.

DOCTRINE AND TACTICS

C-16. **Regular threat.** Doctrine and tactics for regular threats refer to the TTP that guide threat operations. Understanding how the threat prefers to operate aids the commander's understanding of potential threat COAs. TTP for regular threats can generally be grouped in the following categories:

- Offensive tasks: movement to contact, attack, exploitation, and pursuit.
- Defensive tasks: area defense, maneuver defense, retrograde.

C-17. **Irregular threat.** During the analysis of irregular threats, several factors that impact how they operate should be considered:

- What is the strategy? Is it a long-term or a specific model strategy?
- What principles do they use to organization their force? Is secrecy the highest priority requirement or is it the ability to mass capabilities quickly?
- Are political, military psychological, and economic effects considered during plan development? Are these the desired effects? Are they part of the overall strategy employed?
- Is there doctrine or use of doctrinal approaches? Is the doctrine based on training acquired while in service of another country? Is it based on published documents? Is the irregular threat required to follow the procedures of the supported force or government? Has the organization been conducting these types of operations for generations, and the required capabilities, skills, knowledge, and attributes are ingrained, keeping them successful for generations?

C-18. **Hybrid threat.** Threats to the United States and its allies employ hybrid threats as part of a sophisticated, comprehensive, and multidimensional strategy to achieve specific goals and objectives. The doctrine and tactics that guide hybrid threats are similar to Army doctrine and tactics in that strategic, operational, and tactical actions are coordinated to achieve objectives and end states.

C-19. Hybrid threat doctrine is based on countering a threat's capabilities. Hybrid threat often study U.S. and allied military forces and their operations and conduct lessons learned based on their assessments and perceptions. By studying and understanding U.S. and allied military force operations, hybrid threats seek to gain knowledge of when, where, and how to best use their capabilities to gain advantages in the OE.

C-20. Hybrid threats use nations they perceive as threats as baselines for planning adaptive approaches for dealing with the strengths and vulnerabilities of their threats. These hybrid threats 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 warfare aimed at the local population, international opinion, and their threats' domestic population.
- Change the nature of conflict.
- Allow no sanctuary.
- Employ operational exclusion.
- Employ operational shielding.
- Avoid defeat and preserve combat power by evading detection and decisive engagement.

SUPPORT AND RELATIONSHIPS

C-21. **Regular threat.** The location of a regular threat's logistics support structure elements assists intelligence staffs in determining the disposition of maneuver formations. Logistics information critical for effective intelligence analysis includes but is not limited to—

- 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.

C-22. **Irregular threat.** 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 support components include but are not limited to—

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

C-23. **Hybrid threat.** Hybrid threats incorporate the types of support that irregular threats use for sustainment with the traditional logistical support associated with conventional military operations. Because a hybrid threat is a composite of many different groups, these groups often have no standard, readily identifiable organizational relationship. What unites the capabilities and intent of the of the hybrid threat groups is a common purpose—typically opposition to U.S. goals. This unity of purpose can even unite groups that normally would be fighting among themselves.

C-24. Affiliated organizations cooperate 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. Affiliated forces are those irregular threats operating in a military unit's AO such that the unit may be able to sufficiently influence the threats to cooperate with it for a limited time. No command relationship exists between an affiliated force 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

C-25. **Regular threat.** For regular threats, this data also includes critical threat communications nodes such as command posts and logistical control points. This information supports threat templating. With electronic technical data—

- A more accurate evaluation of the threat's vulnerability to electronic countermeasures and deception is made.
- Signals intercept and direction finding for the production of SIGINT is facilitated.
- Support is given to counter threat EW by assessing the threat's EW capabilities.

C-26. **Irregular threat.** When evaluating irregular threats, the lack of a formal organizational structure or architecture impedes developing extensive threat communications network diagrams and an electronic technical database. Available communications range from modern technologies to the most nontechnical, both of which include but are not limited to—

- Radio sets.
- Cellular and satellite phones.
- Military communications systems.
- Radar.
- Commercial and government postal systems.
- Internet.
- Face-to-face.
- Cut-outs.
- Dead-drops.
- Mail and couriers.

C-27. **Hybrid threat.** Hybrid threats employ a combination of capabilities used by regular and irregular threats. Identifying these systems and if and how the threat is overcoming interoperability challenges may provide insights into potential vulnerabilities.

CAPABILITIES AND LIMITATIONS

C-28. **Regular threat.** A regular threat is designed to attack or defend, as necessary, to accomplish objectives. Determining capabilities and limitations for a regular threat requires an understanding of the art and science of war, as well as an understanding of the threat force itself.

C-29. **Irregular threat.** The most challenging capability of an irregular threat is its ability to blend in with the population or to hide in complex terrain. This allows the threat to plan and prepare for an operation and attack at a time and place of its own choosing without interference from friendly forces.

C-30. **Hybrid threat.** From a friendly perspective, the most challenging capability of a hybrid threat is its ability to adapt and transition. The hybrid threat may emphasize speed, agility, versatility, and changeability as the keys to success in a fight against a larger, more powerful opponent or to engage a peer threat just below the threshold of armed conflict.

- **Adaptation.** Adaptation refers to the ability to adjust capabilities based on learning. Threats approach adaptation from two perspectives—natural and directed:
  - **Natural adaptation** occurs as a nation-state or nonstate actor 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 a competitor's strengths or relative position of advantage. Competitors and threats can learn by interacting with their counterparts and adapting their capabilities to seek a position of relative advantage for the next interaction. Like natural adaptation, directed adaptation informs issues of force design, military strategy, and operational designs.
- **Transition.** One of the most dangerous aspects of a hybrid threat is the ability of its components to transition in and out of various forms. Military forces, for example, can remove uniforms, insignias, and other indicators of status and blend in with the local population. Irregular threats might abandon weapons and protest innocence of wrongdoing. Criminals might impersonate local police forces to gain access to a key facility. Therefore, it is important for analysts to archive past TTP as references in data files for use when developing threat models.

C-31. The difficulty of positively identifying hybrid threats is advantageous to threats. OEs are replete with many actors conducting activities counter to U.S. interests. These actors do not have a clear visual signature regarding their status as threats. Often these actors provide signatures similar to friendly or neutral actors.

CURRENT OPERATIONS

C-32. **Regular threat.** The Army's knowledge of regular threats is based on its understanding of these threats before 11 September 2001 (referred to as 9/11). These threats have evolved as the Army has evolved. Intelligence staffs at all echelons continually study these threats to gain a better understanding of them.

C-33. **Irregular threat.** The Army gained valuable experience in combating irregular threats during Operation Iraqi Freedom and Operation Enduring Freedom. Thus, the Army has learned how diverse and adaptive these threats can be. It is unlikely that the irregular threats the Army will face will mirror those it fought in Iraq and Afghanistan. However, threats may have adopted effective tactics from those conflicts. To gain the best understanding of the evolving nature of irregular threats worldwide, intelligence staffs must analyze these threats whenever and wherever they appear.

C-34. **Hybrid threat.** Although the Army believes the primary threat it will face will come from hybrid threats, little is known about the character of these threats. Although the Army has developed a hybrid threat model for training combined arms teams, this model has limited value in preparing the intelligence staff to understand this threat. The current model is a generic construct that does not reflect the threat characteristics of any particular real-world threat. Therefore, intelligence staffs at all levels must continually study hybrid threats wherever they operate. Intelligence staffs must also study historical examples of hybrid threat operations.

HISTORICAL DATA

C-35. **Regular threat.** These threats develop attributes based on how they have been employed and on how they conducted themselves during those employments. While not definitive, understanding a unit's lineage may provide insight into the extent the unit will go to accomplish its objectives. This may also provide insight into what the unit will not do to accomplish its objectives.

C-36. **Irregular threat.** These threats also develop attributes based on how they have been employed on how they conducted themselves during those employments.

C-37. **Hybrid threat.** One result of current operations analysis is the historical record of hybrid threat operations and activities. However, history does provide examples of threats using hybrid approaches against a superior force.

Historical Examples of Hybrid Approaches

- 1754 to 1763—Regular British and French forces fought each other in North America. Irregular Colonial forces fought for the British, and American Indians fought for both sides.
- 1814—The Peninsular War ended after regular and irregular multinational forces from Britain, Portugal, and Spain prevented France from controlling the Iberian Peninsula.
- 1954 to 1976—Viet Cong and the People's Army of Vietnam combined regular and irregular forces to fight French and U.S. forces. Viet Cong organized into conventional and unconventional units.
- 2006—Hezbollah mixed conventional capabilities (such as antiarmor weapons, rockets, and C2 networks) with irregular tactics (including information warfare, nonuniformed combatants, and civilian shielding). This resulted in a tactical stalemate and strategic setback for Israel.
- 2016—Russian, Syrian Army, and Hezbollah forces mixed capabilities to isolate the Free Syrian Army in Aleppo.

MISCELLANEOUS DATA

C-38. **Regular threat.** When evaluating regular threats, miscellaneous data includes biographic data on the commander and other key leaders in the organization. When combined with the other threat characteristics, this information may provide insight on how an enemy commander may react in a particular situation or attempt to solve a particular problem.

C-39. **Irregular threat.** When evaluating irregular threats, miscellaneous data includes information on personalities, culture, and internal organizational processes.

Note. Miscellaneous data associated with hybrid threat characteristics represents a combination of data required for regular and irregular threats.

Appendix D

IPB Cyberspace Considerations

INTEGRATING CYBERSPACE CONSIDERATIONS INTO IPB

D-1. As an essential part of the information environment, there is a massive global dependence on the cyberspace domain for information exchange. With this dependence and the associated inherent vulnerabilities, the cyberspace domain must be considered during each step of the IPB process:

- **Step 1—define the OE:** Visualize cyberspace components and threats through the three layers of cyberspace.
- **Step 2—describe environmental effects on operations:** Use military aspects of terrain.
- **Step 3—evaluate the threat:** Evaluate threats and HVTs in cyberspace against the warfighting functions by performing critical factors analysis (CFA).
- **Step 4—determine threat COAs:**
  - Consider the threat's historical use of cyberspace and incorporate threat COAs.
  - Determine HVT lists within the cyberspace domain.
  - Assist the S-6 staff to identify friendly networks that require protection.

D-2. To gain situational understanding, the following staff sections, in addition to assistance and support from the cyber mission force, provide the G-2/S-2 enough information to develop IPB products that include cyberspace considerations. The G-2/S-2 relies on the—

- G-3/S-3 to task operational assets to report items significant to cyberspace (such as satellite dish locations, cyber cafés, cellular network towers), since the G-3/S-3 is typically aware of maneuver and/or reconnaissance elements moving through specific designated AOs that have the potential to interact with the populace and the ability to visually confirm relevant infrastructure.
- G-6/S-6 for the friendly force network design to determine where the threat can possibly access friendly systems.
- G-9/S-9 to assist in identifying and confirming civil considerations that are pertinent to the cyberspace domain. For example, civil affairs teams may assist in ascertaining existing and planned network infrastructure in the AO, as well as identifying key leaders and landowners to determine their internet presence, activity, or cyber-personas.
- Information operations officer to primarily synchronize and deconflict information-related capabilities employed to support unit operations. With information provided by the intelligence, the information operations officer contributes to IPB by analyzing the information environment and developing the combined information overlay. Working with the intelligence staff, the information operations officer develops products that portray the information infrastructure of the AO and aspects of the information environment that can affect operations. These products include information all audiences and other decision makers, key people, and significant groups in the AO. They also address potential strengths and vulnerabilities of adversaries and other groups. The information operations officer will also assist in identifying how the populace communicates within the logical network layer, such as local government websites, heavily used social media sites, any group or individual blog sites. Additionally, the information operations officer can possibly identify threat TTP for deception and denial of information within the logical layer.
- Cyberspace electromagnetic activities section to provide information on enemy cyber forces' doctrine, tactics, and equipment, and for cyber capabilities for information collection. Cyberspace capabilities cross cue with SIGINT capabilities to provide better situational awareness of threat forces operating in the cyberspace domain.

Note. Although the intelligence, operations, and signal staff sections are the primary collaborators regarding gaining situational understanding in cyberspace, all staff sections are valuable, to some degree, and should not be disregarded during the staff integration process.

STEP 1—DEFINE THE OPERATIONAL ENVIRONMENT

D-3. When defining the OE, cyberspace includes information and its communications. Although there are other variables in cyberspace that warrant attention (such as individuals, organizations, and systems), they either process, disseminate, or act on information.

STEP 1 CYBERSPACE CONSIDERATIONS

D-4. When defining the OE, consider the three layers of cyberspace—physical network, logical network, and cyber-persona. When evaluating the OE, staff collaboration and reachback assets are essential.

Physical Network Layer

D-5. Depicting the physical network layer within the AO allows the intelligence staff to analyze the physical network layer as it relates to friendly and threat operations. Analysts derive the physical network layer depiction from single-source reporting, all-source intelligence products, cyber mission forces reporting, and other reporting sources. These products assist in developing the physical network layer.

D-6. When analyzing the physical network layer, identify—

- Threat C2 systems that traverse the cyberspace domain.
- Critical nodes the threat can use as hop points in the AO and area of influence. ***Note.*** Data packets pass through bridges, routers, and gateways as they travel between their sources and destinations. Each time data packets pass to the next network device, a *hop* occurs.
- Physical network devices in the AO, such as fiber optic cables, internet exchanges, public access points (internet cafés), server farms, and military or government intranets.
- Elements or entities (threat and nonthreat) interested in and possessing the ability to access data and information residing on and moving through the network.
- Physical storage locations with the most critical information and accessibility to that information.
- Critical nodes and entry points the threat is most likely to use to penetrate the network, including mobile tactical communications systems.
- Implemented measures that prevent threat actors from accessing the networks.

Logical Network Layer

D-7. Depicting the threat's logical network layer discloses how and where it conducts cyberspace operations. It is also useful to understand how and where the population exists, socializes, and communicates within the logical network layer. Additionally, network maps often depict the logical network layer in relation to the physical network layer. All-source intelligence analysis can enhance this depiction.

D-8. Reporting from many sources can provide information about the logical network layer of threat cyberspace, including but not limited to protocols, internet protocol address blocks, and operating systems. The network's key systems can be assessed using the depiction on the logical network layer.

D-9. When analyzing the logical network layer, identify—

- Websites or web pages that influence or have a social impact on the AO.
- Friendly logical network configurations and vulnerabilities and the friendly physical network configurations.
- Current activity baselines on friendly networks, if possible.
- Through which uniform resource locaters (known as URLs), internet protocol addresses, and other locations that critical mission data can be accessed on the internet.
- How friendly data is shared and through which software.

- Intrusion methods and how they can be masked.
- Commonly used software applications and critical logical nodes in the AO and area of influence.
- Commonly used encryption techniques and software.
- Threat information portals used in the AO.

Cyber-Persona Layer

D-10. Depicting the threat cyber-persona layer begins with understanding the organizational structure. Assessment of the organizational structure is an all-source intelligence task. Understanding the organizational structure leads to assessing the cyber-personas associated with the organization. These include cyber-personas that represent the organization, subordinate elements, and personnel.

D-11. When analyzing the cyber-persona layer, identify—

- Threat presence in and usage of the cyberspace domain.
- Data and information consumers in the AO.
- Hacktivists in the AO, specifically with the intent to disrupt.
- Entities capable of penetrating the networks.
- How local actors interrelate with the physical network (mobile phone or internet café) and logical network (websites or software) layers.

D-12. A primary objective when analyzing the cyber-persona layer from an all-source perspective is to identify the physical persons that created and/or used cyber-personas of interest. All-source analysts gain valuable insight by using various tools and techniques, such as link diagrams (see ATP 2-33.4) informed by internet and social media usage, linking or associating one or more of the following, both suspected and confirmed, but not limited to cyber-personas, people, websites, internet protocol addresses, organizations or groups, buildings or facilities, and activities.

D-13. While on the internet, multiple users can use a single cyber-persona and a single user can use multiple cyber-personas, as illustrated in figure D-1. A user may have multiple cyber-personas for various reasons. This is not necessarily an indicator of illicit activity. However, multiple users using a single cyber-persona may indicate a group's activity or common affiliations.

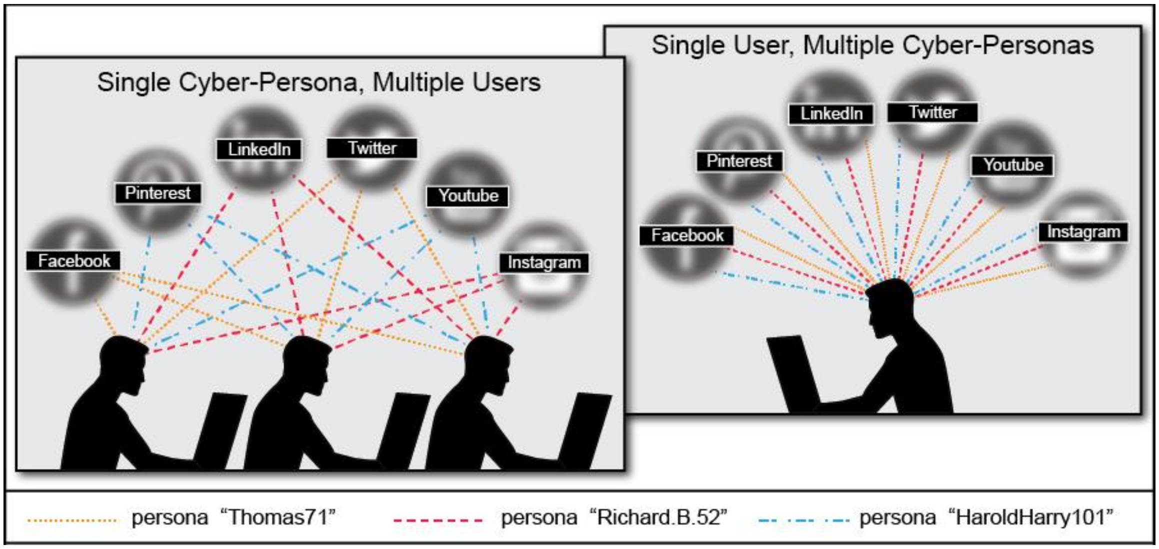


Figure D-1. Single versus multiple cyber-personas

Cyber-Centric Activities and Outputs for Step 1

D-14. The intelligence staff completes the graphic display of significant characteristics and components of cyberspace in relation to the unit's AO and area of influence, as illustrated in figure D-2. If known, it may be beneficial to label those websites frequently visited by the local populace, including Dark websites. Figure D-2 also exhibits the contrasts between a traditional AO overlay and an AO overlay with cyberspace considerations.

> ***Note.*** Since cyberspace is a global domain, threats can potentially affect a BCT's battlefield from anywhere in the world. This must be considered when analyzing and establishing the AOI and area of influence.

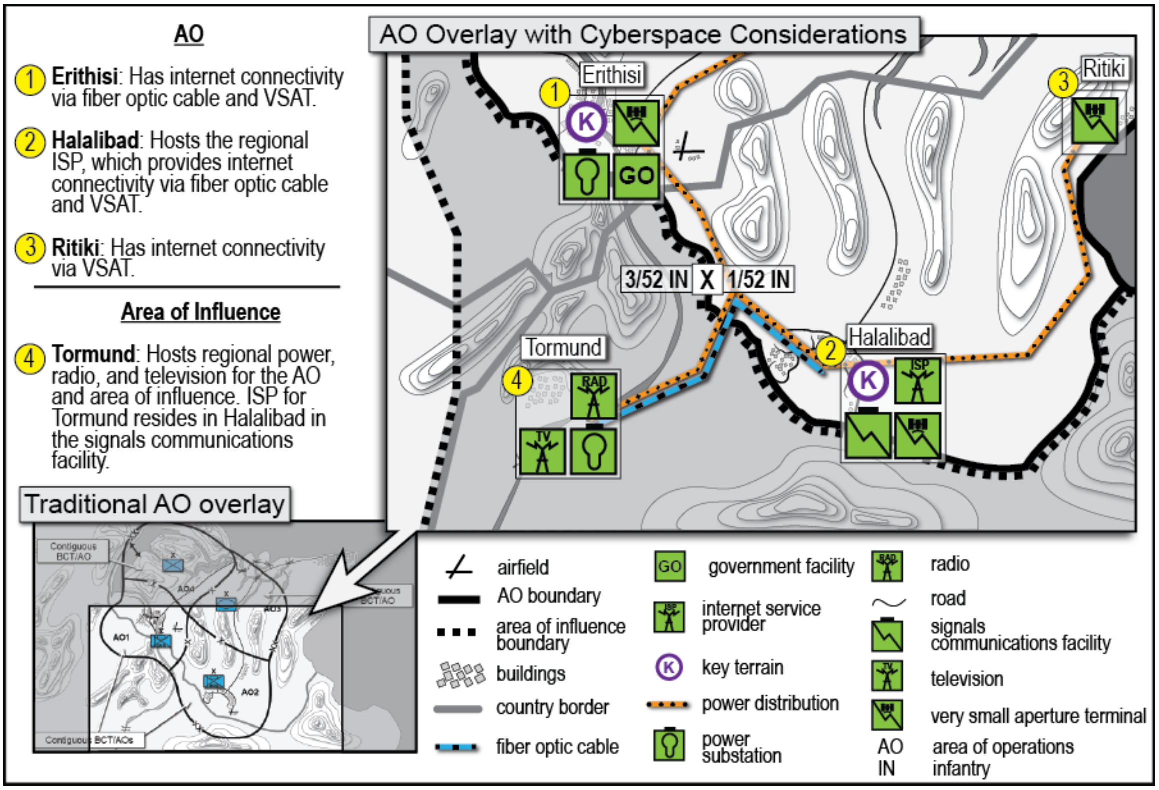

AO
1 Erithisi: Has internet connectivity via fiber optic cable and VSAT.
2 Halalibad: Hosts the regional ISP, which provides internet connectivity via fiber optic cable and VSAT.
3 Ritiki: Has internet connectivity via VSAT.
Area of Influence
4 Tormund: Hosts regional power, radio, and television for the AO and area of influence. ISP for Tormund resides in Halalibad in the signals communications facility.
Traditional AO overlay
Contiguous BCT/AO
AO4
AO1
AO3
AO2
Contiguous BCT/AO
Contiguous BCT/AOs
AO Overlay with Cyberspace Considerations
1 Erithisi
K
GO
3 Ritiki
3/52 IN
X
1/52 IN
4 Tormund
RAD
TV
2 Halalibad
K
ISP
airfield
AO boundary
area of influence boundary
buildings
country border
fiber optic cable
GO government facility
internet service provider
K key terrain
power distribution
power substation
radio
road
signals communications facility
television
very small aperture terminal
AO area of operations
IN infantry

Figure D-2. Area of operations and area of influence example

STEP 2—DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

D-15. Although steps 3 and 4 of the IPB process offer a detailed analysis of threats within the OE, the type of threat and their cyberspace capabilities should be defined during step 2. The significance of a cyber force presence should be considered with and weighed against identified variables within the OE.

Step 2 Cyberspace Considerations

D-16. For environmental effects on operations associated with step 2, describe how the following can affect friendly and threat operations:

- Threats in cyberspace. (See chapter 3 for the traditional approach to threat effects on friendly operations.)
- Terrain in cyberspace.
- Weather, light, and illumination data.
- Civil considerations.

Military Aspects of Terrain

D-17. Conduct terrain analysis of the cyberspace domain using traditional methods. Examine the five military aspects of terrain (OAKOC) factors, which can be displayed in a MCOO. Analyzing terrain in cyberspace, as in geographic terrain, can favor either friendly or threat forces. Table D-1 presents the military aspects of terrain with corresponding cyberspace considerations. This allows commanders to understand the terrain's impact, both geographically and in cyberspace, on friendly and threat operations.

Table D-1. Terrain analysis and corresponding cyberspace considerations

Military aspects of terrain (OAKOC factors)	*Cyberspace considerations*
Observation and fields of fire	Ability to see subnets within networks, intrusion detection systems, password protections, and encryptions used in the area of operations. It is essential to understand what portion of the network can be seen and from where it can be seen. This may include the ability to see using physical surveillance. Additionally, closed networks may prevent observation on friendly and threat networks. Intrusion protection systems may eliminate possible threats across the network.
Avenues of approach	Method of network access, such as an access point, threat intrusion, or path to the physical or logical key terrain, such as switches, routers, servers, and vectors. Mobility corridors can be identified and grouped according to network speed, where slow speeds can cause restricted or severely restricted terrain. The volume of network activity may create additional avenues of approach.
Key terrain	Key terrain can be applied to the physical network, logical network, or cyber-persona layer. Key terrain associated with cyberspace can be considered as a physical node or data that is essential for mission accomplishment. Examples include major lines of communications, key waypoints for observing incoming threats, domain name servers, network operating systems, switches, spectrum-dependent devices, main internet service provider inputs, mission-critical parts of the threat information network. The intelligence staff can determine key terrain in cyberspace by overlapping the threat's critical asset list, mission, and intent. ***Note.*** In cyberspace, it is possible for friendly and threat forces to occupy the same key terrain, potentially without either knowing of the other's presence.
Obstacles	Network features that can impede cyberspace operations include intrusion detection systems, firewalls, antivirus software, password protections, encryptions, reliability of network connectivity, data limits, and write-protections that prevent data manipulation.
Cover and concealment	The threat electromagnetic signature, cyberspace hygiene, noise awareness, and ability to limit attribution are considered cover and concealment within the cyberspace domain. Intelligence staffs determine collaboration or intelligence reach— • If threat actors are hiding their true identity using multiple cyber-personas, honeypots, or Dark webs. • Threat defensive measures (firewalls, software patches, antivirus software, encryption software, nonattributable proxy systems). • Time and volume of network activity. These may support concealment of activity on the network.

Civil Considerations

D-18. When analyzing the environment from a cyberspace perspective, apply civil considerations (ASCOPE) by cross-walking with the operational variables (PMESII-PT). When analyzing the cyberspace domain, intelligence staffs consider the information and infrastructure variables. However, cyberspace operations affect, to varying degrees, the following civil considerations:

- **Areas:** In cyberspace, intelligence staffs should consider cellular phone coverage, internet service providers, and electricity distribution to industrial, commercial, and residential areas.
- **Structures:** Some cyberspace examples include power plants, moveable bridges and dams, communications/broadcast facilities (internet service providers, server farms, cell towers), internet cafés, and any building with an internet connection relevant to the AO or area of influence.
- **Capabilities:** For capabilities in cyberspace, consider internet access (and the capability to throttle or restrict access), cell phones, Wi-Fi, Bluetooth, fiber optic connections, cable television, modern information technological systems, internet and cellular network types.

- **Organizations:** Nonmilitary groups or institutions that can influence the AO (for example, hacktivists, community organizations, journalists, universities, and schools with a cyber curriculum, commercial and industrial unions, outside influencers or regional sympathizers, and online social media groups).
- **People:** Nonmilitary persons encountered by military personnel (for example, religiously and politically motivated hackers, network administrators, technologically proficient individuals, and commercial and industrial workers).
- **Events:** Routine, cyclical, historic, planned, or spontaneous activities and events that significantly affect organizations, people, and military operations.

Cyber-Centric Activities and Outputs for Step 2

D-19. The S-2 ensures the intelligence staff accomplishes the following activities and outputs by the end of step 2, incorporating cyberspace considerations where applicable: threat overlay; threat description table; terrain analysis or MCOO; terrain effects matrix; weather, light, and illumination charts or tables; and civil considerations data files, overlays, and assessments.

Threat Overlay

D-20. A threat overlay graphically depicts the threat's current physical location in the AO, AOI, and area of influence, including the threat's identity, size, location, and strength. A cyberspace perspective (see figure D-3) should evaluate—

- Physical and nonphysical AOs and AOIs by identifying the physical network layer, such as media communications infrastructure and server locations, and the logical network layer, such as hosts or the threat's use of social media sites or websites.
- Known or suspected physical or cyber-personas, threats, groups, or disseminating liaisons—size, strength, and physical or logical locations, if known or suspected.

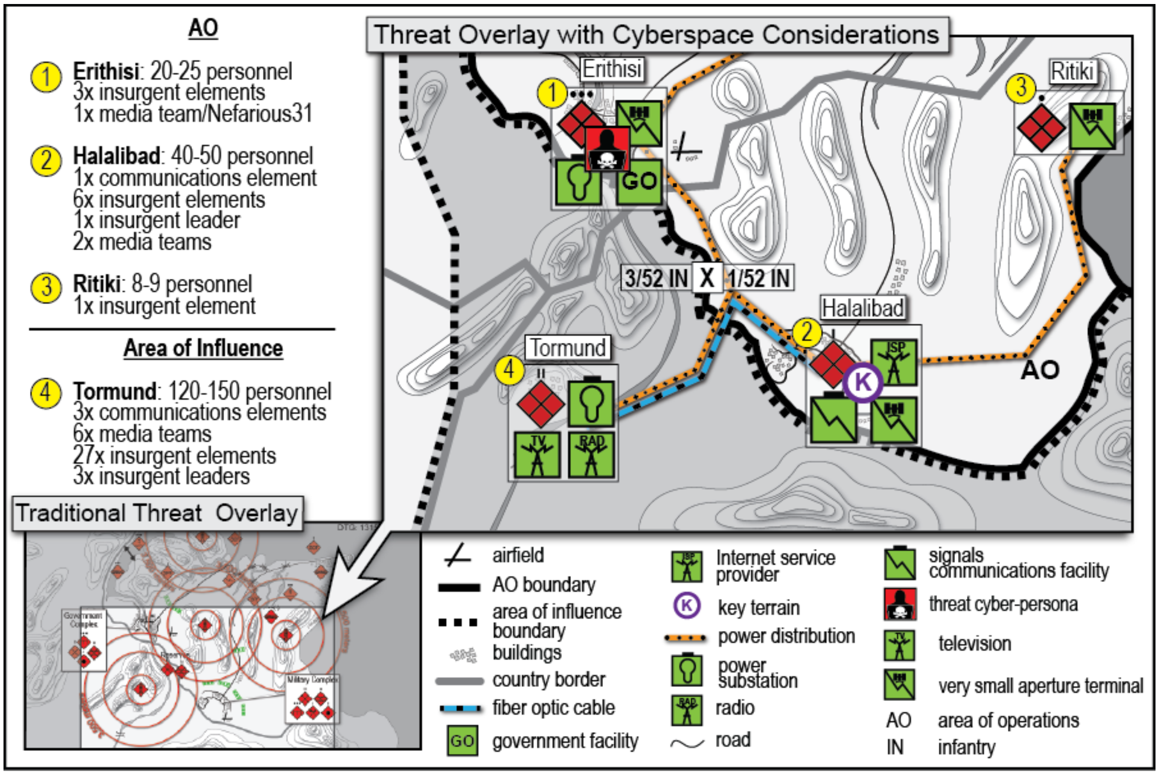


Figure D-3. Threat overlay with cyberspace components example

Threat Description Table

D-21. A threat description table describes the broad capabilities of each threat depicted on the threat overlay (see table D-2). A cyberspace perspective should consider—

- Possible interdependencies between the threat's cyber and military capabilities (for example, the reliance on network communications infrastructure).
- Annotating any known or suspected technical capabilities, expertise, or programs.

Table D-2. Threat description table with cyberspace considerations example

Identity	*Location*	*Disposition*	*Description*
Nefarious31 (cyber-persona)	Erithisi	Operates from internet café as Nefarious31 using open Wi-Fi (802.11) weekly	• Greatest cyber threat in the area of operations • Capable of offensive cyberspace operations using malware • Likely coordinating with government facility to increase cyber capability • Works closely with media elements to assist in propaganda/recruiting effort
2x squads (16-18 personnel)	Erithisi government facility	Population provides sanctuary to threats	• Armed conventional/irregular forces that protect government officials and secure government network • Government facility capable of distributed denial-of-service attack
1x squads (8-9 personnel)	Erithisi southern boundary	Possible screening operations	Armed conventional/irregular forces that prevent U.S. forces from entering or occupying the area
Media element/ Recruitment	Erithisi	Operates from internet café using open Wi-Fi (802.11)	Disseminates threat propaganda to sympathetic population and actors in and around Erithisi, Ritiki, and Halalibad via social media and email campaigns

Modified Combined Obstacle Overlay

D-22. The output from the terrain analysis is used to develop the MCOO, which should reflect the physical network, logical network, or cyber-persona layers of cyberspace when applicable. (See figures D-4 and D-5 on page D-8.) The MCOO traditionally includes natural and man-made OAKOC factors, built-up areas, and civil infrastructure. To add cyberspace considerations into a traditional MCOO, an intelligence staff should include (not all inclusive) public-switched telephone networks, radio stations, media kiosks, internet cafés, electric power, and other supervisory control and data acquisition systems.

Note. Fiber optic lines, which are physical connections that make it part of the physical network layer in cyberspace, are typically co-located or near existing LOCs, such as roads.

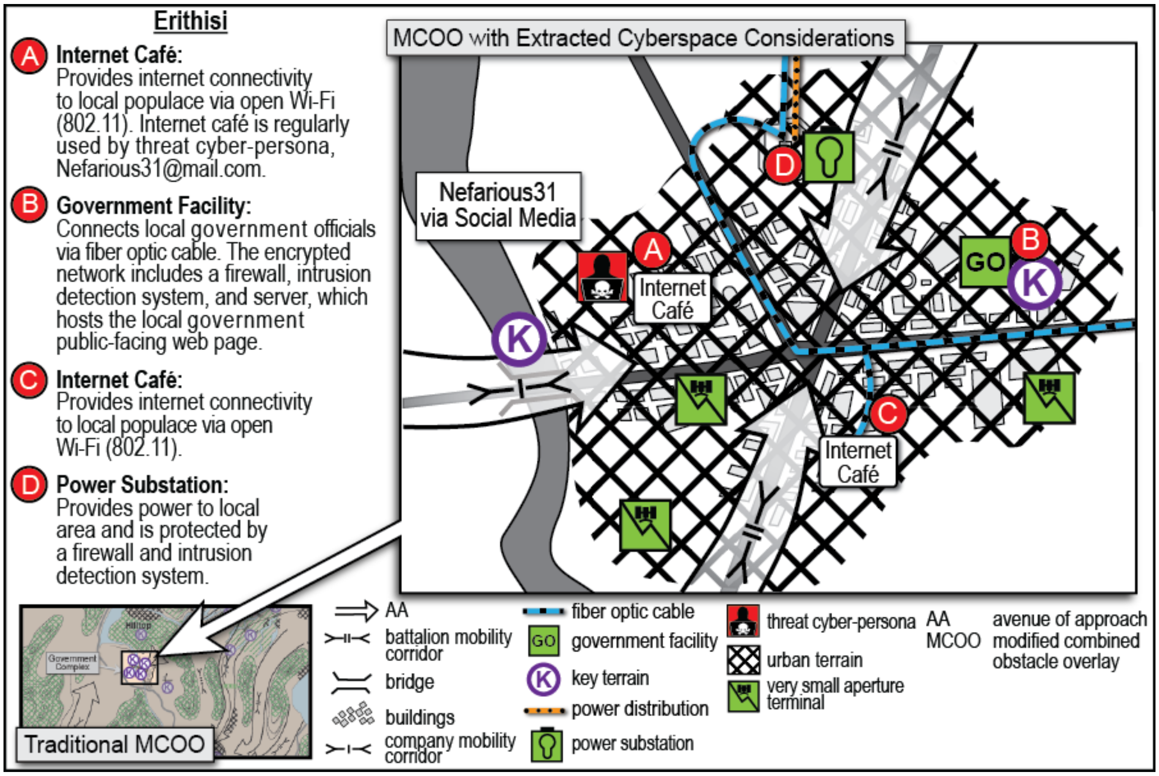

Erithisi
A Internet Café:
Provides internet connectivity to local populace via open Wi-Fi (802.11). Internet café is regularly used by threat cyber-persona, Nefarious31@mail.com.
B Government Facility:
Connects local government officials via fiber optic cable. The encrypted network includes a firewall, intrusion detection system, and server, which hosts the local government public-facing web page.
C Internet Café:
Provides internet connectivity to local populace via open Wi-Fi (802.11).
D Power Substation:
Provides power to local area and is protected by a firewall and intrusion detection system.
MCOO with Extracted Cyberspace Considerations
Nefarious31 via Social Media
A
Internet Café
B
GO
K
C
Internet Café
D
K
Hilltop
Government Complex
Traditional MCOO
AA
battalion mobility corridor
bridge
buildings
company mobility corridor
fiber optic cable
GO government facility
K key terrain
power distribution
power substation
threat cyber-persona
urban terrain
very small aperture terminal
AA avenue of approach
MCOO modified combined obstacle overlay

Figure D-4. MCOO, physical network and cyber-persona layers example

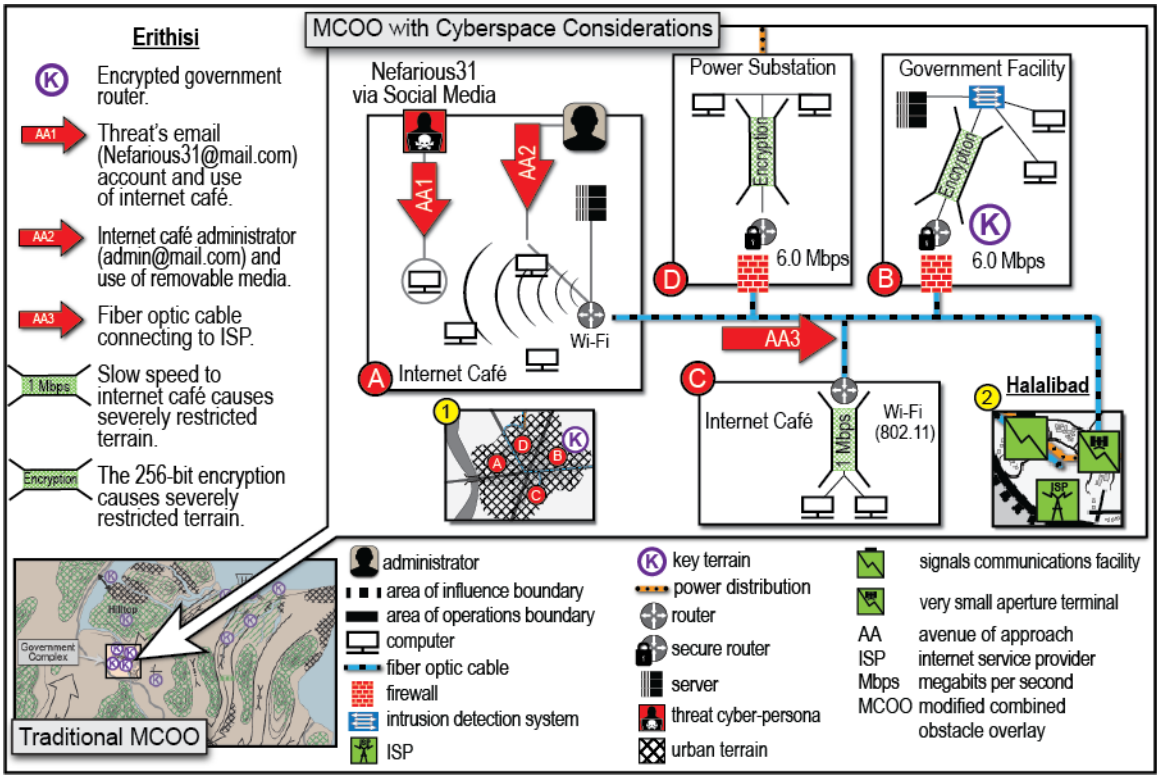

Erithisi
K Encrypted government router.
AA1 Threat's email (Nefarious31@mail.com) account and use of internet café.
AA2 Internet café administrator (admin@mail.com) and use of removable media.
AA3 Fiber optic cable connecting to ISP.
1 Mbps Slow speed to internet café causes severely restricted terrain.
Encryption The 256-bit encryption causes severely restricted terrain.
MCOO with Cyberspace Considerations
Nefarious31 via Social Media
AA1
AA2
Wi-Fi
A Internet Café
Power Substation
Encryption
6.0 Mbps
D
Government Facility
Encryption
K
6.0 Mbps
B
AA3
C
Internet Café
1 Mbps
Wi-Fi (802.11)
1
D
B
K
A
C
2
Halalibad
ISP
Hilltop
Government Complex
Traditional MCOO
administrator
area of influence boundary
area of operations boundary
computer
fiber optic cable
firewall
intrusion detection system
ISP
K key terrain
power distribution
router
secure router
server
threat cyber-persona
urban terrain
signals communications facility
very small aperture terminal
AA avenue of approach
ISP internet service provider
Mbps megabits per second
MCOO modified combined obstacle overlay

Figure D-5. MCOO, physical network, logical network, and cyber-persona layers example

Note. Intelligence staffs, in conjunction with cyber support elements and echelons above corps, develop cyberspace considerations to the MCOO with organic assets.

Terrain Effects Matrix

D-23. Using the MCOO as a guide, a terrain effects matrix describes OAKOC factor effects on friendly and threat operations. Table D-3 presents a terrain effects matrix for operations in the cyberspace domain.

Table D-3. Terrain effects matrix with cyberspace considerations example

OAKOC factors (military aspects of terrain)	*Terrain effects with cyberspace aspects (As related to figures D-4 and D-5)*
Observation and fields of fire	• Internet café networks are wide-open and very accessible, thus allowing ability to see network configurations and the threat's capabilities.
Avenues of approach	• Primary access through unencrypted, open Wi-Fi in internet cafés (Nefarious31 and administrator accounts). • Secondary access through regional internet service provider.
Key terrain	• Regional internet service provider hosts regional power, radio, and television for area of operations. • Internet café router provides internet access to local populace, which is used to spread propaganda throughout the area of operations.
Obstacles	• Intrusion detection systems, firewalls, secure routers, and 256-bit encryptions in both power substation and government facility. • Open Wi-Fi (802.11) in internet cafés with slow download and upload speeds (severely restricted).
Cover and concealment	• Government network defended with intrusion detection systems, firewalls, secure routers, and encryptions. • Power substation also uses intrusion detection systems, firewalls, secure routers, and encryption.

Note. A network component can be associated with more than one military aspect of terrain, such as a firewall that can be both an obstacle and provide cover from fires (on the network).

Weather, Light, and Illumination Charts or Tables

D-24. Weather, light, and illumination charts or tables describe weather, light, and illumination effects on friendly and threat operations. (See paragraph 4-68.) Potential cyberspace considerations comprise any weather, including weather in space, that affects data transmissions, such as solar flares, high winds, and extreme weather conditions, such as sand storms, thunderstorms, or blizzards.

Civil Considerations Data Files, Overlays, and Assessments

D-25. Civil considerations data files may include raw data such as voting locations, base locations, and organizational hierarchies. These data files support and are supplemented by civil consideration overlays, such as, population and demographic overlays, and civil considerations assessments. Cyberspace considerations may include the use of nongovernmental organizations to provide tacit or explicit support, such as proxy media disseminators or internet cafés. Additionally, consider the threat's use of government and noncombatant facilities for cyberspace or media activities or propaganda production.

STEP 3—EVALUATE THE THREAT

D-26. Intelligence staffs determine threat force capabilities, doctrinal principles, and TTP employed by threats in and through the cyberspace domain. The threats' use of cyberspace varies; they use the cyberspace domain differently to accomplish or support objectives. In step 3 of the IPB process, with input from individual intelligence disciplines, the intelligence staff evaluates the threat, creates threat models, develops broad threat COAs (attack, defend, reinforce, and retrograde) or capabilities in a narrative format, and identifies HVTs.

D-27. When creating a threat model that incorporates cyberspace considerations, identify how the threat has executed and integrated cyberspace operations independently of and in concert with traditional operations, and what the threat's capabilities are in and through cyberspace. It is also crucial to realize that the physical manifestation of the threat is not at the core of the threat. For example, where the threat appears is not necessarily where the threat is likely to be. Attributing an attack to a specific threat can be very difficult and consequently makes evaluating the threat especially challenging. For example, the use of a proxy allows the threat to conceal its true location. Tapping into intelligence reach assets is necessary to develop threat models that include TTP or signatures of different threats or groups in cyberspace.

STEP 3 CYBERSPACE CONSIDERATIONS

D-28. When evaluating the threat, understand that threats have varying cyberspace capabilities across all warfighting functions. However, the cyberspace domain likely affects each warfighting function to some degree. Therefore, it is prudent to evaluate how the threat uses the cyberspace domain to support operations by incorporating cyberspace considerations into each warfighting function to increase overall situational understanding. (See table D-4.)

Table D-4. Cyberspace considerations for the warfighting functions

Warfighting function	*Cyberspace considerations*
Mission command	Delegation of authority, synchronization, and direction of forces throughout the cyberspace domain (for example, the use of email or websites to administer guidance to subordinate elements).
Movement and maneuver	Movement of forces, physically or logically, to achieve an advantage over a threat in the cyberspace domain (for example, the execution of a distributed denial of service to disrupt the threat's movement of forces).
Intelligence	The information derived through cyberspace, which enables understanding of the threat, terrain, or civil considerations (for example, the collection of threat open-source data).
Fires	The collective or coordinated use of indirect, cyberspace, missile defense, and joint fires through the targeting process (for example, the threat's use of offensive cyberspace operations or a threat's automated fire systems).
Sustainment	Cyberspace-enabled synchronized or coordinated support and services to enable freedom of maneuver, extending reach and endurance (for example, use of databases or cyberspace-enabled order processes of a threat's equipment or mission essential supplies).
Protection	Cyberspace-enabled methods to preserve the force, allowing commanders to apply maximum combat power (for example, the threat's use of defensive cyberspace operations to prevent geolocation or the targeting of its systems or networks).

D-29. In addition to considering and evaluating traditional threats on the battlefield, it is necessary to evaluate other relevant actors and threats that may conduct operations in cyberspace relevant to the AO:

- **Nation-state actors.** Nations that either conduct operations directly or outsource them to third parties to achieve national goals. They generally have access to domestic resources and personnel not typically available to other actors. They may involve traditional threats as well as traditional allies when conducting espionage.
- **Transnational nonstate actors or terrorists.** Formal and informal organizations not bound by national borders. These actors use cyberspace to raise funds, communicate, recruit, plan operations, destabilize confidence in governments, and conduct terrorist actions within cyberspace.
- **Criminal organizations or multinational cyber syndicate actors.** National or international, these criminal organizations steal information for their use or they sell it to raise capital. Nation states or transnational nonstate actors may use these criminal organizations as surrogates to conduct attacks or espionage through cyberspace.
- **Individual actors, hacktivists, or small groups.** These actors are known to illegally disrupt or gain access to networks or computer systems. Their intentions are as diverse as the number of groups or individual threats in cyberspace. These actors gain access to systems to discover vulnerabilities, sometimes sharing the information with owners. However, they may have a malicious intent. Political motivators often drive their operations, so they use cyberspace to spread their message. These actors can be encouraged or hired by others, such as criminal organizations or nation states, to conceal the attribution of those larger organizations.
- **Insider threats.** Any persons using their access wittingly or unwittingly to harm national security interests through unauthorized disclosure, data modification, espionage, or terrorism.

Note. Friendly elements not practicing proper cybersecurity represent the greatest threat to friendly networks.

CYBER-CENTRIC ACTIVITIES AND OUTPUTS FOR STEP 3

D-30. In step 3, the intelligence staff ensures the development of threat models—the primary outputs for this step that accurately depict how threat forces typically execute operations, and how they historically have reacted in similar circumstances relative to the specified mission and environment. The compilation of these threat models for each identified threat in the AO guides the development of threat COAs in step 4 of the IPB process. Step 3 may require the following IPB activities and outputs with cyberspace considerations, time permitting:

- Creating and updating threat characteristics files.
- Creating or refining the threat model.
- Creating a threat capability statement.

Note. Upon completing steps 3 and 4 of the IPB process, update the intelligence estimate with current threat model details. Additionally, refine and update any requests for information or requests for collection.

Threat Characteristics

D-31. Analyze the threat in cyberspace applying the broad threat characteristics normally considered when analyzing any threat (see chapter 5 and appendix C). Cyberspace considerations may include—

- Attributing electronic devices to specific cyber-personas and/or persons.
- Social networking hierarchy.
- Historical threat TTP or malware signatures.
- C2 nodes.
- Threat intentions towards friendly networks.
- Insider threat potential from host-nation forces operating against friendly forces, or from a foreign intelligence physical threat.

Threat Model

D-32. The threat model comprises three parts:

- Threat template.
- Threat tactics, options, and peculiarities.
- HVT identification.

Threat Template

D-33. A threat template graphically depicts the threat's preferred deployment patterns, dispositions, and capabilities for a type of operation, when not constrained by OE effects. While there are several analytic programs, figure D-6 on page D-12 provides an example of a traditional threat template with cyberspace considerations using the Cyber Kill Chain methodology.

D-34. The Cyber Kill Chain is an analytic framework that describes the seven steps or the process the threat follows to achieve some offensive objective against a friendly network in cyberspace. Regarding IPB, it can be used as a cyber equivalency to a traditional threat template. It depicts a generalized, yet systematic approach that the threat takes to gain access to friendly resources in cyberspace when not constrained by OE effects. Understanding how attacks proliferate, the anatomy of cyberspace attacks, and historical pattern analysis of attackers in the AO can enhance the situational understanding of existing threats in cyberspace.

D-35. The following describes the seven phases of a Cyber Kill Chain:

- **Phase 1: Reconnaissance.** The threat collects information on the target before the actual attack begins.
- **Phase 2: Weaponization.** The threat exploits and creates or obtains a malicious payload to send to a victim associated with the targeted friendly network.
- **Phase 3: Delivery.** The threat sends the malicious payload to the victim by email or other means. This represents one of many intrusion methods the attacker can use.
- **Phase 4: Exploitation.** The threat exploits a vulnerability to execute code on the victim's system.
- **Phase 5: Installation.** The threat installs malware on the victim's system.
- **Phase 6: C2.** The threat creates a C2 channel to continue communications and operations of installed botnet or manipulation of the victim's system.
- **Phase 7: Actions on objectives.** The threat performs the steps to achieve goals inside the friendly forces' network.

Note. The Cyber Kill Chain provides a common model for identifying and preventing cyber intrusions activity; however, the phases can occur nonsequentially.

D-36. Although intelligence staffs have little to no capability to identify or detect activity related to the Cyber Kill Chain, this analytical framework provides a platform for them to articulate logically to commanders current and potential threats against friendly networks, as well as an attack's progress on the friendly network.

D-37. The right half of figure D-6 depicts a generic threat formation for occupying a village or town without OE constraints. The left half of figure D-6 shows the steps and processes the threat's cyber element, which is imbedded with the threat's media element, takes to conduct a nondescript cyberspace attack against a friendly network.

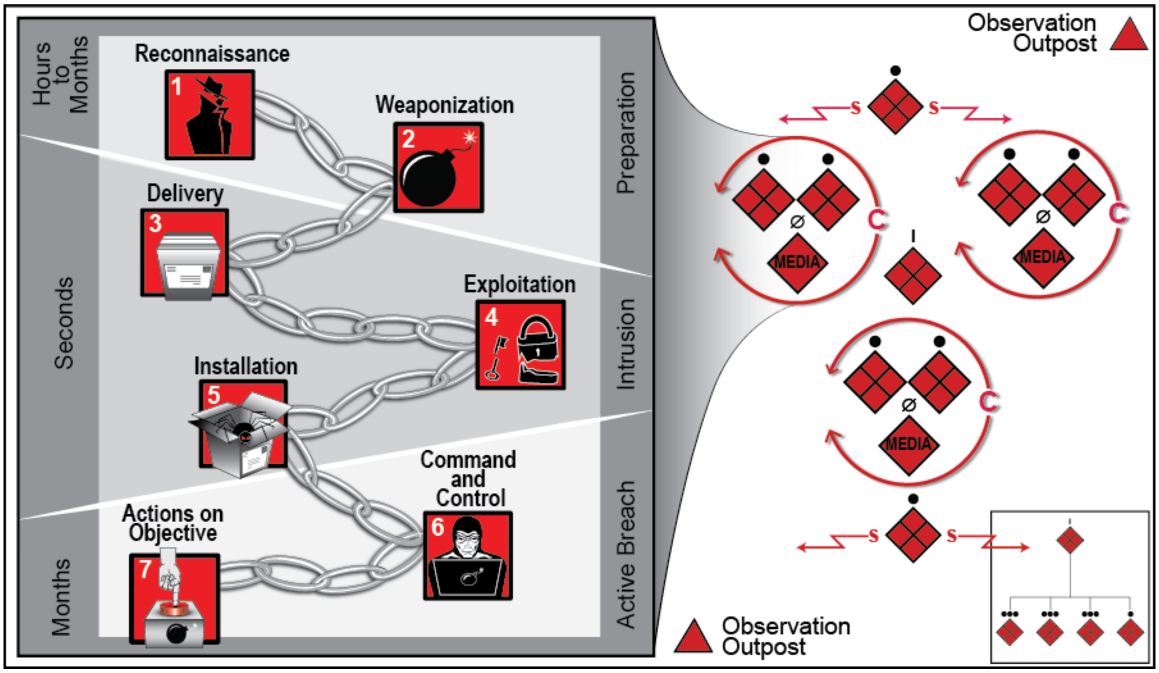


Figure D-6. Threat template with cyberspace considerations example

Threat Tactics, Options, and Peculiarities

D-38. The threat model includes a description of the threat's preferred tactics. To assess threat tactics in cyberspace, identify—

- Similar TTP patterns against comparable networks worldwide.
- Any threats with the intent or capability to penetrate friendly networks, and the specific techniques they use.
- Threats' preferred methods of lateral movement.
- Any common malware used by any threat or threat elements.

High-Value Targets

D-39. HVTs can be depicted and described on the threat template. HVTs related to cyberspace are identified and evaluated using the same resources as traditional methodologies-databases, intelligence studies, patrol debriefs, the threat template with supporting narrative, and tactical judgement.

D-40. The intelligence staff's tactical judgement should be influenced and informed by performing a thorough CFA—normally associated with a center of gravity analysis—of the threat and other relevant actors. A CFA is one of the most useful structured analytic techniques to identify and frame the threat's capabilities in cyberspace. (See JP 5-0.) Additionally, in step 3, regarding general COAs identified in the threat model, a CFA assists in identifying HVTs in cyberspace.

D-41. CFA consists of three major areas, which are evaluated and analyzed:

- *Critical capability* is a means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s) (JP 5-0).
- *Critical requirement* is an essential condition, resource, and means for a critical capability to be fully operational (JP 5-0).
- *Critical vulnerability* is an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects (JP 5-0).

Note. A completed CFA may also act as the catalyst for another analytic tool—the (modified) CARVER criteria tool used in step 4 of the IPB process. (See chapter 5.)

D-42. In evaluating HVTs, the intelligence staff should—

- Identify those assets critical to a threat's ability to conduct primary operations, sequels, or branches using cyberspace operations as a main effort or in a supporting role.
- When assessing HVTs in cyberspace, consider them based on the three layers of cyberspace (physical network, logical network, and cyber-persona).
- Identify those threat units explicitly tasked to conduct offensive cyberspace operations and those specifically tasked to conduct defensive cyberspace operations. The initial HVT list can be determined by mentally war-gaming and thinking through any specified operations under consideration. (See JP 3-12 for more on offensive and defensive cyberspace operations.)

Threat Capabilities

D-43. Identify physical and nonphysical threats' operational patterns and capabilities in cyberspace by considering—

- If threats emit any unique electronic signatures.
- Media's production flow locally, regionally, and globally.
- If threats use any specific malware.
- Threats' or other relevant actors' skill level.
- Networks used to conduct operations and operations security.
- Threats' intent, for example, reconnaissance, espionage, and destructive malware.
- Threats' planning, scanning, and exploitation TTP.
- Threats' exfiltration TTP and their ability to move laterally across networks.
- Threat assets' C2.

D-44. Threat capability statements are used to identify threat capabilities, including cyberspace threat capabilities, and the broad options and supporting operations the threat can conduct to influence the accomplishment of friendly missions. This statement is a narrative that addresses an action the threat can complete. Major units may be portrayed on the threat template along with the activities of each warfighting function.

STEP 4—DETERMINE THREAT COURSES OF ACTION

D-45. In step 4, the final step of the IPB process, intelligence staffs identify and develop the full range of COAs available to the threat and describe threat COAs that can influence friendly operations. They develop the most likely and most dangerous COAs, incorporating cyberspace threats and considerations. The level of detail always depends on the time available.

D-46. It is essential to consider how threat COAs are fundamentally affected by the cyberspace domain. For example, upon identifying methods of threat communications, consider secondary and tertiary effects on threat COAs if any or all of those threat communications are denied through degraded, disrupted, destroyed, or manipulated. Identify HVTs for each COA, such as nodes, C2 centers, communications towers, satellites, internet service providers, fiber optic lines, and local power substations. Additionally, develop initial collection requirements for each COA.

STEP 4 CYBERSPACE CONSIDERATIONS

D-47. When determining threat COAs regarding cyberspace, consider—

- Threats' historical use of cyberspace and possible types of cyberspace operations conducted:
  - Malware—viruses, spyware, worms, network-traveling worms, socially engineered Trojans.
  - Password attacks—brute-force and dictionary attacks.
  - Denial-of-service or distributed denial-of-service attacks.
  - Advanced persistent threat.
  - Phishing attacks.
- Specific units with a task and purpose to produce cyberspace effects in the cyberspace domain.
- Threats' ability and desire to employ cyberspace operations against specific friendly operations.
- If threat forces will be arrayed distinctively based on cyberspace operations or effects.
- Threats that may be located outside of the AO.
- Threat COAs that may use proxies worldwide, which may be outside of the AOI.
- COAs that address the use of the cyberspace domain in completely different ways.

CYBER-CENTRIC ACTIVITIES AND OUTPUTS FOR STEP 4

D-48. At the end of step 4, the S-2 ensures the intelligence staff accomplished the following IPB activities and outputs, including cyberspace considerations, as time allows:

- Refined threat COA statement.
- Threat situation template.
- Event template and event matrix:
  - Identify potential objectives, decision points, NAIs, and TAIs.
  - Provide input to the information collection plan.
- HVT list and input to the HPT list.

Refined Threat Course of Action Statement

D-49. The refined threat COA statement is a narrative that describes the situation template. It should typically contain—

- The threat situation, mission, objectives and end state, and task organization.
- Capabilities.
- Vulnerabilities.

- Decision points.
- The decisive point.
- Failure options.

D-50. Each of these categories should be considered from a cyberspace perspective, either integrating a cyberspace narrative into each category or creating a separate cyberspace narrative at the end of the threat COA statement. Use the technique that best describes the threat's use of cyberspace to the commander. The level of emphasis on cyberspace should be comparable to the threat's use of and effectiveness in cyberspace.

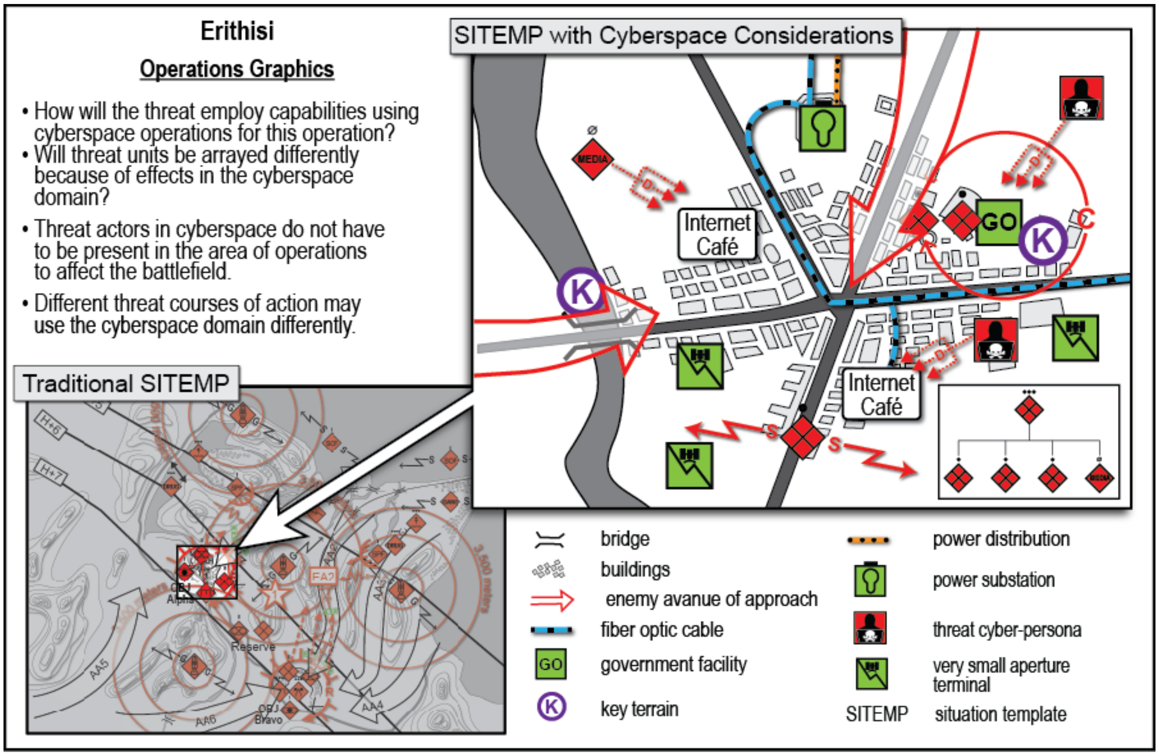
Threat Situation Template

D-51. The threat situation template is a graphic overlay that depicts the threat's expected disposition upon the threat's selection of a COA. Typically, the situation template is accomplished by overlapping the threat template with the MCOO, which incorporates environmental effects on operations, and displaying the threat executing a specific COA.

D-52. In cyberspace, the situation template can depict a threat that is physically located within the AO and integrated with regular threats, as shown in figure D-7. It can also be depicted from the physical network layer perspective, which may also contain logical network elements, as shown in figure D-8 on page D-16.

D-53. The level of cyberspace detail in the situation template should be proportional to the level of the threat in cyberspace and the friendly unit's mission. Each situation template shows an increased level of detail regarding the threat activity in cyberspace. For example, figure D-7 shows a COA with minimal cyberspace components (fiber optic lines, a power substation, power distribution lines, internet cafés, and a very small aperture terminal). However, figure D-8 on page D-16 shows an increased level of cyberspace detail. It depicts a threat COA targeting a friendly network with two different elements.

> ***Note.*** Threats associated with cyberspace may be integrated with larger, regular threats, or they may be independent entities with no known connection to the local threat.



Erithisi

Operations Graphics

- How will the threat employ capabilities using cyberspace operations for this operation?
- Will threat units be arrayed differently because of effects in the cyberspace domain?
- Threat actors in cyberspace do not have to be present in the area of operations to affect the battlefield.
- Different threat courses of action may use the cyberspace domain differently.

Figure D-7. Threat situation template with cyberspace considerations, example 1

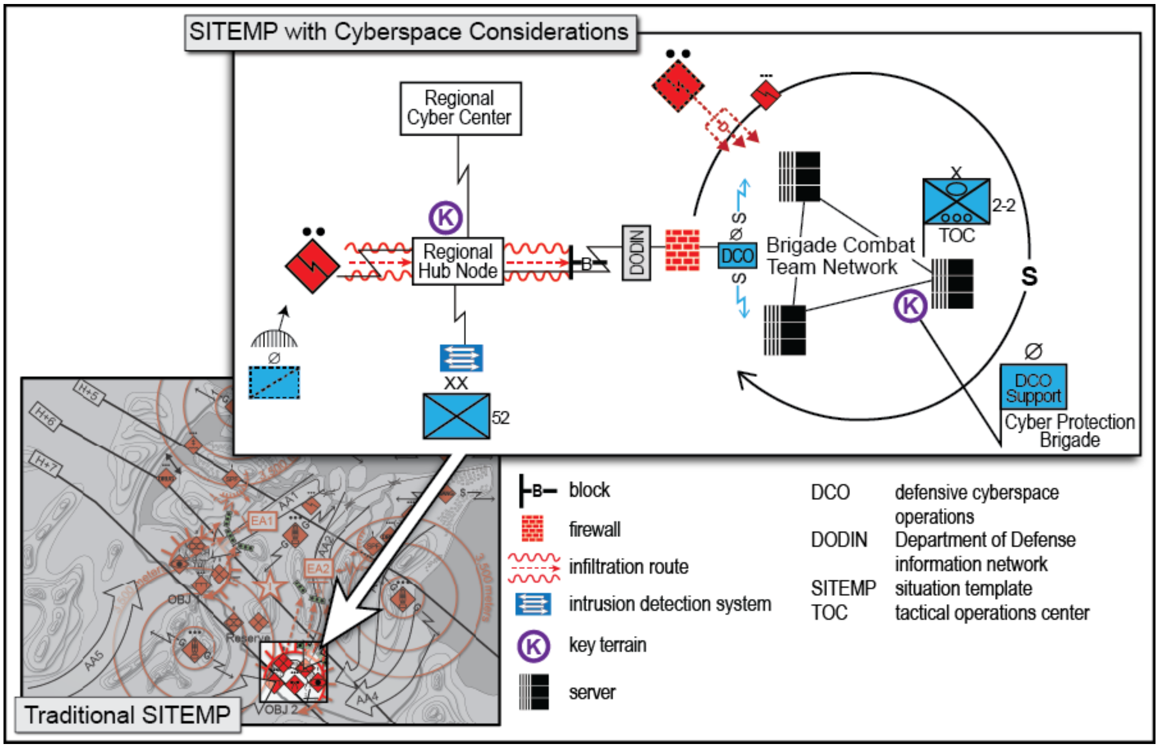

SITEMP with Cyberspace Considerations
Regional Cyber Center
K
Regional Hub Node
B
DODIN
DCO
S
Ø
Brigade Combat Team Network
X
2-2
TOC
S
K
Ø
DCO Support
Cyber Protection Brigade
XX
52
Traditional SITEMP
EA1
EA2
OBJ
OBJ 2
Reserve
AA1
AA2
AA4
AA5
H+5
H+6
H+7
B block
firewall
infiltration route
intrusion detection system
K key terrain
server
DCO defensive cyberspace operations
DODIN Department of Defense information network
SITEMP situation template
TOC tactical operations center

Figure D-8. Threat situation template with cyberspace considerations, example 2

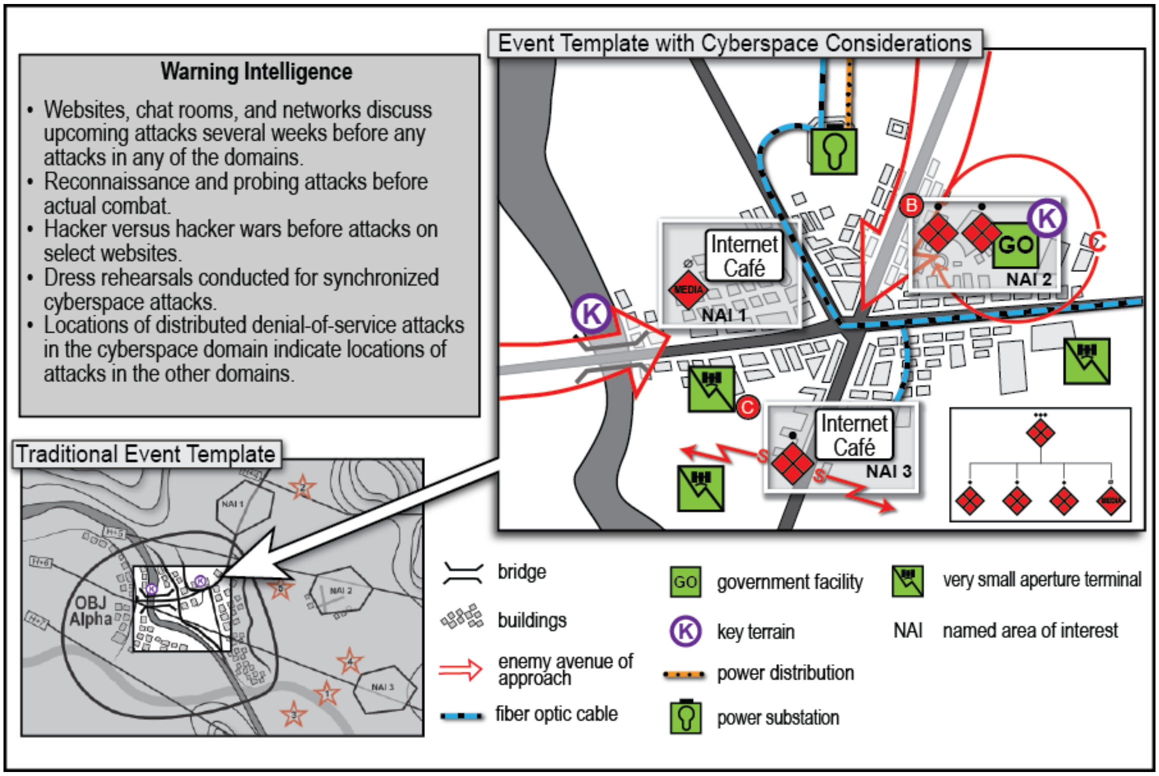
Event Template and Event Matrix

D-54. An event template is a graphic overlay that confirms or denies threat COAs. This enables the development of the information collection plan. An event matrix always accompanies the event. The event template traditionally results from overlapping the developed situation templates to identify those areas or indicators that identify a COA as being unique. Prominent differences are marked as NAIs. In contrast, NAIs in cyberspace are likely not determined by overlapping situation templates and can be physical or logical.

D-55. In cyberspace, as in the land, air, maritime, and space domains, a historical record of TTP on how the threat fights assists in determining NAIs, showing possible, expected activity at a specified location. Consider that NAIs regarding cyberspace are likely related to locations or activity on a network—possibly indicating a specific type of cyberspace operations. Each NAI is linked to an assigned task and the party responsible for collecting and reporting any illicit activity or items associated with those NAIs.

Note. It is not possible to stop all malicious activity on a network. A determination should be made between which systems are mission-critical and need to be secured, versus systems that just need to be monitored.

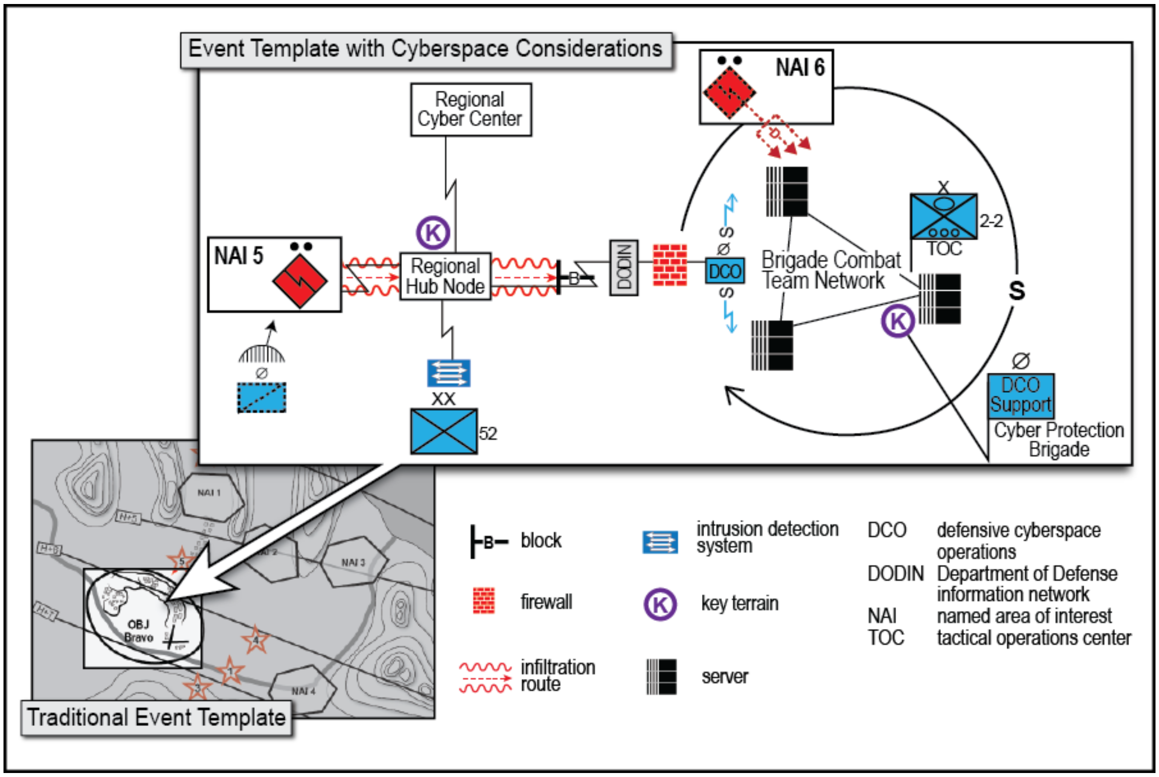
D-56. Figure D-9 illustrates an event template with developed NAIs for a local threat present in the AO. Figure D-10 illustrates the same threats attacking a friendly network, primarily focused on the physical network layer aspect.



Warning Intelligence

- Websites, chat rooms, and networks discuss upcoming attacks several weeks before any attacks in any of the domains.
- Reconnaissance and probing attacks before actual combat.
- Hacker versus hacker wars before attacks on select websites.
- Dress rehearsals conducted for synchronized cyberspace attacks.
- Locations of distributed denial-of-service attacks in the cyberspace domain indicate locations of attacks in the other domains.

Figure D-9. Event template with cyberspace considerations, example 1



Event Template with Cyberspace Considerations
Regional Cyber Center
NAI 6
NAI 5
K
Regional Hub Node
B
DODIN
DCO
S
Ø
S
Brigade Combat Team Network
X
2-2
TOC
S
K
Ø
DCO Support
Cyber Protection Brigade
Ø
XX
52
Traditional Event Template
NAI 1
NAI 2
NAI 3
NAI 4
OBJ Bravo
block
firewall
infiltration route
intrusion detection system
key terrain
server
DCO defensive cyberspace operations
DODIN Department of Defense information network
NAI named area of interest
TOC tactical operations center

Figure D-10. Event template with cyberspace considerations, example 2

D-57. An event matrix describes indicators and activity expected to occur in each NAI. Although there is no prescribed format for the event matrix, it normally associates each NAI and threat decision point with indicators and the times they are expected to occur, as well as COAs they confirm or deny. (See table D-5.)

D-58. The time that a threat activity may or may not occur in cyberspace is likely influenced more by intangible variables such as the stealth and persistence of the resource being used (for example, the malware designated for an attack):

- **Stealth of the resource** refers to the probability that if the threat uses the resource, the resource will still be available for use in the future.
- **Persistence of the resource** refers to the probability that if the threat refrains from using the resource, the resource will still be useable in the future.

D-59. The timing of a threat's cyberspace attack is tied less to typical environmental factors (such as increased visibility due to daylight)—which are considered imperative for some traditional operations—and more to the logical aspects of the network. For example, the volume of network activity may spur threat operations because it can mitigate attribution, which increases stealth.

Table D-5. Event matrix with cyberspace considerations example

Named area of interest	*Indicators*	*Threat decision point*	*Time*	*Threat course of action indicated*
1	• Uses email • Targeting is specific • Sophisticated, appears to come from associate, client, or acquaintance • May be contextually relevant to work	1	Time of cyberspace operations may be synchronized with land or other operations.	Spear-phishing attack
2	• Unusually slow network performance • Unavailability of a particular website • Unable to access any website • Stark increase in the number of spam emails received (also known as an email bomb)	2	Cyberspace operations may be planned over a period of months or years	Denial-of-service attack
3	• Social media sites contain an increase in negative messaging • Intelligence assets discover different media in the area of operations containing threat messaging	3	• Timing may be seasonal or synchronized with other threat operations • Timing may be linked to negative effects of friendly operations	Propaganda campaign

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. Terms for which ATP 2-01.3 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
ADA	air defense artillery
ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AO	area of operations
AOI	area of interest
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
C2	command and control
CAS	close air support
CBRN	chemical, biological, radiological, and nuclear
CFA	critical factors analysis
COA	course of action
DST	decision support template
EMS	electromagnetic spectrum
EW	electronic warfare
FM	field manual
G-1	assistant chief of staff, personnel
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assitant chief of staff, logistics
G-5	assistant chief of staff, plans
G-6	assistant chief of staff, signal
G-9	assistant chief of staff, civil affairs operations
HPT	high-payoff target
HVT	high-value target
IED	improvised explosive device
IPB	intelligence preparation of the battlefield
J-2	intelligence directorate of a joint staff
JP	joint publication
LOC	line of communications

LOS	line of sight
MCOO	modified combined obstacle overlay
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
NAI	named area of interest
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (military aspects of terrain)
OE	operational environment
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
PIR	priority intelligence requirement
S-1	battalion or brigade personnel staff officer
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-4	battalion or brigade logistics staff officer
S-5	battalion or brigade plans staff officer
S-6	battalion or brigade signal staff officer
S-9	battalion or brigade civil affairs operations staff officer
SIGINT	signals intelligence
TAI	target area of interest
TC	training circular
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
U.S.	United States
WMD	weapons of mass destruction

SECTION II – TERMS

air domain

The atmosphere, beginning at the Earth’s surface, extending to the altitude where its effects upon operations become negligible. (JP 3-30)

area defense

A defensive task that concentrates on denying enemy forces access to designated terrain for a specific time rather than destroying the enemy outright. (ADP 3-90)

area of influence

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

That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. (JP 3-0)

area of operations

An operational area defined by a commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. (JP 3-0)

attack

An offensive task that destroys or defeats enemy forces, seizes and secures terrain, or both. (ADP 3-90)

avenue of approach

(Army) A path used by an attacking force leading to its objective or to key terrain. Avenues of approach exist in all domains. (ADP 3-90)

begin morning civil twilight

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)

begin morning nautical twilight

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. (JP 3-09.3)

civil considerations

The influence of manmade infrastructure, civilian institutions, and activities of civilian leaders, populations, and organizations within an area of operations on the conduct of military operations. (ADRP 5-0)

concealment

Protection from observation or surveillance. (FM 3-96)

cover

(Army) Protection from the effects of fires. (FM 3-96)

critical capability

A means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objectives. (JP 5-0)

critical requirement

An essential conditions resource, and means for a critical capability to be fully operational. (JP 5-0)

critical vulnerability

An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects. (JP 5-0)

cyberspace

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

decision point

A point in space and time when the commander or staff anticipates making a key decision concerning a specific course of action. (JP 5-0)

decisive point

A geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an enemy or contribute materially to achieving success. (JP 5-0)

decisive terrain

Key terrain whose seizure and retention is mandatory for successful mission accomplishment. (ADP 3-90).

defensive task

A task conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks. (ADRP 3-0)

electromagnetic spectrum

The entire range of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-13.1)

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

end evening civil twilight

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)

end of evening nautical twilight

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)

end state

The set of required conditions that defines achievement of the commander's objectives. (JP 3-0)

event matrix

A cross-referenced description of the indicators and activity expected to occur in each named area of interest. (JP 2-01.3)

event template

A guide for collection planning that depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted. (JP 2-01.3)

exploitation

An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (JP 2-01.3)

field of fire

The area that a weapon or group of weapons may cover effectively from a given position. (FM 3-90-1)

high-payoff target

A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. (JP 3-60)

high-value target

A target the enemy commander requires for the successful completion of the mission. (JP 3-60)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting threat effects. (ADRP 3-0)

identity intelligence

The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. (JP 2-0)

indicator

In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 2-0)

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information requirements

In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 2-0)

infrastructure reconnaissance

A multidisciplinary reconnaissance focused on gathering technical information on the condition and capacity of existing public systems, municipal services, and facilities within an assigned area of operations. (ATP 3-34.81)

***intelligence preparation of the battlefield**

(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.

key terrain

(Army) An identifiable characteristic whose seizure or retention affords a marked advantage to either combatant. (ADP 3-90)

land domain

The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals. (JP 3-31)

***line of sight**

The unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another.

littoral

Comprises two segments of operational environment: 1. Seaward: the area from the open ocean to the shore, which must be controlled to support operations ashore. 2. Landward: the area inland from the shore that can be supported and defended directly from the sea. (JP 2-01.3)

maritime domain

The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32)

military decision-making process

An interactive planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

mobile defense

A defensive task that concentrates on the destruction or defeat of the enemy through a decisive attack by a striking force. (ADP 3-90)

mobility corridor

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

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. (JP 2-01.3)

movement to contact

(Army) An offensive task designed to develop the situation and to establish or regain contact. (ADP 3-90)

named area of interest

The geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected, usually to capture indications of adversary courses of action. (JP 2-01.3)

objective

The clearly defined, decisive, and attainable goal toward which an operation is directed. (JP 5-0)

observation

The condition of weather and terrain that permits a force to see the friendly, enemy, and neutral personnel and systems, and key aspects of the environment. (ADP 1-02)

obstacle

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)

offensive task

A task conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers. (ADRP 3-0)

operational environment

A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operational framework

A cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations. (ADP 1-01)

order of battle

(joint) The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. (JP 2-01.3)

position of relative advantage

A location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage. (ADRP 3-0)

pursuit

An offensive task designed to catch or cut off a hostile force attempting to escape, with the aim of destroying it. (ADP 3-90)

retrograde

A defensive task that involves organized movement away from the enemy. (ADP 3-90)

risk management

The process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

situational understanding

The product of applying analysis and judgment to relevant information to determine the relationship among the operational and mission variables to facilitate decision making. (ADP 5-0)

situation template

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

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)

space domain

The area above the altitude where atmospheric effects on airborne objects become negligible. (JP 3-14)

space environment

The environment corresponding to the space domain, where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences, and that encompasses the Earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere. (JP 3-59)

space weather

The conditions and phenomena in space and specifically in the near-Earth environment that may affect space assets or space operations. (JP 3-59)

stability tasks

Tasks conducted as part of operations outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADRP 3-07)

striking force

A dedicated counterattack force in a mobile defense constituted with the bulk of available combat power. (ADP 3-90)

target area of interest

The geographical area where high-value targets can be acquired and engaged by friendly forces. (JP 2-01.3)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

terrain analysis

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)

thermal crossover

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. (JP 3-09.3)

threat

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)

troop leading procedures

A dynamic process used by small-unit leaders to analyze a mission, develop a plan, and prepare for an operation. (ADP 5-0)

unified action

The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

unified land operations

Simultaneous offensive, defensive, and stability or defense support of civil authorities tasks to seize, retain, and exploit the initiative to shape the operational environment, prevent conflict, consolidate gains, and win our Nation's wars as part of unified action. (ADRP 3-0)

urban operations

Operations across the range of military operations planned and conducted on, or against objectives on a topographical complex and its adjacent natural terrain, where man-made construction or the density of population are the dominant features. (ATP 3-06)

This page intentionally left blank.

References

All URLs accessed on 24 January 2019.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. January 2019.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

ADP 2-0. *Intelligence*. 4 September 2018.

ADP 3-0. *Operations*. 6 October 2017.

ADRP 3-0. *Operations*. 6 October 2017.

FM 2-0. *Intelligence*. 6 July 2018.

FM 3-0. *Operations*. 6 October 2017.

RELATED PUBLICATIONS

These documents are cited in this publication.

JOINT PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/Doctrine/.

JP 1. *Doctrine for the Armed Forces of the United States*. 25 March 2013.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 21 May 2014.

JP 2-03. *Geospatial Intelligence in Joint Operations*. 5 July 2017.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-04. *Joint Shipboard Helicopter and Tiltrotor Aircraft Operations*. 6 December 2012.

JP 3-06. *Joint Urban Operations*. 20 November 2013.

JP 3-09.3. *Close Air Support*. 25 November 2014.

JP 3-12. *Cyberspace Operations*. 8 June 2018.

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.

JP 3-14. *Space Operations*. 10 April 2018.

JP 3-15. *Barriers, Obstacles, and Mine Warfare for Joint Operations*. 6 September 2016.

JP 3-30. *Command and Control of Joint Air Operations*. 10 February 2014.

JP 3-31. *Command and Control for Joint Land Operations*. 24 February 2014.

JP 3-32. *Command and Control of Joint Maritime Operations*. 8 June 2018.

JP 3-59. *Meteorological and Oceanographic Operations*. 10 January 2018.

JP 3-60. *Joint Targeting*. 28 September 2018.

JP 5-0. *Joint Planning*. 16 June 2017.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/.

ADP 1-01. *Doctrine Primer*. 2 September 2014.

ADP 3-90. *Offense and Defense*. 13 August 2018.

ADP 5-0. *The Operations Process*. 17 May 2012.

ADRP 1-03. *The Army Universal Task List*. 2 October 2015.

ADRP 3-07. *Stability*. 31 August 2012.

ADRP 5-0. *The Operations Process*. 17 May 2012.

AR 25-30. *Army Publishing Program*. 13 June 2018.

ATP 2-01. *Plan Requirements and Assess Collection.* 19 August 2014.

ATP 2-22.6-2. *(U) Signals Intelligence Volume II: Reference Guide*. 20 June 2017.

ATP 2-33.4. *Intelligence Analysis*. 18 August 2014.

ATP 3-01.16. *Air and Missile Defense Intelligence Preparation for the Battlefield (AMD IPB).* 31 March 2016.

ATP 3-06. *Urban Operations*. 7 December 2017.

ATP 3-13.1. *The Conduct of Information Operations*. 4 October 2018.

ATP 3-14.3. *Techniques for Army Space Forces*. 15 February 2018.

ATP 3-18.10. *Special Forces Air Operations*. 24 February 2016.

ATP 3-21.51. *Subterranean Operations*. 21 February 2018.

ATP 3-34.80. *Geospatial Engineering*. 22 February 2017.

ATP 3-34.81. *Engineer Reconnaissance*. 1 March 2016.

ATP 3-36. *Electronic Warfare Techniques*. 16 December 2014.

ATP 3-37.34. *Survivability Operations*. 16 April 2018.

ATP 3-55.4. *Techniques for Information Collection During Operations Among Populations*. 5 April 2016.

ATP 3-60. *Targeting*. 7 May 2015.

ATP 5-0.6. *Network Engagement*. 19 June 2017.

ATP 5-19. *Risk Management*. 14 April 2014.

ATTP 3-06.11. *Combined Arms Operations in Urban Terrain*. 10 June 2011.

FM 3-01. *U.S. Army Air and Missile Defense Operations*. 2 November 2015.

FM 3-07. *Stability*. 2 June 2014.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

FM 3-13. *Information Operations*. 6 December 2016.

FM 3-14. *Army Space Operations*. 19 August 2014.

FM 3-55. *Information Collection*. 3 May 2013.

FM 3-90-1. *Offense and Defense Volume 1*. 22 March 2013.

FM 3-96. *Brigade Combat Team*. 8 October 2015.

FM 6-0. *Commander and Staff Organization and Operations*. 5 May 2014.

FM 6-22. *Leader Development*. 30 June 2015.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

TC 2-91.4. *Intelligence Support to Urban Operations*. 23 December 2015.

TC 7-100.3. *Irregular Opposing Forces*. 17 January 2014.

SOURCES USED

Cyber Kill Chain. *Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense, 2015*. Available online: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

Swinton, Ernest Dunlop. *The Defence of Duffer's Drift*. Washington, DC: The United States Infantry Association. Available online at http://www.benning.army.mil/MCoE/199th/OCS/content/pdf/The%20Defence%20of%20Duffers%20Drift.pdf.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website: https://armypubs.army.mil/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

This page intentionally left blank.

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.

Entries are by paragraph number unless indicated otherwise.

Entries are by paragraph number unless indicated otherwise.

This page intentionally left blank.

This page intentionally left blank.

ATP 2-01.3
1 March 2018

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

Kathleen S. Miller

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1905602

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: To be distributed in accordance with the initial distrubution number (IDN) 116088, requirements for ATP 2-01.3.

This page intentionally left blank.