ATP 2-33.4

Intelligence Analysis

JANUARY 2020

INCORPORATING CHANGE 1, MAY 2025

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

This publication supersedes ATP 2-33.4, dated 18 August 2014.

Headquarters, Department of the Army

This publication is available at Army Knowledge Online (https://armypubs.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

ATP 2-33.4, C1

Change No. 1
Army Techniques Publication
No. 2-33.4

Headquarters
Department of the Army
Washington, DC, 30 May 2025

Intelligence Analysis

1. Change 1 to ATP 2-33.4 (10 January 2020) removes all *critical thinking* copyrighted material used with permission from the Foundation for Critical Thinking, http://www.criticalthinking.org/: *The Thinker's Guide to Analytic Thinking*, 2017, and *The Miniature Guide to Critical Thinking: Concepts and Tools*, 2014, by Dr. Linda Elder and Dr. Richard Paul. Permission to use this copyrighted material in ATP 2-33.4 (10 January 2020) expires in September 2024.

2. Change 1—
   - Removes the Acknowledgement page, changing the pagination of the Introduction.
   - Adds new figure B-1; former figure B-1 becomes figure B-2.
   - Removes table B-1.
   - Renames and modifies appendix B, to include a revised discussion of critical and creative thinking and the addition of a historical vignette.

3. A plus sign (+) marks modified content.

4. ATP 2-33.4, 30 May 2025, is changed as follows:

Remove Old Pages	Insert New Pages
pages i, ii, iii, iv, v, ix, xi, xii, xiii, xiv	pages i, ii, iii, iv, v, ix, x, xi, xii
pages 1-7, 1-8	pages 1-7, 1-8
pages B-1 through B-14	pages B-1 through B-11
page References-3	page References-3
pages Index-1 through Index-4	pages Index-1 through Index-4

5. An updated Authentication page has amended the prior authentication reflected in the rear of this publication.

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

This page intentionally left blank.

*ATP 2-33.4

Army Techniques Publication
No. 2-33.4

Headquarters
Department of the Army
Washington, DC, 10 January 2020

Intelligence Analysis

Contents

Page

PREFACE vii

+INTRODUCTION ix

PART ONE FUNDAMENTALS

Chapter 1 UNDERSTANDING INTELLIGENCE ANALYSIS 1-1
Intelligence Analysis Overview 1-1
Conducting Intelligence Analysis 1-5
Intelligence Analysis and Collection Management 1-8
The All-Source Intelligence Architecture and Analysis Across the Echelons 1-9
Intelligence Analysis During Large-Scale Ground Combat Operations 1-11
Intelligence Analysis During the Army's Other Strategic Roles 1-13

Chapter 2 THE INTELLIGENCE ANALYSIS PROCESS 2-1
Overview 2-1
The Phases of the Intelligence Analysis Process 2-1

Chapter 3 ALL-SOURCE ANALYTICAL TASKS 3-1
Overview 3-1
Generate Intelligence Knowledge (ART 2.1.4) 3-2
Perform Intelligence Preparation of the Battlefield (ART 2.2.1) 3-3
Provide Warnings (ART 2.1.1.1) 3-3
Perform Situation Development (ART 2.2.2) 3-4
Provide Intelligence Support to Targeting and Information Operations (ART 2.4) 3-4

PART TWO TASK TECHNIQUES

Chapter 4 ANALYTIC TECHNIQUES 4-1
Overview 4-1
Applying Structured Analytic Techniques 4-1

Chapter 5 BASIC AND DIAGNOSTIC STRUCTURED ANALYTIC TECHNIQUES 5-1

Section I – Basic Structured Analytic Techniques 5-1
Sorting 5-1
Chronologies 5-4

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

*This publication supersedes ATP 2-33.4, dated 18 August 2014.

Matrices 5-6
Weighted Ranking 5-7
Link Analysis 5-8
Event Tree 5-12
Event Mapping 5-13
Section II – Diagnostic Structured Analytic Techniques 5-15
Key Assumptions Check 5-15
Quality of Information Check 5-16
Indicators/Signposts of Change 5-18
Chapter 6 ADVANCED STRUCTURED ANALYTIC TECHNIQUES 6-1
Section I – Contrarian Structured Analytic Techniques 6-1
Analysis of Competing Hypotheses 6-1
Devil's Advocacy 6-3
Team A/Team B 6-4
High-Impact/Low-Probability Analysis 6-5
"What If?" Analysis 6-6
Section II – Imaginative Structured Analytic Techniques 6-7
Brainstorming 6-8
Functional Analysis Using Critical Factors Analysis 6-9
Outside-In Thinking 6-10
Red Hat/Team Analysis 6-11

PART THREE INTELLIGENCE ANALYSIS CONSIDERATIONS

Chapter 7 ANALYTIC SUPPORT TO ARMY FORCES AND OPERATIONS 7-1
Overview 7-1
Analysis Across the Echelons 7-1
Support to Functional Elements 7-3
Analysis Across the Army's Strategic Roles 7-6
Chapter 8 ANALYSIS AND LARGE-SCALE GROUND COMBAT OPERATIONS 8-1
Overview 8-1
Tactical to Operational Situation: An Enemy Attack 8-1
Chapter 9 MANAGING LONG-TERM ANALYTICAL ASSESSMENTS 9-1
Overview 9-1
The Basics of Analytic Design 9-1
Collaboration During Analytic Design 9-6
Transitioning from the Analytic Design Process to Presenting the Results 9-6
Crosswalking Analytic Design with Tactical Intelligence Analysis 9-7
Appendix A AUTOMATION SUPPORT TO INTELLIGENCE ANALYSIS A-1
+Appendix B INTELLIGENCE ANALYTICAL SKILLS B-1
Appendix C ANALYTIC STANDARDS AND ANALYSIS VALIDATION C-1
Appendix D THREAT CONSIDERATIONS DURING LARGE-SCALE GROUND COMBAT OPERATIONS D-1
Appendix E INTELLIGENCE PRODUCTION E-1
Appendix F INTELLIGENCE SUPPORT TO TARGETING F-1

GLOSSARY **Glossary-1**
REFERENCES **References-1**
INDEX **Index-1**

Figures

+Introductory figure. Intelligence analysis at a glance x
Figure 1-1. Achieving situational awareness and understanding 1-1
Figure 1-2. Intelligence analysis within doctrinal constructs 1-3
Figure 1-3. Information and intelligence reporting example 1-4
Figure 1-4. Analytic standards 1-8
Figure 1-5. All-source analysis across the echelons 1-10
Figure 1-6. Key aspects of the operational framework 1-12
Figure 2-1. The intelligence analysis process 2-2
Figure 3-1. The all-source analytical tasks 3-1
Figure 4-1. Applying analytic techniques to understand the operational environment 4-2
Figure 4-2. Structured analytic techniques summarized 4-3
Figure 5-1. Sorting data using a pattern analysis plot sheet example 5-3
Figure 5-2. Timeline example 5-5
Figure 5-3. Time event chart example 5-5
Figure 5-4. Threat intentions matrix example 5-7
Figure 5-5. Weighted ranking (steps 1–5) to determine the threat's most likely COA 5-8
Figure 5-6. Weighted ranking (step 6) to determine the threat's most likely COA 5-8
Figure 5-7. Link diagram example 5-10
Figure 5-8. Association matrix example 5-11
Figure 5-9. Activities matrix example 5-11
Figure 5-10. Event tree example 5-13
Figure 5-11. Event mapping example 5-14
Figure 6-1. Analysis of competing hypotheses used during step 4 of the IPB process 6-3
Figure 6-2. Team A/Team B used during step 4 of the IPB process 6-5
Figure 6-3. Functional analysis using critical factors analysis 6-10
Figure 6-4. Outside-in thinking used during step 2 of the IPB process 6-11
Figure 8-1. Brigade combat team situation example 8-2
Figure 8-2. Division situation example 8-4
Figure 8-3. Tactical/Operational (corps) situation example 8-6
Figure 9-1. Analytic design steps 9-2
Figure 9-2. Frame the question/issue 9-3
Figure 9-3. Review and assess knowledge 9-3
Figure 9-4. Review resources 9-4
Figure 9-5. Select the analytic approach/methodology and plan project 9-4
Figure 9-6. Develop knowledge 9-5

Figure 9-7. Perform analysis 9-5
Figure 9-8. Evaluate analysis 9-6
Figure A-1. Intelligence analysis enabled by DCGS-A A-3
+Figure B-1. Critical thinking nested within the intelligence analysis process B-2
+Figure B-2. Types of reasoning examples B-5
Figure C-1. Estimative language: expressions of likelihood C-2
Figure E-1. Annex B (Intelligence) to the operation order example E-2
Figure E-2. Appendix 1 (Intelligence Estimate) example E-4
Figure E-3. Intelligence running estimate example E-5
Figure E-4. Intelligence summary example E-6
Figure E-5. Graphic intelligence summary example E-8
Figure E-6. Intelligence report example E-8
Figure E-7. Periodic intelligence report example E-9
Figure F-1. High-payoff target list example F-4
Figure F-2. Example target selection standard matrix F-5
Figure F-3. Battle damage assessment chart (based on threat organization) F-10
Figure F-4. Battle damage assessment chart (based on location) F-10

Tables

Table 1-1. Intelligence analysis during large-scale ground combat operations 1-11
Table 1-2. Intelligence analysis during the other Army strategic roles 1-14
Table 2-1. Evaluation ratings for source reliability and information accuracy 2-5
Table 5-1. Sorting technique 5-2
Table 5-2. Chronologies technique 5-4
Table 5-3. Matrices technique 5-6
Table 5-4. Weighted ranking technique 5-7
Table 5-5. Link analysis technique 5-9
Table 5-6. Event tree technique 5-12
Table 5-7. Event mapping technique 5-14
Table 5-8. Key assumptions check technique 5-15
Table 5-9. Quality of information check technique 5-16
Table 5-10. Questioning guideline for checking information quality 5-17
Table 5-11. Indicators/Signposts of change technique 5-18
Table 6-1. Analysis of competing hypotheses technique 6-2
Table 6-2. Devil’s advocacy technique 6-3
Table 6-3. Team A/Team B technique 6-4
Table 6-4. High-impact/Low-probability analysis technique 6-6
Table 6-5. “What if?” analysis technique 6-7
Table 6-6. Brainstorming structured technique 6-8
Table 6-7. Functional analysis technique using critical factors analysis 6-9

Table 6-8. Outside-in thinking technique 6-10
Table 6-9. Red hat/team analysis technique 6-12
Table 7-1. Intelligence analysis support to functional elements 7-3
Table 7-2. Intelligence requirements associated with operations to shape 7-6
Table 7-3. Intelligence requirements associated with operations to prevent 7-7
Table 7-4. Intelligence requirements associated with large-scale ground combat operations 7-7
Table 7-5. Intelligence requirements associated with the offense 7-9
Table 7-6. Intelligence requirements associated with the defense 7-10
Table 7-7. Intelligence requirements associated with operations to consolidate gains 7-11
Table 8-1. Intelligence analysis (brigade combat team) example 8-2
Table 8-2. Intelligence analysis (division) example 8-5
Table 8-3. Intelligence analysis (tactical/operational [corps]) example 8-7
Table 9-1. Analytic design to tactical intelligence analysis crosswalk 9-7
Table C-1. Analytical actions and levels of rigor C-5
Table D-1. Threat analysis by warfighting function example D-2
Table D-2. Analyst considerations based on threat equipment capabilities D-4
Table E-1. Support to orders and briefings E-11
Table F-1. Battle damage assessment components F-9

This page intentionally left blank.

Preface

ATP 2-33.4 provides fundamental information to a broad audience, including commanders, staffs, and leaders, on how intelligence personnel conduct analysis to support Army operations. It describes the intelligence analysis process and specific analytic techniques and information on the conduct of intelligence analysis performed by intelligence personnel, especially all-source analysts, across all intelligence disciplines. Additionally, ATP 2-33.4 describes how intelligence analysis facilitates the commander's decision making and understanding of complex environments.

The principal audience for ATP 2-33.4 is junior to midgrade intelligence analysts conducting intelligence analysis. This publication provides basic information on intelligence analysis for commanders, staffs, and other senior military members.

ATP 2-33.4 readers must have an understanding of the following:

- Intelligence doctrine described in ADP 2-0 and FM 2-0.
- Collection management described in ATP 2-01.
- Intelligence preparation of the battlefield (IPB) described in ATP 2-01.3.
- Operational doctrine described in ADP 3-0 and FM 3-0.
- Joint targeting described in JP 3-60.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 6-27.)

This publication contains copyrighted material.

ATP 2-33.4 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

ATP 2-33.4 applies to the Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve unless otherwise stated.

The proponent of ATP 2-33.4 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Directorate of Doctrine and Intelligence Systems Training, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-DST-D (ATP 2-33.4), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017; by email to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

ATP 2-33.4 discusses doctrinal techniques—descriptive methods for performing missions, functions, or tasks as they apply to intelligence analysis. ATP 2-33.4—

- Describes the intelligence analysis process.
- Discusses structured analytic techniques and the methods for implementing them.
- Describes unique considerations related to intelligence analysis.

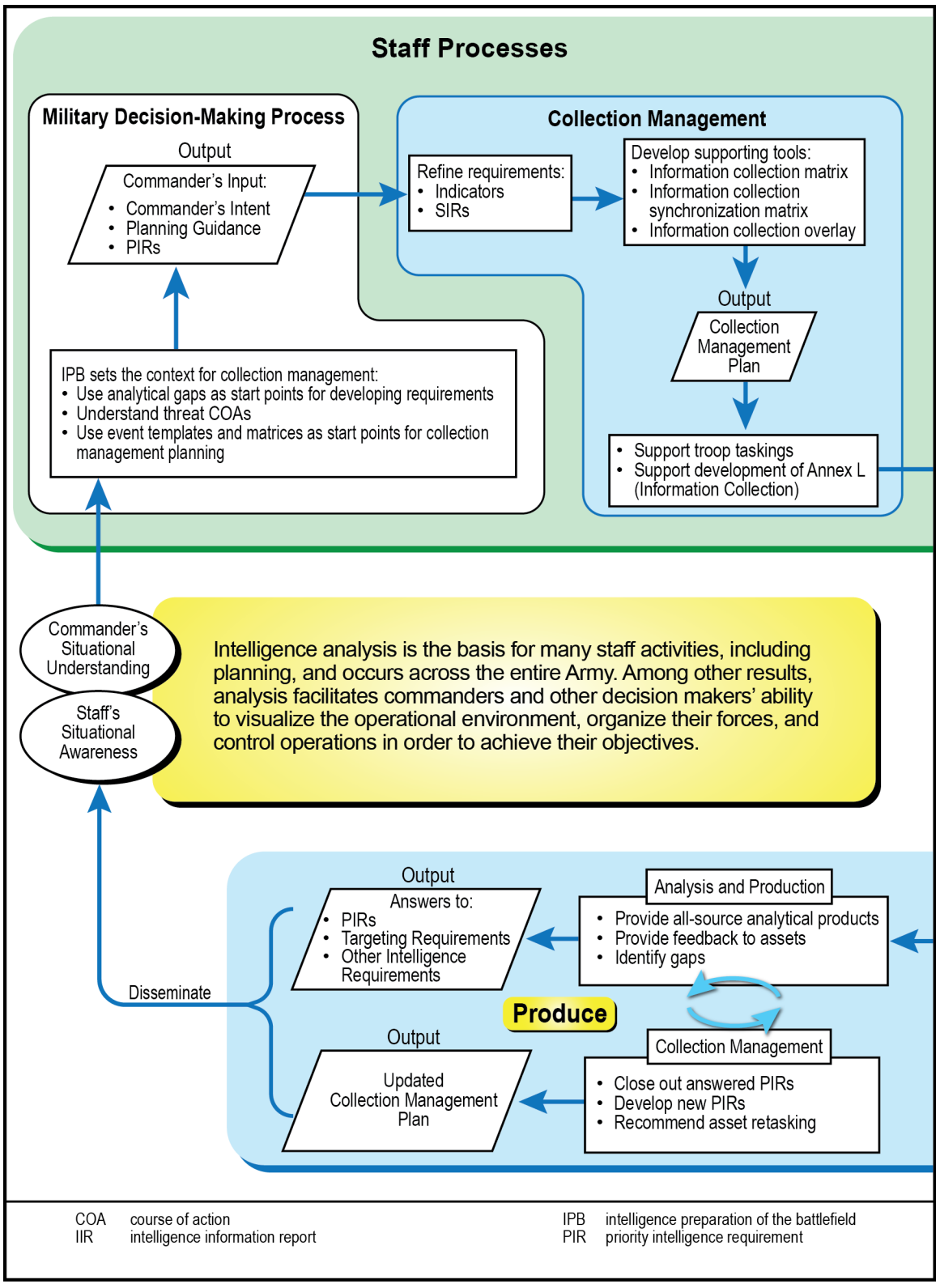
ATP 2-33.4 does not discuss—

- The Army's intelligence fundamentals and the intelligence warfighting function. See ADP 2-0 and FM 2-0 for the fundamentals.
- Techniques used to perform IPB and collection management. See ATP 2-01.3 and ATP 2-01, respectively.
- Information on how individual intelligence disciplines conduct specific tasks. See the appropriate intelligence discipline Army techniques publications.
- Specific organizational structures and manning information and specific techniques at echelons above corps, corps and divisions, and/or brigade combat teams. See classified ATP 2-19.1, ATP 2-19.3, and/or ATP 2-19.4, respectively.

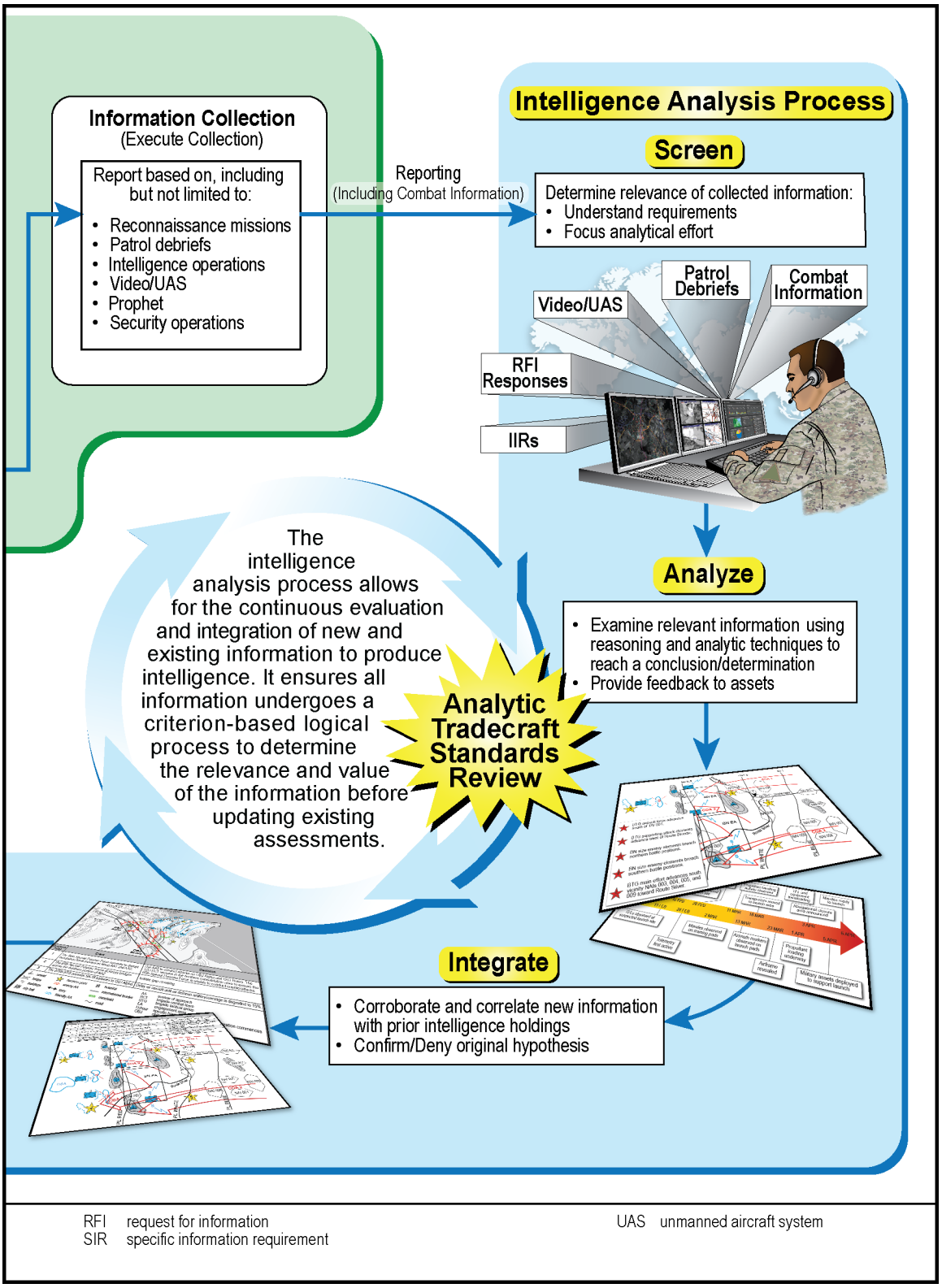
Intelligence analysis is central to intelligence. It is the basis for many staff activities, including planning, and occurs across the entire Army. Among other results, analysis facilitates commanders and other decision makers' ability to visualize the operational environment (OE), organize their forces, and control operations to achieve their objectives. To understand the role of intelligence analysis, intelligence professionals must understand how intelligence analysis corresponds with other staff processes, especially the military decision-making process and information collection (including collection management).

+The introductory figure on pages x and xi displays the intelligence analysis process and shows how intelligence analysis fits with the other staff processes to facilitate the commander's understanding:

- The commander's initial intent, planning guidance, and priority intelligence requirements (PIRs) drive the collection management plan.
- The entire staff, led by the intelligence and operations staffs, develops the information collection plan that results in reporting.
- All-source intelligence is based on information from all intelligence disciplines, complementary intelligence capabilities, and other available sources, such as reconnaissance missions, patrol debriefs, and security operations.
- Information collected from multiple sources moves through the intelligence analysis process, resulting in intelligence.
- The intelligence staff conducts all-source analysis and produces timely, accurate, relevant, predictive, and tailored intelligence that satisfies the commander's requirements and facilitates the commander's situational understanding and the staff's situational awareness.



+Introductory figure. Intelligence analysis at a glance



+Introductory figure. Intelligence analysis at a glance (*continued*)

ATP 2-33.4 updates and describes the fundamentals of intelligence analysis. ATP 2-33.4 has nine chapters and six appendixes:

- **Chapter 1** provides an overview of intelligence analysis based on the Army's mission, providing intelligence professionals with the fundamentals they must understand to conduct intelligence analysis. The overview also includes the role of intelligence analysis in the Army's mission to fight for intelligence as peer threats counter information collection efforts and during large-scale ground combat operations.
- **Chapter 2** describes the intelligence analysis process (screen, analyze, integrate, and produce) and how it will be executed to answer the commander's PIRs.
- **Chapter 3** identifies and defines the all-source analytical tasks and how their application facilitates commanders and other decision makers' visualization.
- **Chapter 4** discusses intelligence analysts' use of analytic techniques and tools to solve intelligence problems and to limit analytical errors. This chapter introduces those structured analytic techniques discussed further in chapters 5 and 6.
- **Chapter 5** describes the basic and diagnostic structured analytic techniques, which improve the assessment and presentation of a finished intelligence product.
- **Chapter 6** describes those advanced structured analytic techniques required by analytic teams to prove or disapprove current or sometimes opposing analytical assessments. These techniques allow for greater absorption of alternative perspectives through cognitive processes.
- **Chapter 7** discusses how the tasks performed by intelligence analysts differ significantly based on the echelon, the supported functional element, the Army's strategic roles, and the specific mission.
- **Chapter 8** presents three tactical to operational examples that illustrate the situation a unit might encounter along the forward edge of the battle area with friendly and threat forces poised to engage in large-scale ground combat.
- **Chapter 9** discusses managing long-term analytical assessments, also referred to as analytic design, to ensure the analytical effort is properly focused and carefully planned and executed, and analytical results are communicated effectively to the requestor.
- **Appendix A** briefly describes the role of automation in enabling intelligence analysis to facilitate real-time collaboration, detailed operational planning, and support to collection management.
- +**Appendix B** provides intelligence analytical skills for intelligence analysts, detailing critical and creative thinking, basic thinking abilities, and how to avoid analytical pitfalls—all of which when applied ensure accurate, timely, and reliable intelligence to the commander. These skills are essential for anyone conducting analysis, but not necessarily through the intelligence analysis process.
- **Appendix C** details the Intelligence Community Analytic Standards established by Intelligence Community Directive 203, as well as the integration of the standards into Army intelligence analysis in action.
- **Appendix D** describes the threat and provides threat considerations based on threat doctrine, capabilities, and equipment that may assist intelligence analysts during large-scale ground combat operations in identifying likely threat requirements.
- **Appendix E** discusses intelligence production, specifically those reports and presentations required to support operations.
- **Appendix F** discusses how intelligence analysts support the overall targeting effort.

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).
- 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 *G-2/S-2* and *G-3/S-3* to denote the *division or corps/battalion or brigade intelligence staff officer* and *division or corps/battalion or brigade operations staff officer*, respectively.
- Uses the term *threat*, which includes all enemies and adversaries that are part of the OE.

PART ONE

Fundamentals

Chapter 1

Understanding Intelligence Analysis

INTELLIGENCE ANALYSIS OVERVIEW

1-1. *Analysis* is the compilation, filtering, and detailed evaluation of information to focus and understand that information better and to develop knowledge or conclusions. In accordance with ADP 6-0, *information* is, in the context of decision making, data that has been organized and processed in order to provide context for further analysis (ADP 6-0). Information generally provides some of the answers to the *who*, *what*, *where*, *when, why*, and *how* questions. *Knowledge* is, in the context of decision making, information that has been analyzed and evaluated for operational implications (ADP 6-0). Knowledge assists in ascribing meaning and value to the conditions or events within an operation. Analysis performed by intelligence personnel assists in building the commander's knowledge and understanding. ADP 6-0 provides an in-depth discussion on how commanders and staffs process data to progressively develop their knowledge to build and maintain their situational awareness and understanding. (See figure 1-1.)

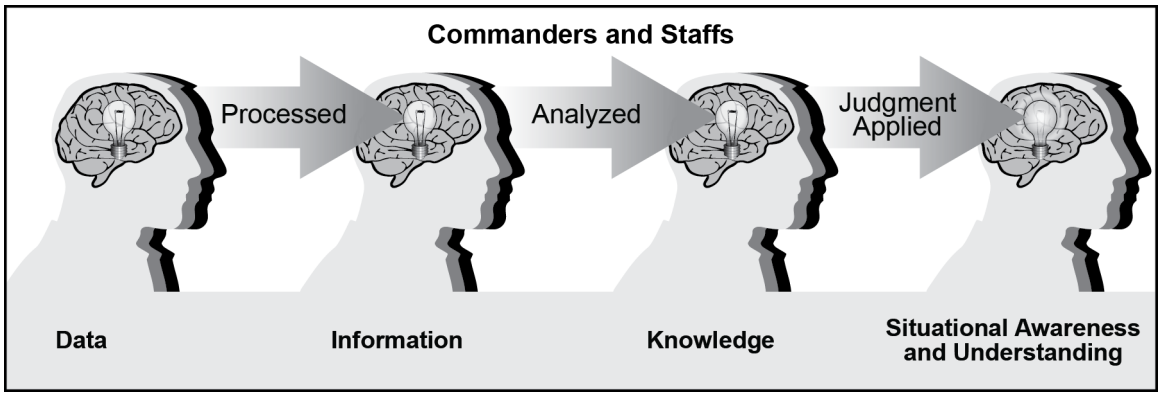


Figure 1-1. Achieving situational awareness and understanding

1-2. Analysis is the basis for many staff activities, including planning, and occurs across the entire Army. Among other results, analysis facilitates commanders and other decision makers' ability to visualize the operational environment (OE), organize their forces, and control operations in order to achieve their objectives.

1-3. Intelligence analysis is a form of analysis specific to the intelligence warfighting function. It is continuous and occurs throughout the intelligence and operations processes. *Intelligence analysis* is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production (ADP 2-0). Analysts conduct intelligence analysis to produce timely, accurate, relevant, and predictive intelligence for dissemination to the commander and staff. The purpose of intelligence analysis is to describe past, current, and attempt to predict future threat capabilities, activities, and tactics; terrain and weather conditions; and civil considerations.

1-4. Army forces compete with an adaptive enemy; therefore, perfect information collection, intelligence planning, intelligence production, and staff planning seldom occur. Information collection is not easy, and a single collection capability is not persistent and accurate enough to provide all of the answers. Intelligence analysts will be challenged to identify erroneous information and enemy deception, and commanders and staffs will sometimes have to accept the risk associated with incomplete analysis based on time and information collection constraints.

1-5. Some unique aspects of intelligence analysis include—

- The significant demand on analysts to compile and filter vast amounts of information in order to identify information relevant to the operation.
- The need for analysts to clearly separate confirmed facts from analytical determinations and assessments.
- Insight into how the physical environment (terrain, weather, and civil considerations) may affect operations.
- The ability to assess complex situations across all domains and the information environment.

1-6. Although ATP 2-33.4 is the primary publication for the intelligence analyst, it is designed to be used with ADP 2-0, *Intelligence*, and FM 2-0, *Intelligence*. ADP 2-0 discusses various aspects of intelligence analysis within a few different doctrinal constructs (see figure 1-2):

- As one of the four intelligence core competencies in chapter 2.
- As an inherent part of the steps and continuous activities of the intelligence process in chapter 3.
- As a part of or closely related to all-source intelligence, single-source intelligence capabilities, and intelligence processing, exploitation, and dissemination capabilities in chapter 4.

1-7. Intelligence analysis comprises single-source analysis and all-source analysis. ADP 2-0 discusses both single-source and all-source intelligence capabilities. As shown in figure 1-2, single-source intelligence capabilities comprise the intelligence disciplines, complementary intelligence capabilities, and multifunction intelligence units. Single-source and all-source intelligence capabilities include but are not limited to—

- Single-source analytical elements:
  - Brigade combat team (BCT) human intelligence (HUMINT) analysis cell.
  - Division signals intelligence cell.
  - Corps counterintelligence analysis cell.
  - Brigade through corps geospatial intelligence cells.
- All-source analytical elements:
  - Battalion intelligence cell.
  - Brigade intelligence support element (also known as BISE).
  - Division analysis and control element (ACE).
  - Corps ACE.
  - Theater army ACE.
  - National Ground Intelligence Center (NGIC).

Note. In this publication, all-source analytical elements include the intelligence staff for each unit as well as its supporting analytical element when applicable.

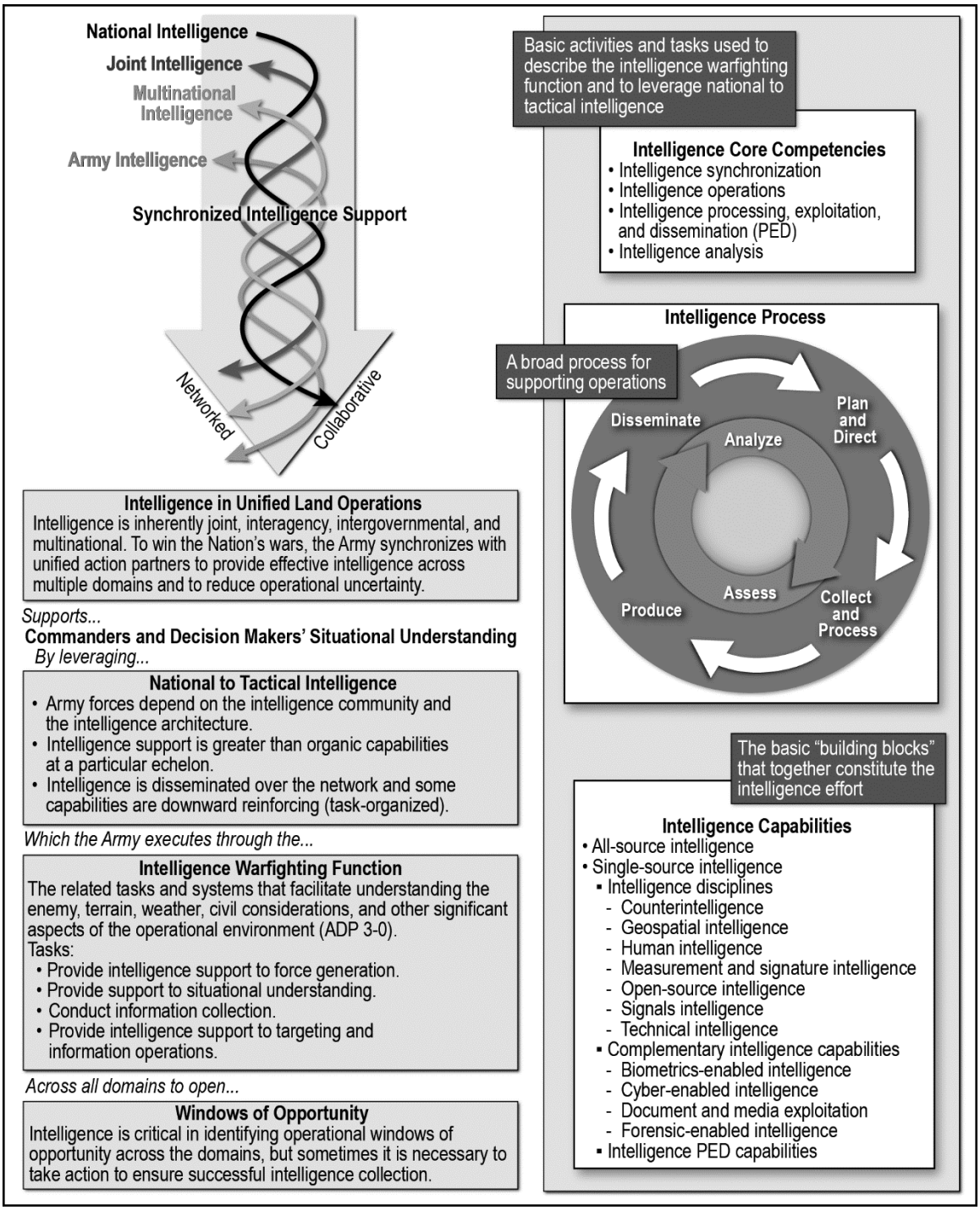


Figure 1-2. Intelligence analysis within doctrinal constructs

SINGLE-SOURCE ANALYSIS

1-8. Single-source collection is reported to single-source analytical elements. Single-source analytical elements conduct continuous analysis of the information provided by single-source operations. Following single-source analysis, analytical results are disseminated to all-source analytical elements for corroboration, to update the common operational picture, and to refine all-source intelligence products. A continuous analytical feedback loop occurs between all-source analytical elements, single-source analytical elements, and collectors to ensure effective intelligence analysis. Figure 1-3 provides a simplified example of this single-source to all-source information flow for HUMINT reporting and analysis at the BCT level.

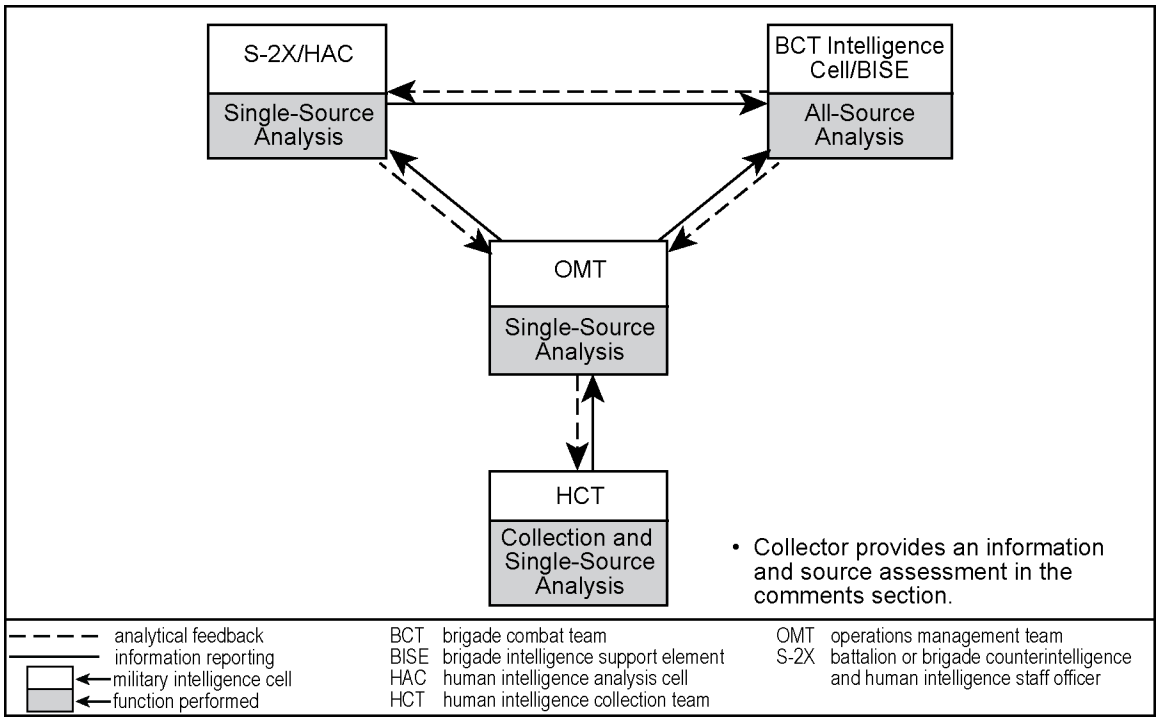


Figure 1-3. Information and intelligence reporting example

1-9. Several portions of this publication apply to single-source analysis, especially the intelligence analysis process in chapter 2 and the analytic techniques in chapters 4 through 6. Specific doctrine on single-source analysis is contained in the following publications:

- Intelligence disciplines:
  - For counterintelligence analysis, see ATP 2-22.2-1, *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities*, chapter 4.
  - For HUMINT analysis, see FM 2-22.3, *Human Intelligence Collector Operations*, chapter 12.
  - For open-source intelligence analysis, see ATP 2-22.9, *Open-Source Intelligence*, chapters 1, 2, and 3.
  - For signals intelligence analysis, see ATP 2-22.6-2, *Signals Intelligence Volume II: Reference Guide*, appendix G.
- Complementary intelligence capabilities:
  - For biometrics-enabled intelligence analysis (the foundation of identity intelligence), see ATP 2-22.82, *Biometrics-Enabled Intelligence*, chapter 7.
  - For document and media exploitation (DOMEX) analysis, see ATP 2-91.8, *Techniques for Document and Media Exploitation*, chapter 9.

ALL-SOURCE ANALYSIS AND PRODUCTION

1-10. Various all-source analytical elements integrate intelligence and information from all relevant sources (both single-source and other information collection sources) to provide the most timely, accurate, relevant, and comprehensive intelligence possible and to overcome threat camouflage, counterreconnaissance, and deception. All-source analytical elements, such as the brigade intelligence support element or ACE, are functionally aligned to support the commander and the intelligence staff. The intelligence staff is integrated with the rest of the staff to ensure they have a thorough understanding of the overall operation, the current situation, and future operations. Additionally, all-source analytical elements often corroborate their analytical determinations and intelligence products through access to and collaboration with higher, lower, and adjacent all-source analytical elements.

1-11. All-source intelligence analysts use an array of automation and other systems to perform their mission. (See appendix A.) From a technical perspective, all-source analysis is accomplished through the fusion of single-source information with existing intelligence in order to produce intelligence. For Army purposes, *fusion* is consolidating, combining, and correlating information together (ADP 2-0). Fusion occurs as an iterative activity to refine information as an integral part of all-source analysis and production.

1-12. With the vast amounts of information and broad array of all-source intelligence capabilities, the G-2/S-2 provides the commander and staff with all-source intelligence. All-source intelligence products inform the commander and staff by facilitating situational understanding, supporting the development of plans and orders, and answering priority intelligence requirements (PIRs), high-payoff targets (HPTs), and other information requirements.

1-13. The G-2/S-2 can use single-source intelligence to support the commander and staff. In those instances, it is best to first send that single-source intelligence to the all-source analytical element to attempt to quickly corroborate the information. Corroboration reduces the risk associated with using that single-source intelligence by comparing it to other information reporting and existing intelligence products. Following corroboration and dissemination of the intelligence to the commander and staff, the all-source analytical element incorporates the single-source intelligence into the various all-source intelligence products and the threat portion of the common operational picture.

1-14. In certain situations and specific organizations, especially at echelons above corps, a single-source analytical element can produce single-source intelligence products for dissemination to the commander and staff without all-source corroboration. However, there is significant risk in using uncorroborated single-source intelligence at the tactical level. For example, a BCT commander may choose to make decisions based on a single HUMINT report. This is similar to the commander using combat information to make decisions during an operation. In those situations, the commander and G-2/S-2 should be aware of and try to mitigate the risk associated with using uncorroborated single-source reporting and intelligence.

Note. *Combat information* is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements (JP 2-01).

CONDUCTING INTELLIGENCE ANALYSIS

1-15. The goal of intelligence analysis is to provide timely and relevant intelligence to commanders and leaders to support their decision making. Intelligence analysis requires the continuous examination of information and intelligence about the threat and significant aspects of the OE. To be effective, an intelligence analyst must—

- Understand and keep abreast of intelligence doctrine.
- Maintain complete familiarity on all aspects of the threat, including threat capabilities, doctrine, and operations.

- Have knowledge on how to account for the effects of the mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations [METT-TC]) and operational variables (political, military, economic, social, information, infrastructure, physical environment, and time [PMESII-PT]) on operations.
- Thoroughly understand operational doctrine (especially FM 3-0, *Operations*), operational and targeting terminology, and operational symbology.

1-16. Analysts conduct intelligence analysis to ultimately develop effective intelligence. They do this by applying the basic thinking abilities (information ordering, pattern recognition, and reasoning) and critical and creative thinking, all described in appendix B. FM 2-0 describes the characteristics of effective intelligence as accurate, timely, usable, complete, precise, reliable, relevant, predictive, and tailored. Beyond those characteristics, intelligence analysts must also understand the six aspects of effective analysis:

- Embracing ambiguity.
- Understanding intelligence analysis is imperfect.
- Meeting analytical deadlines with the best intelligence possible.
- Thinking critically.
- Striving to collaborate closely with other analysts.
- Adhering to analytic standards as much as possible.

EMBRACING AMBIGUITY

1-17. Intelligence personnel must accept and embrace ambiguity in conducting analysis as they will never have all the information necessary to make certain analytical determinations. Intelligence analysts will be challenged due to the constantly changing nature of the OE and the threat and to the fog of war—all imposed during large-scale ground combat operations, creating complex, chaotic, and uncertain conditions. Intelligence analysts must understand the OE is complex; embrace ambiguity; and recognize and mitigate their own or others' biases, challenge their assumptions, and continually learn while conducting analysis across the breadth of operations.

1-18. Analysts operate within a time-constrained environment and with limited information. Therefore, they may sometimes produce intelligence that is not as accurate and detailed as they would prefer. Having both an adequate amount of information and extensive subject matter expertise does not guarantee the development of logical or accurate determinations. To be effective, analysts must have—

- A detailed awareness of their commander's requirements and priorities.
- An understanding of the limitations in information collection and intelligence analysis.
- A thorough knowledge of the OE and all aspects of the threat.
- Expertise in applying the intelligence analysis process and analytic techniques.

1-19. The effective combination of the aforementioned bullets provides intelligence analysts with the best chance to produce accurate and predictive intelligence and also to detect threat denial and deception efforts. To adequately account for complexity and ambiguity, intelligence analysts should continually identify gaps in their understanding of the OE and the threat, and factor in those gaps when conducting intelligence analysis.

ANALYTICAL IMPERFECTION

1-20. Given the ambiguity, fog of war, and time-constraints, intelligence analysts must accept imperfection. As much as possible, analysts should attempt to use validated facts, advanced analytic techniques, and objective analytical means. However, using them and providing completely objective and detailed analytical determinations may be challenging, especially during tactical operations. Analysts should also consider that logical determinations are not necessarily facts.

1-21. When presenting analytical determinations to the commander and staff, intelligence personnel must ensure they can answer the *so what* question from the commander's perspective. Additionally, they should clearly differentiate between what is relatively certain, what are reasonable assumptions, and what is unknown, and then provide the degree of confidence they have in their determination as well as any significant issues associated with their analysis. This confidence level is normally subjective and based on—

- The collection asset's capability (reliability and accuracy).
- Evaluation criteria.
- The confidence in the collected data.
- The analyst's expertise and experience.
- Intelligence gaps.
- The possibility of threat deception.

1-22. Intelligence analysts should be prepared to explain and justify their conclusions to the commander and staff. Over time, the all-source analytical element should learn the most effective way to present analytical determinations to the commander and staff. A deliberate and honest statement of what is relatively certain and what is unknown assists the commander and staff in weighing some of the risks inherent in the operation and in creating mitigation measures.

MEETING ANALYTICAL DEADLINES

1-23. Analysts must gear their efforts to the time available and provide the best possible intelligence within the deadline. Operational planning and execution deadlines often impose challenging time constraints that analysts must meet. Analysts must often produce intelligence without all of the information that would result in a more thorough or certain analytical determination. Analysts must meet the deadline because a quick analytical assessment in time to affect staff planning and friendly courses of action (COAs) is far better than a perfect analytical assessment that is received too late to affect staff planning.

CRITICAL THINKING

1-24. +Intelligence analysts must know how to arrive at logical, well-reasoned, and unbiased conclusions as a part of their analysis. Analysts strive to reach determinations based on facts and reasonable assumptions, but providing accurate intelligence assessments and predictions about enemy actions is difficult. Discerning facts, making assumptions, and inferring accurately are challenging with an uncooperative and adaptive enemy. For example, analysts cannot know what an enemy commander or staff is thinking; consequently, they can make decisions based on incorrect information, assumptions, emotions, and/or undisciplined thinking. Additionally, during operations, actions can occur by accident. Therefore, critical thinking—disciplined and self-reflective thinking—is essential to analysis. Applying critical and creative thinking provides more holistic, logical, ethical, and unbiased analyses and determinations. This will improve the quality of intelligence analysis although intelligence results will not be perfect. Even when an assessment is not perfect, it can be invaluable to planning because it addresses different possible enemy intents and COAs, associated probabilities, and likely implications. Despite significant time-constraints and stress due to combat situations, intelligence analysts with solid critical thinking habits provide better analysis. (See appendix B for mor information on critical and creative thinking.)

COLLABORATION

1-25. Commanders, intelligence and other staffs, and intelligence analysts must collaborate. They should actively share and question information, perceptions, and ideas to better understand situations and produce intelligence. Collaboration is essential to analysis; it ensures analysts work together to achieve a common goal effectively and efficiently. Analysts can leverage national to tactical intelligence, using Department of Defense (DOD) intelligence capabilities, to enable analytical collaboration and assist them in producing intelligence.

1-26. Through collaboration, analysts develop and enhance professional relationships, access each other's expertise, enhance their understanding of the issues, and expand their perspectives on critical analytical issues. Collaboration is another means, besides critical thinking, by which intelligence analysts avoid potential pitfalls, such as mindsets and biases, and detect threat denial and deception efforts. (For information on analytical pitfalls, see appendix B.)

ADHERING TO ANALYTIC STANDARDS

1-27. As much as possible, the conclusions reached during intelligence analysis should adhere to analytic standards, such as those established by the Director of National Intelligence in Intelligence Community Directive (ICD) 203, to determine the relevance and value of the information before updating existing assessments. (See figure 1-4.) These standards govern the production and evaluation of national intelligence analysis to meet the highest standards of integrity and rigorous analytic thinking. Although created for national-level intelligence agencies, these analytic standards are also valid at the operational and tactical levels. (See appendix C for a detailed discussion of the analytic standards.)

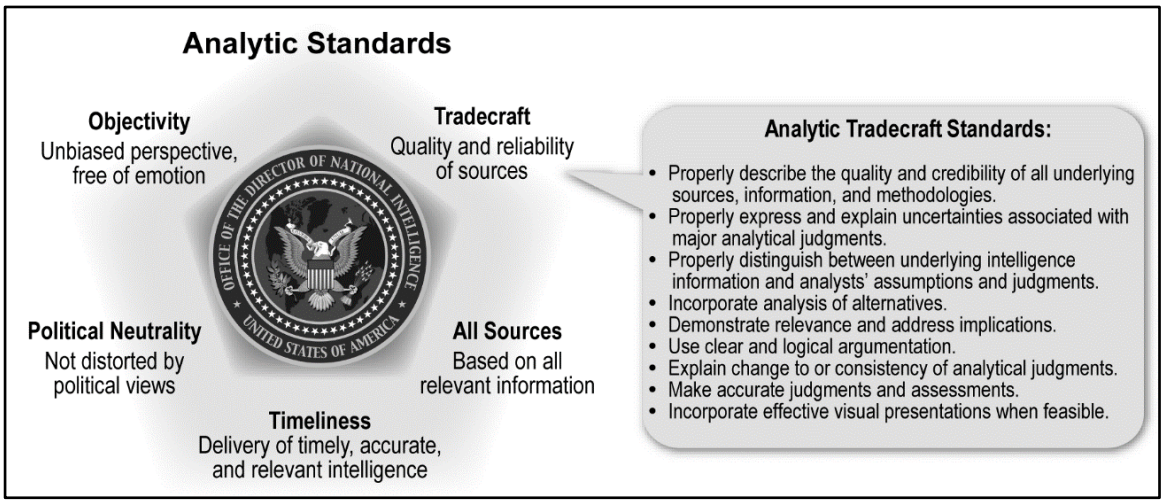


Figure 1-4. Analytic standards

INTELLIGENCE ANALYSIS AND COLLECTION MANAGEMENT

1-28. While collection management is not part of intelligence analysis, it is closely related. Analysis occurs inherently throughout collection management, and intelligence analysts must understand the information collection plan.

1-29. Collection management is a part of the larger information collection effort. Information collection is an integrated intelligence and operations function. ATP 2-01 discusses collection management in detail. The intelligence staff performs the collection management process in collaboration with the operations staff. The collection management process comprises the following tasks:

- Develop requirements.
- Develop the collection management plan.
- Support tasking and directing.
- Assess collection.
- Update the collection management plan.

Note. *Plan requirements and assess collection*, as an information collection task, has been replaced with the term *collection management*.

1-30. The intelligence warfighting function focuses on answering commander and staff requirements, especially PIRs, which are part of the commander's critical information requirements. Intelligence analysis for a particular mission begins with information collected based on commander and staff requirements (which are part of collection management); those requirements are usually developed within the context of existing intelligence analysis. Together, these two activities form a continuous cycle—intelligence analysis supports collection management and collection management supports intelligence analysis. The G-2/S-2 must synchronize these two activities, and analysts and personnel within both activities must cooperate and collaborate closely to enable effective intelligence support.

1-31. Intelligence analysis and collection management overlap or intersect in several areas. While not all inclusive, the following includes some of these areas:

- The all-source intelligence architecture and analysis across the echelons are important aspects of planning effective information collection. To answer the PIR and present the commander and staff with a tailored intelligence product, there must be adequate time. Collection management personnel must understand the all-source intelligence architecture and analysis across the echelons and consider those timelines.
- Collection management personnel depend on the intelligence analysis of threats, terrain and weather, and civil considerations in order to perform the collection management process. Intelligence preparation of the battlefield (IPB) often sets the context for collection management:
  - Intelligence analytical gaps are the start points for developing requirements.
  - All-source analysts and collection management personnel must understand the threat COAs and how to execute those COAs as reflected in the situation templates.
  - Event templates and event matrices are the start points for developing subsequent collection management tools.
- All-source analysts and collection management personnel—
  - Use and refine threat indicators during the course of an operation.
  - Mutually support and track threat activities relative to the *decide*, *detect*, *deliver*, and *assess* (also called D3A) functions of the targeting methodology.
  - Must confer before answering and closing a PIR.
- The effectiveness of intelligence analysis is an integral part of assessing the effectiveness of the information collection plan during collection management.

1-32. A disconnect between intelligence analysis and collection management can cause significant issues, including a degradation in the overall effectiveness of intelligence support to the commander and staff. Therefore, intelligence analysts and collection management personnel must collaborate closely to ensure they understand PIRs, targeting and information operations requirements (when not expressed as PIRs), threat COAs and other IPB outputs, the current situation, and the context/determinations surrounding current threat activities.

THE ALL-SOURCE INTELLIGENCE ARCHITECTURE AND ANALYSIS ACROSS THE ECHELONS

1-33. All-source analysis, collaboration, and intelligence production occur both within and between echelons. Intelligence analysts not only integrate the broad array of information collected and intelligence produced at their echelon, but they also collaborate across the various echelons and the intelligence community to benefit from the different knowledge, judgments, experience, expertise, and perceptions—all invaluable to the analytical effort. Intelligence analysis is facilitated by an all-source push (deliberately sending) and pull (accessing from a different unit) of information and intelligence. Figure 1-5 on page 1-10 depicts single-source collection and analysis as a layer of the all-source intelligence architecture across the echelons. Chapter 7 details intelligence analysis across the echelons.

1-34. At the different echelons, based on a number of factors, the intelligence staff and supporting all-source analytical element are divided into teams to support the various command posts and to perform the various all-source analytical tasks. There is no standard template on how best to structure the all-source analytical effort. The G-2/S-2 decides on an all-source structure that is optimized to support command and control and is requirements-driven based on ongoing operations.

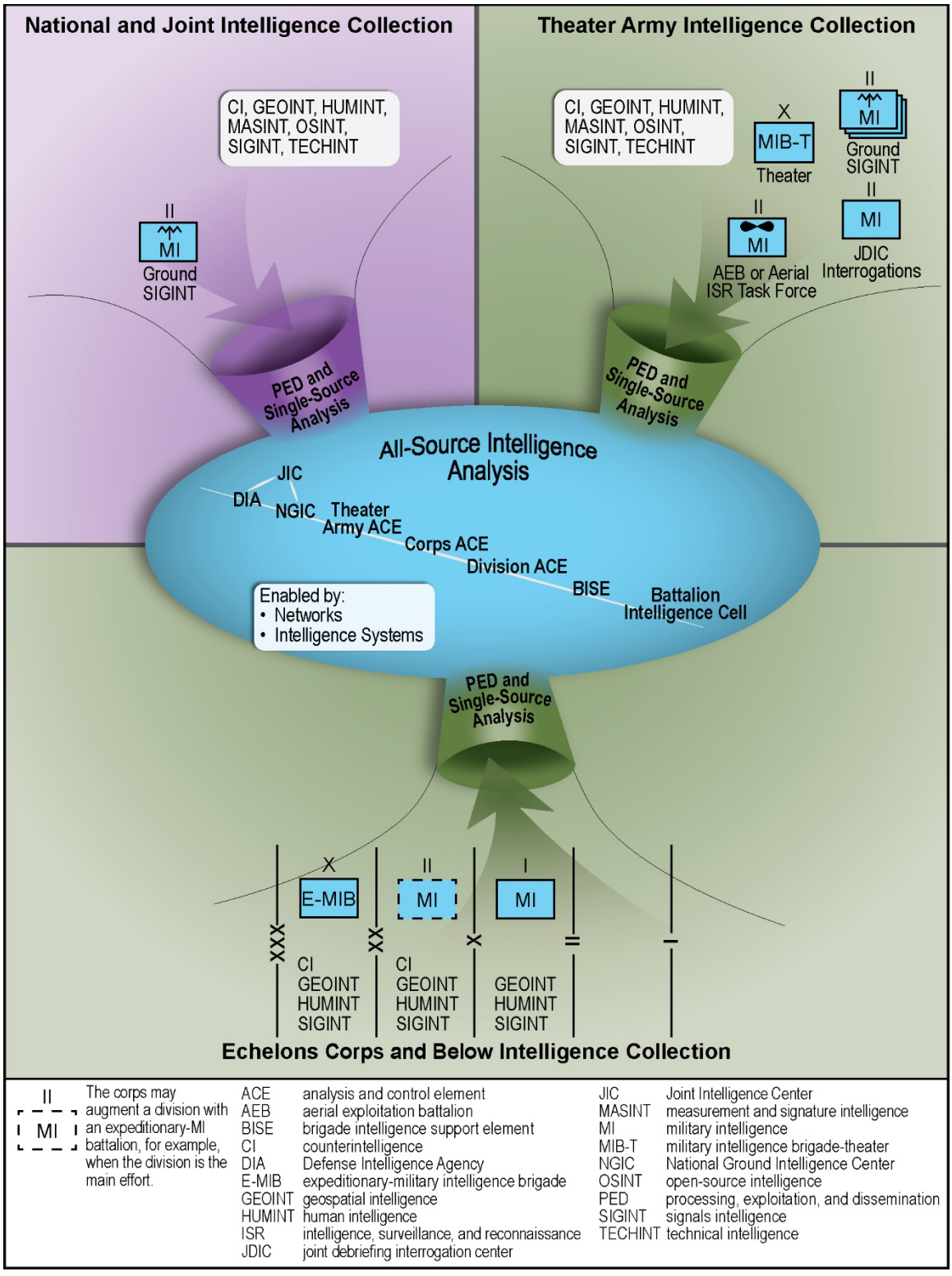


Figure 1-5. All-source analysis across the echelons

INTELLIGENCE ANALYSIS DURING LARGE-SCALE GROUND COMBAT OPERATIONS

1-35. FM 3-0, published in October 2017, provided a new operational focus for the Army and introduced the Army's strategic roles (shape OEs, prevent conflict, prevail in large-scale ground combat, and consolidate gains). FM 3-0 clearly states that while Army forces cannot focus solely on large-scale ground combat operations at the expense of other missions, Army forces cannot afford to be unprepared for large-scale combat operations in an increasingly unstable world. ADP 2-0, published in July 2019, and FM 2-0, published in July 2018, reinforce this focus, providing extensive discussions on intelligence within large-scale ground combat operations.

1-36. ADP 3-0, *Operations*, published in July 2019, provided a definition for large-scale combat operations and created a new term, large-scale ground combat operations. *Large-scale combat operations* are extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives (ADP 3-0). *Large-scale ground combat operations* are sustained combat operations involving multiple corps and divisions (ADP 3-0).

1-37. While the fundamentals of intelligence analysis remain constant across the Army's strategic roles, large-scale ground combat operations create some unique challenges for the intelligence analyst. (See table 1-1.) The fluid and chaotic nature of large-scale ground combat operations will cause the greatest degree of fog, friction, uncertainty, and stress on the intelligence analysis effort. Army forces will have to fight for intelligence as peer threats will counter information collection efforts, forcing commanders to make decisions with incomplete and imperfect intelligence. These realities will strain all-source analysis.

Table 1-1. Intelligence analysis during large-scale ground combat operations

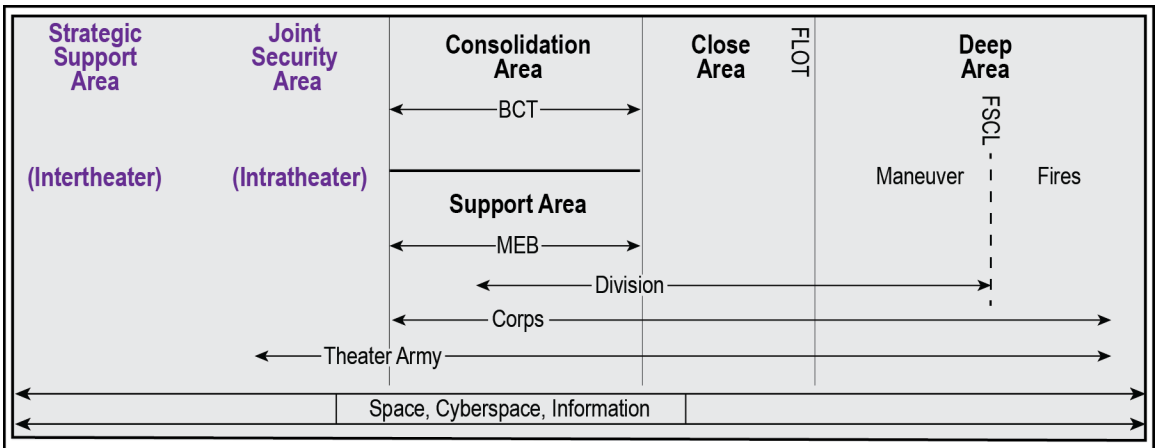
Army strategic role	*Intelligence analysis support*
Prevail in large-scale ground combat	Analysts— • Perform intelligence preparation of the battlefield as part of the military decision-making process to support deployment into a theater of operations. • While collecting and screening information, immediately report relevant combat information to the commander. • Ensure all analysis efforts support the unit commander's intent and guidance, established during the military decision-making process. • Continually update the running estimates and disseminate products to commanders and staffs. • Support current operations—integrate information by updating the common operational picture and continually communicating with other staff sections. • Support target development and detection by ensuring collection plans support the overall targeting plan.

1-38. Over the past 20 years, the Nation's peer threats have increased their capabilities and gained an understanding of United States (U.S.) and allied operations. According to ADP 3-0, a peer threat is an adversary or enemy able to effectively oppose U.S. forces worldwide while enjoying a position of relative advantage in a specific region. Peer threats—

- Can generate equal or temporarily superior combat power in geographical proximity to a conflict area with U.S. forces.
- May have a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary.
- Generate tactical, operational, and strategic challenges in order of magnitude more challenging militarily than other adversaries.
- Can employ resources across multiple domains to create lethal and nonlethal effects with operational significance throughout an OE.
- Seek to delay deployment of U.S. forces and inflict significant damage across multiple domains in a short period to achieve their goals before culminating.

1-39. During large-scale ground combat operations, intelligence analysts will have to predict and track rapidly evolving events across the various threat capabilities. (See appendix D.) For this reason, intelligence analysts must understand many of the operational concepts discussed in FM 3-0 and discussed from an intelligence perspective in FM 2-0. These doctrinal concepts include—

- **Multi-domain operations**, including **windows of opportunity**, discussed in FM 3-0, chapter 1, and FM 2-0, chapter 1.
- **Positions of relative advantage**, discussed in FM 3-0, chapter 1.
- **Operational art**, discussed in ADP 3-0, chapter 2, and FM 3-0, chapter 1.
- The new **operational framework**, discussed in FM 3-0, chapter 1, and FM 2-0, chapter 1.
- The new **key physical aspects of the operational framework**, discussed in FM 2-0, chapter 1. (See figure 1-6.)
- **Fighting for intelligence**, discussed in FM 3-0, chapter 2, and FM 2-0, chapter 6.



The strategic support area describes the area extending from a theater of operations to a continental United States base, or another combatant commander's area of responsibility, that contains those organizations, LOCs, and other agencies required in the field. It includes the air and seaports supporting the flow of forces and sustainment into the theater.

The joint security area is a specific surface area, designated by the joint force commander, to facilitate protection of joint bases and their connecting LOCs that support joint operations.

The consolidation area is the portion of the commander's AO that is designated to facilitate the security and stability tasks necessary for freedom of action in the close area and to support the continuous consolidation of gains.

The support area is the portion of the commander's AO that is designated to facilitate the positioning, employment, and protection of the base sustainment assets required to sustain, enable, and control operations.

The close area is the portion of a commander's AO assigned to subordinate maneuver forces.

The deep area is the portion of the commander's AO that is not assigned to subordinate units.

The deep area is divided into —

- Deep area (maneuver): The zone between the FLOT and the FSCL is typically the area over which friendly ground forces intend to maneuver in the near future and is also the area where joint air interdiction operations are normally executed through the air support operations center/direct air support center.
- Deep area (fires): Interdiction best describes how Army and joint fires are typically employed in the deep area. *Interdiction* is an action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives (JP 3-03).

AO area of operations
BCT brigade combat team
FLOT forward line of own troops
FSCL fire support coordination line
LOC line of communications
MEB maneuver enhancement brigade

Figure 1-6. Key aspects of the operational framework

1-40. As in all operations, intelligence drives operations and operations support intelligence; this relationship is continuous. The commander and staff need effective intelligence in order to understand threat centers of gravity, goals and objectives, and COAs. Precise intelligence is also critical to target threat capabilities at the right time and place and to open windows of opportunity across domains. Commanders and staffs must have detailed knowledge of threat strengths, weaknesses, equipment, and tactics to plan for and execute friendly operations.

1-41. Commanders and staffs accept some risks and operational uncertainty in all operations, especially during large-scale ground combat operations. The commander must allocate adequate time for information collection and intelligence analysis or determine the balance between time allotted to collection and analysis and to operational necessity. When there is not enough time for adequate information collection and intelligence analysis, the all-source analytical element must inform the G-2/S-2 of the gaps, issues, and risks, so the G-2/S-2 can inform the commander. In those cases, that unit must depend on the higher echelon all-source analytical element for additional support and overwatch.

1-42. One of the ultimate goals of intelligence analysis is to assist the unit in identifying and opening an operational window of opportunity to eventually achieve a position of relative advantage. Opening a window of opportunity often requires a significant amount of intelligence analysis in order to achieve a high degree of situational understanding. This will be difficult as friendly forces are often at a disadvantage in conducting information collection against the threat. Therefore, opening an operational window of opportunity may have to start with operations that support intelligence. In a sense, this is opening an information collection window of opportunity as part of the effort to fight for intelligence.

1-43. The staff must thoroughly plan, find creative solutions, and collaborate across echelons to overcome information collection challenges. Once friendly forces have an open window of opportunity to execute information collection, intelligence analysts will receive more information and should be able to provide timely and accurate intelligence products, updates, and predictive assessments. This timely and accurate intelligence can then assist friendly forces in opening subsequent windows of opportunity to reach positions of relative advantage.

1-44. Facilitating the commander and staff's situational understanding of the various significant aspects of the OE is challenging. Intelligence analysis must address important considerations across all domains and the information environment as well as support multi-domain operations. Intelligence analysis must include all significant operational aspects of the interrelationship of the air, land, maritime, space, and cyberspace domains; the information environment; and the electromagnetic spectrum. Intelligence analysts use information and intelligence from the joint force, U.S. Government, the intelligence community, and allies to better understand and analyze the various domains and peer threat capabilities.

INTELLIGENCE ANALYSIS DURING THE ARMY'S OTHER STRATEGIC ROLES

1-45. As part of a joint force, the Army operates across the strategic roles (shape OEs, prevent conflict, prevail in large-scale ground combat, and consolidate gains) to accomplish its mission to organize, equip, and train its forces to conduct sustained land combat to defeat enemy ground forces and to seize, occupy, and defend land areas. The unique aspects of large-scale ground combat operations were discussed in paragraphs 1-35 through 1-44. Each strategic role presents unique challenges and is often characterized by different analytical tasks, products, product timelines, and specific requirements. (See table 1-2 on page 1-14.)

Table 1-2. Intelligence analysis during the other Army strategic roles

Army strategic role	*Intelligence analysis support*
Shape operational environments	Analysts— • During periods of peace, identify peer threats or hostile element actions in regionally significant areas. This includes supporting contingency planning. • Develop regional expertise and generate intelligence knowledge for possible contingencies. • Provide warning intelligence at echelons above corps. • Identify second and third order effects of all friendly actions based on the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time). • Assist with security force assistance and theater engagement efforts and, when possible, in building an initial allied intelligence analysis architecture. • Support realistic training to improve regional awareness of potential peer threat capabilities and hybrid scenarios. • Conduct focused analysis as regional tensions increase and update operation plans as required.
Prevent conflict	
Consolidate gains	Analysts— • Assess the operational environment and identify how the local population reacts to stability operations. • Use diagnostic structured analytic techniques (see chapter 4) to compare their original estimates of the operational environment and identify changes that may affect stability operations. • Assess operational considerations for improvements to transition control to legitimate civil authorities.

Chapter 2

The Intelligence Analysis Process

OVERVIEW

2-1. Both all-source and single-source intelligence analysts use the intelligence analysis process. The process supports the continuous examination of information, intelligence, and knowledge about the OE and the threat to generate intelligence and reach one or more conclusions. Appendix B provides an overview of three analytic skills: basic thinking abilities, critical and creative thinking, and avoiding analytical pitfalls. Chapters 4 through 6 provide analytic techniques for conducting qualitative analysis. The application of the analytic skills and techniques assist analysts in evaluating specific situations, conditions, entities, areas, devices, or problems.

2-2. The intelligence analysis process includes the continuous evaluation and integration of new and existing information to produce intelligence. It ensures all information undergoes a criterion-based logical process, such as the analytic tradecraft standards established by ICD 203, to determine the relevance and value of the information before updating existing assessments. (See appendix C for a detailed discussion on the analytic tradecraft standards.)

2-3. The intelligence analysis process is flexible and applies to any intelligence discipline. Analysts may execute the intelligence analysis process meticulously by thoroughly screening information and applying analytic techniques, or they may truncate the process by quickly screening collected information using only basic structured analytic techniques. The process becomes intuitive as analysts become more proficient at analysis and understanding their assigned OE. The intelligence analyst uses collected information to formulate reliable and accurate assessments.

THE PHASES OF THE INTELLIGENCE ANALYSIS PROCESS

2-4. The phases of the intelligence analysis process are interdependent. (See figure 2-1 on page 2-2.) Through time and experience, analysts become more aware of this interdependence. The phases of the intelligence analysis process are—

- **Screen (collected information):** Determining the relevance of the information collected.
- **Analyze:** Examining relevant information.
- **Integrate:** Combining new information with current intelligence holdings to begin the effort of developing a conclusion or assessment.
- **Produce:** Making a determination or assessment that can be disseminated to consumers.

Note. *Relevant information* is all information of importance to the commander and staff in the exercise of command and control (ADP 6-0).

2-5. To successfully execute the intelligence analysis process, it is critical for analysts to understand the PIRs and other requirements related to the current OE and mission. This understanding assists analysts in framing the analytic problem and enables them to separate facts and analytical judgments. Analytical judgments form by generating hypotheses—preliminary explanations meant to be tested to gain insight and find the best answer to a question of judgment. (See chapter 6 for more on generating hypotheses.)

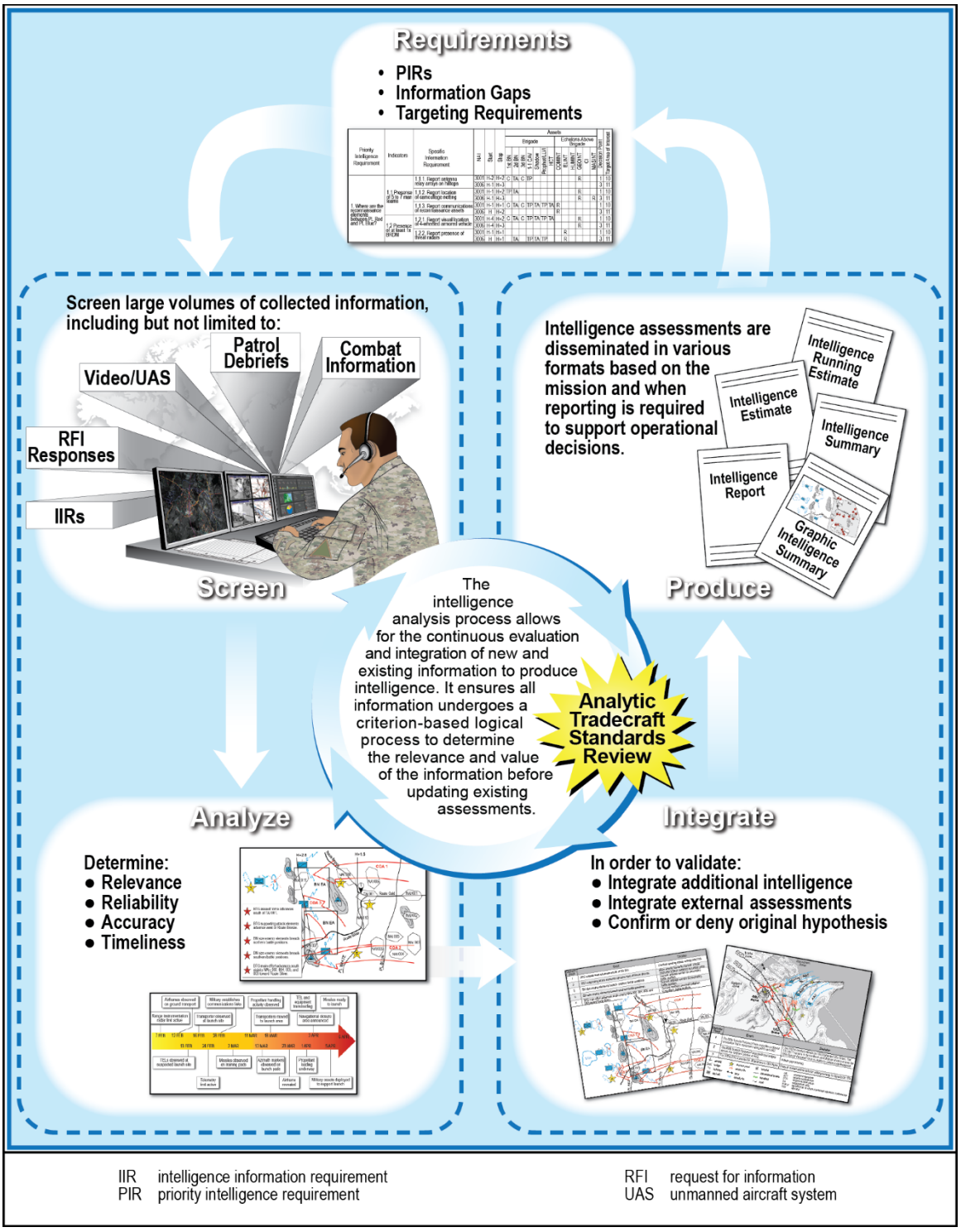


Figure 2-1. The intelligence analysis process

2-6. The following begins a series of examples that walk the reader through the intelligence analysis process from the reporting of requirements to the production and dissemination of intelligence to the commander and staff.

Example: Division Commander's PIRs

PIR 1: Will the motorized rifle division use the tank brigade as a southward exploitation force?

PIR 2: Where is the motorized rifle division's multiple launch rocket system (MLRS) battalion?

PIR 3: Where will displaced civilians impede U.S. combat forces' movement north?

Collection in the past hour provided six pieces of information for analysts to process and answer the commander's PIRs:

- Possible identification of two threat MLRSs as well as support equipment traveling west to east at 20 kilometers per hour along a road 15 kilometers north of the 1 BCT forward locations.
- Threat motorized rifle battalion in company strength engaging adjacent 2 BCT forward positions attempting to seize a hilltop out of sector at a (PK1234) general four-digit grid.
- The 1 BCT reports harassing small arms engagements along forward battalion locations.
- Approximately 28 or 30 threat tanks detected in convoy formations 40 kilometers north of the 1 BCT forward locations.
- Threat air defense elements active near possible headquarters and artillery locations detected.
- Multiple-source reporting that a threat tank brigade is preparing to advance south, seeking to exploit lead division penetration of 1 BCT forward positions.

SCREEN COLLECTED INFORMATION

2-7. During the execution of single-source intelligence or all-source analysis, analysts continuously filter the volume of information or intelligence received through the continuous push and pull of information. It is during the *screen* phase that analysts sort information based on relevancy and how it ties to the analytical questions or hypotheses they developed to fill information gaps. They do this by conducting research and accessing only the information that is relevant to their PIRs, mission, or time. Analysts also screen the volume of information based on the information source's reliability and the information accuracy, as explained in paragraphs 2-12 through 2-15.

2-8. Time permitting, analysts research by accessing information and intelligence from databases, the internet (attributed to open-source information), collaborative tools, broadcast services, and other sources such as automated systems. This screening enables analysts to focus their analytical efforts on only the information that is pertinent to their specific analytic problem. (See ATP 2-22.9 for more information on open-source information; see appendix A for more information on automated systems.)

Note. The relevancy of the information may change as the situation changes. For example, analysts may want to focus their analysis on information not older than 45 days about an armored division in garrison; however, this information may quickly become irrelevant as time elapses and the tactical situation changes.

Example: Screen

Upon screening the six pieces of information in response to collection requirements supporting PIRs 1 and 2, intelligence analysts focused on tank and MLRS/artillery activities. They kept four and discarded two of the pieces of information:

- **Keep for further analysis:** Possible identification of two threat MLRSs as well as support equipment traveling west to east at 20 kilometers per hour along a road 15 kilometers north of the 1 BCT forward locations.
- **Discard:** Threat motorized rifle battalion in company strength engaging adjacent 2 BCT forward positions attempting to seize a hilltop out of sector at a general four-digit grid.
- **Discard:** The 1 BCT reports harassing small arm engagements along forward battalion locations. (It does not relate to the PIRs.)
- **Keep for further analysis:** Approximately 28 or 30 threat tanks detected in convoy formations 40 kilometers north of the 1 BCT forward locations.
- **Keep for further analysis:** Threat air defense artillery elements active near possible headquarters and artillery locations detected.
- **Keep for further analysis:** Multiple-source reporting that a threat tank brigade is preparing to advance south, seeking to exploit lead division penetration of 1 BCT forward positions.

ANALYZE

2-9. Analysts examine relevant information or intelligence using reasoning and analytic techniques, which enable them to see information in different ways and to reveal something new or unexpected. It may be necessary to gain more information or apply a different technique, time permitting, until a conclusion is reached or a determination is made.

2-10. Analysts also analyze the volume of information based on the information source's reliability and the information accuracy, as screening information is continuous. This occurs when analysts receive information they immediately recognize as untrue or inaccurate based on their knowledge or familiarity with the analytic problem. Analysts should not proceed with the analysis when there is a high likelihood that the information is false or part of a deception, as this may lead to inaccurate conclusions. False information and deception are more prevalent today with the proliferation of misinformation commonly found in social media readily available on the internet.

2-11. Analysts may decide to retain or exclude information based on results from the *screen* phase. While the excluded information may not be pertinent to the current analytical question, the information is maintained in a unit repository as it may answer a follow-on question from a new analytical question.

2-12. During operations, intelligence analysts must consider information relevancy, reliability, and accuracy to perform analysis:

- **Relevancy:** Analysts examine the information to determine its pertinence about the threat or OE. Once the information is assessed as relevant, analysts continue with the analysis process.
- **Reliability:** The source of the information is scrutinized for reliability. If the source of the information is unknown, the level of reliability decreases significantly.
- **Accuracy:** Unlike reliability, accuracy is based on other information that can corroborate (or not) the available information. When possible, analysts should obtain information that confirms or denies a conclusion in order to detect deception, misconstrued information, or bad data or information. Additionally, when possible, analysts should characterize their level of confidence in that conclusion.

Note. **Exception:** Combat information, as defined in paragraph 1-14. (See FM 3-13 and FM 3-55.)

2-13. There are marked differences in evaluating the accuracy of information between higher and lower echelons. Higher (strategic) echelons have more sources of information and intelligence than lower (tactical) echelons, giving higher echelons more opportunities to confirm, corroborate, or refute the accuracy of the reported data. The role of higher echelons in evaluating the credibility (or probable truth) of information differs from its role in evaluating the reliability of the source (usually performed best by the echelon closest to the source).

2-14. Information is evaluated for source reliability and accuracy based on a standard system of evaluation ratings for each piece of information, as indicated in table 2-1; *reliability* is represented by a letter and *accuracy* by a number. Single-source intelligence personnel assign the rating, and it is essential for all-source personnel to understand the evaluation of validated intelligence sources.

Table 2-1. Evaluation ratings for source reliability and information accuracy

Reliability	
A	**Completely reliable:** Clearly a known source or reliable information.
B	**Usually reliable:** A known source that provides reliable information.
C	**Fairly reliable:** A source that has reported on information with a degree of reliability.
D	**Not usually reliable:** Typically, a source who provides information with a heavy bias, or past data was not validated.
E	**Unreliable:** Information provided is not reliable; typically, information cannot be confirmed by any means possible with any degree of certainty.
F	**Reliability cannot be judged:** There is no basis for estimating the reliability.
Accuracy	
1	**Confirmed by other sources:** One can state with certainty there is corroborating information.
2	**Probably true:** There is no actual proof, but no reason exits to assess; the source of the information is already available.
3	**Possibly true:** Information may not at present be available to refute the accuracy.
4	**Doubtfully true:** There is information that contradicts the accuracy.
5	**Improbable:** No confirmation, and the information contradicts other reliable/accurate sources.
6	**Truth cannot be judged:** Information does not meet the criteria above.

2-15. Reliable and accurate information is integrated into the analytical production. Data that is less reliable or accurate is not discarded; it is retained for possible additional screening with other established information or if new requirements arise that are relevant to existing data. Analysts are encouraged to read information rated as *F6* (reliability = F; accuracy = 6) to determine if it has relevancy although the source cannot be confirmed and the information accuracy is questionable. As friendly forces collect more information and that information is included in all-source or single-source intelligence analysis, the information originally rated as F6 may subsequently be rated as more reliable and accurate.

Example: Analyze

From the screened information, analysts analyze the retained information (bolded):

- **Possible identification of two MLRSs as well as support equipment traveling west to east at 20 kilometers per hour along a road 15 kilometers north of the 1 BCT forward locations.** Key elements of information include (1) the location of MLRSs maneuvering north, parallel to the division area of operations (AO), which would enable elements to stop and fire, as needed, and (2) the possible identification of two MLRSs with trailing support equipment. Requests for information include (1) the identification of the types of MLRSs and support equipment, (2) the location of the MLRSs if they have stopped, and (3) the observed activity if the location of the MLRSs has been detected.
- **Approximately 28 to 30 threat tanks detected in convoy formations 40 kilometers north of the 1 BCT forward locations.** Analysts determine that the tanks detected are 40 kilometers outside of the 1 BCT AO. However, the predictive analytical assessment identifies this as possible reinforcements likely to enter the AO within the next 24 to 48 hours.
- **Threat air defense elements active near possible headquarters and artillery locations detected.** Key elements of information include the headquarters and artillery locations. The presence of air defense artillery indicates a protected site. The 1 BCT forward positions are in range of threat artillery.
- **Multiple-source reporting that a threat tank brigade is preparing to advance south, seeking to exploit lead division penetration of 1 BCT forward positions**. Key elements of information include a tank brigade preparing to advance in the direction of 1 BCT forward positions. The tank brigade is identified as an exploitation element to penetrate friendly positions.

Note. The information of threat action outside of the immediate division area of interest was passed to the corps; it did not confirm or deny any threat COAs although the report came from a reliable source. The various reports caused some further refinements to the information collection plan.

INTEGRATE

2-16. As analysts reach new conclusions about the threat activities during the *analyze* phase, they should corroborate and correlate this information with prior intelligence holdings using reasoning and analytic techniques. Analysts determine how new information relates to previous analytical conclusions. New information may require analysts to alter or validate initial conclusions. Analysts must continue to evaluate and integrate reliable and accurate information relevant to their mission.

2-17. Analysts resume the analysis based on questions (hypotheses) they established during the *screen* and *analyze* phases. At this point, analysts begin to draw conclusions that translate into an initial determination that is likely to require additional analysis and, in certain instances, additional collection. They employ the analytic tradecraft standards to assess probabilities and confidence levels; they employ the action-metrics associated with analytical rigor to draw accurate conclusions. However, some of these conclusions may present alternative COAs not previously considered during IPB. These COAs must be presented to the commander and staff because they might have operational implications. (Appendix C discusses the analytic tradecraft standards and the action-metrics associated with analytical rigor.)

2-18. Hypotheses are tested and often validated during the *integrate* phase and become the basis for analytical production. To properly validate the hypotheses, analysts must demonstrate analytical rigor to determine the analytical sufficiency of their conclusions and be willing to present those points that prove the accuracy of their assessment.

Example: Integrate

From the four pieces of information, analysts tentatively determine the intent of the tank brigade (likely the motorized rifle division identified during the military decision-making process [MDMP] effort). Analysts conclude the tank brigade will most likely advance south against 1 BCT forward positions within 12 hours if the threat assesses there is a window of opportunity. Additionally, analysis indicates an artillery grouping is repositioning in the range of friendly forces to support the exploitation effort.

Corps, adjacent division, and multinational reporting and confirmation that MLRSs and support equipment are traveling west to east compels the division to collaborate with the adjacent division to confirm the intent and objective of the threat elements.

Note. Analysts must request additional collection on tank, headquarters, and artillery locations to verify current conclusions and initiate the targeting process.

PRODUCE

2-19. Intelligence and operational products are mutually supportive and enhance the commander and staff's situational understanding. Intelligence products are generally categorized by the purpose for which the intelligence was produced. The categories can and do overlap, and the same intelligence and information can be used in each of the categories. JP 2-0 provides an explanation for each of the categories:

- Warning intelligence.
- Current intelligence.
- General military intelligence.
- Target intelligence.
- Scientific and technical intelligence.
- Counterintelligence.
- Estimative intelligence.
- Identity intelligence.

2-20. Intelligence analysis results in the production and dissemination of intelligence to the commander and staff. Intelligence analysts produce and maintain a variety of products tailored to the commander and staff and dictated by the current situation, standard operating procedures (SOPs), and battle rhythms. (See appendix E for a detailed discussion on intelligence production.)

Note. When disseminating intelligence products, intelligence analysts must recognize when intelligence information at a higher classification is essential for the commander's awareness. Intelligence analysts and the intelligence staff must adhere to all appropriate U.S. laws, DOD regulations, classification guidelines, and security protocols. (See AR 380-28.)

The classification of U.S. intelligence presents a challenge in releasing information during multinational operations although sharing information and intelligence as much as possible improves interoperability and trust. Commanders and staffs should understand U.S. and other nations' policies about information sharing, since the early sharing of information (during planning) ensures effective multinational operations.

2-21. An analyst's ultimate goal is finding threat vulnerabilities and assisting the commander and staff in exploiting those vulnerabilities—despite having answered the commander's PIR. If the intelligence analysis does not answer the commander's PIR, the analyst should reexamine the guidance, consider recommending different collection strategies, and review information previously discarded as nonessential. Sometimes, the cause for not answering the requirement is the analyst's misunderstanding of the commander's PIR or guidance, thus the analyst must return to the original question posed by the commander and reevaluate the initial hypothesis.

2-22. In tactical units, analysts must understand that their adjacent and especially their subordinate units may have degraded communications. In those cases, analysts at each echelon must develop their own conclusions and assessments and should use their unit's primary, alternate, contingency, and emergency (known as PACE) plan to facilitate continuous dissemination of their products and assessments (see FM 3-0).

Example: Produce

Following additional collection at specific points of interest, analysts confirm the tank brigade's role as the exploitation force and MLRS battalion locations. Refined collection improves the data and information necessary to target those units and answer PIRs 1 and 2.

Chapter 3
All-Source Analytical Tasks

OVERVIEW

3-1. Through the application of the all-source analytical tasks, intelligence analysis facilitates commanders and other decision makers' ability to visualize the OE, organize their forces, and control operations to achieve their objectives. The all-source analytical tasks are—

- Generate intelligence knowledge.
- Perform IPB.
- Provide warnings.
- Perform situation development.
- Provide intelligence support to targeting and information operations.

3-2. In any operation, both friendly and threat forces will endeavor to set conditions to develop a position of relative advantage. Setting these conditions begins with generate intelligence knowledge, which provides relevant knowledge about the OE that is incorporated into the Army design methodology and used later during other analytical tasks. During the MDMP, the intelligence staff leads IPB and conducts continuous intelligence analysis to understand the OE and the options it presents to friendly and threat forces. The commander and staff continuously assess information, operations, and changes in the OE. Warning intelligence, situation development, and intelligence support to targeting assist them in further shaping the OE to facilitate mission success. These all-source analytical tasks are included within the intelligence warfighting function tasks of the Army Universal Task List (also called AUTL), captured in FM 2-0, appendix B. Each specific task is identified with an Army tactical task (ART) number, such as ART 2.1.4 for the generate intelligence knowledge task. (See figure 3-1.)

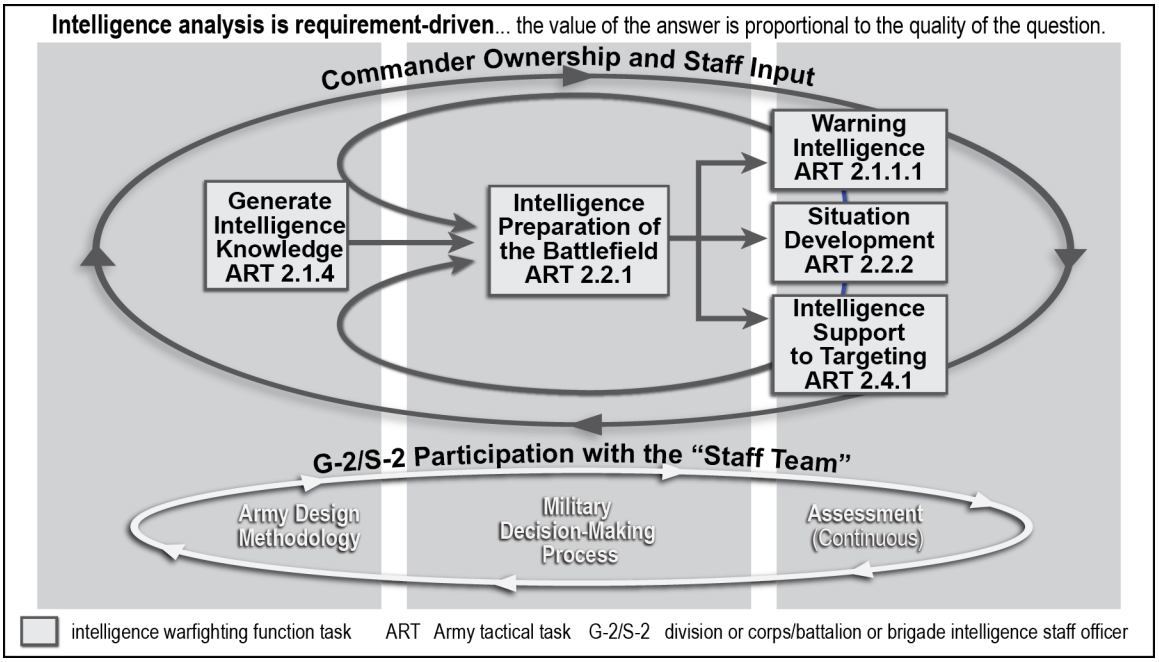


Figure 3-1. The all-source analytical tasks

3-3. The continuous assessment of collected information also mitigates risk to friendly forces while identifying opportunities to leverage friendly capabilities to open a window of opportunity. Analysis presents the commander with options for employing multiple capabilities and gaining a position of relative advantage over the threat.

3-4. For each all-source analytical task, the challenge for the intelligence analyst is understanding the unique requirements and considerations based on the situation, operational echelon, and specific mission. For example, targeting requirements at the brigade level narrowly focus on targets within that brigade's AO. Whereas theater army-level targeting synchronizes and uses operations conducted by one or more corps to reach operational objectives. Another example includes long-term analytical assessments, which are usually produced at the strategic and operational levels of warfare (see chapter 9).

3-5. There are many forms of analysis associated with unique operational activities. One important example of these types of activities is identity activities, which result in 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 activities are described as a collection of functions and actions conducted by maneuver, intelligence, and law enforcement components. Identity activities recognize and differentiate one person from another to support decision making. Identity activities include—

- The collection of identity attributes and physical materials.
- The processing and exploitation of identity attributes and physical materials.
- All-source analytical efforts.
- The production of identity intelligence and DOD law enforcement criminal intelligence products.
- The dissemination of those intelligence products to inform policy and strategy development, operational planning and assessment, and the appropriate action at the point of encounter.

GENERATE INTELLIGENCE KNOWLEDGE (ART 2.1.4)

3-6. Generate intelligence knowledge is a continuous task driven by the commander. It begins before receipt of mission and enables the analyst to acquire as much relevant knowledge as possible about the OE for the conduct of operations. Information is obtained through intelligence reach, research, data mining, database access, academic studies, intelligence archives, publicly available information, and other information sources, such as biometrics, forensics, and DOMEX. The information and intelligence obtained can be refined into specific knowledge for use during mission analysis through functional analysis, which is discussed in chapter 6 of this publication.

3-7. Generate intelligence knowledge includes the following five tasks, which facilitate creating a foundation for performing IPB and mission analysis:

- **Develop the foundation to define threat characteristics:** Analysts create a database of known hostile threats and define their characteristics in a general location. Analysts can refine and highlight important threats through functional analysis that can be prioritized later during steps 3 and 4 of the IPB process.
- **Obtain detailed terrain information and intelligence:** Analysts describe the terrain of a general location and categorize it by environment type. For example, desert and jungle environments have distinguishing characteristics that can assist in analyzing terrain during step 2 of the IPB process.
- **Obtain detailed weather and weather effects information and intelligence:** Analysts describe the climatology of a general location and forecast how it would affect future operations. Analysts should rely on the Air Force staff weather officer of their respective echelons to assist in acquiring weather support products, information, and knowledge. If the staff weather officer is not readily available, analysts should use publicly available information and resources. Information regarding climatology characteristics can assist in analyzing weather effects during step 2 of the IPB process.
- **Obtain detailed civil considerations information and intelligence:** Analysts identify civil considerations (areas, structures, capabilities, organizations, people, and events [ASCOPE]) within a general location. Analysts can refine this information further when they receive a designated area of interest and can assist in determining how civil considerations will affect friendly and threat operations during step 2 of the IPB process.

- **Complete studies:** Although analysts do not have a specific operation, mission, or area of responsibility when generating intelligence knowledge, they can compile information into products based on the commander's guidance. This supports the commander's visualization and completes studies for dissemination. Completed studies or products include country briefs, written assessments, or graphics. These products inform the commander and staff on current and historic situations that may affect future operations when a mission is received.

PERFORM INTELLIGENCE PREPARATION OF THE BATTLEFIELD (ART 2.2.1)

3-8. Analytical support begins during the MDMP. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). Commanders use the MDMP to visualize the OE and the threat, build plans and orders for extended operations, and develop orders for short-term operations within the framework of a long-range plan. During the mission analysis step of the MDMP, intelligence analysts lead the IPB effort; however, they cannot provide all of the information the commander requires for situational understanding. Other staff sections or supporting elements assist in producing and continuously refining intelligence products tailored to the commander's requirements and the operation. (See ATP 2-01.3 for IPB information.)

3-9. As analysts begin the IPB process, they should have a general understanding of their OE based on intelligence produced and acquired when generating intelligence knowledge. IPB is a four-step process:

- **Step 1—Define the OE.** The intelligence staff identifies 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. During step 1, the AO, area of interest, and area of influence must also be identified and established.
- **Step 2—Describe environmental effects on operations.** 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. The entire staff determines the effects of friendly and threat force actions on the population.
- **Step 3—Evaluate the threat.** Evaluating the threat is understanding how a threat can affect friendly operations. Step 3 determines threat force capabilities and the doctrinal principles and tactics, techniques, and procedures that threat forces prefer to employ.
- **Step 4—Determine threat COAs.** 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 the 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.

PROVIDE WARNINGS (ART 2.1.1.1)

3-10. Across the range of military operations, various collection assets provide early warning of threat action. As analysts screen incoming information and message traffic, they provide the commander with advanced warning of threat activities or intentions that may change the basic nature of the operation. These warnings enable the commander and staff to quickly reorient the force to unexpected contingencies and to shape the OE.

3-11. Analysts can use analytic techniques and their current knowledge databases to project multiple scenarios and develop indicators as guidelines for providing warning intelligence. 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). Analysts project future events and identify event characteristics that can be manipulated or affected. Characteristics that cannot be manipulated or affected should be incorporated into unit SOPs as warning intelligence criteria. (See ATP 2-01 and ATP 2-01.3 for more information on indicators.)

PERFORM SITUATION DEVELOPMENT (ART 2.2.2)

3-12. Intelligence analysis is central to situation development, as it is a process for analyzing information and producing current intelligence concerning the relevant aspects of the OE within the AO before and during operations. Analysts continually produce current intelligence to answer the commander's requirements, update and refine IPB products, and support transitions to the next phase of an operation. (For more information on situation development, see FM 2-0.)

Note. In addition to the AO, intelligence analysts should also consider and include relevant aspects of the OE within the area of influence and area of intelligence responsibility that impact the commander's AO.

3-13. Analysts continually analyze the current situation and information to predict the threat's next objective or intention. During step 3 of the IPB process, analysts compare the current situation with their threat evaluations to project multiple scenarios and develop indicators. Understanding how the threat will react supports the planning of branches and sequels, affording the commander multiple COAs and flexibility on the battlefield during current operations. For example, observing a threat unit in a defensive posture may indicate an offensive operation within a matter of hours. Providing this information to the commander enables the staff to pursue a different COA that can place friendly units in a better position of relative advantage. The commander may use a flanking maneuver on the threat since it is in a relatively stationary position, hindering the future offensive operation.

PROVIDE INTELLIGENCE SUPPORT TO TARGETING AND INFORMATION OPERATIONS (ART 2.4)

3-14. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Across all echelons and intelligence disciplines, intelligence analysis provides relevant and timely intelligence to support targeting (both lethal and nonlethal). The staff uses this intelligence during the targeting process, which uses the *decide*, *detect*, *deliver*, and *assess* methodology. (See appendix F for more on intelligence support to targeting.)

3-15. Intelligence analysis, starting with the IPB effort, supports target development and target detection:

- **Intelligence analysis support to target development:** Target development involves the systematic analysis of threat forces and operations to determine high-value targets (HVTs) (people, organizations, or military units the threat commander requires for successful completion of the mission), HPTs (equipment, military units, organizations, groups, or specific individuals whose loss to the threat contributes significantly to the success of the friendly COA), and systems and system components for potential engagement through maneuver, fires, electronic warfare, or information operations.
- **Intelligence analysis support to target detection:** Intelligence analysts establish procedures for disseminating targeting information. The targeting team develops the sensor and attack guidance matrix to determine the sensors required to detect and locate targets. Intelligence analysts incorporate these requirements into the collection management tools, which assist the operations staff in developing the information collection plan.

3-16. *Information operations* is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). Intelligence support to military information operations pertains to the collection of information essential to define the information environment, understand the threat's information capabilities, and assess or adjust information-related effects. Continuous and timely intelligence is required to accurately identify the information environment across the physical, informational, and cognitive dimensions, including the operational variables (PMESII-PT). Intelligence support to military information operations focuses on the following:

- Aspects of the information environment that influence, or are influenced by, the threat.
- Understanding threat information capabilities.

- Understanding the methods by which messages are transmitted and received in order to assess the cognitive reception and processing of information within the target audience.
- Assessing information-related effects (target audience motivation and behavior, measure of effectiveness, and information indicators of success or failure).

This page intentionally left blank.

PART TWO

Task Techniques

Chapter 4

Analytic Techniques

OVERVIEW

4-1. Intelligence analysts use cognitive processes and analytic techniques and tools to solve intelligence problems and limit analytical errors. The specific number of techniques and tools applied depends on the mission and situation. The basic thinking abilities for intelligence analysis and critical and creative thinking, all described in appendix B, facilitate analysis and improve the probability of accurate conclusions. Intelligence analysts must be as accurate as possible to assist in ensuring mission success.

4-2. The following distinguishes between a technique, tool, and method:

- **Technique** is a way of doing something by using a special knowledge or skill. An analytic technique is a way of looking at a problem, which results in a conclusion, assessment, or both. A technique usually guides analysts in thinking about a problem instead of providing them with a definitive answer as typically expected from a method.
- **Tool** is a component of an analytic technique that facilitates the execution of the technique but does not provide a conclusion or assessment in and of itself. Tools facilitate techniques by allowing analysts to display or arrange information in a way that enables analysis of the information. An example of a tool is a link diagram or a matrix. Not all techniques have an associated tool.
- **Method** is a set of principles and procedures for conducting qualitative analysis.

APPLYING STRUCTURED ANALYTIC TECHNIQUES

4-3. Structured analysis assists analysts in ensuring their analytic framework—the foundation upon which they form their analytical judgments—is as solid as possible. It entails separating and organizing the elements of a problem and reviewing the information systematically. Structured analytic techniques provide ways for analysts to separate the information into subsets and assess it until they generate a hypothesis found to be either feasible or untrue. Structured analytic techniques—

- Assist analysts in making sense of complex problems.
- Allow analysts to compare and weigh pieces of information against each other.
- Ensure analysts focus on the issue under study.
- Force analysts to consider one element at a time systematically.
- Assist analysts in overcoming their logic fallacies and biases.
- Ensure analysts see the elements of information. This enhances their ability to identify correlations and patterns that would not appear if not depicted outside the mind.
- Enhance analysts' ability to collect and review data. This facilitates thinking with a better base to derive alternatives and solutions.

4-4. Applying the appropriate structured analytic technique assists commanders in better understanding and shaping the OE. One technique may not be sufficient to assist in answering PIRs; therefore, analysts should use multiple techniques, time permitting. For example, determining the disposition and composition of the threat in the OE is like attempting to put the pieces of a puzzle together. Employing multiple analytic techniques facilitates the piecing of the puzzle, thus creating a clearer picture. (See figure 4-1.) Structured analytic techniques are categorized as the following and summarized in figure 4-2:

- Basic—provide insight that supports problem solving. (See chapter 5.)
- Diagnostic—make analysis more transparent. (See chapter 5.)
- Advanced:
  - Contrarian—challenge current thinking. (See chapter 6.)
  - Imaginative—develop new insights. (See chapter 6.)

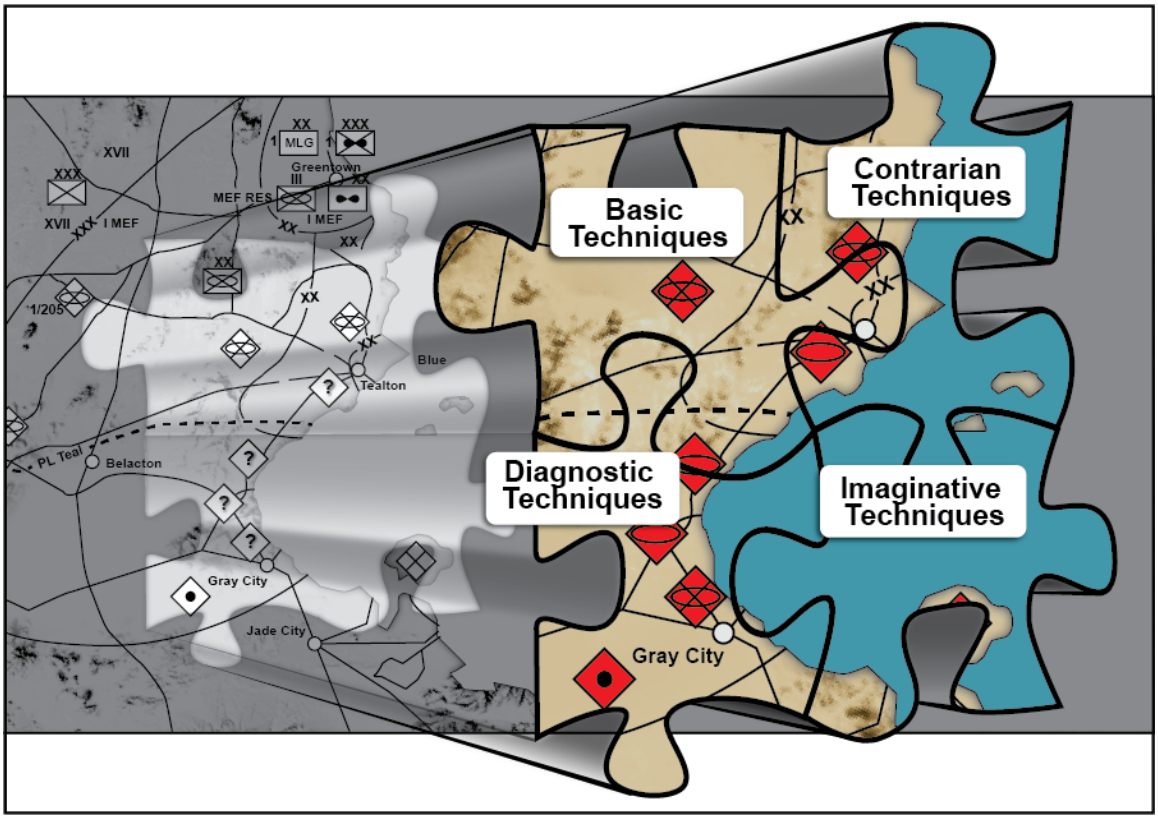


Figure 4-1. Applying analytic techniques to understand the operational environment

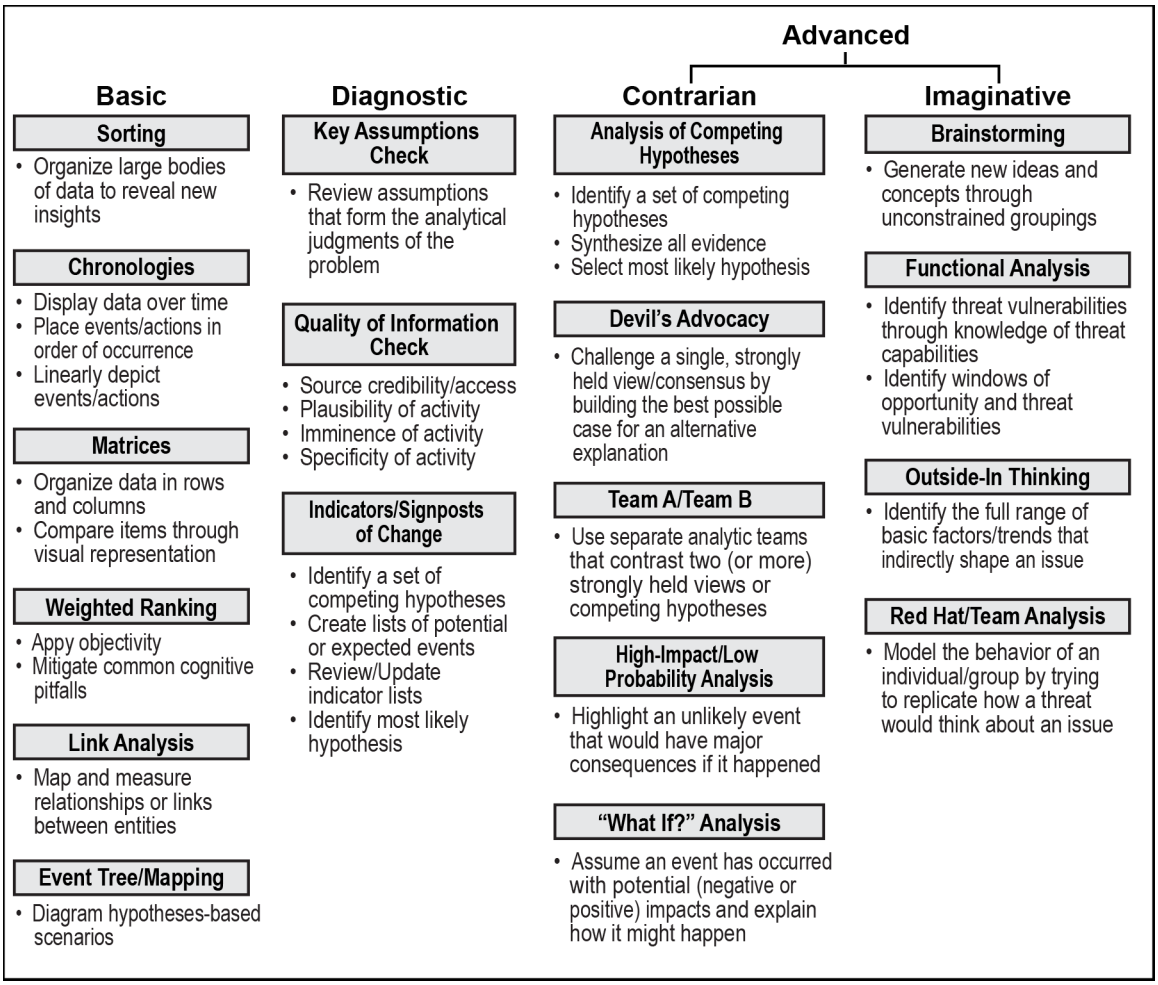


Figure 4-2. Structured analytic techniques summarized

4-5. For thorough analysis, analysts should incorporate as many appropriate techniques as possible into their workflow. Although this may be more time consuming, analysts become more proficient at using these techniques, ultimately reducing the amount of time required to conduct analysis. The exact techniques and tools incorporated, as well as the order in which to execute them, are mission- and situation-dependent. There is no one correct way to apply these techniques as each analyst's experience, preference, and situation are influencing factors.

4-6. Analysts can apply structured analytic techniques in the *analyze* and *integrate* phases of the intelligence analysis process to assist them in solving analytic problems. The analytic problem can vary depending on the echelon or mission. For example, an analytic problem could be forecasting the future stability of a specific country, while another could be trying to identify an HVT. The results of structured analytic techniques and tools, such as link diagrams or quad-charts, are not always incorporated into intelligence products such as intelligence estimates or intelligence running estimates (see FM 2-0). However, analysts may use these results to inform their analytical products; they should maintain these results in a repository for future reference.

4-7. The vast amount of information that analysts must process can negatively affect their ability to complete intelligence assessments timely and accurately; therefore, analysts should be proficient at using both manual and automated methods to conduct structured analysis. Additionally, analysts conduct analysis from varying environments and echelons in which the availability of automation and network connectivity may not be fully mission capable.

Applying Analytic Techniques Throughout the Intelligence Analysis Process

UNDERSTAND THE REQUIREMENTS: A human intelligence analysis cell (HAC) is tasked to help find the composition and disposition of the threat's integrated air defense system (IADS) on the battlefield. This task supports one of the division commander's PIRs. The division's HUMINT elements have been attempting to collect information from captured detainees, defectors, and internally displaced persons. Additionally, HUMINT sources are sensitized to look for radar dishes and missiles.

SCREEN THE COLLECTED INFORMATION: The HAC receives multiple HUMINT reports on various topics, but it focuses on those reports that support the PIR related to IADSs.

The HAC assesses the value of the reports by determining the *relevance* of the information to the PIR, the *reliability* of the source of the information, and the *accuracy* of the information itself:

- **Relevance:** The HAC searches HUMINT databases for all HUMINT reporting in theater related to IADSs and tailors its query to receive reports not older than 120 days (date) and within the boundaries of its AO (location). The HAC discovers that there are 20 reports on hand possibly related to IADSs within the specified date and geographic location. **(Overall relevance is estimated as high.)**
- **Reliability:** The HAC looks for duplication in the reporting, which can occur when one HUMINT source provides multiple HUMINT collection teams the same information. The HAC finds one duplicate report and eliminates it, leaving 19 reports on hand to analyze. The HAC also determines that one of the sources lacks credibility and eliminates the one report associated with that source, reducing the number to 18 reports. **(Overall reliability of sources is estimated as moderate.)**
- **Accuracy:** The HAC examines the 18 reports and determines that most of them have marginally accurate information because they lack grids for any locations. Despite this, the HAC does not eliminate these reports. **(Overall accuracy is estimated as moderate.)**

Screening results: The HAC compiles first-hand information from multiple credible sources about missiles on the backs of large trucks within the division's AO, and from another credible source who reported an increase in the number of trucks with missiles in the last 30 days.

ANALYZE: The HAC considers the information against its current knowledge level and uses sorting, a basic structured analytic technique, to categorize the information and determine what it now reveals or what gaps still exist. The HAC uses the Distributed Common Ground System-Army (DCGS-A) and combatant command-specific databases to further examine the quality of the information to determine if there are any signs of a deception effort. The HAC then generates multiple hypotheses based on the information and determines that the reporting indicates the discovery of a threat supply point. The HAC challenges the hypothesis using contrarian techniques, such as devil's advocacy and team A/team B, to ensure the analysis is thorough (see chapter 6).

Initial analytical determination: Based on the reports and analytic techniques employed, the HAC determines that an unidentified truck with possible missiles will arrive at a general location every few days. The geographical area is a 1,500-meter location on the north side of a specific ridgeline. The HAC postulates that this general location may be a threat supply point for an unknown missile-type weapons system. The HAC reports a moderate level of confidence in its assessment. (See appendix C for more information on likelihoods and confidence levels.)

INTEGRATE: The HAC, requiring more information to further develop the analytic problem, expands the parameters of its previous database query by including the area of interest and HUMINT reporting not older than 150 days. This query returns the same reports as the previous query as well as additional reports from other HUMINT teams and other government agencies operating both inside and outside the division's AO. The reports are assessed as reliable and fairly accurate since the information about these items was preexisting.

Applying Analytic Techniques Throughout the Intelligence Analysis Process (*continued*)

INTEGRATE (*continued*): The following includes key findings in the HUMINT reports:

- The reports from other government agencies contain photographs of trucks with missiles, identified as logistics vehicles, transporting possible SA-17 missiles to and from unknown locations. The photographs were taken at a specific grid location showing the direction of travel towards the division's AO.
- An organic HUMINT report from inside the division's AO, not initially related to IADSs, now reveals links or indicators that, when combined with previous holdings, may provide information related to IADSs. In this report, the source reported loud military trucks travelling frequently near the source's home. Additionally, the source's description of the trucks matched those in the photographs of the other government agencies' reports. The source's residence is located along the main highway between where the photographs were taken and where the increase in trucks with missiles was reported. Furthermore, source reporting indicates that the trucks are loaded with missiles when heading towards the division's AO, but they are empty when heading away from the division's AO.

Note. Single-source analysts may be able to skip to the *produce* phase if no other information on the topic is available.

Final analytical determination: This new information, when integrated with the previous holdings and structured analytic techniques and tools, allows the HAC to refine its initial analytical determination. The HAC postulates that SA-17s are likely to arrive north of Ridgeline Borisenko within the grid square 38JCH1126 every few days. The HAC maintains a moderate level of confidence in its assessment. When the date of the postulated event elapses, the HAC will be able to further define the reliability of the sources and accuracy of the information.

PRODUCE: The HAC disseminates this newly produced intelligence in a summary that contains the determination that SA-17s will arrive north of Ridgeline Borisenko. The summary of HUMINT reporting is disseminated to the commander and shared with all other intelligence elements within the division.

This page intentionally left blank.

Chapter 5
Basic and Diagnostic Structured Analytic Techniques

SECTION I – BASIC STRUCTURED ANALYTIC TECHNIQUES

5-1. Basic structured analytic techniques are the building blocks upon which further analysis is performed. They are typically executed early in the intelligence effort to obtain an initial diagnosis of the intelligence problem through revealing patterns. The basic structured analytic techniques described in this publication are—

- **Sorting technique:** Organizing large bodies of data to reveal new insights.
- **Chronologies technique:**
  - Displaying data over time.
  - Placing events or actions in order of occurrence.
  - Linearly depicting events or actions.
- **Matrices technique:**
  - Organizing data in rows and columns.
  - Comparing items through visual representation.
- **Weighted ranking technique:**
  - Facilitating the application of objectivity.
  - Mitigating common cognitive pitfalls.
- **Link analysis technique:** Mapping and measuring relationships or links between entities.
- **Event tree and event mapping techniques:** Diagramming hypotheses-based scenarios.

5-2. These techniques—

- Improve assessments by making them more rigorous.
- Improve the presentation of the finished intelligence in a persuasive manner.
- Provide ways to measure progress.
- Identify information gaps.
- Provide information and intelligence.

SORTING

5-3. Sorting is a basic structured analytic technique used for grouping information in order to develop insights and facilitate analysis. This technique is useful for reviewing massive data stores pertaining to an intelligence challenge. Sorting vast amounts of data can provide insights into trends or abnormalities that warrant further analysis and that otherwise would go unnoticed. Sorting also assists in reviewing multiple categories of information that when divided into components presents possible trends, similarities, differences, or other insights not readily identifiable. Table 5-1 on page 5-2 briefly describes when to use the sorting technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-1. Sorting technique

Sorting: *A basic structured analytic technique for organizing a large amount of data in a manner that often yields new insights.*		
When to use	**Value added**	**Potential pitfalls**
Sorting data early in the analysis process is advantageous. It is most effective when information elements can be arranged into categories and subcategories to gain insights not readily identifiable. Sorting is particularly effective during initial data collection and hypotheses generation.	Sorting vast amounts of data can provide insights into trends or anomalies that warrant further analysis. This technique can highlight new or additional analytic insights into an old or new intelligence problem.	Improper sorting can hide valuable insights as easily as it can illuminate them. This occurs more frequently if data is not standardized.

5-4. **Method.** The following steps outline the process of sorting:

- **Step 1:** Arrange the information into categories to determine which categories or combination of categories might show trends or abnormalities that would provide insight into the problem being studied.
- **Step 2:** Review the listed facts, information, or hypotheses in the database to identify key fields that may assist in uncovering possible patterns or groupings.
- **Step 3:** Group those items according to the schema of the categories defined in step 1.
- **Step 4:** Choose a category and sort the information within that category. Look for any insights, trends, or oddities.
- **Step 5:** Review (and re-review) the sorted facts, information, or hypotheses to determine alternative ways to sort them. List any alternative sorting schema for the problem. One of the most useful applications of this technique is sorting according to multiple schemas and examining results for correlations between data and categories. For example, analysts identify from the sorted information that most attacks occurring on the main supply route also occur at a specific time.

5-5. A pattern analysis plot sheet is a common analysis tool for sorting information. (See figure 5-1.) It can be configured to determine threat activity as it occurs within a specified time. The pattern analysis plot sheet is a circular matrix and calendar. Each concentric circle represents one day and each wedge in the circle is one hour of the day. In figure 5-1, the information categories pertain to tactical surface-to-surface missile (also called SSM) launches arranged according to the days of the week and the times of day. For example, four Surface-to-Surface Missile B launches occurred during the last week of the month on alternate weekdays, mainly in the early hours of the day. The threat could be conducting launches during the early morning hours when people are just waking up and at their most vulnerable.

5-6. This method of sorting allows analysts to determine various aspects of an event, such as the type and timing of a particular event, and assists collection managers in allocating collection assets in space and time. Although the pattern analysis plot sheet is a sorting tool, it can also overlap with chronologies since analysts commonly use it to capture and display data over time.

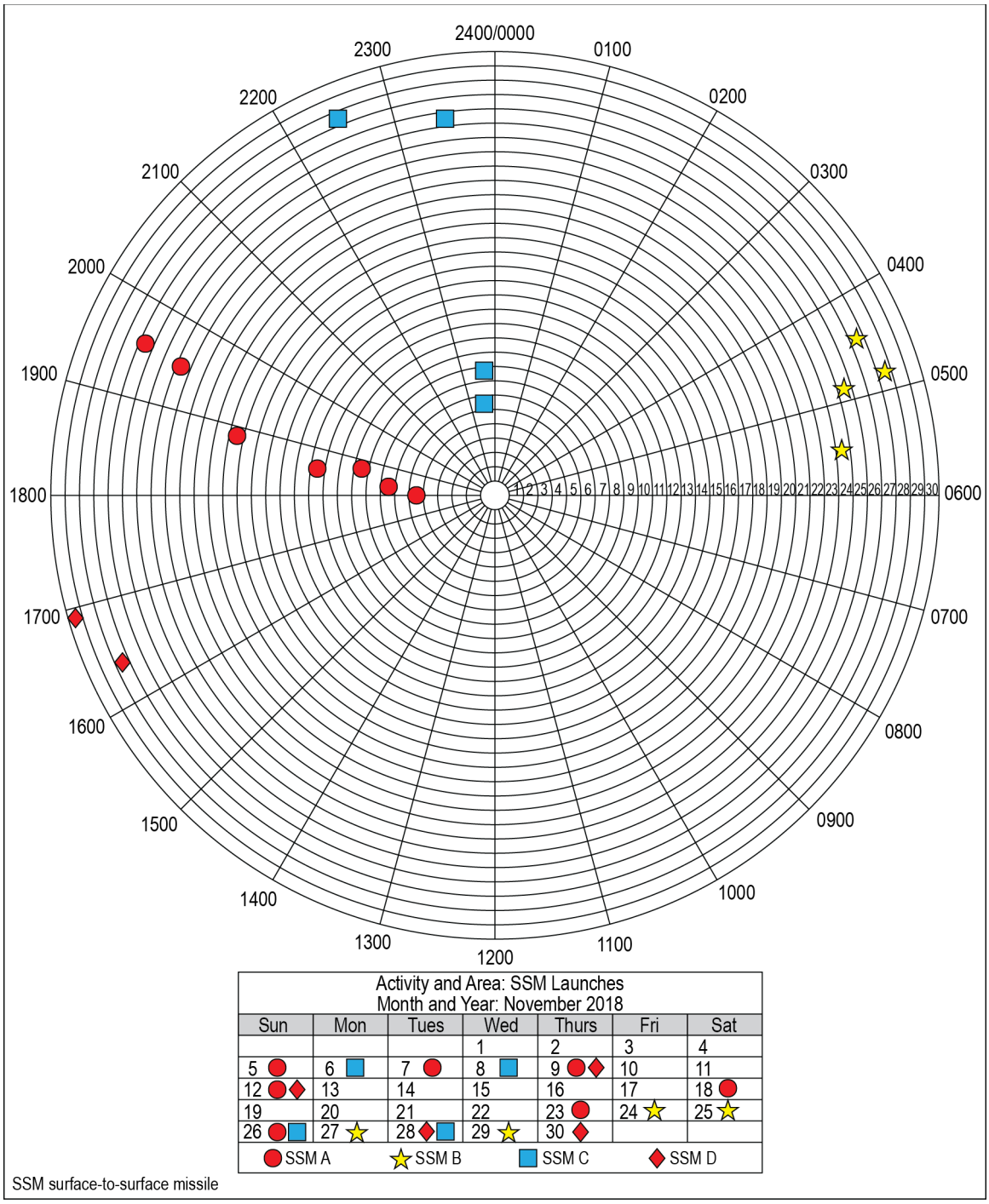


Figure 5-1. Sorting data using a pattern analysis plot sheet example

CHRONOLOGIES

5-7. A chronology is a list that places events or actions in the order they occurred; a timeline is a graphical depiction of those events. Analysts must consider factors that may influence the timing of events. For example, the chronological time of events may be correlated to the lunar cycle (moonset), religious events, or friendly patrol patterns. Timelines assist analysts in making these types of determinations. Table 5-2 briefly describes when to use the chronologies technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-2. Chronologies technique

Chronologies: *Technique for displaying data over time.*		
When to use	**Value added**	**Potential pitfalls**
The chronologies technique assists in organizing events or actions. It is useful for understanding the timing and sequence of relevant events as well as identifying significant events and gaps. The events may have a cause-and-effect relationship, or they may not. While timelines may be developed at the onset of an analytical task to ascertain the context of the activity being analyzed, they are also used in reviewing intelligence studies to discover causes for intelligence failures as they highlight significant events.	Chronologies assist in identifying patterns and correlations between events. This technique enables analysts to relate seemingly random events to the overarching situation and highlight or identify significant changes. It also assists in discovering trends, issues, or anomalies. Timelines depict information in a format easily understood in a briefing.	Analysts must be careful not to assume that events following earlier events are caused by the earlier events; there may be no causal relationship. The validity of this technique may be minimized if analysts fail to find contextual events that relate to the information in the chronology or timeline.

5-8. **Method.** Creating a chronology or timeline involves three steps:

- **Step 1:** List relevant events by the date or in order each occurred. Analysts should ensure they properly reference the data.
- **Step 2:** Review the chronology or timeline by asking the following questions:
  - What are the temporal distances between key events? If lengthy, what caused the delay? Are there missing pieces of data that may fill those gaps that should be collected?
  - Did analysts overlook pieces of intelligence information that may have had an impact on the events?
  - Conversely, if events seem to happen more rapidly than expected, is it possible that analysts have information related to multiple-event timelines?
  - Are all critical events necessary and shown for the outcome to occur?
  - What are the intelligence gaps?
  - What are indicators for those intelligence gaps?
  - What are the vulnerabilities in the timeline for collection activities?
  - What events outside the timeline could have influenced the activities?
- **Step 3:** Summarize the data along the line. Sort each side of the line by distinguishing between types of data. For example, depict intelligence reports above the timeline and depict significant activities below the timeline. Multiple timelines may be used and should depict how and where they converge.

5-9. Timelines are depicted linearly and typically relate to a single situation or COA. (See figure 5-2.) Multilevel timelines allow analysts to track concurrent COAs that may affect each other. Analysts use timelines to postulate about events that may have occurred between known events. They become sensitized to search for indicators, so the missing events are found and charted. Timelines may be used in conjunction with other structured analytic techniques, such as the event tree technique (see paragraph 5-22), to analyze complex networks and associations.

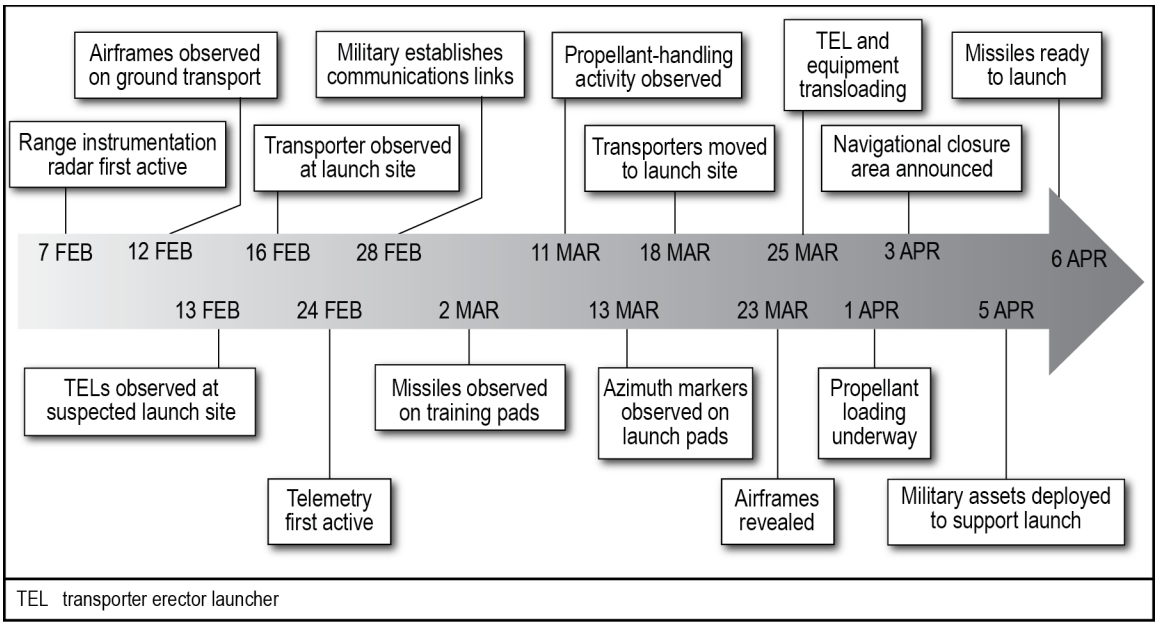


Figure 5-2. Timeline example

5-10. Figure 5-3 illustrates a time event chart, which is a variation of a timeline using symbols to represent events, dates, and the flow of time. While there is great latitude in creating time event charts, the following should be considered when creating them:

- Depict the first event as a triangle.
- Depict successive events as rectangles.
- Mark noteworthy events with an X across the rectangles.
- Display the date on the symbol.
- Display a description below the symbol.
- If using multiple rows, begin each row from left to right.

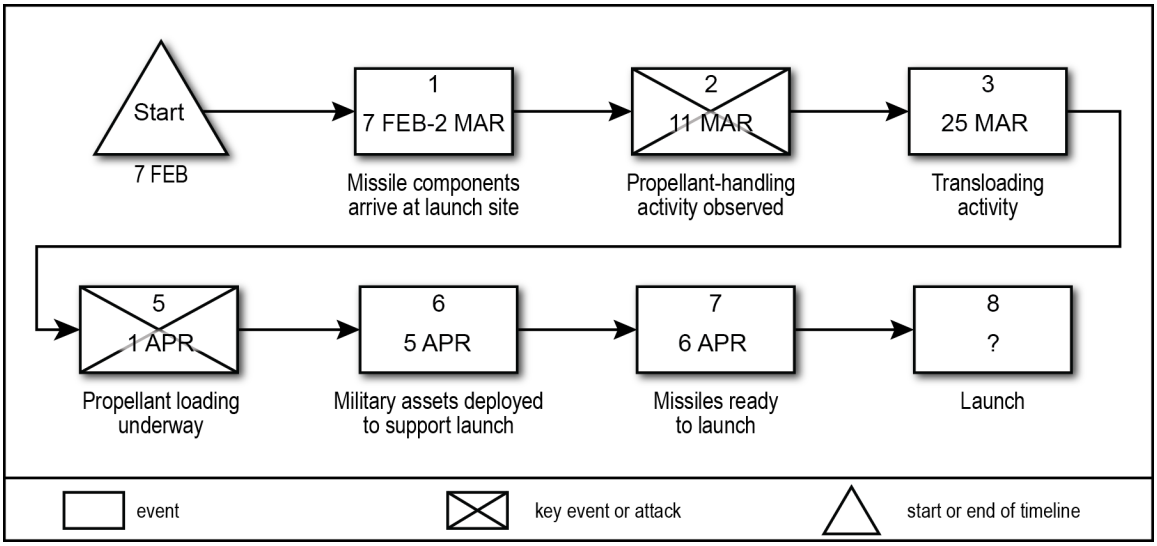


Figure 5-3. Time event chart example

MATRICES

5-11. A matrix is a grid with as many cells as required to sort data and gain insight. Whenever information can be incorporated into a matrix, it can provide analytic insight. A matrix can be rectangular, square, or triangular; it depends on the number of rows and columns required to enter the data. Three commonly used matrices are the—

- **Threat intentions matrix—**assists in efficiently analyzing information from the threat's point of view based on the threat's motivation, goals, and objectives. (See paragraph 5-14.)
- **Association matrix—**identifies the existence and type of relationships between individuals as determined by direct contact.
- **Activities matrix—**determines connections between individuals and any organization, event, entity, address, activity, or anything other than persons.

Note. Since the association and activity matrices closely relate to link analysis, they are described under the link analysis technique. (See paragraph 5-21.)

5-12. A key feature of the matrices analytic technique is the formulation of ideas of what may occur when one element of a row interacts with the corresponding element of a column. This differs from other matrices, such as the event matrix (described in ATP 2-01.3), in which the elements of the columns and rows do not interact to formulate outcomes; the matrix is primarily used to organize information. Table 5-3 briefly describes when to use the matrices technique, as well as the value added and potential pitfalls associated with using this technique. comparison

Table 5-3. Matrices technique

Matrices: *Technique that uses analytic tools for sorting and organizing data to facilitate comparison and analysis.*		
When to use	**Value added**	**Potential pitfalls**
A matrix is useful when there are more options or intricate data to conceptualize at one time without the aid of visual representations.	A matrix is useful for isolating critical data when there are vast amounts of information relevant to an issue, such as collected open-source information for a country study to generate intelligence knowledge; it facilitates comparing the options. When used to review data related to options, such as in a threat intentions matrix, this technique enables the analytical focus on each option, thus improving comparisons.	A matrix's two-dimensional design limits its use for collating data on complex issues; leaving out pertinent data can oversimplify an issue.

5-13. **Method.** The following steps outline the process for constructing a matrix (see figure 5-4):

- **Step 1:** Draw a matrix with enough columns and rows to enter the two sets of data being compared.
- **Step 2:** Enter the range of data or criteria along the uppermost horizontal row and the farthest left vertical column leaving a space in the upper left corner of the matrix.
- **Step 3:** In the grid squares in between, annotate the relationships, or lack thereof, in the cell at the intersection between two associated data points.
- **Step 4:** Review the hypotheses developed about the issue considering the relationships shown in the matrix; if appropriate, develop new hypotheses based on the insight gained from the matrix.

5-14. The following steps pertain to the threat intentions matrix technique (see figure 5-4):

- **Step 1:** Enter the decision options believed to be reasonable from the threat's viewpoint along the farthest left vertical column.
- **Step 2:** Enter the objectives for each option from the threat's viewpoint in the *objectives* column.
- **Step 3:** Enter the benefits for each option from the threat's viewpoint in the *benefits* column.
- **Step 4:** Enter the risks for each option from the threat's viewpoint in the *risks* column.

- **Step 5:** Fill in the *implications* column, which transitions the analyst from the threat's viewpoint to the analyst's viewpoint. Enter the implications from the threat's viewpoint and then add a slash (/) and enter the implications from the analyst's viewpoint.
- **Step 6:** Enter the indicators from the analyst's viewpoint in the *indications* column. This provides a basis for generating collection to determine as early as possible which option the threat selected.

	Objectives	***Benefits***	***Risks***	***Implications***	***Indications***
White House	Destroy most important United States (U.S.) symbol	Ultimate show of power	Miss target or shot down	Threat gains in stature/U.S. drawn into war, bled economically	• Unusual interest in White House air defenses • Extremists taking pilot training
Terrorist Attack	• Mass casualties • Instill fear	• Show of power • Media attention	• Adequate training • Maintain secrecy	Threat gains in stature/mass casualties can damage economy	• Unusual surveillance • Pilot training • Familiarizing with the area
Wall Street	Hurt the U.S. economy	• Aid recruitment • Show of power	• Adequate training • Maintain secrecy	Threat gains in stature/difficult to determine attacker	• Unusual surveillance • Pilot training • Familiarizing with the area

Figure 5-4. Threat intentions matrix example

WEIGHTED RANKING

5-15. The weighted ranking technique is a systematic approach that provides transparency in the derivation and logic of an assessment. This facilitates the application of objectivity to an analytic problem. To simplify the weighted ranking technique, this publication introduces subjective judgments instead of dealing strictly with hard numbers; however, objectivity is still realized. This technique requires analysts to select and give each criterion a weighted importance from the threat's viewpoint. Analysts use the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (also called CARVER) matrix tool to employ this technique to support targeting prioritization. (See ATP 3-60.) The insight gained from how each criterion affects the outcome allows for a clear and persuasive presentation and argumentation of the assessment.

5-16. Weighted ranking assists in mitigating common cognitive pitfalls by converting the intelligence problem into a type of mathematical solution. The validity of weighting criteria is enhanced through group discussions, as group members share insights into the threat's purpose and viewpoint; red hat/team analysis can augment this technique. Weighted ranking uses matrices to compute and organize information. Table 5-4 briefly describes when to use the weighted ranking technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-4. Weighted ranking technique

Weighted ranking: *Technique that provides clarity among many alternatives by applying weighting to criteria to provide an overall score for each alternative.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use weighted ranking when there is a need for transparency in the reasoning used to derive an assessment. The targeting selection process is an example of when this technique is advantageous.	Weighted ranking adds validity to an assessment of alternatives, options, and hypotheses by mitigating biases and mindsets, which may result in the unsystematic and therefore inconsistent use of criteria.	Weighted ranking takes more time than many other basic structured analytic techniques and relies on a fair number of mathematical computations. This may cause analysts to avoid the technique.

5-17. **Method.** The following steps describe how to accomplish a simplified weighted ranking review of alternative options:

- **Step 1:** Create a matrix and develop all options and criteria related to the analytical issue. Figure 5-5 depicts the *options* as types of operations and the *criteria* as the five military aspects of terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment [OAKOC]).
- **Step 2:** Label the left, uppermost column/row of the matrix as options and fill the column with the types of operations generated in step 1.
- **Step 3:** List the criteria (OAKOC) generated in step 1 in the top row with one criterion per column.
- **Step 4:** Assign weights and list them in parentheses next to each criterion. Depending on the number of criteria, use either 10 or 100 points and divide them based on the analyst's judgment of each criterion's relative importance. Figure 5-5 shows how the analyst assigned the weights from the threat's perspective to the OAKOC factors using 10 points.
- **Step 5:** Work across the matrix one option (type of operation) at a time to evaluate the relative ability of the option to satisfy the corresponding criterion from the threat's perspective. Using the 10-point rating scale, assign 1 as low and 10 as high to rate each option separately. (See figure 5-5 for steps 1 through 5.)
- **Step 6:** Work across the matrix again, one option at a time, and multiply the criterion weight by the option rating and record this number in each cell. (See figure 5-6.)

Options	***Criteria***					
	Observation and fields of fire (2)	Avenues of approach (1)	Key terrain (1)	Obstacles (3)	Cover and concealment (3)	Total
Integrated attack	**7**	**8**	**6**	**3**	**6**	
Limited objective attack	**5**	**6**	**8**	**2**	**4**	
Spoiling attack	**7**	**3**	**2**	**5**	**8**	
Counterattack	**4**	**3**	**2**	**5**	**4**	
Maneuver defense	**7**	**3**	**2**	**2**	**8**	
Area defense	**5**	**2**	**4**	**7**	**8**	

Figure 5-5. Weighted ranking (steps 1–5) to determine the threat's most likely COA

Options	***Criteria***					
	Observation and fields of fire (2)	Avenues of approach (1)	Key terrain (1)	Obstacles (3)	Cover and concealment (3)	Total
Integrated attack	**7(2) = 14**	**8(1) = 8**	**6(1) = 6**	**3(3) = 9**	**6(3) = 18**	**55**
Limited objective attack	**5(2) = 10**	**6(1) = 6**	**8(1) = 8**	**2(3) = 6**	**4(3) = 12**	**42**
Spoiling attack	**7(2) = 14**	**3(1) = 3**	**2(1) = 2**	**5(3) = 15**	**8(3) = 24**	**58**
Counterattack	**4(2) = 8**	**3(1) = 3**	**2(1) = 2**	**5(3) = 15**	**4(3) = 12**	**40**
Maneuver defense	**7(2) = 14**	**3(1) = 3**	**2(1) = 2**	**2(3) = 6**	**8(3) = 24**	**49**
Area defense	**5(2) = 10**	**2(1) = 2**	**4(1) = 4**	**7(3) = 21**	**8(3) = 24**	**61**

Figure 5-6. Weighted ranking (step 6) to determine the threat's most likely COA

LINK ANALYSIS

5-18. Link analysis, often known as network analysis, is a technique used to evaluate the relationships between several types of entities such as organizations, individuals, objects, or activities. Visualization tools augment this technique by organizing and displaying data and assisting in identifying associations within complex networks. Although analysts can perform link analysis manually, they often use software to aid this technique. Link analysis programs are standard components in the Army's intelligence systems, from theater to company levels.

Performing Link Analysis Manually

A manual approach to link analysis is using small sticky notes of paper on a whiteboard. The analyst labels the notes to represent different entities and nodes and places them on the whiteboard. Using markers, the analyst links the entities and nodes. This method has several benefits:

- A larger picture may be seen on a whiteboard than on a computer monitor; many automated systems present limited views.
- It allows movement of the entities, quick redrawing of links, and color-coding using different markers.
- It allows analysts to perform link analysis together in OEs with intermittent connectivity and limited bandwidth.

Note. Other manual practices include using a corkboard with thumbtacks, colored string or thread or incorporating a map to add geographic context.

5-19. Analysts may use link analysis to focus on leaders and other prominent individuals, who are sometimes critical factors in the AO. Analysts use personality files—often obtained from conducting identity activities using reporting and biometrics, forensics, and DOMEX data—to build organizational diagrams that assist them in determining relationships between critical personalities and their associations to various groups or activities. This 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 2-01.3 for more information on assessing personalities and personality files.) Table 5-5 briefly describes when to use the link analysis technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-5. Link analysis technique

Link analysis: *Technique that maps and measures relationships or links among individuals, groups, or organizations.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use link analysis whenever individuals, groups, group activities, or process networks are being reviewed for insight. Analysts can use this technique to inform the targeting process and for assessing personalities, as accomplished during step 3 of the intelligence preparation of the battlefield process.	Link analysis can clarify what is known and what may be missing about the network being analyzed. Analysts can identify key nodes and hubs for social, organizational, and infrastructure networks, giving insight into relationships and potential vulnerabilities. Link analysis products are easily understood in briefings.	Analysts could assume (incorrectly) that a central figure in a network is the leader because of the number of connections to that figure. Analysts also might ignore the temporal aspect of the relationships and assume they are concurrent. Link analysis provides a freeze-frame look at an activity and seldom conveys change over time unless paired with a timeline or other multidimensional approach.

5-20. **Method.** The following steps describe how to construct a simple link analysis diagram:

- **Step 1:** Extract entities and the information about their relationships from intelligence holdings that include but are not limited to biometrics, forensics, and DOMEX information.
- **Step 2:** Place entity associations into a link chart using link analysis software or a spreadsheet or by drawing them manually:
  - Use separate shapes for different types of entities, for example, circles for people, rectangles for activities, and triangles for facilities. (See figure 5-7 on page 5-10.)
  - Use colored and varying types of lines to show different activities, for example, green solid lines for money transfers, blue dotted lines for communications, and solid black lines for activities. This differentiation typically requires a legend. (See figure 5-7 on page 5-10.)
- **Step 3:** Analyze the entities and links in the link chart.
- **Step 4:** Review the chart for gaps, significant relationships, and the meaning of the relationships based on the activity occurring. Ask critical questions of the data such as—
  - Which entity is central or key to the network?
  - Who or what is the initiator of interactions?
  - What role does each entity play in the network?

- Who or what forms a bridge or liaison between groups or subgroups?
- How have the interactions changed over time?
- Which nodes should be targeted for collection or defeat?

- **Step 5:** Summarize what is observed in the chart and draw interim hypotheses about the relationships.

5-21. The three types of visualization tools used in link analysis to record and visualize information are—

- Link diagram. (See figure 5-7.)
- Association matrix. (See figure 5-8.)
- Activities matrix. (See figure 5-9.)

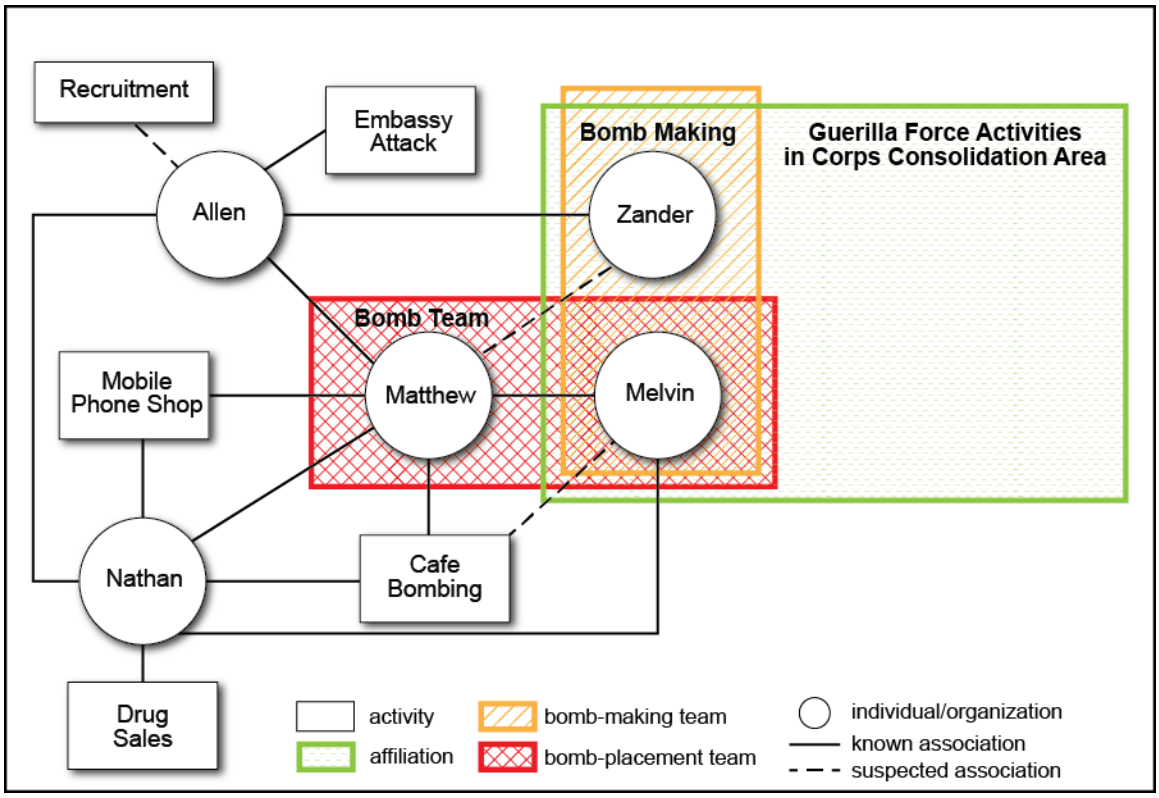


Figure 5-7. Link diagram example

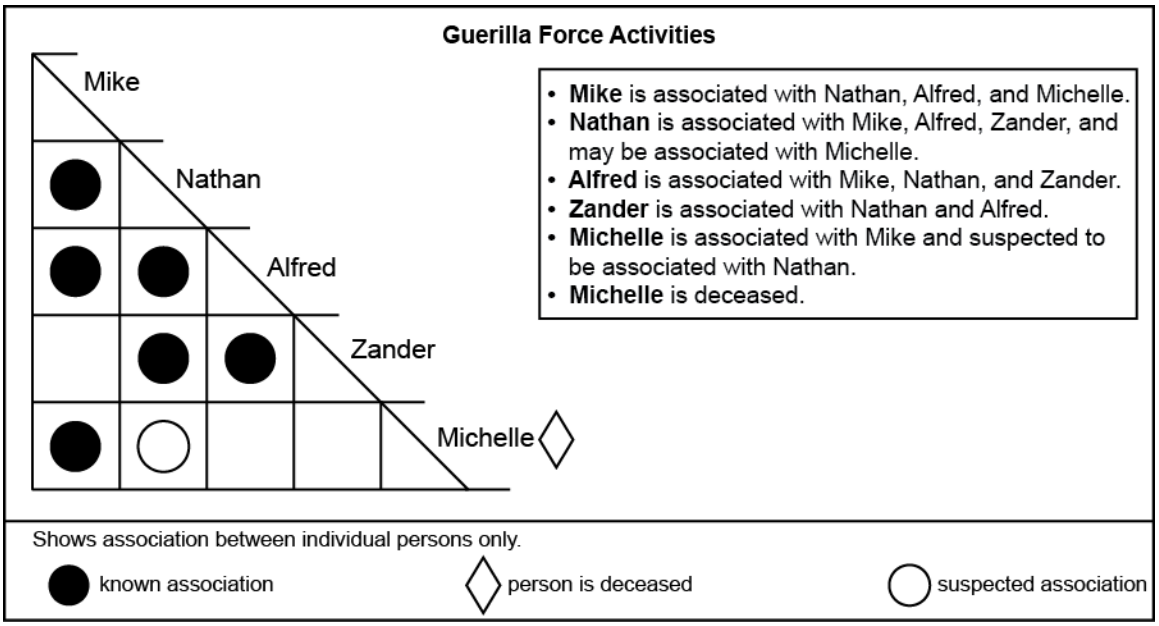


Figure 5-8. Association matrix example

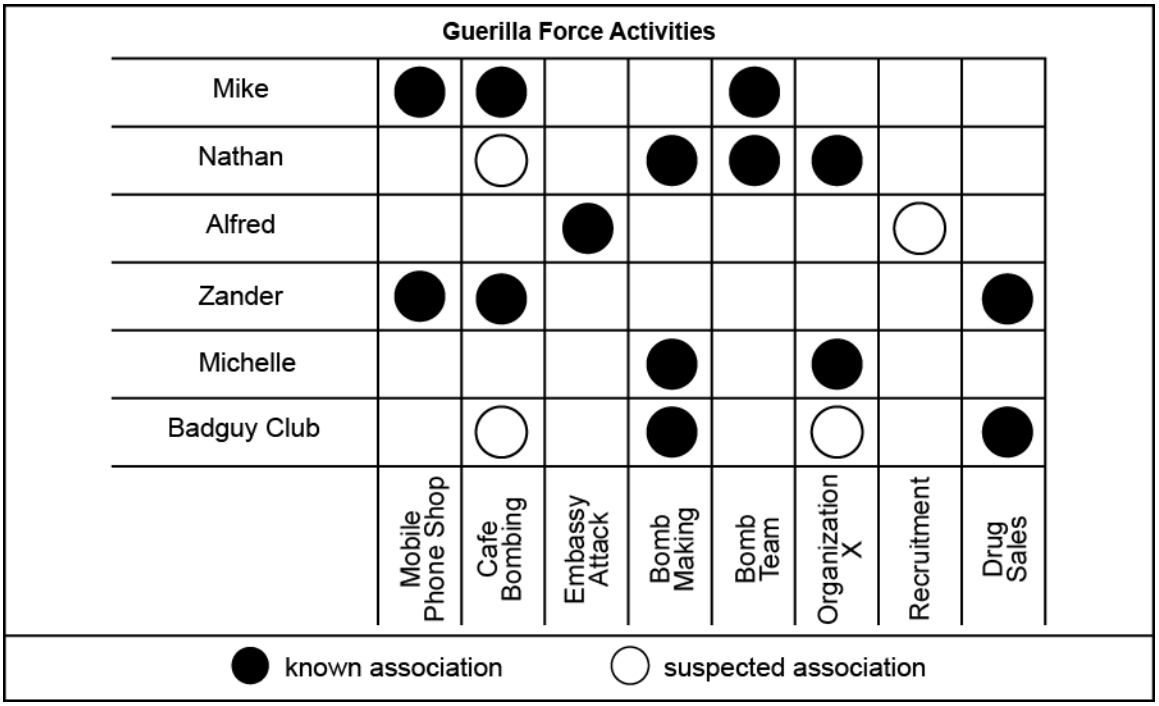


Figure 5-9. Activities matrix example

EVENT TREE

5-22. The event tree is a structured analytic technique that enables analysts to depict a possible sequence of events, including the potential branches of that sequence in a graphical format. An event tree works best when there are multiple, mutually exclusive options that cover the spectrum of reasonable alternatives. It clarifies the presumed sequence of events or decisions between an initiating event and an outcome. Table 5-6 briefly describes when to use the event tree technique, as well as the value added and potential pitfalls associated with this using technique. The following are pointers for analysts using the event tree technique:

- Use this technique in conjunction with weighted ranking, hypothesis-review techniques, and subjective probability to gain added insights.
- Leverage the expertise of a group of analysts during the construction of an event tree to ensure all events, factors, and decision options are considered.

Table 5-6. Event tree technique

Event tree: *A graphical depiction of a potential temporal sequence of events, including potential junctures within the event sequence.*		
When to use	**Value added**	**Potential pitfalls**
Analysts can use an event tree to clarify alternative event sequences with potential future outcomes or at least unknown outcomes related to an intelligence problem.	An event tree is a visual tool that analysts can use to depict a threat's options with decision points, which may provide insight into potential threat vulnerabilities. Event trees also provide an excellent method of determining collection requirements for indications that a decision has been made or events have unfolded in one of the alternative branches of the tree.	An intelligence failure can occur when the threat selects an unforeseen option arising from ignorance or when an unidentified event occurs.

5-23. **Method.** The following outlines the steps for creating event trees (see figure 5-10):

- **Step 1:** Identify the intelligence issue/problem (antigovernment protest in Egypt).
- **Step 2:** Identify the mutually exclusive and complete set of hypotheses that pertain to the intelligence issue/problem (Mubarak resigns or Mubarak stays).
- **Step 3:** Decide which events, factors, or decisions (such as variables) will have the greatest influence on the hypotheses identified in step 2.
- **Step 4:** Decide on the sequencing for when these factors are expected to occur or affect one another.
- **Step 5:** Determine the event options (Mubarak stays—hardline, reforms, some reforms) within each hypothesis and establish clear definitions for each event option to ensure collection strategies to monitor events are effective.
- **Step 6:** Construct the event tree from left to right. Each hypothesis is a separate main branch. Start with the first hypothesis and have one branch from this node for each realistic path the first event can take. Proceed down each event option node until the end state for that subbranch is reached. Then move to the next hypothesis and repeat the process.
- **Step 7:** Determine what would indicate a decision has been made at each decision point for each option to use in generating an integrated collection plan.
- **Step 8:** Assess the implications of each hypothesis on the intelligence problem.

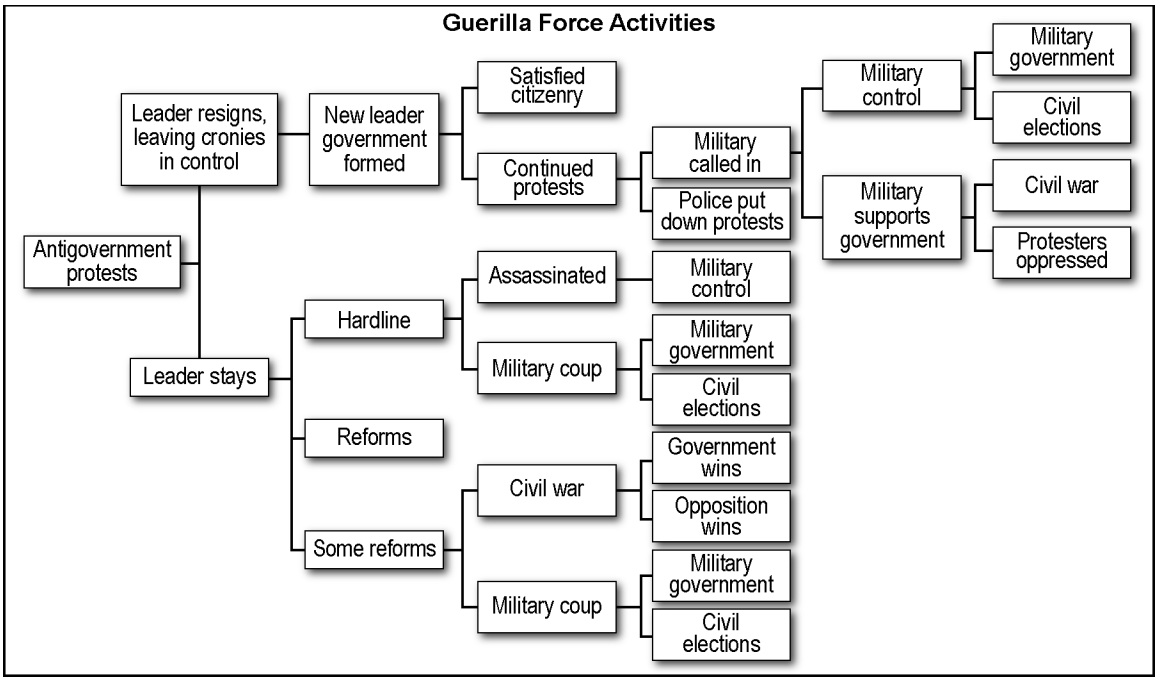


Figure 5-10. Event tree example

EVENT MAPPING

5-24. The event mapping technique uses brainstorming to assist in diagraming scenarios/elements stemming from analyst-derived hypotheses. Scenarios/Elements are linked around a central word or short phrase representing the issue/problem to be analyzed. (See paragraph 6-20 for more information on brainstorming.)

5-25. Event mapping scenarios/elements are arranged intuitively based on the importance of the concepts, and they are organized into groups, branches, or areas. Using the radial diagram format in event mapping assists in mitigating some bias, such as implied prioritization, anchoring, or other cognitive biases derived from hierarchy or sequential arrangements. Table 5-7 on page 5-14 briefly describes when to use the event mapping technique, as well as the value added and potential pitfalls associated with using this technique. The following includes event mapping general rules:

- Start with a blank medium such as paper or use a piece of stationery with adhesive on the back to make notes on a whiteboard.
- Think in terms of key words, phrases, or symbols that represent ideas and words.
- Annotate ideas as they occur, wherever they fit.
- Do not judge or hold back. Develop the map in the direction the topics flow—do not be limited by the map's appearance.
- As the map expands, strive to be more detailed.
- Use arrows or other visual aids to show the links between events in the scenario.
- Use color, as appropriate, to represent key players such as economics, military opposition groups, science, culture, and internal and external political pressures.

Table 5-7. Event mapping technique

Event mapping: *A mind-mapping diagram that represents the scenarios in hypotheses linked around a central issue.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use this technique when a nonlinear method is desired to generate, visualize, structure, and delineate the events in a scenario or hypotheses related to the intelligence issue/problem.	Event mapping uses a radial diagram that encourages a brainstorming approach. The many associations in event maps promote creativity in generating new ideas and associations not previously considered. This technique facilitates annotating indicators of change in developing collection plans.	Unconstrained event mapping can become overly detailed, lose focus, and include events and scenarios that lack relevance to the issue/problem analysts are studying.

5-26. **Method.** The following outlines the steps for applying event maps (see figure 5-11):

- **Step 1:** Place the word or symbol representing the issue/problem to be analyzed in the center of the medium from which the event map will be constructed.
- **Step 2:** Add symbols/words to represent possible actions/outcomes around the central issue/problem.
- **Step 3:** Link the possible actions/outcomes to the central issue or problem. If desired, use colors to indicate the major influence the link represents. For example, use green for economic links, red for opposition groups, or purple for military forces. Colors may also be used to differentiate paths for ease of reference.
- **Step 4:** Continue working outward, building the scenario of events into branches and subbranches for each hypothesis in detail.
- **Step 5:** If ideas end, move to another area or hypothesis.
- **Step 6:** When creativity wanes, stop and take a break. After the break, return and review the map and make additions and changes as desired.
- **Step 7:** As an option, number the links or decision points for each hypothesis. On a separate piece of paper, write down the evidence for each number to be collected that would disprove that link or decision. Use the lists for each number to develop an integrated collection strategy for the issue/problem.

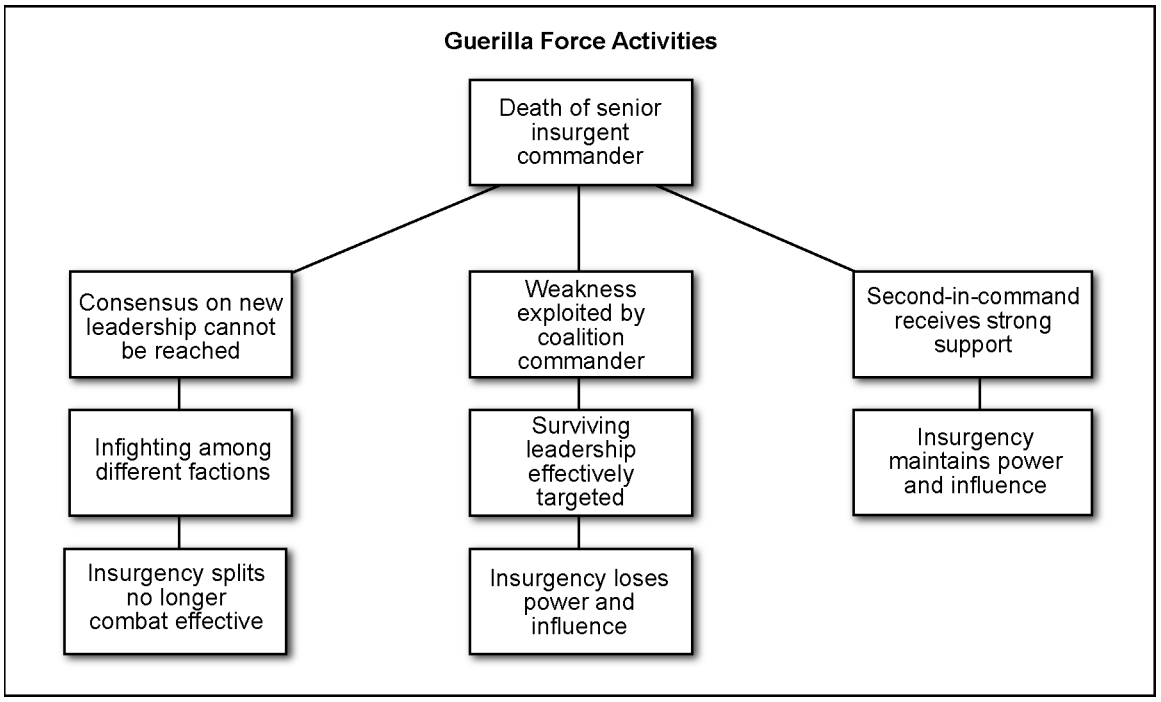


Figure 5-11. Event mapping example

SECTION II – DIAGNOSTIC STRUCTURED ANALYTIC TECHNIQUES

5-27. Diagnostic structured analytic techniques make analytical arguments, assumptions, and/or intelligence gaps more transparent. They are often used in association with most other analytic techniques to strengthen analytical assessments and conclusions. The most commonly used diagnostic techniques are—

- **Key assumptions check technique:** Reviewing assumptions that form the analytical judgments of the problem.
- **Quality of information check technique:**
  - Source credibility and access.
  - Plausibility of activity.
  - Imminence of activity.
  - Specificity of activity.
- **Indicators/Signposts of change technique:**
  - Identifying a set of competing hypotheses.
  - Creating lists of potential or expected events.
  - Reviewing/Updating indicator lists.
  - Identifying most likely hypotheses.

KEY ASSUMPTIONS CHECK

5-28. A key assumption is any hypothesis that analysts have accepted to be true and forms the basis of an assessment. For example, analysts may focus exclusively on analyzing key technical military variables of a military force and assume that a force will operate in a particular environment such as a desert, open plain, or arctic setting. The goal of this technique is not to undermine or abandon key assumptions; rather, it is to make them explicit and identify what information or developments would demand rethinking them.

5-29. Rechecking assumptions is valuable at any time before finalizing judgments. Key assumptions checks should be collaborative because an analyst cannot effectively self-check. Table 5-8 describes when to use this technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-8. Key assumptions check technique

Key assumptions check: *An exercise in explicitly listing and challenging key working assumptions that underlie the basic analysis.*		
When to use	**Value added**	**Potential pitfalls**
A key assumptions check is most beneficial at the beginning of an analytic project. Analysts typically identify key assumptions during step 2 of the military decision-making process.	Explicitly identifying working assumptions during an analytic project assists analysts in— • Explaining the logic of the analytical argument and exposing faulty logic. • Understanding key factors that shape an issue. • Stimulating thinking about an issue. • Uncovering hidden relationships and links between key factors. • Identifying developments that would cause them to abandon an assumption. • Preparing for changed circumstances that could surprise them.	Identifying hidden assumptions is difficult because they are ideas believed to be true, albeit often subconsciously. Therefore, the assumptions are seldom examined and almost never challenged.

5-30. **Method.** Checking for key assumptions requires analysts to consider how their analysis depends on the validity of certain evidence. The following four-step process assists analysts in checking key assumptions:

- **Step 1:** Review what the current analytic line of thinking on the issue appears to be:
  - What do analysts think they know?
  - What key details assist analysts in accepting that the assumption is true?
- **Step 2:** Articulate the evidence, both stated and implied in finished intelligence, accepted as true.

- **Step 3:** Challenge the assumption by asking why it must be true and is it valid under all conditions. What is the degree of confidence in those initial answers?
- **Step 4:** Refine the list of key assumptions to contain only those that must be true in order to sustain the analytic line of thinking. Consider under what circumstances or based on what information these assumptions might not be true.

5-31. Analysts should ask the following questions during this process:

- What is the degree of confidence that this assumption is true?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or key factor?
- If the assumption proves to be wrong, would it significantly alter the analytic line of thinking? How?
- Has this process identified new factors that require further analysis?

QUALITY OF INFORMATION CHECK

5-32. Weighing the validity of sources is a key feature of any analytical assessment. Establishing how much confidence analysts have in their analytical judgments should be based on the information's reliability and accuracy. Analysts should perform periodic checks of the information for their analytical judgments; otherwise, important analytical judgments may become anchored to poor-quality information.

5-33. Determining the quality of information independent of the source of the information is important in ensuring that neither duly influences the other. Not understanding the context in which critical information has been provided makes it difficult for analysts to assess the information's validity and establish a confidence level in the intelligence assessment. A typically reliable source can knowingly report inaccurate information, and a typically unreliable source can sometimes report high-quality information. Therefore, it is important to keep the two reviews—source and information—separate. Table 5-9 briefly describes when to use the quality of information check technique, as well as the value added and potential pitfalls associated with using this technique. This technique—

- Provides the foundation for determining the confidence level of an assessment and clarity to an analyst's confidence level in the assessment.
- Provides an opportunity to catch interpretation errors and mitigate assimilation or confirmation bias based on the source:
  - **Assimilation bias** is the modification and elaboration of new information to fit prior conceptions or hypotheses. The bias is toward confirming a preconceived answer.
  - **Confirmation bias** is the conditions that cause analysts to undervalue or ignore evidence that contradicts an early judgment and value evidence that tends to confirm already held assessments.
- Identifies intelligence gaps and potential denial and deception efforts.

Table 5-9. Quality of information check technique

Quality of information check: *A way to evaluate the completeness and validity of available information separately from the source.*		
When to use	**Value added**	**Potential pitfalls**
This technique should be initially applied during the screen phase of the analysis process. Periodic reviews of the quality of information should be conducted to prevent assumptions or weak judgments from becoming facts over time. Checking the quality of information is an ongoing, continuous process.	A thorough quality of information check provides analysts with an accurate assessment of "what we know" and "what we do not know." Additionally, this technique provides validity to analysts' confidence levels in assessments.	Analysts can become susceptible to circular reporting and source-based bias when reviewing the quality of information. Analysts may not consider that critical information may sometimes be found in reports from sources judged to have a low level of access or a poor record.

5-34. **Method.** For an information review to be fully effective, analysts need as much background information on sources as is possible. At a minimum, analysts should perform the following steps:

- **Step 1:** Review all sources of information for accuracy; identify any of the more critical or compelling sources. (For example, a human source with direct knowledge is compelling.)
- **Step 2:** Determine if analysts have sufficient and/or strong collaboration between the information sources.
- **Step 3:** Reexamine previously dismissed information considering new facts or circumstances.
- **Step 4:** Ensure any circular reporting is identified and properly flagged for other analysts; analysis based on circular reporting should also be reviewed to determine if the reporting was essential to the judgments made. (For example, a human source's purpose for providing information may be to deceive.)
- **Step 5:** Consider whether ambiguous information has been interpreted and qualified properly. (For example, a signals intelligence transcript may be incomplete.)
- **Step 6:** Indicate a level of confidence analysts can place on sources that may likely figure into future analytical assessments.

5-35. Analysts can use table 5-10 as a questioning guideline. Table 5-10 is not an all-inclusive list of questions, as it does not include every intelligence discipline. It is a start point for analysts to check the quality of the information; analysts can expand the list of questions to include other intelligence disciplines.

Table 5-10. Questioning guideline for checking information quality

Counterintelligence/Human intelligence
• Who wrote the report, and to what organization does the report writer belong? • What changes have been made to the data since the original collection? • What is the collector's evaluation of the information in the report? • Can the source's purpose be ascertained? • Was the information first-, second-, or third-hand? • Is there information from a different intelligence discipline that corroborates this report? • Is the information consistent or inconsistent with previous information? • Does the analyst have any concerns that denial and deception may be in the information? Why?
Geospatial intelligence
• What is the frequency of collection? When does it occur (time/day)? Have there been any recent changes to the frequency of collection or exploitation? • Are additional images being taken at different times? • Is the target aware of overhead imagery capabilities? • Are geospatial intelligence-based indicators being used to assess the site or the activity? • Is there a geospatial aspect to the information?
Signals intelligence
• Communications intelligence: ▪ Is this a complete transcript (verbatim) or a processed (analyzed) summary of the traffic? ▪ Was this report a snippet of a much longer conversation? ▪ Did the collection shortfall preclude capturing all the traffic? • Electronic intelligence: ▪ Is the signal correlated to any events or activities? ▪ What was the duration of the collection? ▪ What is the frequency of the collection? When does it occur (time/day)? ▪ Are additional signals being collected at different times? ▪ Is there additional intelligence that correlates with this emitter activity? ▪ Has the activity been corroborated by another form of intelligence?

Note. Analysts should consciously avoid relating the source to the information until the quality of information check is complete. If relating the source to the quality of information changes the opinion of the information, analysts must ensure they can articulate why. Analysts should develop and employ a spreadsheet to track the information and record their confidence levels in the quality of information as a constant reminder of the findings.

INDICATORS/SIGNPOSTS OF CHANGE

5-36. The indicators/signposts of change technique is primarily a diagnostic tool that assists analysts in identifying persons, activities, developments, or trends of interest. Indicators/Signposts of change are often tied to specific scenarios created by analysts to help them identify which scenario is unfolding. Indicators/Signposts of change are a preestablished set of observable phenomena periodically reviewed to help track events, spot emerging trends, and warn of unanticipated change. These observable phenomena are events expected to occur if a postulated situation is developing. For example, some of the observable events of a potential protest include—

- The massive gathering of people at a specific location.
- People's rallying cries posted as messages on social media.
- An adjacent country's aggressive national training and mobilization drills outside of normal patterns.

5-37. Analysts and other staff members create a list of these observable events and the detection and confirmation of these indicators enable analysts to answer specific information requirements that answer PIRs. Collection managers often use these lists to help create an intelligence collection plan. A list of indicators allows analysts to track developments and build a more concrete case for analytical judgments.

5-38. This technique aids other structured analytic techniques that require hypotheses generation as analysts create indicators that can confirm or deny these hypotheses. Analysts may use indicators/signposts of change to support analysis during all operations of the Army's strategic roles and to assist them in identifying a change in the operations. Table 5-11 briefly describes when to use the indicators/signposts of change technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-11. Indicators/Signposts of change technique

Indicators/Signposts of change: *A preestablished set of observable phenomena periodically reviewed to help track events, spot emerging trends, and warn of unanticipated change.*		
When to use	**Value added**	**Potential pitfalls**
The technique can be used whenever analysts need to track an event over time to monitor and evaluate changes. It can also amplify other structured analytic techniques and support collection management and current operations.	By providing an objective baseline for tracking events or targets, indicators/signposts of change instill rigor into the analysis process and enhance the credibility of analytical judgments.	Poor indicators can lead to analytic failures. This technique requires analysts to continually check the validity of the indicators as their original assumptions may be outdated or too narrow in focus.

5-39. **Method.** Whether used alone or in combination with other structured analysis, the process is the same. When developing indicators, analysts start from the event, work backwards, and include as many indicators as possible. The following outlines the steps to the indicators/signposts of change technique:

- **Step 1:** Identify a set of competing hypotheses or scenarios.
- **Step 2:** Create separate lists of potential activities, statements, or events expected for each hypothesis or scenario.
- **Step 3:** Regularly review and update the indicator lists to see which are changing.
- **Step 4:** Identify the most likely or most correct hypothesis or scenario based on the number of changed indicators observed.

Note. Analysts should avoid making an assessment based on a single indicator. Integrating multiple indicators is essential for analysts to obtain the clearest picture and assists in mitigating threat deception efforts.

Chapter 6
Advanced Structured Analytic Techniques

SECTION I – CONTRARIAN STRUCTURED ANALYTIC TECHNIQUES

6-1. Contrarian structured analytic techniques challenge ongoing assumptions and broaden possible outcomes. They assist analysts in understanding threat intentions, especially when not clearly stated or known. Contrarian techniques explore the problem from different (often multiple) perspectives. This allows analysts to better accept analytic critique and grant greater avenues to explore and challenge analytical arguments and mindsets. Proper technique application assists analysts in ensuring preconceptions and assumptions are thoroughly examined and tested for relevance, implication, and consequence.

6-2. The contrarian structured analytic techniques described in this publication are—

- **Analysis of competing hypotheses (ACH) technique:** Evaluating multiple hypotheses through a competitive process in order to reach unbiased conclusions and attempting to corroborate results.
- **Devil's advocacy technique:** Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.
- **Team A/Team B technique:** Using separate analytic teams that contrast two (or more) strongly held views or competing hypotheses.
- **High-impact/Low-probability analysis technique:** Highlighting an unlikely event that would have major consequences if it happened.
- **What if? analysis technique:** Assuming an event has occurred with potential (negative or positive) impacts and explaining how it might happen.

ANALYSIS OF COMPETING HYPOTHESES

6-3. Analysts use ACH to evaluate multiple competing hypotheses in order to foster unbiased conclusions. Analysts identify alternative explanations (hypotheses) and evaluate all evidence that will disconfirm rather than confirm hypotheses. While a single analyst can use ACH, it is most effective with a small team of analysts who can challenge each other's evaluation of the evidence.

6-4. ACH requires analysts to explicitly identify all reasonable alternatives and evaluate them against each other rather than evaluate their plausibility one at a time. ACH involves seeking evidence to refute hypotheses. The most probable hypothesis is usually the one with the least evidence against it, not the one with the most evidence for it. Conventional analysis generally entails looking for evidence to confirm a favored hypothesis. Analysts sometimes integrate the weighted ranking technique with ACH; this can help elevate one hypothesis in favor of another. Table 6-1 on page 6-2 briefly describes when to use the ACH technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-1. Analysis of competing hypotheses technique

Analysis of competing hypotheses (ACH): *A technique that uses a matrix as a tool to aid judgment on issues requiring careful weighting of alternative explanations or conclusions.*		
When to use	**Value added**	**Potential pitfalls**
ACH is highly effective when there is a large amount of data to absorb and evaluate. It is particularly appropriate when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments. This technique is useful for generating predictive assessments, as required, during step 4 of the intelligence preparation of the battlefield process.	ACH helps analysts overcome the following common mistakes that can lead to inaccurate forecasts: • Susceptibility to being unduly influenced by a first impression based on incomplete data, an existing analytic line of thought, or a single explanation that seems to fit well enough. • Lack of generating a full set of explanations or hypotheses at the outset of a project. • Reliance on evidence to support their preferred hypothesis, but that is also consistent with other explanations.	There are occasions when there is not enough evidence to arrive at a conclusion using ACH, or when the evidence is unbalanced enough—such as when using intelligence primarily from a single source—to lead to an inaccurate conclusion.

6-5. **Method.** Simultaneous evaluation of multiple competing hypotheses is difficult to accomplish without using tools. Retaining these hypotheses in working memory and then assessing how each piece of evidence interacts with each hypothesis is beyond the mental capabilities of most individuals. To manage the volume of information, analysts use a matrix as a tool to complete ACH. (See figure 6-1.) The following outlines the steps used to complete ACH:

- **Step 1:** Identify the intelligence problem.
- **Step 2:** Identify all possible hypotheses related to the intelligence problem.
- **Step 3:** Gather and make a list of all information related to the intelligence problem.
- **Step 4:** Prepare a matrix with each hypothesis across the top and each piece of information down the left side.
- **Step 5:** Determine if each piece of information is consistent or inconsistent with each hypothesis.
- **Step 6:** Refine the matrix. Reconsider the hypotheses and remove information that has no diagnostic value.
- **Step 7:** Draw tentative conclusions about the relative likelihood of each hypothesis.
- **Step 8:** Analyze if conclusions rely primarily on a few critical pieces of information.
- **Step 9:** Report conclusions.
- **Step 10:** Identify milestones for future observation that may indicate events are taking a different course than expected.

Guerilla Force Activities				
Evidence / Hypothesis (H)	H1 Threat 1/Threat 2 targets SECSTATE at summit.	H2 Threat 1/Threat 2 targets summit to disrupt peace process.	H3 Threat 1 targets SECSTATE at summit.	H4 Threat 1 targets summit to disrupt peace process.
Threat 1 facilitates attack on security force in AO (internet video post crediting Threat 2).	?	C	?	C
Threat 1 coordinates for *exterior talent* to execute security force bombing.	I	C	C	I
Threat 1 is more than a facilitator (completes security force bombing personally).	?	?	?	?
Threat 1 establishes safe house in AO in mid-June.	C	C	C	I
Threat 1 attempts to move targeting resources in AO in mid-June (exterior talent four personnel from unknown country).	C	C	C	I
Threat 1 references *conference* in AO in July and requests for *sales partner* and additional material.	C	C	C	I
Threat 1 facilitates attack on hotel in capital (no video - no credit).	I	C	C	I
No reporting on Threat 1 post attack on hotel in capital.	?	?	?	?
AO area of operations C consistent	I inconsistent SECSTATE Secretary of State			? neutral

Figure 6-1. Analysis of competing hypotheses used during step 4 of the IPB process

DEVIL'S ADVOCACY

6-6. Analysts use the devil's advocacy technique for reviewing proposed analytical conclusions. They are usually not involved in the deliberations that led to the proposed analytical conclusion. Devil's advocacy is most effective when used to challenge an analytic consensus or a key assumption about a critically important intelligence question. In some cases, analysts can review a key assumption and present a product that depicts the arguments and data that support a contrary assessment. Devil's advocacy can provide further confidence that the current analytic line of thought will endure close scrutiny. Table 6-2 briefly describes when to use the devil's advocacy technique, as well as the value added and potential pitfalls associated with using this technique. Devil's advocacy can lead analysts to draw one of three conclusions:

- Analysts ignored data or key lines of argument that undermine their analysis and should restart the analysis process.
- The analysis is sound, but more research is warranted in select areas.
- Key judgments are valid, but a higher level of confidence in the bottom-line judgments is warranted.

Table 6-2. Devil's advocacy technique

Devil's advocacy: *The process of challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.*		
When to use	**Value added**	**Potential pitfalls**
This technique is useful when there is concern about seemingly widespread unanimity amongst analysts on a critical issue. Analysts should assume the role of the devil's advocate if they have some doubts about a widely held view, or a leader might designate that analysts challenge the prevailing wisdom in order to reaffirm the group's confidence in those assessments.	Devil's advocacy challenges the current consensus to ensure analysts do not overlook alternate possibilities. It highlights the weaknesses in a current analytical judgment or assists in reaffirming analysts' confidence in the conclusion by— • Explicitly challenging key assumptions. • Identifying any faulty logic or information. • Presenting alternative hypotheses.	Those who strongly advocate an analytical judgment will resist a devil's advocacy approach. This technique challenges assumptions, but it can turn into an analytical argument with analysts taking sides rather than exploring the issue at hand.

6-7. **Method.** The following outlines the steps for the devil's advocacy technique:

- **Step 1:** Present the main analytical conclusion.
- **Step 2:** Outline the main points and key assumptions and characterize the evidence supporting the current analytical view.
- **Step 3:** Select one or more assumptions that appear the most susceptible to challenge.
- **Step 4:** Review the data used to determine questionable validity, possible deception, and the existence of gaps.
- **Step 5:** Highlight evidence that supports an alternative hypothesis or contradicts current thinking.
- **Step 6:** Present findings that demonstrate flawed assumptions, poor evidence, or possible deception.

6-8. Analysts should consider the following when conducting the devil's advocacy technique:

- Sources of uncertainty.
- Diagnosticity of evidence.
- Anomalous evidence.
- Changes in the broad environment.
- Alternative decision models.
- Availability of cultural expertise.
- Indicators of possible deception.
- Information gaps.

TEAM A/TEAM B

6-9. Team A/Team B is a process for comparing, contrasting, and clarifying two (or more) equally valid analytical assessments. Multiple teams of analysts perform this process, each working along different lines of analysis. Team A/Team B involves separate analytic teams that analyze two (or more) views or competing hypotheses. Team A/Team B is different from devil's advocacy, which challenges a single dominant mindset instead of comparing two (or more) strongly held views. Team A/Team B recognizes that there may be competing, and possibly equally strong, mindsets on an issue that needs to be clarified. A key requirement to ensure technique success is equally experienced competing mindsets. This mitigates unbalanced arguments. Table 6-3 briefly describes when to use the team A/team B technique, as well as the value added and potential pitfalls associated with using this technique.

Note. If opposing positions are well established, it can be useful to place analysts on teams that advocate positions they normally do not support; forcing analysts to argue the other side can make them more aware of their own mindsets.

Table 6-3. Team A/Team B technique

Team A/Team B: *Use of independent teams to contrast two (or more) strongly held views or competing hypotheses.*		
When to use	**Value added**	**Potential pitfalls**
If there are at least two competing views on a key issue, then team A/team B may be the appropriate technique to apply. Use when there are equally strong mindsets held on an issue that needs to be clarified.	This technique may help opposing groups see merit in each other's perspective. This reduces friction and differences by allowing those holding opposing views to feel their hypotheses have been given equal attention.	If the two teams are unequally matched, then the two views may receive an unequal amount of support.

6-10. **Method.** The following steps outlines the steps of the team A/team B technique (see figure 6-2):

- **Step 1:** Identify the two (or more) competing hypotheses.
- **Step 2:** Form teams and designate individuals to develop the best case for each hypothesis.
- **Step 3:** Review information that supports each respective position.
- **Step 4:** Identify missing information that would support or bolster the hypotheses.
- **Step 5:** Prepare a structured argument with an explicit discussion of—
  - Key assumptions.
  - Key evidence.
  - The logic behind the argument.
- **Step 6:** Set aside the time for a formal debate or an informal brainstorming session.

- **Step 7:** Have an independent jury of peers listen to the oral presentation and be prepared to question the teams about their assumptions, evidence, and/or logic.
- **Step 8:** Allow each team to present its case, challenge the other team's argument, and rebut the opponent's critique of its case.
- **Step 9:** The jury considers the strength of each presentation and recommends possible next steps for further research and collection efforts.

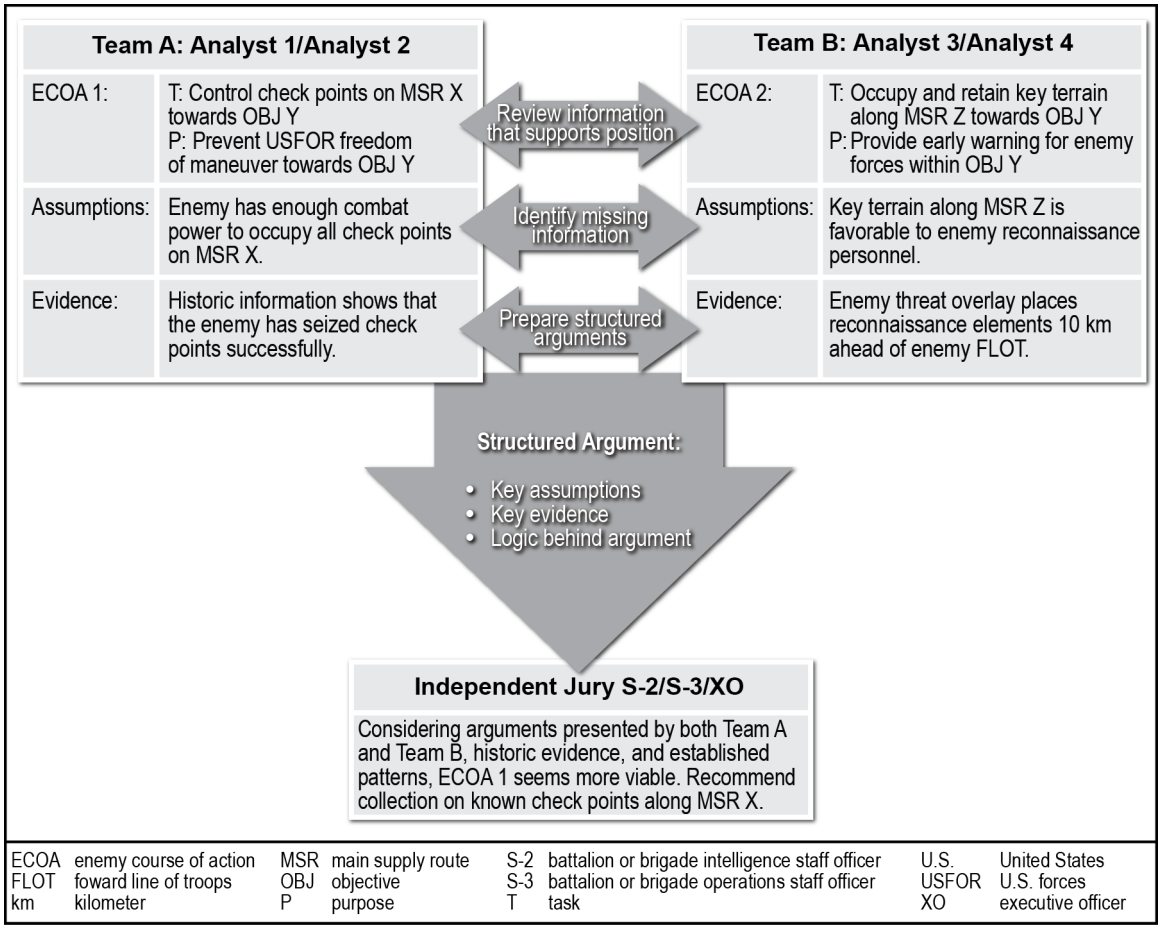


Figure 6-2. Team A/Team B used during step 4 of the IPB process

HIGH-IMPACT/LOW-PROBABILITY ANALYSIS

6-11. The high-impact/low-probability analysis technique sensitizes analysts to the potential impact that seemingly low-probability events could have on U.S. forces. New and often fragmentary data suggesting that a previously unanticipated event might occur is a trigger for applying this technique.

6-12. Mapping out the course of an unlikely, yet plausible event may uncover hidden relationships between key factors and assumptions; it may also alert analysts to oversights in the analytic line of thought. This technique can augment hypotheses-generating analytic techniques.

6-13. The objective of high-impact/low-probability analysis is exploring whether an increasingly credible case can be made for an unlikely event occurring that could pose a major danger or open a window of opportunity. Examining the unlikely allows analysts to develop indicators that may provide early warnings of a shift in the situation. By periodically reviewing those indicators, analysts are likely to counter any prevailing mindset that such a development is highly unlikely. Table 6-4 on page 6-6 briefly describes when to use high-impact/low-probability analysis, as well as the value added and potential pitfalls associated with using this technique.

Table 6-4. High-impact/Low-probability analysis technique

High-impact/Low-probability analysis: *Provides decision makers with an early warning that a seemingly unlikely but impactful event might actually occur.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use high-impact/low-probability analysis to analyze a threat's worst-case scenario.	This technique allows analysts to explore the consequences of an event—particularly an event not deemed likely by conventional wisdom—without having to challenge the main-line judgment or argue about how likely an event is to occur.	Analysts that communicate the likelihood of low-probability events occurring may cause intelligence assessment consumers to disregard those events. Therefore, analysts should use caution when communicating likelihoods. Additionally, high-impact/low-probability analysis is sometimes confused with "what if" analysis.

6-14. **Method.** An effective high-impact/low-probability analysis involves the following steps:

- **Step 1:** Define the high-impact outcome clearly. This will justify examining what may be deemed a very unlikely development.
- **Step 2:** Devise one or more plausible pathways to the low-probability outcome. Be precise, as it may aid in developing indicators for later monitoring.
- **Step 3:** Insert possible triggers or changes in momentum if appropriate (such as natural disasters, sudden key leader health problems, or economic or political turmoil).
- **Step 4:** Brainstorm plausible but unpredictable triggers of sudden change.
- **Step 5:** Identify a set of indicators for each pathway that help anticipate how events are likely to develop and periodically review those indicators.
- **Step 6:** Identify factors that could deflect a bad outcome or encourage a positive one.

"WHAT IF?" ANALYSIS

6-15. "What if?" analysis is a technique for challenging a strong mindset that an event will not occur or that a confidently made forecast may not be entirely justified. "What if?" analysis is similar to high-impact/low-probability analysis; however, it does not focus on the consequences of an unlikely event. "What if" analysis attempts to explain how the unlikely event might transpire. It also creates an awareness that prepares analysts to recognize early signs of a significant change.

6-16. "What if" analysis can also shift focus from asking whether an event will occur to working from the premise that it has occurred. This allows analysts to determine how the event might have happened. This technique can augment hypotheses-generating analytic techniques using multiple scenario generation or ACH. "What if?" analysis shifts the question from "How likely is the event?" to the following:

- How could the event possibly occur?
- What would be the impact of the event?
- Has the possibility of the event happening increased?

6-17. Like other contrarian techniques, "what if?" analysis must begin by stating the conventional analytic line of thought and then stepping back to consider alternative outcomes that are too important to dismiss no matter how unlikely. Table 6-5 briefly describes when to use the "what if?" analysis, as well as the value added and potential pitfalls associated with using this technique.

Table 6-5. "What if?" analysis technique

"What if?" analysis: *Assumes that an event has occurred with a potential for a major or negative impact and then explains how it came about using hindsight.*		
When to use	**Value added**	**Potential pitfalls**
Using this technique is important when a judgment relies on limited information or unproven assumptions. "What if?" analysis is also a logical follow-up to a key assumptions check that identifies an assumption that is critical to an important estimate but about which there is some doubt.	This technique opens the mind to think differently and creatively. It also provides decision makers a better sense of what can be done to prevent a development from occurring. Additionally, the technique facilitates developing indicators for a potential event.	"What if?" analysis is sometimes confused with high-impact/low-probability analysis. Analysts may waste time if the event hypothesized is inconceivable.

6-18. **Method.** The "what if?" analysis steps are similar to the high-impact/low-probability analysis steps once analysts have established the event itself:

- **Step 1:** Assume the event has happened.
- **Step 2:** Select some triggering events that permitted the scenario to unfold to help make the "what if?" more plausible (for example, the death of key leader, a natural disaster, an economic or political event that might start a chain of other events).
- **Step 3:** Develop a chain of reasoning based on logic and evidence to explain how this outcome could have occurred.
- **Step 4:** Think backwards from the event in concrete ways, specifying what must occur at each stage of the scenario.
- **Step 5:** Identify one or more plausible pathways to the event; it is likely that more than one will appear possible.
- **Step 6:** Generate an indicators/signposts of change list to detect the beginnings of the event.
- **Step 7:** Consider the scope of positive and negative consequences and their relative impact.
- **Step 8:** Monitor the indicators developed periodically.

High-Impact/Low-Probability Analysis Versus "What If?" Analysis

- High-impact/Low-probability analysis primarily warns decision makers that recent, unanticipated developments suggest an event, previously deemed highly unlikely, might occur. It projects forward, extracting from recent evidence or information.
- Conversely, "what if?" analysis does not typically require new evidence or anomalous information as a trigger. It looks back, imagining a surprising outcome and then mapping several ways that outcome could occur.

SECTION II – IMAGINATIVE STRUCTURED ANALYTIC TECHNIQUES

6-19. Imaginative structured analytic techniques assist analysts in approaching an analytic problem from different and multiple perspectives. This technique also broadens analysts' selection of potential COAs, thus reducing the chance of missing unforeseen outcomes. Imaginative techniques facilitate analysts' ability to forecast events and generate ideas creatively. Additionally, the proper application of imaginative techniques can assist in identifying differences in perspectives and different assumptions among analytic team members. The most commonly used imaginative techniques are—

- **Brainstorming technique:** Generating new ideas and concepts through unconstrained groupings.
- **Functional analysis technique:**
  - Identifying threat vulnerabilities through knowledge of threat capabilities.
  - Identifying windows of opportunity and threat vulnerabilities.

- **Outside-in thinking technique:** Identifying the full range of basic factors and trends that indirectly shape an issue.
- **Red hat/team analysis technique:** Modeling the behavior of an individual or group by trying to replicate how a threat would think about an issue.

BRAINSTORMING

6-20. Brainstorming is a widely used technique for stimulating new thinking; it can be applied to most other structured analytic techniques as an aid to thinking. Brainstorming is most effective when analysts have a degree of subject matter expertise on the topic of focus.

6-21. Brainstorming should be a very structured process to be most productive. An unconstrained, informal discussion might produce some interesting ideas, but usually a more systematic process is the most effective way to break down mindsets and produce new insights. The process involves a **divergent thinking phase** to generate and collect new ideas and insights, followed by a **convergent thinking phase** for grouping and organizing ideas around key concepts. Table 6-6 briefly describes when to use the brainstorming technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-6. Brainstorming structured technique

Brainstorming: *A technique that involves a group process for generating new ideas and concepts.*		
When to use	**Value added**	**Potential pitfalls**
Typically, analysts apply structured brainstorming when they begin a project to help generate a range of hypotheses about an issue or when amplifying other analytic techniques.	This technique can maximize creativity in the thinking process. Structured brainstorming allows analysts to see a wider range of factors that might bear on the topic than they would otherwise consider. It can spark new ideas, ensure a comprehensive look at a problem, raise questions, and prevent premature consensus.	There may not be enough time to apply structured brainstorming correctly, to include establishing rules and generating ideas. Additionally, analysts may censor each other's ideas.

6-22. **Method.** As a two-phase process, brainstorming elicits the most information from brainstorming participants:

- **Phase 1—Divergent thinking phase:**
  - **Step 1:** Distribute a piece of stationery with adhesive and pens/markers to all participants. Typically, a group of 10 to 12 people works best.
  - **Step 2:** Pose the problem in terms of a focal question. Display it in one sentence on a large easel or whiteboard.
  - **Step 3:** Ask the group to write down responses to the question, using key words that will fit on the small piece of stationery.
  - **Step 4:** Stick all of the notes on a wall for all to see—treat all ideas the same.
  - **Step 5:** When a pause follows the initial flow of ideas, the group is reaching the end of its collective conventional thinking, and new divergent ideas are then likely to emerge. End phase 1 of the brainstorming after two or three pauses.
- **Phase 2—Convergent thinking phase:**
  - **Step 6:** Ask group participants to rearrange the notes on the wall according to their commonalities or similar concepts. Discourage talking. Some notes may be moved several times as they begin to cluster. Copying some notes is permitted to allow ideas to be included in more than one group.
  - **Step 7:** Select a word or phrase that characterizes each grouping or cluster once all of the notes have been arranged.
  - **Step 8:** Identify any notes that do not easily fit with others and consider them as either isolated thoughts or the beginning of an idea that deserves further attention.
  - **Step 9:** Assess what the group has accomplished in terms of new ideas or concepts identified or new areas that require more work or further brainstorming.

- **Step 10:** Instruct each participant to select one or two areas that deserve the most attention. Tabulate the votes.
- **Step 11:** Set the brainstorming group's priorities based on the voting and decide on the next steps for analysis.

FUNCTIONAL ANALYSIS USING CRITICAL FACTORS ANALYSIS

6-23. Critical factors analysis (CFA) is an overarching analytic framework that assists analysts in identifying threat critical capabilities, threat critical requirements, and threat critical vulnerabilities that they can integrate into other structured analytic techniques. This assists friendly forces in effectively identifying windows of opportunity and threat vulnerabilities. At echelons above corps, CFA assists in identifying threat centers of gravity that friendly forces can use for operational planning:

- *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, or 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. CFA is often presented as a stand-alone technique; however, it shares characteristics found in other imaginative techniques. For the purposes of this publication, CFA is categorized under imaginative techniques.

6-24. To conduct CFA successfully, identify threat critical capabilities. The more specific the threat critical capability, the more specificity analysts can apply to threat critical capabilities, requirements, and vulnerabilities. CFA is more effective when conducted by a team of experienced analysts. Additionally, structured brainstorming can amplify this technique. Analysts can determine windows of opportunity by identifying the common denominator or entity that encompasses those identified threat critical capabilities, requirements, and vulnerabilities. Identified threat critical vulnerabilities are used to develop the HVT list in IPB, step 3, and then later prioritized by the fires cells. (See figure 6-3 on page 6-10.) Table 6-7 briefly describes when to use the functional analysis technique using CFA, as well as the value added and potential pitfalls associated with using this technique.

Table 6-7. Functional analysis technique using critical factors analysis

Functional analysis using critical factors analysis (CFA): The application of the knowledge of common and necessary military functions to specific threat capabilities.		
When to use	**Value added**	**Potential pitfalls**
Analysts should conduct functional analysis using CFA when attempting to identify windows of opportunity and threat vulnerabilities. This is often completed when evaluating the threat during step 3 of the intelligence preparation of the battlefield process.	Functional analysis may also act as the catalyst for other analytic tools such as the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (also called CARVER) matrix tool for prioritizing targets.	Units may not have enough experienced personnel to apply this technique effectively, as multiple analysts are optimal. There may not be enough time to conduct a thorough functional analysis.

6-25. **Method.** The following outlines those steps necessary to conduct CFA (see figure 6-3 on page 6-10):

- **Step 1:** Create a quad-chart. Identify a specific threat mission objective.
- **Step 2:** Identify all threat critical capabilities that are essential to achieve the threat mission objective and input in the top-right quadrant of the chart. (Threat must be able to achieve X.)
- **Step 3:** Identify all threat critical requirements—conditions or resources integral to critical capabilities developed in step 1—and input in the bottom-right quadrant of the chart. (To achieve X, the threat needs Y.)
- **Step 4:** Identify all threat critical vulnerabilities—elements related to threat critical requirements developed in step 2 that appear exposed or susceptible (at risk)—and input in the bottom-left quadrant of the chart. (The threat cannot lose Z.)

- **Step 5:** Analyze the chart to determine the windows of opportunity by identifying the common denominator (or entity) that encompasses those identified threat critical capabilities, requirements, and vulnerabilities and input in the top-left quadrant of the chart.
- **Step 6:** Identify all listed critical factors that friendly forces can directly affect to identify potential targets or topics for further collection.

Windows of Opportunity	**Threat Critical Capabilities**
Friendly force opportunities to attack: • Attack during threat movement because threat command and control limited during maneuver. • Attack at night because threat air limited to daytime.	• Maneuver in depth to disrupt friendly main effort. • Mass combat fire against friendly light reconnaissance force. • Speed presents two options against which to defend. • Capability to seize windows of opportunity.
Threat Critical Vulnerabilities	**Threat Critical Requirements**
• Command and control limited during maneuver. • Maneuver space and routes can be interdicted. • Supply elements vulnerable to attack. • Threat air limited to daytime and visual meteorological conditions. • Special operations forces insertion phase vulnerable to interdiction.	• Command and control. • Maneuver space and routes. • Long-range artillery and multiple launch rocket assets. • Available ammunition. • Available fuel. • Defensive counterair. • Available special operations forces support. • Available air transport to support insertion.

Figure 6-3. Functional analysis using critical factors analysis

OUTSIDE-IN THINKING

6-26. The outside-in thinking technique assists analysts in identifying the broad range of factors, forces, and trends that may indirectly shape an issue—such as global, political, environmental, technological, economic, or social forces—outside their area of expertise, but that may profoundly affect the issue of concern. This technique is useful for encouraging analysts to think critically because they tend to think from inside out, focusing on factors most familiar in their specific area of responsibility.

6-27. Outside-in thinking reduces the risk of missing important variables early in the analysis process; it should be the standard process for any project that analyzes potential future outcomes. This technique works well for a group of analysts responsible for a range of functional and/or regional issues. Table 6-8 briefly describes when to use the outside-in thinking technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-8. Outside-in thinking technique

Outside-in thinking: *A technique used to identify the range of systemic forces, factors, and trends that could shape an issue, allowing analysts to incorporate this broader conceptual framework into their analysis.*		
When to use	**Value added**	**Potential pitfalls**
Outside-in thinking is most useful in the early stages of an analytic project when the goal is to identify all critical, external factors that could influence how a particular situation will develop.	This technique encourages analysts to think about their issues in a wider conceptual and contextual framework. By recasting the problem in much broader and fundamental terms, analysts are more likely to uncover additional factors, an important dynamic, or a relevant alternative hypothesis.	Analysts tend to think from inside out, focusing on factors that are most familiar in their specific area of responsibility.

6-28. **Method.** The following outlines those steps of outside-in thinking (see figure 6-4):

- **Step 1:** Identify the topic of study.
- **Step 2:** Brainstorm all key factors (operational variables [PMESII-PT]) that could impact the topic.

- **Step 3:** Employ the mission variables (METT-TC) to trigger new ideas.
- **Step 4:** Focus on those key factors over which a commander can exert some influence.
- **Step 5:** Assess how each of those factors could affect the analytic problem.
- **Step 6:** Determine whether those factors can impact the issue based on the available evidence.

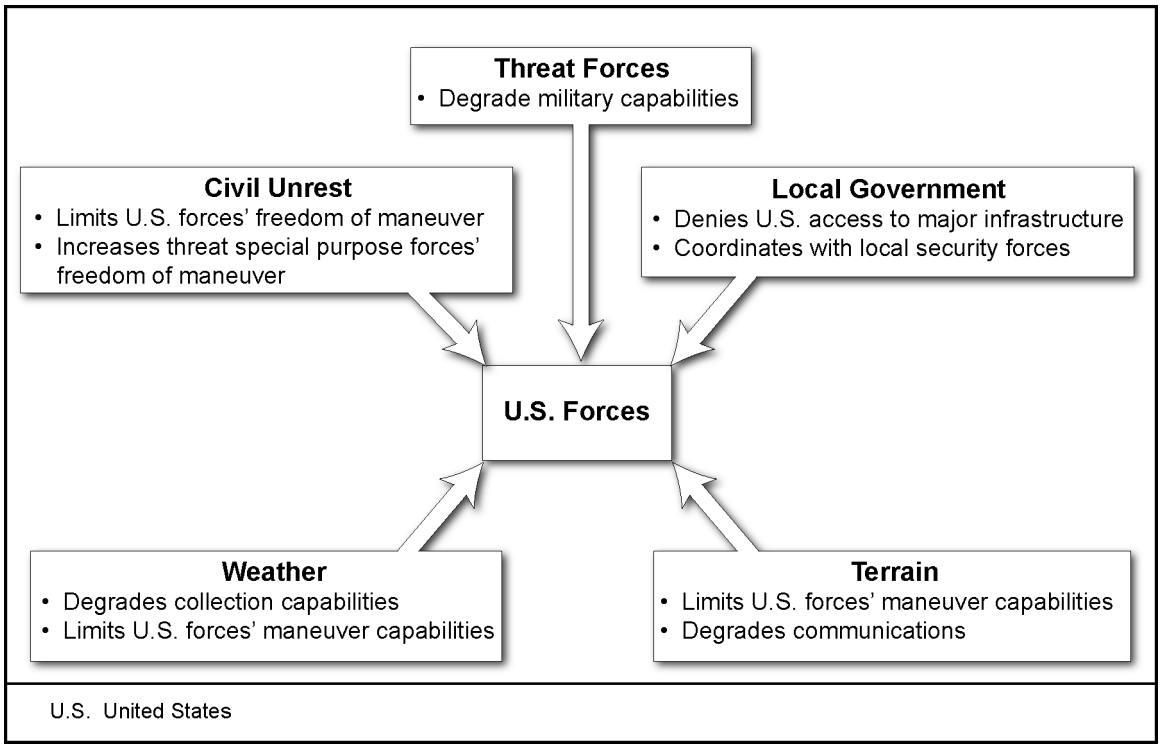


Figure 6-4. Outside-in thinking used during step 2 of the IPB process

RED HAT/TEAM ANALYSIS

6-29. The red hat/team analysis technique facilitates analysts' modeling of threat behavior by attempting to formulate ideas on how the threat would think about an issue. Red hat/team analysis is also a type of reframing technique performed by analysts attempting to solve an intelligence problem by using a different perspective. They attempt to perceive threats and opportunities as would the threat in order to categorize the threat. Categories include but are not limited—

- Command and control.
- Movement and maneuver.
- Intelligence.
- Fires.
- Sustainment.
- Protection.
- Cyberspace.

6-30. Red hat/team analysis is of limited value without a deep understanding of the threat—especially threat doctrine—and the threat's environment, which can affect the threat's decision making. Authoritarian leaders, military leaders, and small cohesive groups, such as terrorist cells, are candidates for this type of analysis. Analysts commonly use red hat/team analysis as a key input to step 2 of the MDMP. Table 6-9 on page 6-12 briefly describes when to use the red hat/team analysis technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-9. Red hat/team analysis technique

Red hat/team analysis: *A technique that aims to predict the behavior of a threat by trying to replicate how the threat thinks by way of analysts putting themselves "in the threat's shoes."*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use this technique when attempting to forecast behaviors, especially threat behaviors. Analysts typically conduct this type of analysis during step 4 of the intelligence preparation of the battlefield process or when supporting war gaming during the military decision-making process.	The conscious effort to imagine the situation as the target perceives it assists analysts in gaining a different and usually more accurate perspective of the problem or issue.	Analysts challenged to forecast how a threat may behave risk falling into a "mirror-image" exercise. That is, analysts may incorrectly conduct red hat/team analysis from the perspective that the threat shares the same motives, values, or understanding of an issue as they do. Additionally, analysts may assume that the threat will behave according to the same assumptions, culture, and doctrine as analysts would if faced with the same threats or opportunities.

6-31. **Method.** The following outlines the steps to conduct red hat/team analysis:

- **Step 1:** Identify the situation and ask how the threat would respond to the situation.
- **Step 2:** Emphasize the need to avoid mirror imaging. Define the cultural and personal norms that would influence the threat's behavior (use operational variables [PMESII-PT]/civil considerations [ASCOPE] and threat characteristics, threat doctrine, and threat intentions matrices as aids).
- **Step 3:** Develop first-person questions that the threat would ask about the situation.
- **Step 4:** Present results and describe alternative COAs the threat would pursue.

Note. Some publications differentiate between red hat analysis and red team analysis, while others describe them as being the same. When differentiated, red team analysis is categorized as a contrarian technique. For this publication, the two techniques are synonymous.

PART THREE

Intelligence Analysis Considerations

Chapter 7

Analytic Support to Army Forces and Operations

OVERVIEW

7-1. Although the intelligence analysis process does not change, the tasks performed by intelligence analysts differ significantly based on the echelon, the supported functional element, the Army strategic role, and the specific mission. As with many tasks, the most significant factor affecting analysis is time. Time includes both the amount of time to analyze a problem and the timeliness of the final analytical assessment to the decision maker.

7-2. Operations, such as large-scale ground combat operations, are often especially time-constrained for decision makers and analysts. Therefore, care must be taken to provide timely, quality analytical assessments. For example, during large-scale offensive operations, the terrain designated to various echelons to seize, retain, and exploit the initiative dictates the friendly operating tempo within assigned boundaries. A battalion S-2 is assigned a very narrow frontage, while a brigade S-2 looks at a larger area that potentially encompasses a frontage based on assigned and attached maneuver elements according to the assigned mission. However, a brigade conducting consolidation area security might look for bypassed and irregular forces and terrorists within a large and complex area.

ANALYSIS ACROSS THE ECHELONS

7-3. Intelligence analysts conduct analysis during combat operations to support Army forces at all echelons. The commander's need for the continuous assessment of enemy forces focuses intelligence analysis. The analytical output of the intelligence warfighting function assists commanders in making sound and timely decisions. Analysts must understand at which points in an operation the commander needs specific PIRs answered in order to support upcoming decision points. This understanding assists analysts in creating a timeline for conducting analysis and identifying when information is no longer of value to the commander's decision making.

7-4. Analytical elements at NGIC and at echelons above corps focus primarily on strategic- to operational-level analytic problems, analytical elements at the corps level focus on both tactical- and operational-level analytic problems, and analytical elements at echelons below corps focus on tactical-level analytic problems. The strategic, operational, and tactical levels of warfare assist commanders—informed by the conditions of their OEs—in visualizing a logical arrangement of forces, allocating resources, and assigning tasks based on a strategic purpose:

- *Strategic level of warfare* is the level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives (JP 3-0). At the strategic level, leaders develop an idea or set of ideas for employing the instruments of national power (diplomatic, informational, military, and economic) in a synchronized and integrated fashion to achieve national objectives.
- *Operational level of warfare* is the level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas (JP 3-0). The operational level links the tactical employment of forces to national and military strategic objectives, focusing on the design, planning, and execution of operations using operational art. (See ADP 3-0 for a discussion of operational art.)
- *Tactical level of warfare* is the level of warfare at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces (JP 3-0). The tactical level of warfare involves the employment and ordered arrangement of forces in relation to each other.

NATIONAL AND JOINT ANALYTIC SUPPORT

7-5. Intelligence analysis support to national organizations and the joint force focuses on threats, events, and other worldwide intelligence requirements. For the Army, the United States Army Intelligence and Security Command (INSCOM) is the lead organization to provide all-source and single-source intelligence capabilities to Army Service component commands. INSCOM includes functional brigades, units, and elements that provide general support, general support reinforcing, or direct support to theaters through intelligence reach, or they may be force-tailored for deployment to support the joint force. NGIC, which is under INSCOM, serves as the Army's Service Intelligence Center all-source analytical effort for general military intelligence, science and technology intelligence, and identity intelligence, all of which focus on the land domain. National and joint intelligence activities are continuous and reach across the range of military operations to provide continuous analytic support, including warning intelligence, to senior levels of the U.S. Government and DOD. (See JP 2-01 for more information on national and joint analytic support.)

THEATER ARMY

7-6. At the theater army level, intelligence analysis supports the combatant commander's operational mission requirements by enabling the theater command to apply capabilities to shape and prevent potential threat action. Theater army-level analytical activities include but are not limited to—

- Supporting theater campaign plans.
- Developing expertise to analyze threat characteristics within a region.
- Long-term analysis of a region and/or country that enables warning intelligence of imminent threat ground operations.
- Detailed analysis of multi-domain specific requirements.
- Serving as the Army's interface to national and joint support for operational and tactical forces.

7-7. Analysts assigned to the theater army-level all-source intelligence cell can expect to work with other Services as well as other nations. Analytical assessment support to future operations focuses on threat activities, intent, and capabilities beyond 168 hours within a designated global region assigned to the combatant commander.

CORPS

7-8. The corps G-2 and associated analytical elements, along with the ACE, further refine operational planning provided by the theater army, and they produce and update a broad range of intelligence products to support corps operations. These intelligence products, as well as constant collaboration between echelons, assist subordinate commands (division or brigade) in their planning. The corps ACE provides the most in-depth analysis at the tactical level to support the deep fight. Analytical assessment support to future operations focuses on threat activities, intent, and capabilities for the next 96 to 168 hours. (For more information on intelligence products, see appendix E.)

DIVISION

7-9. The division G-2, supported by the intelligence cell, advises the commander on how to leverage the intelligence warfighting function to support operations. The G-2 assists the commander in synchronizing intelligence operations; coordinates activities and systems that facilitate understanding the threat, terrain and weather, and other relevant aspects of the OE (such as key populations, groups, and organizations); and supervises the intelligence cell. The intelligence cell requests, receives, and analyzes information from multiple sources to produce and distribute intelligence products; it consists of most of the intelligence staff and an attached Air Force weather team.

BRIGADE COMBAT TEAM

7-10. The BCT S-2 is the principal intelligence advisor to the BCT commander. The S-2 coordinates activities and systems that facilitate understanding the threat, terrain and weather, and other relevant aspects of the area of interest (such as key populations, groups, and organizations). Additionally, the BCT S-2 supports security programs and oversees the BCT intelligence cell. The intelligence cell requests, receives, and analyzes information from multiple sources to produce and distribute intelligence products. The cell's geospatial engineer team manages the Standard Sharable Geospatial Foundation and geospatial information and services for the BCT, supporting the entire BCT with geospatial data and terrain analysis products.

BATTALION

7-11. Battalion-level intelligence analysis within the battalion intelligence section is rudimentary and focuses on a 12- to 24-hour period. Specifically, the battalion intelligence section focuses on IPB threat capabilities.

SUPPORT TO FUNCTIONAL ELEMENTS

7-12. The Army is committed to providing intelligence support across most unique functional elements. Although all of these elements perform IPB and collection management, the intelligence analysis requirements for these elements vary significantly based on the commander's designated mission; therefore, when assigned, intelligence analysts must learn the mission-specific intelligence analysis requirements for their functional element, identified in table 7-1.

Table 7-1. Intelligence analysis support to functional elements

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Air defense (AD) or air and missile defense	AD elements exist across all echelons. They establish AD plans to engage hostile ballistic missiles, aircraft, cruise missiles, and unmanned aircraft systems within the operational environment (OE).	Analysis focuses on air threats consisting of aircraft and missile technologies capable of controlling the air domain and influencing maneuverability within the land domain. Analysts must consider threat-to-friendly AD systems from threat air assets, as this is a United States (U.S.) or coalition Air Force mission.	JP 3-01 FM 3-01
Aviation	Aviation operations consist of aircraft (fixed- and rotary-wing) activities, airfield operations, and Army-level air traffic services.	Analysis support includes basic intelligence activities with additional knowledge of enemy aircraft and AD systems and capabilities. Army aviation operations require intelligence preparation of the battlefield (IPB) and collection support.	FM 3-04

Table 7-1. Intelligence analysis support to functional elements (*continued*)

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Chemical, biological, radiological, and nuclear (CBRN)	CBRN units support the Army across all echelons by identifying CBRN threats on the battlefield. This includes CBRN passive defense preventive measures to minimize friendly unit vulnerability to CBRN threat/hazard effects. CBRN reconnaissance and surveillance provide the command with detailed, timely, and accurate information to inform decision making or answer the commander's critical information requirements about CBRN threats or hazards.	Analysis support includes basic intelligence activities with additional knowledge of enemy capabilities to employ CBRN capabilities against friendly forces and toxic industrial material or dual-use facilities. Army CBRN operations require IPB and collection support to guide CBRN reconnaissance element collection efforts.	ATP 3-11.36 ATP 3-11.37 FM 3-11
Civil affairs (CA)	CA operations enhance awareness of and manage interactions with the OE civil component, identify and mitigate underlying causes of instability in the civil society, or apply functional specialty skills, which are normally the civil government's responsibility.	Analysis support focuses on IPB and threats to civil considerations (areas, structures, capabilities, organizations, people, and events [ASCOPE]).	FM 3-53 FM 3-57
Cyberspace	Cyberspace elements provide defensive cyberspace operations to the Army as well as to global commands.	Analysis support to cyberspace operations is a developing process and requires examination of current cyberspace operational concepts. Army cyberspace operations require unique cyberspace IPB and collection support.	FM 3-12
Engineer	Engineer activities include geospatial support, construction, real property maintenance activities, sustainment of lines of communications (LOCs), engineer logistics management, base camp development, mobility and countermobility functions, including river speeds, wet gap crossing bank slope, obstacle types and orientation, enemy engagement area development activities, and percentage of enemy survivability positions dug.	Basic analysis support to engineering activities is necessary to identify threats and enemy force activities. Army operational and tactical engineer operations require IPB and collection support. All staff sections rely on Army engineers to provide Standard Sharable Geospatial Foundation and geospatial and terrain analysis for mission planning, command and control/current operations, and geospatial intelligence products.	ATP 3-90.4 ATP 3-90.8 FM 3-34
Explosive ordnance disposal/ Counter-improvised explosive device/ Counter-explosive hazard	Large-scale ground combat operations support includes— • Targeting and remediating threat munitions production, storage, and employment. (Contingency) • Defeating explosive threats to the force. • Mitigating explosive hazards via training the force. • Neutralizing explosive hazards via attacking threat networks.	Analysis supports— • Characterizing threat capabilities in the context of conventional and unconventional munitions and explosive hazards, including CBRN threats. • Detecting, identifying, and targeting threat munition and explosive hazard production and storage capabilities, facilities, and networks. • Describing the threat's use of munitions and explosive hazards to support training.	JP 3-15.1 ATP 3-90.37 ATP 4-32 ATP 4-32.1
Medical	The complexities of the range of military operations require medical support to military and civilian considerations (ASCOPE).	Intelligence analysts advise the medical command on nuclear/chemical surety and CBRN operations. Reference the National Center for Medical Intelligence for all-source medical intelligence assessments.	FM 4-02

Table 7-1. Intelligence analysis support to functional elements (*continued*)

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Military police (MP)	MPs provide the Army's policing, investigations, and corrections capabilities to enable protection, preserve the force, and promote the rule of law. MPs execute these capabilities via the three MP disciplines: police operations, detention operations, and security and mobility support.	Analysis enables MP commanders' situational understanding, battlefield visualization, and force protection programs by providing relevant criminal threat and friendly information that impacts operational and tactical environments. Army MP operations and overall effects require IPB and collection support.	ATP 3-39.10 ATP 3-39.20 ATP 3-39.30 FM 3-39 FM 3-63
Psychological operations	Military information support operations support corps and divisions in providing tactical-level analysis and augmentation that include language and cultural expertise, regional analysis, and mass communications delivery capabilities.	Analysis support to military information support operations includes performing IPB, specifically threat and civil considerations (ASCOPE) analysis.	FM 3-53
Signal	The signal element supports all levels of Army commands and provides Army communications and communications security—Department of Defense information network (DODIN) operations.	Analysis support is wide-ranging, from global threat analysis to support of threat communications capabilities within a given OE. DODIN operations require IPB and collection support.	FM 6-02
Space	The Army space force is a multicomponent organization of space support elements that conduct theater space operations and planning, integrate and coordinate space capabilities, and support commanders in exercising command and control through space operations.	Analysis support to the Army Space and Missile Defense Command is unique; therefore, it provides new intelligence personnel upon arrival. Army space operations require unique space IPB and collection support.	FM 3-14
Special operations forces (SOF)	*Army special operations forces* are those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations (JP 3-05). SOF include CA, psychological operations, Rangers, special forces, special mission units, and Army special operations aviation forces assigned to the U.S. Army Special Operations Command—all supported by the 528th Sustainment Brigade (Special Operations) (Airborne).	Analysis support includes efforts to defeat joint, transregional, all-domain, multifunctional threats and to facilitate Army special operations over a multi-domain extended battlefield in large-scale ground combat operations. Within the range of military operations, analysis assists commanders in developing the appropriate lines of effort and lines of operations to destroy threat networks, shape conditions, deter threats, and influence relevant actors. A common factor of special operations and associated activities is that special operations units conducting operations are either operating among populations or supporting others in permissive or uncertain environments. This factor requires nuanced information and intelligence products to ensure special operations units' consistent interactions with populations contribute to the success of the mission instead of being a detriment to the mission. Most importantly, operating among populations requires an understanding that the populations and subgroups within it are important, potential centers of gravity, sources of power, and often the basis to long-term stability.	ADP 3-05

Table 7-1. Intelligence analysis support to functional elements (*continued*)

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Sustainment	Sustainment doctrine focuses on the four elements of sustainment: logistics, personnel services, financial management, and health service support to unified land operations.	Analysis support includes basic intelligence activities with additional knowledge of logistics, LOCs, medical or health services, and, to some extent, personnel services and financial management. Army sustainment operations require IPB and collection support.	ADP 4-0

ANALYSIS ACROSS THE ARMY'S STRATEGIC ROLES

7-13. Intelligence analysts must consider all intelligence requirements for operations to shape, prevent, prevail in large-scale ground combat, and consolidate gains. However, the conduct of these operations is associated with the combatant command, as designated by the DOD, and with OE conditions.

SHAPE OPERATIONAL ENVIRONMENTS

7-14. Table 7-2 lists some of the unique considerations and intelligence requirements associated with operations to shape OEs. (For more information on shaping OEs, see FM 2-0's chapter 5.)

Table 7-2. Intelligence requirements associated with operations to shape

Unique considerations	*Intelligence requirements associated with shaping operational environments*
Key leaders	• Identify key leaders (politics, military, economic, social, information, infrastructure). • Evaluate the amount of influence of each leader. • Describe the local populace's opinion of each leader. • Perform link analysis for each leader's social and professional circles. • Research general biographical information.
Threat intent/critical capabilities	• Identify the critical resources the threat requires by capability. • Define the end state the threat is attempting to achieve. • Define decision points to reach the threat organization's end state. • Research open-source reporting on the threat. • Determine the threat's current phase of operations. • Project the threat's likely courses of action and potential crisis issues/flash points. (This should also develop indicators.)
Training activities	• Locate training locations. • Describe the threat training cycle. • Define threat capabilities by warfighting function. • Identify if new threat capabilities are being trained. • Describe how training is sustained.
Political activities	• Evaluate the effectiveness of the government. • Describe the local populace's opinion about the government. • Identify the government's critical requirements by capabilities. • Identify goals the government is attempting to achieve.

PREVENT CONFLICT

7-15. Table 7-3 lists some of the unique considerations and intelligence requirements associated with operations to prevent conflict. (For more information on preventing conflict, see FM 2-0's chapter 5.)

Table 7-3. Intelligence requirements associated with operations to prevent

Unique considerations	*Intelligence requirements associated with preventing conflict*
Mobilization actions	• Describe how the threat will conduct operations. • Evaluate if any windows of opportunity are present from the current situation and disposition. • Identify friendly risks based on the current situation and disposition. • Identify key terrain. • Identify areas that can limit friendly and threat freedom of movement.

PREVAIL IN LARGE-SCALE GROUND COMBAT

7-16. Table 7-4 lists some of the common considerations and intelligence requirements associated with large-scale ground combat operations.

Table 7-4. Intelligence requirements associated with large-scale ground combat operations

Considerations	*Intelligence requirements associated with large-scale ground combat*
Conventional forces and special operations forces	• Describe the threat using intelligence preparation of the battlefield (IPB). • Identify the threat's mission statement and intent. • Identify threat requirements that enable the threat to meet its end state. • Identify the threat commander's acceptable risk. • Identify the threat commander's decision points.
Irregular forces/Terrorists	• Identify irregular forces that friendly forces may encounter. • Describe irregular forces' capabilities by warfighting function. • Determine irregular forces' unique missions. • Identify when irregular forces will interdict/impede friendly force movement. • Locate where irregular forces will observe friendly forces. • Determine irregular forces' high-value targets. • Determine irregular forces' fire support.
Other adversaries (terrorist organizations, criminal organizations, individual relevant actors)	• Identify adversaries' purpose, intent, and motivations. • Identify adversaries' structure, organization, and networks. • Conduct human network analysis. • Identify adversaries' perspectives, intentions, strengths, vulnerabilities, susceptibilities, opportunities, issues, goals, and influence. • Identify nexuses between individual adversarial organizations. • Identify nexuses between adversarial organizations and conventional, special operations, and irregular forces.
Consolidation area	• **Bypassed enemy forces:** ▪ Identify the current disposition of potential stay-behind forces. ▪ Evaluate if the projected attrition of threat personnel is accurate. ▪ Describe how local nationals are reacting to stay-behind forces. ▪ Identify the goals of the stay-behind forces. • **Enemy special operations forces:** ▪ Identify potential safe havens. ▪ Identify potential civilian groups that may provide support. ▪ Identify the most likely tactics, techniques, and procedures that will be employed. ▪ Identify which friendly capabilities are most vulnerable to attack. • **Criminal organizations:** ▪ Identify activities that will impede friendly operations. ▪ Identify activities that will degrade public security. ▪ Determine which organizations can be levied as friendly proxies.

Table 7-4. Intelligence requirements associated with large-scale ground combat operations (*continued*)

Considerations	*Intelligence requirements associated with large-scale ground combat*
Consolidation area (*continued*)	• **Terrorist organizations:** ▪ Identify leaders in the area of operations that may be connected to terrorist activities. ▪ Describe successful terrorist activities that have occurred in the area of operations. ▪ Determine the most plausible, deadliest attack that may potentially occur. ▪ Identify resources terrorists require to conduct attacks. ▪ Describe the tactics, techniques, and procedures employed by terrorists. • **Irregular forces:** ▪ Place large emphasis/focus on civil considerations (ASCOPE). ▪ Identify resources the local populace requires. ▪ Determine if and describe how irregular forces are using those resources as leverage. ▪ Determine which populations are filling irregular force ranks. ▪ Determine which population areas are sympathetic to irregular force activities. ▪ Determine who has influence over irregular forces. • **Local population critical needs:** ▪ Identify the status of the basic infrastructure, including water, heating and cooling resources, electricity, medical, waste collection, roads, bridges, railways, seaports, airports, telecommunications, law enforcement, and emergency services. ▪ Identify key personnel required to manage the infrastructure. ▪ Coordinate analysis with attached or supporting civil affairs and psychological operations forces and organic staffs. ▪ Integrate infrastructure status into the common operational picture. • **Enemy reconsolidation and identification of capabilities.**
Support area	• Evaluate the infrastructure. • Determine refugee flow. • Identify obstacles to continuing activities.

ASCOPE areas, structures, capabilities, organizations, people, and events

OFFENSIVE AND DEFENSIVE OPERATIONS IN LARGE-SCALE GROUND COMBAT

7-17. Whether in offensive or defensive operations, the intelligence analysis process conducted does not differ drastically. In offensive and defensive operations during large-scale ground combat, the operating tempo is accelerated and therefore, intelligence analysis is accelerated. Regardless of the type of operation, all-source intelligence is the primary capability within the intelligence warfighting function that aids commanders' understanding of their OE. (See ADP 3-90 for a detailed discussion on offensive and defensive operations.)

Offensive Operations

7-18. An *offensive operation* is an operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers (ADP 3-0). The main differences between offensive and defensive operations are the focus and detail level of analysis required for determining the enemy's defensive framework and the effects of terrain on friendly maneuver. Additionally, the enemy often employs capabilities using different tactics and techniques, depending on the specific offensive or defensive operation. Offensive operations are either force-oriented or terrain-oriented. Force-oriented offensive operations focus on the enemy. Terrain-oriented offensive operations focus on seizing and retaining control of the terrain and facilities. Detailed IPB products, such as a modified combined obstacle overlay with intervisibility lines or an event template, must be developed to depict this information. (See ATP 2-01.3.) Table 7-5 lists some of the intelligence requirements associated with offensive operations.

Table 7-5. Intelligence requirements associated with the offense

Determine the enemy's likely purpose and type of defense: area defense, mobile defense, or retrograde.
Determine the enemy's likely end state, objectives, decision points, culmination point, strengths, vulnerabilities, and scheme of maneuver.
Identify military aspects of terrain (OAKOC) and weather effects that support enemy defensive operations: • Terrain that allows reconnaissance and security outposts to be arranged in depth along choke points and terrain features that canalize friendly forces to attrite U.S. forces and diminish U.S. combat power in depth. • Terrain, including subterranean, that allows the enemy to tie obstacles to existing terrain features to support enemy defensive positions. (See ATP 3-21.51 for more on subterranean terrain.) • Favorable air and ground avenues of approach for an enemy counterattack. • Terrain that canalizes friendly attacking forces. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems.
Identify military aspects of terrain (OAKOC) and weather effects that support friendly offensive operations: • Favorable ground and air mobility corridors. • Areas with significant concealment and/or cover. • Terrain that allows forces to bypass obstacles and enemy positions. • Infiltration routes. • Landing zones. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems. • Favorable weather for using obscuration or chemical weapons.
Identify the location and orientation of enemy counterreconnaissance and security units, obstacles, engagement areas, main battle areas, reserve units, and likely counterattack routes.
Within each enemy defensive area, identify specific primary, secondary, tertiary locations of enemy infantry, armored, antitank, mortar, and other units and systems, and the potential use of camouflage.
Determine the likely use and identify the location of enemy command and control nodes, reconnaissance and surveillance assets, long-range fires, artillery and rocket units, air defense systems, rotary aviation units, close air support, engineer units, ammunition and logistics nodes, CBRN units, electronic warfare assets, and special operations forces.
Determine the enemy's likely use of information warfare, cyberattacks, and denial and deception operations.
Determine the impact of significant civil considerations (ASCOPE) on friendly and enemy operations such as hindering movement on lines of communications, medical and health considerations, and the housing and feeding of a displaced population.
ASCOPE areas, structures, capabilities, organizations, people, and events CBRN chemical, biological, radiological, and nuclear OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment U.S. United States

Defensive Operations

7-19. A *defensive operation* is an operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations (ADP 3-0). Defensive operations retain decisive terrain or deny the enemy access to a vital area, attrite or fix the enemy as a prelude to offensive operations, counter a surprise action by the enemy, or increase the enemy's vulnerability by forcing the enemy to concentrate its forces.

7-20. The main differences between defensive operations and other decisive action are the focus and detail level of analysis required for determining the enemy's offensive framework and the effects of terrain on friendly defensive operations. Table 7-6 on page 7-10 lists some of the intelligence requirements associated with defensive operations.

Table 7-6. Intelligence requirements associated with the defense

Determine the enemy's likely purpose (for example, terrain- or force-oriented) and type of offense.
Determine the enemy's likely end state, objectives, decision points, culmination point, strengths, vulnerabilities, and scheme of maneuver.
Identify military aspects of terrain (OAKOC) and weather effects that support enemy offensive operations: • Favorable ground corridors and air avenues of approach. • Areas with significant concealment and/or cover. • Terrain, including subterranean, that allows forces to bypass obstacles and friendly positions. (See ATP 3-21.51 for more on subterranean terrain.) • Infiltration routes. • Landing zones. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems. • Favorable weather for using obscuration or chemical weapons.
Identify military aspects of terrain (OAKOC) and weather effects that support friendly defensive operations: • Terrain that allows friendly forces to tie obstacles to existing terrain features to supports friendly defensive positions. • Favorable air and ground avenues of approach for a counterattack. • Terrain that canalizes enemy attacking forces. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems.
Identify the location of enemy assembly areas, ammunition and logistics nodes, forward aviation locations, and likely movement routes into the friendly area of operations.
Template and track the composition, disposition, likely routes, and time phase lines of reconnaissance and surveillance, security, advanced engineering, infiltrating, and air assault units.
Template and track the composition, disposition, likely routes, and time phase lines of advance guard, main body, antitank, reserve, and second echelon units.
Template and track specific locations where the enemy will conduct key maneuver tasks, such as occupying support by fire positions and dismounting infantry, or where friendly units may be isolated in defensive positions due to the enemy's use of artillery scatterable mines.
Determine the likely use and template the location of enemy command and control nodes, long-range fires, artillery and rocket units, air defense systems, attack helicopter units, close air support, engineer units, CBRN units, electronic warfare assets, and special operations forces.
Determine the enemy's likely use of information warfare, cyberattacks, and denial and deception operations.
Determine the impact of significant civil considerations (ASCOPE) on friendly and enemy operations such as hindering movement on lines of communications, medical and health considerations, and the housing and feeding of a displaced population.
ASCOPE areas, structures, capabilities, organizations, people, and events CBRN chemical, biological, radiological, and nuclear OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment

CONSOLIDATE GAINS

7-21. Commanders continually (through all phases of the operation) consider activities necessary to consolidate gains and achieve the end state. Operations to consolidate gains require a dynamic intelligence effort to conduct offensive and defensive operations that do not create secondary impacts to consolidating gains (for example, destroying key infrastructure) while also supporting the execution of area security and stability operations.

Consolidate Gains Concurrent with Large-Scale Ground Combat Operations

7-22. Table 7-7 lists some of the unique considerations and intelligence requirements associated with operations to consolidate gains during large-scale ground combat operations.

Table 7-7. Intelligence requirements associated with operations to consolidate gains

Unique considerations	*Intelligence requirements associated with consolidating gains*
Assessments	• Conduct battle damage assessments. • Evaluate the effectiveness of friendly operations. • Determine if there are any remaining stay-behind forces. • Describe the composition of any stay-behind forces (bypassed/isolated conventional forces, irregular/special purpose forces, terrorists or insurgents). • Evaluate how remaining threat forces are still able to operate. • Determine if there are any areas still sympathetic to threat forces. • Describe how remaining threat forces are able to sustain operations. • Identify the leadership that remaining forces are looking to for guidance. • Determine the security of hazardous materials and facilities that can be used in the production of weapons of mass destruction.
Transition	• Identify the recipient of the transfer of authority. • Determine if the organization is able to enforce and achieve its intent. • Determine if the organization has enough manpower to meet its intent. • Identify what resources the organization requires to meet its goals. • Determine if the organization can use all information networks to reach the populace effectively.

Consolidate Gains Through Stability Operations

7-23. A *stability operation* is an operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADP 3-0). In stability operations, success is measured differently from offensive and defensive operations. Time may be the ultimate arbiter of success: time to bring safety and security to an embattled populace; time to provide for the essential, immediate humanitarian needs of the people; time to restore basic public order and a semblance of normalcy to life; and time to rebuild the institutions of government and market economy that provide the foundations for enduring peace and stability. (See ADP 3-07 for information on stability operations.)

7-24. The main difference between stability operations and other decisive action is the focus and degree level of analysis required for the civil aspects of the environment. Unlike major combat—an environment dominated by offensive and defensive operations directed against an enemy force—stability operations encompass various military missions, tasks, and activities that are not enemy-centric.

7-25. Constant awareness and shared understanding of civil considerations (ASCOPE) about the environment are crucial to long-term operational success in stability operations. Analysts should classify civil considerations into logical groups (tribal, political, religious, ethnic, and governmental). Intelligence analysis during operations that focus on the civil population requires a different mindset and different techniques than an effort that focuses on defeating an adversary militarily.

7-26. Some situations (particularly crisis-response operations) may require analysts to focus primarily on the effects of terrain and weather, as in the case of natural disasters, including potential human-caused catastrophes resulting from natural disasters. Disasters (such as windstorms, hurricanes, typhoons, floods, tsunamis, wildfires, landslides, avalanches, earthquakes, and volcanic eruptions) may occur without warning. Human-caused catastrophes (such as civil conflict, acts of terrorism, sabotage, or industrial accidents) may develop over time. The speed at which an event occurs dictates how analysts will conduct their assessments and with whom they will share their intelligence.

This page intentionally left blank.

Chapter 8
Analysis and Large-Scale Ground Combat Operations

OVERVIEW

8-1. In future operations, intelligence analysis considerations should include a combination of factors (or elements) that analysts must understand to support the commander. Multi-domain operation considerations differ by echelon. These considerations have their greatest impact on Army operations during large-scale ground combat. Despite the natural tendency to focus on the land domain during large-scale ground combat, analysts must look across the OE or AO to determine how the air, land, and maritime domains affect Army efforts and how those effects may open windows of opportunity for Army forces to create favorable conditions and positions of relative advantages for U.S. and coalition forces.

8-2. Situation development enables commanders to see and understand the battlefield in enough time and detail to make sound tactical decisions. Situation development assists in locating and identifying threat forces; determining threat forces' strength, capabilities, and significant activities; and predicting threat COAs. Situation development assists commanders in effectively employing available combat resources where and when decisive battles will be fought, preventing commanders from being surprised.

8-3. Commanders and staffs require timely, accurate, relevant, and predictive intelligence to successfully execute offensive and defensive operations in large-scale ground combat operations. The challenges of fighting for intelligence during large-scale ground operations emphasize a close interaction between the commander and staff, since the entire staff supports unit planning and preparation to achieve situational understanding against a peer threat. Since each echelon has a different situational understanding of the overarching intelligence picture, the analytical focus differs from one echelon to another. For example, updated intelligence analysis at the corps level could influence a commander's decisions at the BCT level because corps-level requirements differ from BCT-level requirements. Therefore, it is important for intelligence analysts to understand the missions, key tasks, and end state of higher and subordinate forces to ensure they maintain a holistic understanding of the OE. Although each echelon has a different analytical focus, the techniques, tools, and methods employed to conduct analysis do not change. (See FM 2-0 for more information on fighting for intelligence and all-source intelligence capabilities at each echelon.)

TACTICAL TO OPERATIONAL SITUATION: AN ENEMY ATTACK

8-4. The following three examples walk an intelligence analyst from the tactical to operational situation of an enemy attack, demonstrating the necessity for analysts to possess a broad understanding of the OE and the friendly forces' scheme of maneuver. The examples illustrate the situation a unit might encounter along the forward edge of the battle area (FEBA) with friendly and enemy forces poised to engage in large-scale ground combat. In this situation, many friendly and enemy units have deployed to gain a tactical advantage at the onset of combat.

TACTICAL-LEVEL EXAMPLE (BRIGADE COMBAT TEAM)

8-5. The BCT has already completed the MDMP and issued orders, and intelligence analysts have been providing periodic reports and products to support situation development as the situation unfolds. The battle noncommissioned officer receives a spot report that elements of a motorized rifle regiment have crossed the border/FEBA. (See figure 8-1 on page 8-2.) The commander wants to confirm the enemy's intent to cross the border before engaging the enemy.

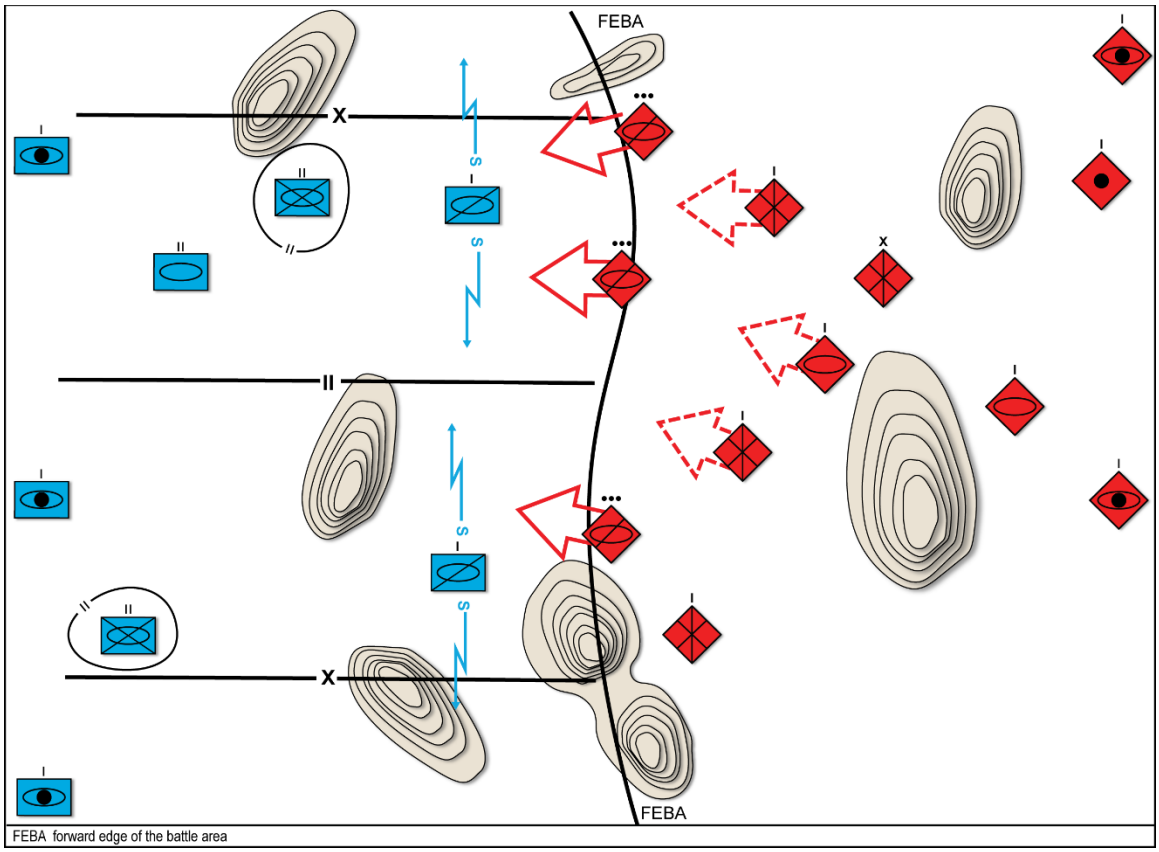


Figure 8-1. Brigade combat team situation example

8-6. Additional information received confirms reporting from forward reconnaissance elements. Intelligence reporting from single-source intelligence analysis indicates movement west of multiple company-sized tank and motorized rifle elements. The intelligence also reveals possible supporting artillery elements. (See table 8-1.)

Table 8-1. Intelligence analysis (brigade combat team) example

Brigade combat team intelligence analysis example			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
• General items of relevancy to screen in a tactical sense: ▪ Indicators of threat activities for the next 24 to 48 hours. ▪ Changes in the operational environment that will affect operations. ▪ Enemy maneuvers within the area of operations. • Analysts initiate analysis based on a spot report that meets these criteria.	Analysts should form their initial hypothesis based on information assessed to be relevant in the *screen* phase.	Analysts should compare their new hypothesis to current intelligence holdings.	Analysts make their final assessment and produce a likely course of action (COA) for the commander to make a decision.

Table 8-1. Intelligence analysis (brigade combat team) example (*continued*)

Brigade combat team intelligence analysis example (continued)			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
Based on the spot report, the commander provides the following specific requirement, which the intelligence section needs to address: Confirm the enemy's intent to cross the border.	Based on multiple reports indicating enemy forces maneuvering to the west, analysts must assess: • How this movement will support the enemy commander's intent and end state? • How much will the enemy commander commit to this movement? • Will the amount of force committed by the enemy commander drive friendly units to a decision point?	During step 3 of the intelligence preparation of the battlefield (IPB) process, step 3, analysts will have described the enemy to have the minimum products: • Written enemy description (Annex B [Intelligence]). • Situational order of battle. • Threat graphic template. • Threat capabilities matrix.	• Intelligence analysis assessment: At a minimum, battalion plus of motorized rifle supported with tank elements are crossing the border, and an enemy surprise attack by follow-on elements is likely. • Based on the assessment, the friendly commander confirms the enemy's intent to cross the border and provides guidance to assume attack positions to block the enemy advance.
Analysts screen the following based on the specific requirement and tactical guidelines: • Reporting from forward reconnaissance corroborates spot report. • Reporting from single-source analysis indicates movement, including the possible movement of additional elements.	Analysts may use the following analytic techniques: • Chronologies (*Basic*) to understand the enemy's intent and end state by examining historic operations the enemy has conducted. • Key assumptions check (*Diagnostic*) on the enemy's likely intent to enlighten how much the enemy will commit to the movement. • Analysis of competing hypothesis (*Diagnostic*) to project if the friendly commander will be faced with a decision point.	• Based on the enemy description and threat capabilities matrix: Analysts refine enemy movement to add the size of unit (as directed by the commander, but at least two levels down) and type (motorized rifle with tanks). • Based on the situational order of battle: Analysts assess the enemy commander will likely commit follow-on elements. • With a refined size and type of enemy units moving to the west, combined with the projected amount of force committed, the friendly commander must make a decision based on the enemy COA. • Analysts may use the team A/ team B (*Advanced*) analytic technique to war-game their assessed enemy COA, ensuring all variables are considered and their COA is viable. • Analysts may use the red hat/ analysis (*Advanced*) analytic technique in conjunction with their threat capabilities matrix to ensure the enemy intent in their initial hypothesis agrees with current intelligence holdings.	The intelligence analysis process is continuous, and analysts should now consider: • What information can be exploited by combat assessment from the block? • What single-source reporting generates post-mission? • Does the threat model derived in IPB, step 3, require changes? • What should be adjusted for information collection to fully answer the requirement?

TACTICAL-LEVEL EXAMPLE (DIVISION)

8-8. Figure 8-2 illustrates a similar enemy attack but with U.S. division graphics. The enemy's most likely COA is an attack orientated on at least two ground avenues of approach through canalizing terrain. At least one tank division with four brigade elements and two self-propelled artillery battalions will attack as the main effort. In addition to the tank and motorized rifle elements crossing the FEBA, there are elements of at least one tank brigade with self-propelled artillery advancing west.

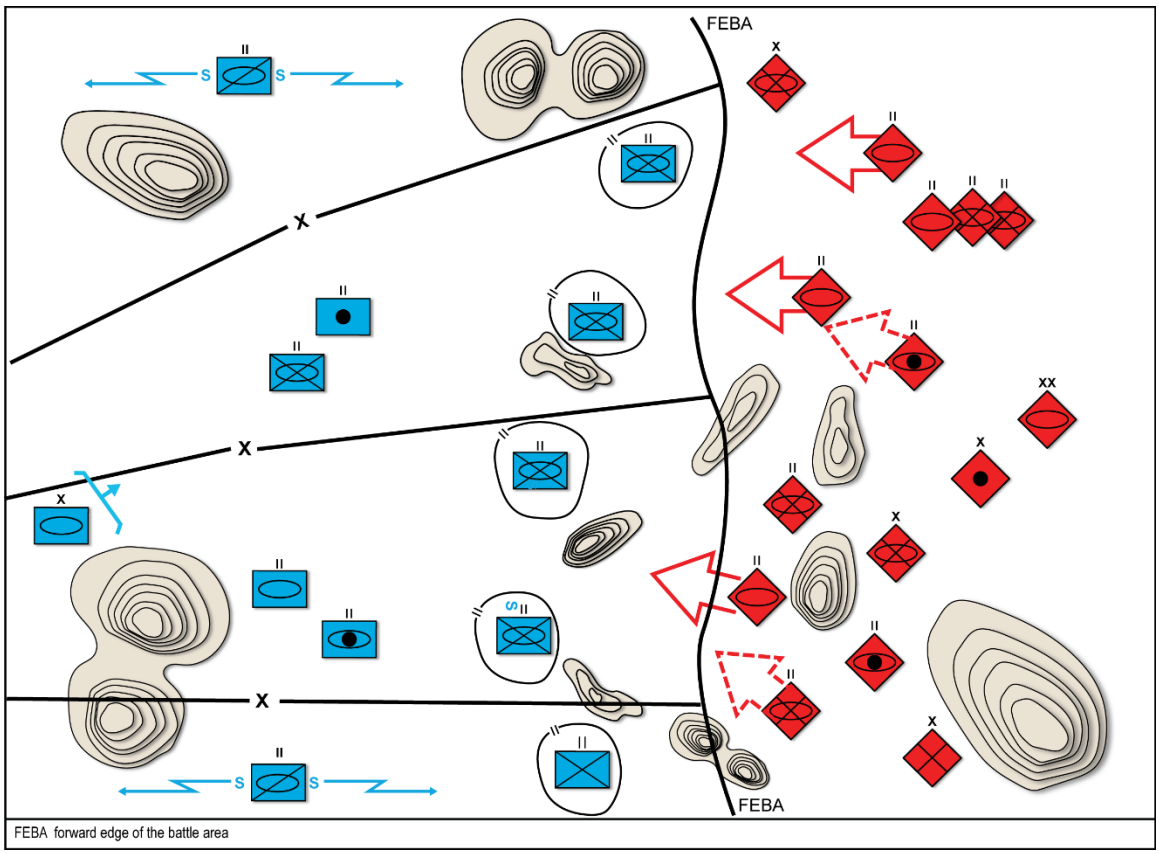


Figure 8-2. Division situation example

8-9. Division analysts assess that elements of the tank division are advancing west to engage friendly forces. The combat information and available intelligence seem to initially support an enemy division frontal attack with infantry and motorized rifle brigades penetrating the FEBA to destroy friendly defenses and allow follow-on units to secure primary and secondary objectives. (See table 8-2.)

Table 8-2. Intelligence analysis (division) example

Division intelligence analysis example			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
• General items of relevancy to screen in an operational sense: ▪ Indicators of enemy activities for the next 48 to 168 hours. ▪ Changes in the operational environment that will affect subordinate commands. ▪ Enemy maneuvers that will affect subordinate unit's areas of responsibility (AORs). • Analysts initiate analysis based on reports of enemy orientation on two avenues of approach through canalizing terrain that meets these criteria.	Analysts should form their initial hypothesis based on information assessed to be relevant in the *screen* phase.	Analysts should compare their new hypothesis to current intelligence holdings.	Analysts make their final assessment and produce a likely course of action (COA) for the commander to make a decision.
Based on the orientation, the commander provides the following specific requirement, which the intelligence section needs to address: Project the enemy's future operations for the next 96 to168 hours and how they will affect subordinate units.	Based on the reports indicating enemy forces in attack position, analysts must assess: • What is the enemy commander's end state for this attack? • What resources would be a priority for the enemy commander to commit these forces to an attack? • Will the enemy attack force subordinate units to a decision point?	During intelligence preparation of the battlefield, analysts will have described the enemy and operational environment to have the minimum products: • Modified combined obstacle overlay (MCOO). • Threat model. • Situational order of battle.	• Intelligence analysis assessment: Two motorized rifle brigades are advancing west to engage friendly forces. The enemy is likely to conduct a division frontal attack with infantry and motorized rifle brigades in order to penetrate the forward edge of the battle area to destroy friendly defenses and allow follow-on units to secure primary or secondary objectives. • Based on the assessment, the friendly commander may plan for the enemy's future operations and dispatch orders to subordinate units.
Analysts screen the following based on the specific requirement and operational guidelines: • At least one tank division with four brigade elements in attack position. • Two self-propelled artillery battalions in attack position. • At least one artillery brigade advancing west.	Analysts may use the following analytic techniques: • Quality of information check (*Diagnostic*) to refine and validate the projected orientation and power of enemy forces in the area of operations. • Weighted ranking (*Diagnostic*) to prioritize enemy capabilities to identify critical actions that could greatly affect friendly forces.	• Based on the MCOO: Canalizing terrain will force the armored brigades to engage friendly forces east. • Based on the threat model: The enemy is likely to conduct a divisional attack to cross the border and employ follow-on units to secure the key terrain. • With a refined intent to seize key terrain and a defined method verified by reporting and intelligence analysis, the friendly commander can maneuver subordinate units into a block. • Analysts may use the high impact/low probability (*Advanced*) analytic technique to identify, for subordinate units, indicators of pending offensive operations within their AORs. • Analysts may use the functional analysis (*Advanced*) analytic technique to verify the center of gravity proposed in the initial hypothesis.	The intelligence analysis process is continuous, and analysts should now consider: • What information can be exploited by subordinate units from the block? • How will the enemy benefit from the seizure of the key terrain? • Is there favorable terrain to friendly forces that could mitigate the canalizing terrain in future operations?

Table 8-2. Intelligence analysis (division) example (*continued*)

Division intelligence analysis example (continued)			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
	Based on the initial hypothesis, analysts should consider: • What domains can friendly forces leverage to gain an advantage on the enemy? • Are there any windows of opportunity across the domains? • What is the best way to allocate assets based on the windows of opportunity?	• Canalizing terrain can create areas of interest that can be targeted or collected on by air assets. • With an anticipated block, analysts should placement of obstacles for enemy forces. • Are there any elements within the situational order of battle that can apply cyberspace electromagnetic activities (CEMA)? • What effect will CEMA have on navigation and communications assets?	The analyst must disseminate the corresponding products with the applicable domain operator: • Share named and target area of interest overlays with joint force assets. • Share MCOOs and additional terrain analysis with engineer units to support subordinate commands. • Provide electronic warfare and signal units with enemy CEMA capabilities to mitigate system interruptions.

TACTICAL/OPERATIONAL-LEVEL EXAMPLE (CORPS)

8-10. Figure 8-3 provides information about the OE that assists in understanding, at a macro level, the enemy. Understanding that the enemy is conducting a large-scale attack contextualizes the situation for the tactical/operational commander and influences critical decisions. Knowing the enemy is conducting a general attack to likely seize the city of Sawburg influences the tactical and operational commanders' employment of forces, acceptance of risk, and determination to hold key terrain.

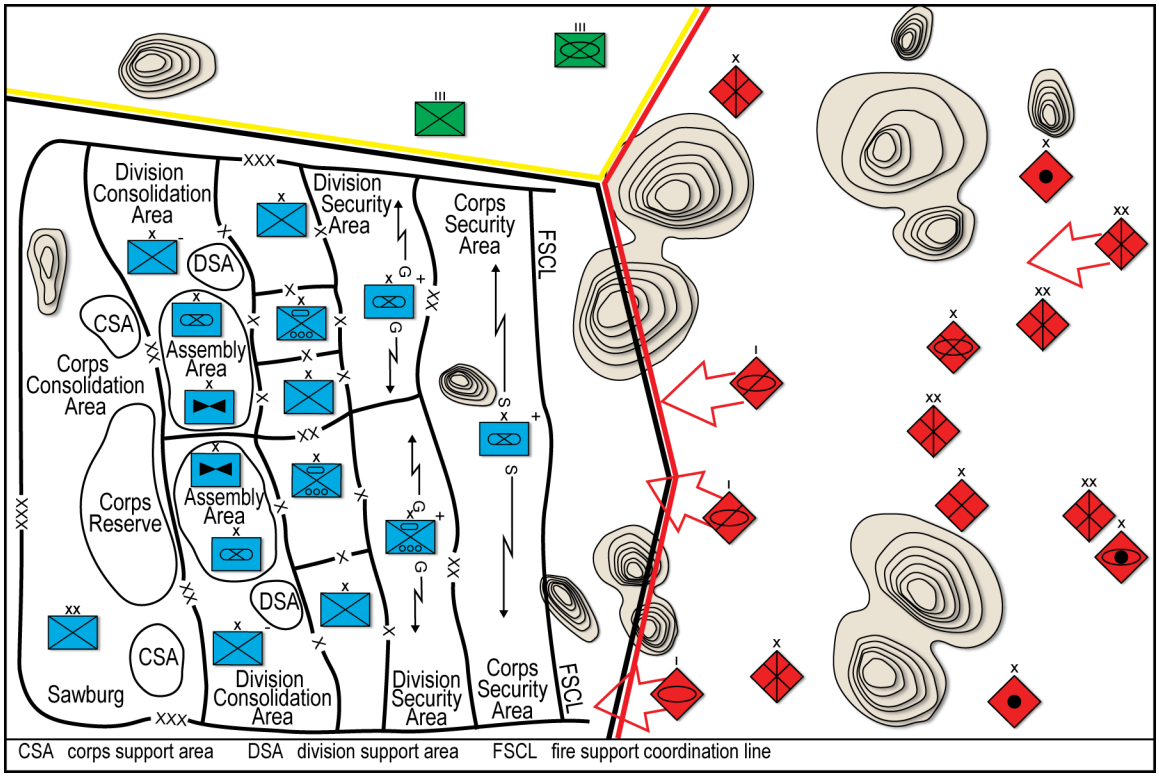


Figure 8-3. Tactical/Operational (corps) situation example

8-11. Based on reporting, the enemy has additional forces in the area, including a second tank division three to four days away in tactical-march formations. The friendly force commander is forced to commit ready forces to stop the enemy force advance since reserve elements are not available. (See table 8-3.)

Table 8-3. Intelligence analysis (tactical/operational [corps]) example

Corps intelligence analysis example			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
• Based on the reports indicating enemy forces in attack position, analysts need to assess: ▪ Indicators of threat activities beyond 168 hours. ▪ Changes in the operational environment (OE) that will affect subordinate commands. ▪ Indicators that help shape and prevent potential threat action. • Analysts initiate analysis based on understanding why the enemy is attacking.	Analysts should form their initial hypothesis based on information assessed to be relevant in the *screen* phase.	Analysts should compare their new hypothesis to current intelligence holdings.	Analysts make their final assessment and produce a likely course of action (COA) for the commander to make a decision.
Based on this understanding, the commander provides the following specific requirement, which the intelligence section needs to address: Project the enemy's future operations for the next 96 to168 hours and establish the operational acceptance of risk.	Based on understanding the OE, analysts must assess: • What is the enemy commander's end state for seizing the key terrain? • How will the enemy commander use the key terrain if it is seized? • How much time will it take the enemy commander to maneuver forces to the border?	During mission analysis, analysts will have described the enemy and OE to have the minimum products: • Threat model. • Annex B (Intelligence) (to describe the enemy's likely intentions and end state). • Enemy COAs.	• Intelligence analysis assessment: The enemy conducts a general attack to likely seize Sawburg to influence the tactical and operational commanders' employment of forces, acceptance of risk, and determination to hold key terrain. • Based on the assessment, the friendly commander understands the enemy is attempting to push friendly units to a decision point and must plan to mitigate those operations.
Analysts screen the following based on the specific requirement and operational guidelines: • Location of key terrain is Sawburg. • Enemy composition and disposition in vicinity of friendly units.	Analysts may use the following analytic techniques: • Event trees (*Basic*) to develop initial scenarios of potential enemy actions. • Indicators/Signposts of change (*Diagnostic*) to establish a list of indicators to specific methods of offense being employed by the enemy. • Link analysis (*Basic*) to examine the relationship of resources, organizations, and other entities within the area of operations.	• Based on the threat model: Analysts assess the enemy commander to use armored divisions to conduct an attack. • Based on Annex B (Intelligence): It is likely the enemy will want to control Sawburg for resources. • Based on general enemy COAs: There is likely another tank division 3 to 4 days away from the projected battle zone. • Analysts could use the "what if?" (*Advanced*) analytic technique to generate the multiple outcomes of the operation, applying analytical rigor to their initial hypothesis. • Analysts could use the outside-in thinking (*Advanced*) analytic technique from other members or the staff or organization to gain insight on how favorable the key terrain would be for the enemy commander.	The intelligence analysis process is continuous, and analysts should now consider: • How will adjacent country (green) react to operations? • Are there any maneuvers that can mitigate the offensive enemy operation? • Can information collection refine enemy intentions?

Table 8-3. Intelligence analysis (tactical/operational [corps]) example (*continued*)

Corps intelligence analysis example			
Multi-domain considerations for intelligence analysis			
Screen	***Analyze***	***Integrate***	***Produce***
	Based on the initial hypothesis, analysts should consider: • What domains can friendly forces leverage to gain an advantage over the enemy? • What joint assets should be allocated to subordinate commands?	• Can the information environment develop indicators for enemy intentions? • Has the enemy leveraged information operations on Sawburg? • Reconnaissance in depth may have to be conducted by air assets on tank divisions 3 to 4 days away. • Are cyberspace electromagnetic activities (CEMA) vulnerable within the enemy's navigation and communications systems?	• Analysts must disseminate the corresponding products with the applicable domain operator: ▪ Provide named areas of interest (NAIs) for information collection to gain insight to Sawburg and their disposition to friendly and enemy forces. ▪ Share NAI and target area of interest overlays with joint force assets for reconnaissance in depth. • Analysts should synchronize with the CEMA cell to develop a better understanding of enemy intentions. • Analysts should use CEMA capabilities in conjunction with nonlethal targeting efforts.

Chapter 9

Managing Long-Term Analytical Assessments

OVERVIEW

9-1. Any echelon can conduct long-term intelligence analysis, which is simply analysis over a longer period of time (several months or longer). There are many forms of long-term analysis, such as long-term analytical assessments. Formal (authoritative or exploratory) long-term analytical assessments are usually associated with operational- and strategic-level intelligence units and organizations because these assessments are resource-intensive. Intelligence analysts at the tactical level can use some of the steps and substeps discussed in this chapter in order to improve their analysis, but they rarely apply all of the steps of the process.

9-2. Managing long-term analytical assessments, also referred to as analytic design in this chapter, ensures the analytical effort results in the best possible assessment. Analytic design ensures the analytical effort is properly focused, carefully planned and executed, and that the analytical results are effectively communicated to the requestor. The Defense Intelligence Agency published a helpful document, *Analytic Design: Analytic Tradecraft Guidance from the DI Research Director*, which served as the basis for this chapter.

9-3. Long-term analytical assessments are produced using a deliberate and specific execution of the intelligence analysis process over a longer period of time that closely complies with the Intelligence Community Analytic Standards (to include the analytic tradecraft standards) established in ICD 203. This form of analysis includes the careful management of the overall effort, dedicating significant resources to the effort (for example, analysis is conducted by an analytic team), executing various iterations of analysis, and applying advanced structured analytic techniques within the effort.

Note. Intelligence personnel should not use this chapter to develop criteria and standards for tactical-level intelligence analysis. This chapter covers the basics of analytic design but does not cover all the information needed to develop formal long-term analytical assessments. Specifically, some of the analytic techniques and the use of models and automated simulations are not discussed in this publication.

THE BASICS OF ANALYTIC DESIGN

9-4. Managing long-term analytical assessments is accomplished by performing seven analytic design steps, as shown in figure 9-1 on page 9-2:

- **Step 1:** Frame the question/issue.
- **Step 2:** Review and assess knowledge.
- **Step 3:** Review resources.
- **Step 4:** Select the analytic approach/methodology and plan project.
- **Step 5:** Develop knowledge.
- **Step 6:** Perform analysis.
- **Step 7:** Evaluate analysis.

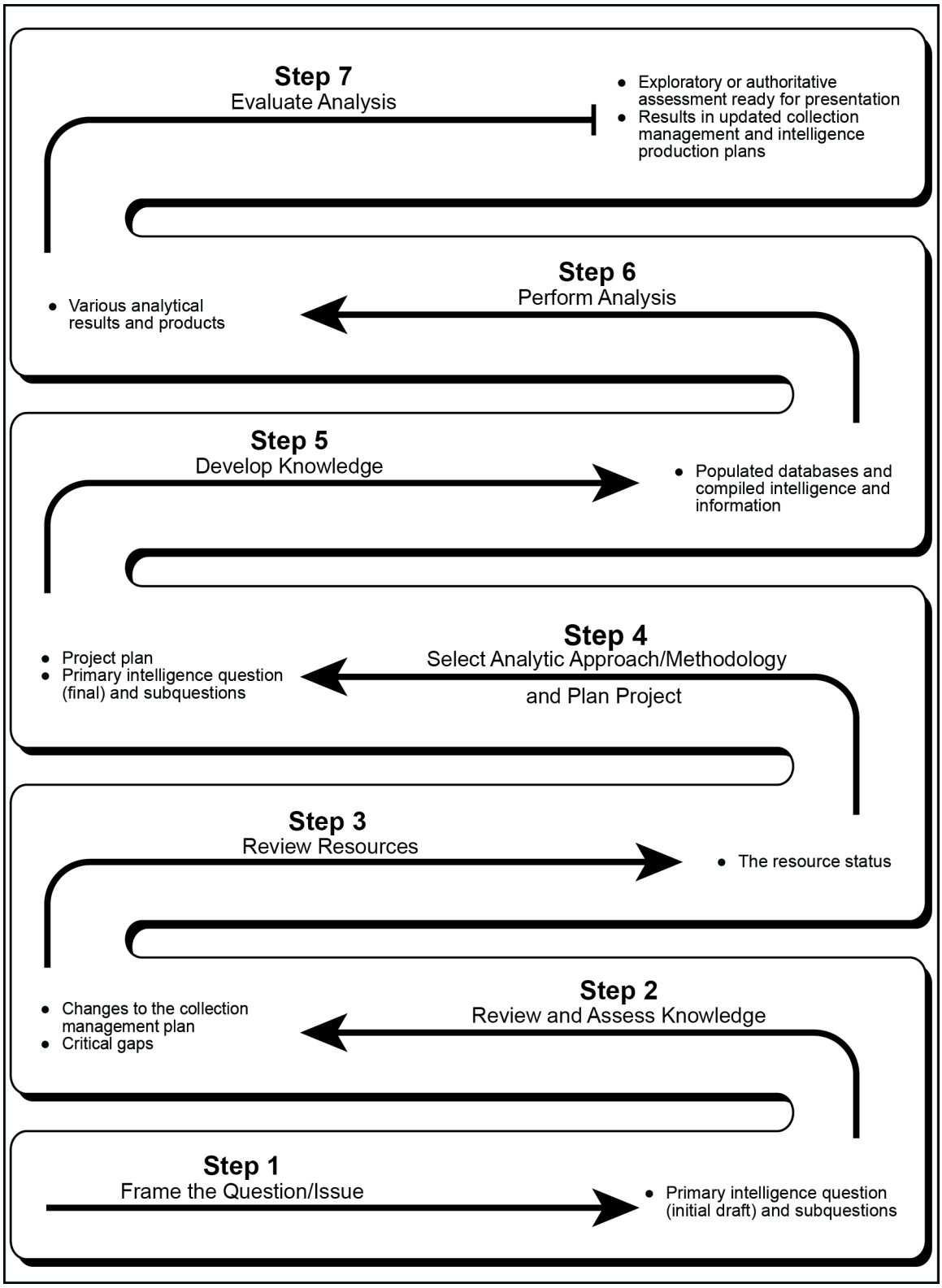


Figure 9-1. Analytic design steps

FRAME THE QUESTION/ISSUE

9-5. Properly framing the question greatly increases the chance of successful long-term analysis. The analytic team starts with understanding the requestor's requirement by identifying relevant topics and issues that break down into a primary question that can be analyzed. Framing the question includes refining and scoping the question to carefully capture the requestor's expectations, mitigate bias, craft an objective analytic question, and develop subquestions. This step results in an initial draft of the primary intelligence question and is followed by reviewing and assessing existing knowledge. (See figure 9-2.)

Note. Do not confuse the frame the question/issue step with the "frame" activities associated with the Army design methodology. (For information on the Army design methodology, see ATP 5-0.1)

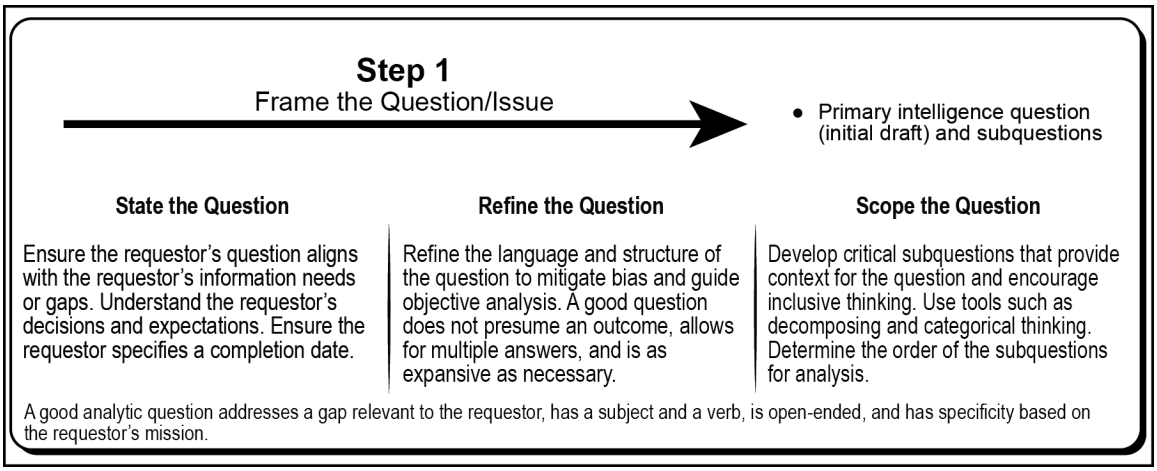


Figure 9-2. Frame the question/issue

REVIEW AND ASSESS KNOWLEDGE

9-6. Reviewing and assessing knowledge involves an overlap of the analytical effort with collection management. Step 2 includes reviewing available information and intelligence, the collection management plan, and results of on-going intelligence collection, as well as identifying information gaps. (See figure 9-3.)

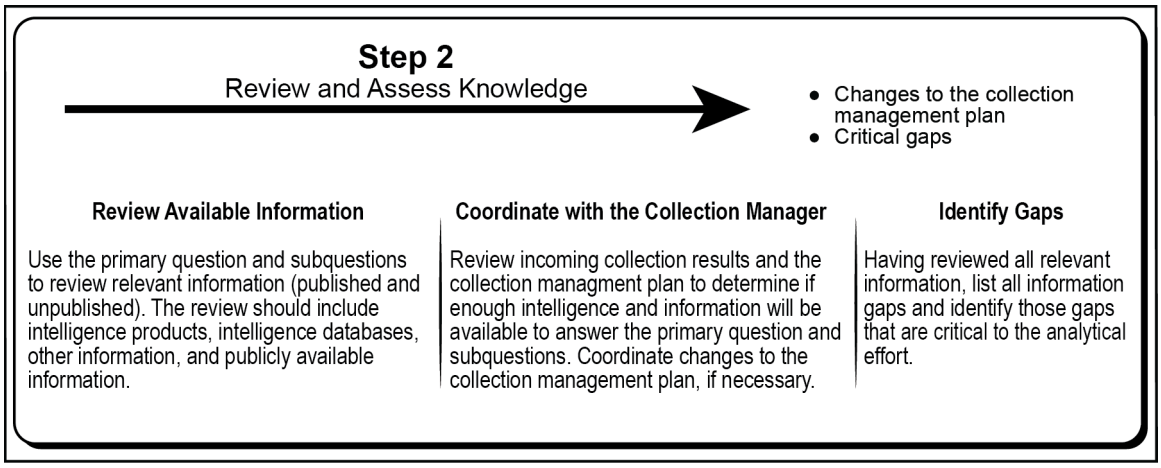


Figure 9-3. Review and assess knowledge

REVIEW RESOURCES

9-7. After understanding what knowledge is available and identifying information gaps, the next step is reviewing available resources, such as tools, personnel, and time. (See figure 9-4.)

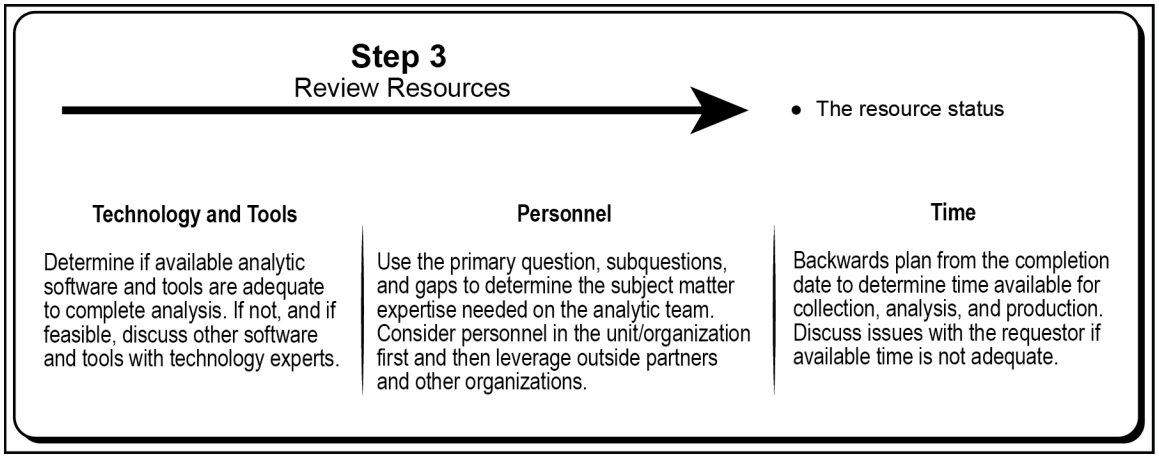


Figure 9-4. Review resources

SELECT THE ANALYTIC APPROACH/METHODOLOGY AND PLAN PROJECT

9-8. Using the results of steps 1 through 3, the analytic team finalizes the primary intelligence question and subquestions, selects the analytic approach/methodology, and develops a project plan. The analytic approach/methodology includes the specific analytic techniques, who will perform each technique, and the sequence of those techniques to ensure analytic insight and mitigate bias. (See figure 9-5.)

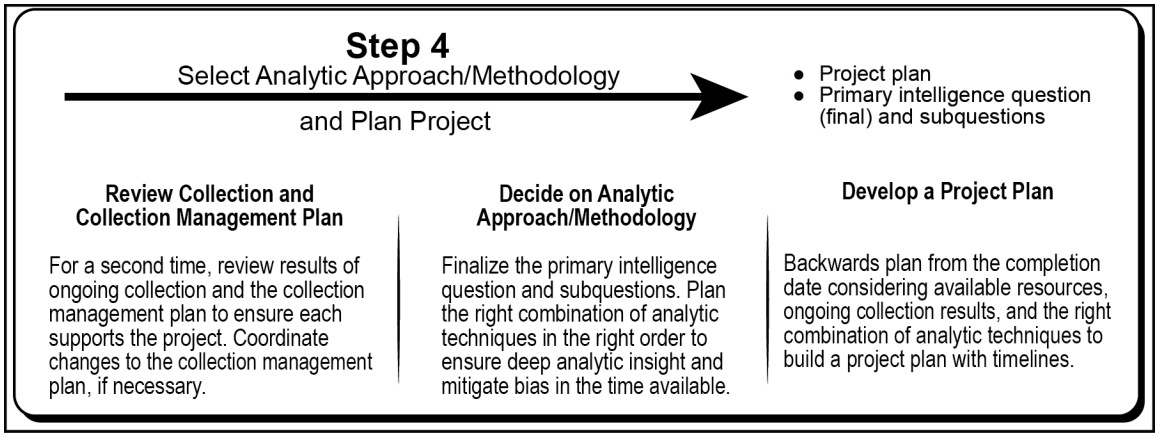


Figure 9-5. Select the analytic approach/methodology and plan project

DEVELOP KNOWLEDGE

9-9. Developing knowledge is the last step before performing analysis. Although discussed as a separate step in the process, developing knowledge occurs continually throughout the process. The analytic team gathers all relevant intelligence and information through ongoing collection, intelligence reach, and internal research. (See figure 9-6.)

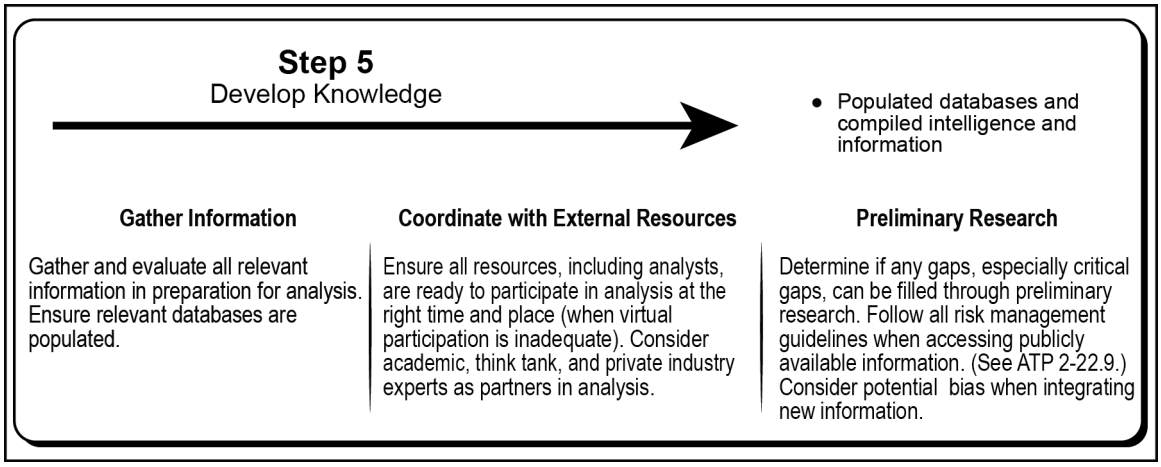


Figure 9-6. Develop knowledge

PERFORM ANALYSIS

9-10. Steps 1 through 5 set the stage for the deliberate execution of analytic techniques, to include adjusting the project plan, if necessary, and assessing the analytical results using the context that was developed while framing the question/issue. (See figure 9-7.)

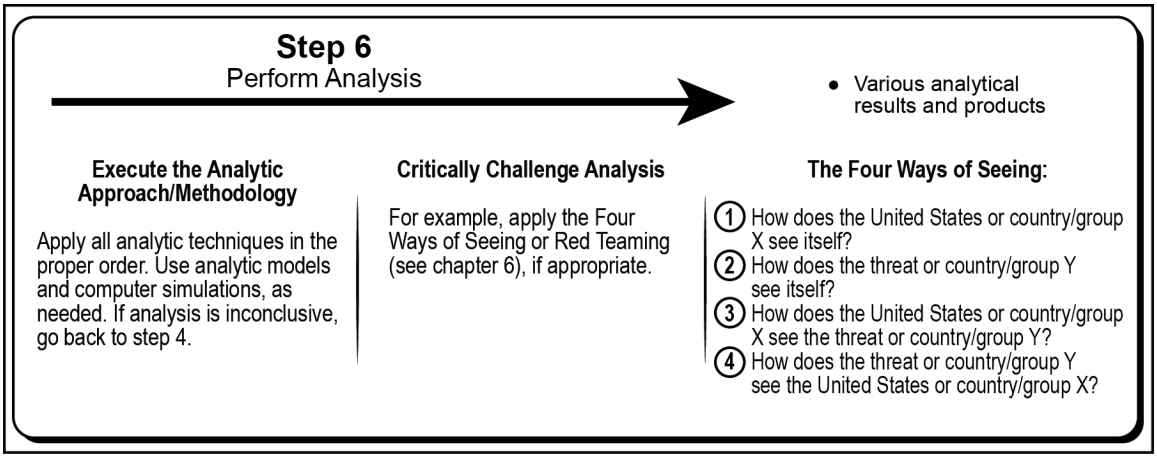


Figure 9-7. Perform analysis

EVALUATE ANALYSIS

9-11. Evaluating analysis, the final step of the process, results in the final analytical results and associated information necessary to make a presentation to the requestor. Evaluating analysis includes assessing the analytical results and the impact of analytic gaps and unconfirmed assumptions, performing analysis of alternatives, and assigning a confidence level to the analytic answer. (See figure 9-8.)

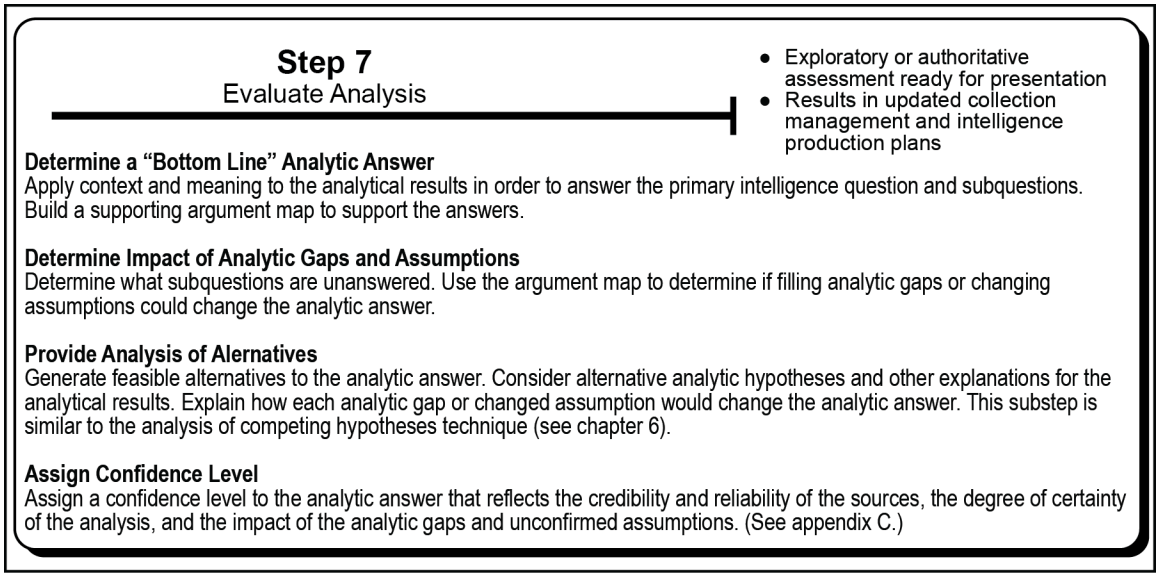


Figure 9-8. Evaluate analysis

COLLABORATION DURING ANALYTIC DESIGN

9-12. Collaboration is critical to long-term analytical assessments and occurs between different stakeholders across the intelligence community. This collaboration ensures a diversity of perspective and depth in expertise that is impossible through any other means. Four specific areas in which collaboration is invaluable are—

- **Bias mitigation:** Analytic teams with diverse backgrounds and different perspectives can effectively identify and check assumptions, interpret new information, and determine the quality of various types of information.
- **Framing/Knowledge review:** Analytic teams can engage early in the process to build context, craft analytic questions, share information sources, and develop analytical issues.
- **Methodology building:** Analytic teams assess the credibility of the analytic approach and clarity of the argument through various means, including peer reviews.
- **Perform analysis:** Analytic teams can perform various analytic techniques, identify hypotheses, and analyze alternatives as a group to improve the quality of the analytical effort.

TRANSITIONING FROM THE ANALYTIC DESIGN PROCESS TO PRESENTING THE RESULTS

9-13. Managing long-term analytical assessments includes not only presenting an analytic answer but also a confidence level to the answer and alternative hypotheses or explanations for gaps and uncertainty. During evaluate analysis, the last step of the process, the analytic team decides whether the question requires more analysis, and therefore, whether the assessment is exploratory or authoritative and ready to present to the requestor. If the results are ready for presentation, the analytic team deliberately prepares to present those results. Transitioning from long-term analysis to presenting the analytic answer includes stepping back from that analysis, reviewing the assessment, and clarifying the relevance of the analytical results. Then the analytic team determines—

- **What is the message:** The message characterizes whether the assessment is authoritative or exploratory and includes the "bottom line" of the assessment. Additionally, the assessment includes any shifts in analysis that occurred over time, any impacts on the requestor (decisions and future focus areas), the confidence level, alternative hypotheses, and indicators.
- **What is the analytical argument:** The analytic team develops an outline for logically progressing through the analytical assessment. An argument map is a useful tool to ensure a logical analytical flow during the presentation and to ensure the message is easily understood. The team may use basic interrogatives (*who, what, when, where, why,* and *how*) or a similar tool to capture the critical elements of the message to present to the requestor.
- **What are critical gaps and assumptions:** Gaps and assumptions identified during the evaluate analysis step become limitations to the certainty of the analytical assessment, and, in some cases, drive future analytical efforts. The analytic team may insert gaps and assumptions within the message and clearly discuss the level of impact on the assessment (for example, in the source summary statement or in the "bottom line" statement).
- **What reasonable analytical alternatives remain:** For authoritative assessments, answering the questions *"what if I am wrong"* and *"what could change my assessment"* provides analysis of alternatives that should be included in the assessment to explain what remains uncertain.
- **What product or products should be presented:** Determine the best format for the presentation that facilitates the discussion of the argument. If it is exploratory analysis, the format should allow the analytic team to effectively describe the new understanding of the topic and its relevance to the requestor. The team should consider the following when choosing the format: requestor preference, specific tasking/requirement, complexity of the argument, urgency/time constraints, and potential interest of others.

CROSSWALKING ANALYTIC DESIGN WITH TACTICAL INTELLIGENCE ANALYSIS

9-14. Tactical intelligence analysis and analytic design have similarities but also differ in a number of ways. Tactical operations are often chaotic and time-constrained, and therefore, driven by specific commander-centric requirements (for example, PIRs and targeting requirements). The commander and staff plan and control operations by employing several standard Army planning methodologies, including but not limited to the Army design methodology, the MDMP, and Army problem solving. (See ADP 5-0 for a discussion of these methodologies.) Large portions of steps 1 through 5 of analytic design equate to the Army's time-tested planning processes, namely the Army design methodology, the MDMP (including IPB), and Army problem solving. Parts of steps 1 through 5 also equate to generate intelligence knowledge, which is a continuous task that develops general intelligence knowledge for subsequent intelligence analysis (see paragraphs 3-6 and 3-7).

9-15. Many of the doctrinal concepts presented in this and other publications are consistent with the analytic design steps discussed in this chapter. Table 9-1 provides a crosswalk of the analytic design steps to various Army doctrinal concepts and their associated references.

Table 9-1. Analytic design to tactical intelligence analysis crosswalk

Analytic design step	*Doctrinal concepts and references*
Step 1: Frame the question/ issue	• ATP 2-33.4: ▪ Develop commander's PIRs, par. 1-30. ▪ Frame the analytic problem with PIRs and other requirements, par. 2-5 and figure 2-1. ▪ Commander's visualization of the OE and threat, pars. 3-8 and 3-9. • ADP 5-0: Identify requirements to support decision points, pars. 1-40–1-43. • ATP 2-01: Refine PIRs into SIRs and indicators, par. 2-9. • ATP 5-0.1: Frame OEs, chapter 3.
Step 2: Review and assess knowledge	• ATP 2-33.4: ▪ Include information and intelligence from all available sources, par. 1-44. ▪ Screen collected information, pars. 2-7 and 2-8. ▪ Review information previously discarded as nonessential, par. 2-21. • ATP 2-01: Plan collection management, par. 1-4. • ATP 5-0.1: Share knowledge and build consensus, par. 1-32. • ATP 2-01.3: Identify intelligence gaps in knowledge, par. 1-16.

Table 9-1. Analytic design to tactical intelligence analysis crosswalk (*continued*)

Analytic design step	*Doctrinal concepts and references*
Step 3: Review resources	• ATP 2-33.4: ▪ Identify planning and execution deadlines, par. 1-23. ▪ Collaborate with available analytic assets, pars. 1-25 and 1-26. ▪ Identify all-source intelligence architecture requirements, pars. 1-32 and 1-33. ▪ Identify availability of time, tools, services, and other sources, pars. 2-8 and 7-2. • FM 2-0: ▪ Leverage intelligence, par. 1-19. ▪ Determine intelligence reach relationships, par. 1-25. • FM 3-55: Conduct information collection with organic and nonorganic resources, par. 1-28. • ATP 2-01: Evaluate resources, par. 4-2. • MI Pub 2-01.2: ▪ Plan the intelligence architecture, chapter 1. ▪ Prepare the intelligence architecture, chapter 2.
Step 4: Select analytic approach/methodology and plan project	• ATP 2-33.4: ▪ Determine optimal all-source structure to address the question, par. 1-34. ▪ Chapter 4, *Analytic Techniques.* ▪ Chapter 5, *Basic and Diagnostic Structured Analytic Techniques*. ▪ Chapter 6, *Advanced Structured Analytic Techniques.* • ATP 2-01: Plan collection management, par. 3-2. • ATP 5-0.1: Plan to facilitate decision making, pars. 1-7–1-10.
Step 5: Develop knowledge	• ATP 2-33.4: ▪ Think critically, par. 1-24. ▪ Screen collected information, pars. 2-7 and 2-8. ▪ Integrate new information with prior holdings, pars. 2-16–2-18. ▪ Review information previously discarded as nonessential, par. 2-21. ▪ Generate intelligence knowledge, pars. 3-6 and 3-7. • ADP 2-0: Generate knowledge through the intelligence process, par. 3-4. • FM 2-0: Access information through intelligence reach, pars. 1-25–1-33. • FM 3-55: Gather data to support primary information collection tasks and operations, par. 1-30.
Step 6: Perform analysis	• ATP 2-33.4: ▪ Conduct intelligence analysis, pars. 1-15 and 1-16. ▪ Reach determination based on facts and assumptions, par. 1-24. ▪ Chapter 2, *The Intelligence Analysis Process.* ▪ Chapter 4, *Analytic Techniques.* ▪ Chapter 5, *Basic Diagnostic Structured Analytic Techniques.* ▪ Chapter 6, *Advanced Structured Analytic Techniques.* ▪ Appendix B, *Cognitive Considerations for Intelligence Analysts.* (This appendix describes thinking abilities, critical and creative thinking, and avoiding analytical pitfalls.)
Step 7: Evaluate analysis	• ATP 2-33.4: ▪ Answer the *'so what'* from the commander's perspective, par. 1-21. ▪ Determine relevancy before producing assessments, par. 1-27. ▪ Appendix B, *Cognitive Considerations for Intelligence Analysts.* (This appendix describes thinking abilities, critical and creative thinking, and avoiding analytical pitfalls.) ▪ Appendix C, *Analytic Standards and Analysis Validation.* (This appendix discusses the analytic standards that govern intelligence analysis.)

Doctrinal references:	**Legend:**	
ADP 2-0, *Intelligence*	MI Pub	military intelligence publication
ADP 5-0, *The Operations Process*	OE	operational environment
ATP 2-01.3, *Intelligence Preparation of the Battlefield*	par./pars.	paragraph/paragraphs
ATP 2-33.4, *Intelligence Analysis*	PIR	priority intelligence requirement
ATP 5-0.1, *Army Design Methodology*	SIR	specific information requirement
FM 2-0, *Intelligence*		
FM 3-55, *Information Collection*		
MI Pub 2-01.2, *Establishing the Intelligence Architecture*		

Appendix A

Automation Support to Intelligence Analysis

AUTOMATION ENABLERS

A-1. Many different automation and communications systems are vital to intelligence analysis; they facilitate real-time collaboration, detailed operational planning, and support to collection management. Software updates and emerging technologies continue to improve current intelligence analysis systems to operate more effectively in garrison and in deployed environments.

A-2. Automation processing capabilities and tools readily available on today's computers enable the intelligence analysis process. The software or related programs in current automation systems allow intelligence analysts to screen and analyze significantly more data than in previous years. The development of analytical queries, data management tools, and production and dissemination software enhances the intelligence analysis process, facilitating the commander's situational understanding and timely decision making across all echelons.

A-3. Automation is crucial to intelligence analysis; there are four aspects for analysts to consider:

- Automation is a key enabler to the processing and fusion of compatible information and intelligence, but the individual analyst remains essential in the validation of any assessment.
- The analyst must still be heavily involved in building specific queries, analyzing the final assessment, and releasing intelligence.
- Automation relies on the cyberspace domain, which requires extensive defensive actions to ensure data is not corrupted from collection to dissemination. Deception and corruption within the cyberspace domain are likely occurrences; therefore, they require monitoring by both cyberspace experts and intelligence analysts.
- Automation relies on available communications to receive, assess, and disseminate information across the command at all echelons. During periods of disrupted or degraded communications, the intelligence analyst must understand and may have to execute intelligence analysis without the aid of automation.

DISTRIBUTED COMMON GROUND SYSTEM-ARMY

A-4. All communications, collaboration, and intelligence analysis within the intelligence warfighting function are facilitated by the DCGS-A—the intelligence element of Army command and control systems and an Army program of record. DCGS-A can leverage the entire national, joint, tactical, and multinational intelligence community for intelligence reach and federated analysis. DCGS-A enables the intelligence analysis process through software tools, as shown in figure A-1 on page A-3. The following highlights some of the most significant tools across the phases of the intelligence analysis process:

- **Screen:**
  - ***Axis Pro/Link Diagram*** is a software product used for data analysis and investigations that assists in mapping and understanding threat networks comprising threat equipment, units, facilities, personnel, activities, and events.
  - ***Threat Characteristics Workstation*** provides tools to develop and manage threat characteristics, track battle damage assessments (BDAs), and create doctrinal and dynamic situation templates. The workstation also allows analysts to create graphic and written comparisons of threat capabilities and vulnerabilities, which are included in the intelligence estimate.
  - ***Weather Client*** allows analysts to identify segments of the battlefield that require an in-depth evaluation of weather effects on friendly and threat operations. This evaluation gives the commander a general overview of potential effects throughout the AO.

- ***MovINT Client*** provides an integrated, temporal view of the battlefield, and aggregates air- and ground-force locations, moving target intelligence, aircraft videos, sensor points of interest, and target locations.

- **Analyze**:
  - ***SOCET GXP*** (also known as Softcopy Exploitation Toolkit Geospatial Exploitation Product), an advanced geospatial intelligence software solution, uses imagery from satellite and aerial sources to identify, analyze, and extract ground features, allowing for rapid product creation.
  - ***Terra Builder/Explorer*** provides professional-grade tools for manipulating and merging imagery and elevation data of different sizes and resolutions into a geographically accurate terrain database. It also allows analysts to view, query, analyze, edit, present, and publish geospatial data.
  - ***Text Extraction*** allows analysts to quickly extract information from reports, associate elements with relationships, and identify existing matches in the database.
  - ***ArcGIS*** (also known as Arc Geographic Information System) allows analysts to visualize, edit, and analyze geographic data in both two- and three-dimensional images and has several options for sharing with others.
- **Integrate:**
  - ***Multifunction workstation interface***, a customizable interface that streamlines workflow, supports the commander's operations by providing accurate and timely intelligence and analysis to support Army forces.
  - ***ArcGIS***. (See description under **Analyze**.)
  - ***Google Earth***, a geo-browser that accesses satellite and aerial imagery, ocean bathymetry, and other geographic data of a network, represents the Earth as a three-dimensional globe.
- **Produce:**
  - ***Office 2013*** is a suite of productivity applications that includes Microsoft Word, Excel, PowerPoint, Outlook, OneNote, Publisher, Access, InfoPath, and Link.
  - ***Multifunction workstation interface***. (See description under **Integrate**.)
  - ***i2 Analyst Notebook*** is a software product used for data analysis and investigation. It is part of the Human Terrain System, an Army program that embeds social scientists with combat brigades.

A-5. DCGS-A, like any automation system, is subject to software updates, including changes to the current hardware as well as lifecycle replacements. As such, future versions may include greater analytical cross discipline and domain collaboration and improved interoperability with command and control systems and knowledge management components. (See figure A-1.)

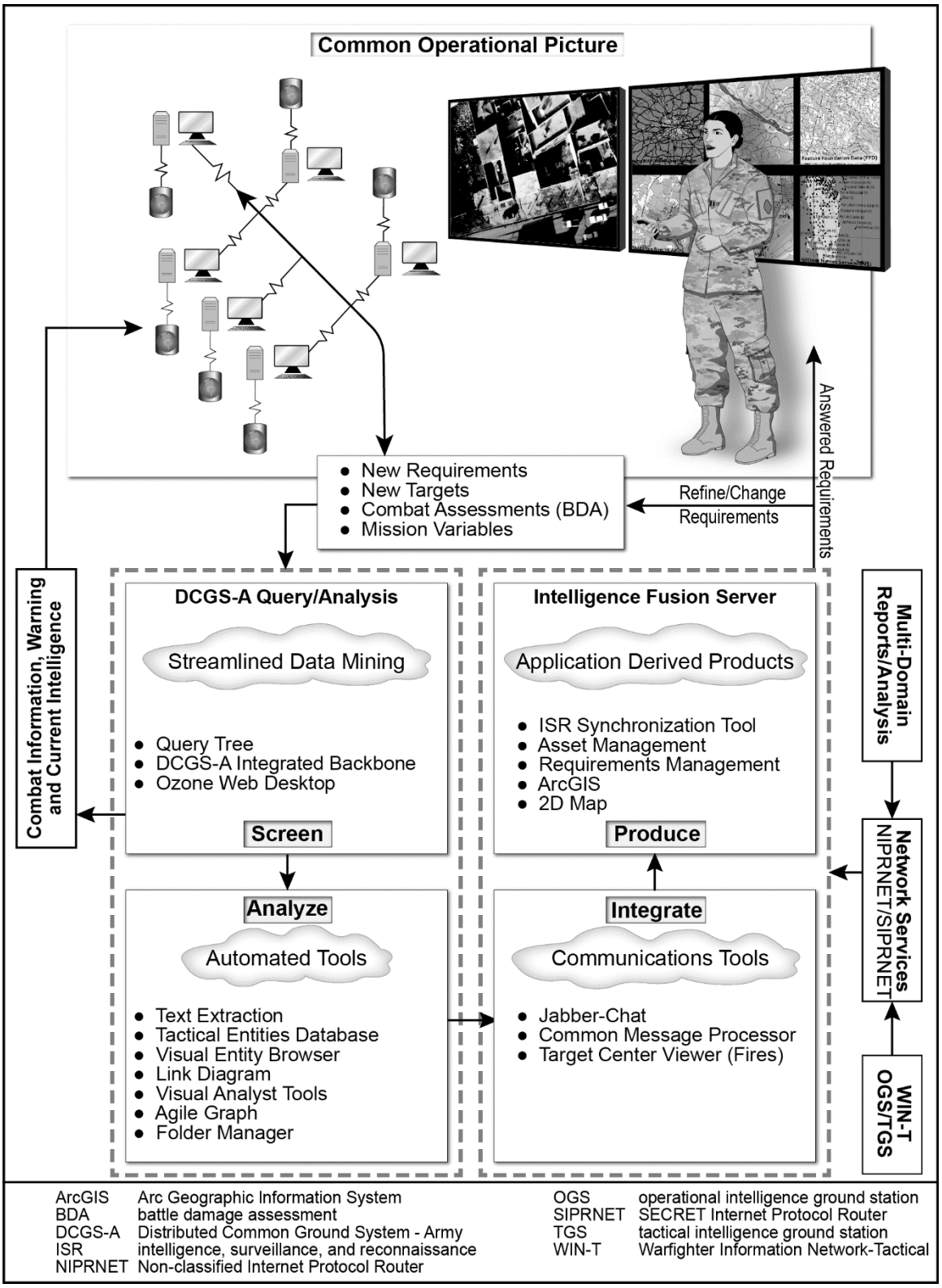


Figure A-1. Intelligence analysis enabled by DCGS-A

This page intentionally left blank.

Appendix B
Intelligence Analytical Skills

OVERVIEW

B-1. Intelligence analytical skills support collecting, visualizing, and examining information in detail to make accurate analytical conclusions. These skills enable analysts to complete various analytic tasks through deliberate thought processes to examine a situation critically and without bias.

THE INTELLIGENCE ANALYST

B-2. Intelligence analysis support to any operation involves separating useful information from misleading information, using experience and reasoning, and reaching an assessment or conclusion based on fact and/or sound judgment. The conclusion is based on the intelligence analyst's—

- Experience, skill, knowledge, and understanding of the operation.
- Knowledge of the various intelligence disciplines.
- Knowledge of information collection.
- Understanding of the threats within an OE.
- In-depth understanding of the threat's military and political structure.

B-3. The intelligence personnel conducting the analysis of information and intelligence use basic to advanced tradecraft skills and tools and integrated automated programs to sort raw forms of data and information and apply research skills to formulate an assessment. Analysts are responsible for the timely dissemination and/or presentation (proper writing and presentation techniques) of known facts and assumptions regarding the OE to the commander and staff. There are established tradecraft standards that direct the individual or group of analysts to ensure the analysis meets a common ethic to achieve analytical excellence.

B-4. Intelligence analysts follow guidelines, such as the ICD 203 Intelligence Community Analytic Standards, that promote a common ethic for achieving analytical rigor and excellence and personal integrity in analytical practices. (See appendix C.) Additionally, they must build their foundational understandings and integrate their learned skills—critical thinking, creative thinking, and embracing ambiguity. Intelligence analysts must be willing to change their determinations over time. Training, knowledge, and experience further develop analysts' expertise, as these aspects are essential in helping analysts deal with the uncertain and complex environments.

B-5. The OE is complex, and the threat attempts to hide its objectives, intent, and capabilities when possible. Therefore, intelligence analysts embrace ambiguity, recognize and mitigate their own or others' biases, challenge their assumptions, and continually learn during analysis. To assist in mitigating some of the uncertainty associated with conducting intelligence analysis, analysts should increase their proficiency in using analytic techniques and tools, including automated analytic tools and systems, to identify gaps in their understanding of the OE. Furthermore, to be effective, intelligence analysts must have a thorough understanding of their commanders' requirements and the intelligence analysis process (see chapter 2), which directly contributes to satisfying those requirements.

CRITICAL AND CREATIVE THINKING

B-6. Thinking includes awareness, perception, reasoning, and intuition; it is naturally influenced by emotion, experience, bias, assumptions, and sometimes poor reasoning skills. Some important aspects of critical thinking are rational, logical, self-directed, self-disciplined, and self-monitored thinking. Creative thinking examines problems from a fresh perspective to develop innovative solutions. Examples of creative thinking include breaking old habits of thought, questioning the status quo, visualizing a future, and devising unique responses to problems. There is a broad, long-standing, and helpful body of knowledge covering critical and creative thinking across academia, publications, and educational materials. Current critical

thinking literature has expanded the field to include aspects like creativity, imagination, discovery, reflection, empathy, subjectivity, and ambiguity.

B-7. ADP 5-0 and FM 5-0 discuss critical and creative thinking within the context of the operations process and effective planning. Together, critical and creative thinking assist commanders and staffs in understanding situations, making decisions, directing actions, and assessing operations. Critical thinking assists the commander and staff in—

- Questioning information, assumptions, conclusions, and points of view to evaluate evidence, develop understanding, and clarify goals.
- Finding new perspectives, frames of reference, and other creative means to solve military problems.
- Identifying causes of problems, arriving at justifiable conclusions, and making good judgments.
- Countering personal and group biases and avoiding logic errors.

B-8. The application of critical and creative thinking within the Army differs based on the warfighting function or another function of that thinking—which is especially true for intelligence analysis. The characteristics of effective intelligence (timely, relevant, and tailored, accurate and reliable, predictive, useable, complete, and precise) in FM 2-0 and the analytical standards captured in ICD 203 have long included elements of critical and creative thinking. Among the many benefits of improved analysis, critical and creative thinking assist in meeting the analytical standards in ICD 203 and in detecting enemy propaganda, disinformation, and deception.

B-9. Analysts obviously think in order to transform information into intelligence. They use analytic techniques and an understanding of the requirements, area knowledge, and experience to try to provide accurate, meaningful assessments to commanders and staffs. Thinking becomes critical thinking when analysts use a self-reflective and self-disciplined approach to the intelligence analysis process (see figure B-1).

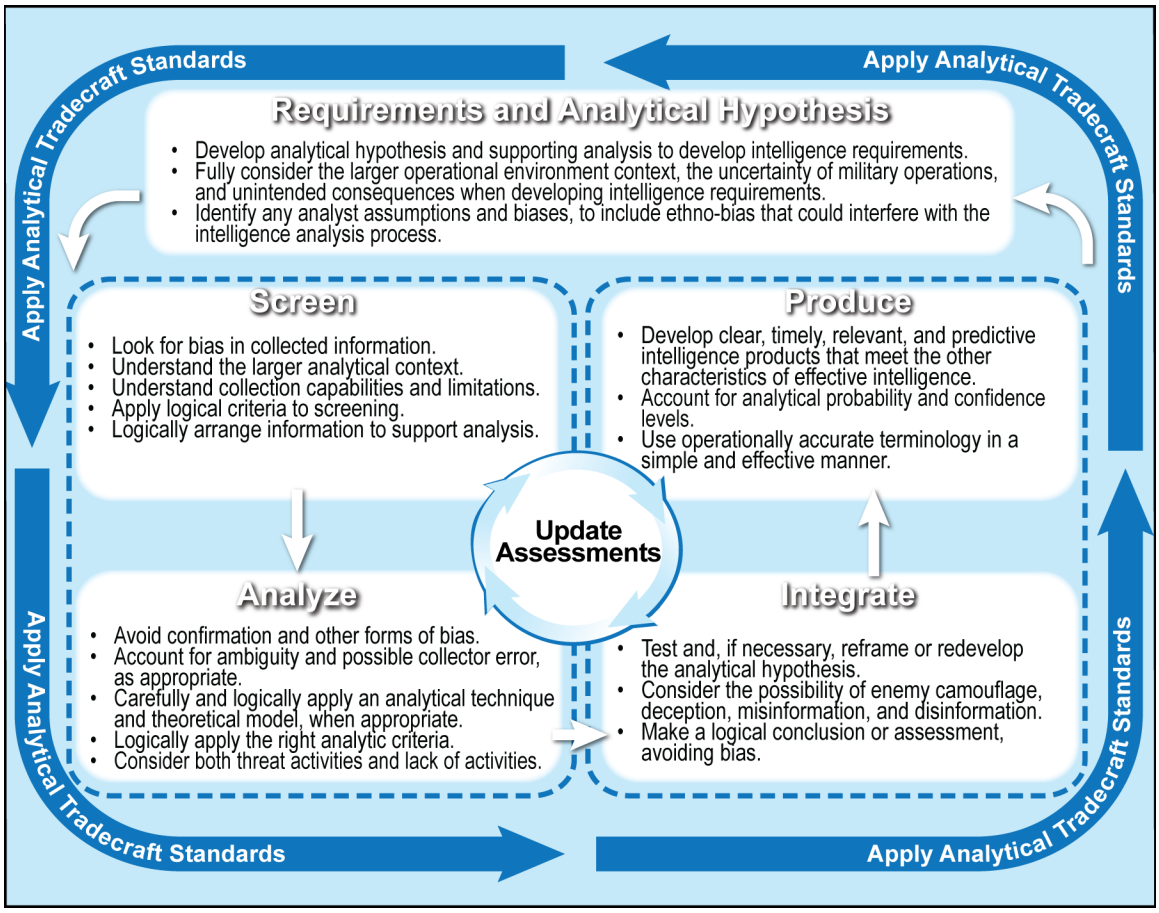


Figure B-1. Critical thinking nested within the intelligence analysis process

B-10. Intelligence analysts apply critical thinking skills to provide more holistic, logical, ethical, and unbiased analysis and conclusions. Critical thinking always includes—

- Carefully applying basic thinking skills.
- Avoiding analytical pitfalls, to include overcoming biases.

B-11. The most important step in building critical thinking skills is to begin a course of personal study and practice with a goal of improving the ability to reason logically and with as little bias as possible. This means moving beyond Army doctrine and other Army professional writing to begin a broad course of self-study. Most of the body of thought concerning critical thinking extends across various civilian professions and disciplines, particularly those in academia. The discussion in this publication is a glimpse of what should become a life-long professional endeavor.

B-12. The following includes other practical ways to improve critical and creative thinking:

- Continually examine world viewpoints and find other viewpoints, including key theories in the study of morals, values, political science, military theory, and intelligence. For example, within international relations, geography, and political science, key theories—such as realism, liberalism, nihilism, democratic piece theory, economic piece theory, Mahan's sea power theory, and Mackinder's heartland theory—have dominated thinking. An understanding of these theories is critical when analysts conduct analysis or predict outcomes without knowing how they or the adversary views the world. Continual examination of key theories/viewpoints also assists analysts in identifying biases in their thinking.
- Become a lifelong learner and pursue higher education, including courses on logic, reasoning, and critical thinking. One does not know what one does not know. Different educational resources and experiences build knowledge.
- Pursue or request job positions (even if temporary) that enable growth. Exposure to a variety of intelligence positions across as many echelons as possible supports *learning by doing* and broadens analysts' knowledge base.
- Read, write, and rewrite. Read relevant professional publications and articles, including those from existing reading lists, based on key self-development topics. Contribute article submissions to professional journals, such the Military Intelligence Professional Bulletin (also known as MIPB).
- Edit other analyst's writings. Editing assists analysts in becoming better readers and writers.
- Think out loud, collaborate, and debate ideas in a collegial manner. Provide and explore ideas to help solve complicated issues. This trait assists analysts in identifying their own logic flaws and biases.
- Study and prepare to debate a strongly opposed position until it can be debated as well as someone who believes in the position.
- Conduct extensive studies of other cultures to understand how they developed and their view of the world. Take that understanding to compare and contrast those other cultures with the culture/cultures within the United States.

CAREFULLY APPLYING BASIC THINKING SKILLS

B-13. Army intelligence personnel are required to use basic thinking abilities and complex skills to analyze information. These skills relate to an analyst's ability to think. Intelligence analysis focuses primarily on thinking. Intelligence analysts must continually strive to improve the quality of their thinking to support the commander's requirements. The three basic thinking abilities for intelligence analysis are—

- Information ordering.
- Pattern recognition.
- Reasoning.

INFORMATION ORDERING

B-14. *Information ordering* is the ability to follow previously defined rules or sets of rules to arrange data in a meaningful order. In the context of intelligence analysis, this ability allows analysts, often with technology's assistance, to arrange information in ways that permit analysis, synthesis, and a higher level of understanding. The arrangement of information according to certain learned rules leads analysts to make conclusions and disseminate the information as intelligence. However, such ordering can be inherently limiting; analysts may not seek alternative explanations because the known rules lead to an easy conclusion.

PATTERN RECOGNITION

B-15. Humans detect and impose patterns on apparently random entities and events in order to understand them, often doing this without awareness. Intelligence analysts impose or detect patterns to identify relationships, and often to infer what they will do in the future. Pattern recognition lets analysts separate the important from the less important, even the trivial, and conceptualize a degree of order out of apparent chaos. However, imposing or seeking patterns can introduce bias. Analysts may impose culturally defined patterns on random aggregates rather than recognize inherent patterns, thereby misinterpreting events or situations.

REASONING

B-16. *Reasoning* is what allows humans to process information and formulate explanations in order to assign meaning to observed actions and events. The quality of any type of reasoning is based on how well analysts' analytic skills have been developed, which occurs through practice and application. Improving analytic skills occurs by implementing individual courses of study and organizational training strategies.

B-17. There are four types of reasoning that guide analysts in transforming information into intelligence:

- **Deductive reasoning** is using given factual information or data to infer other facts through logical thinking. It rearranges only the given information or data into new statements or truths; it does not provide new information. Therefore, deductive reasoning is, *"If this is true, then this is also true."*
- **Inductive reasoning** is looking at given factual information or data for a pattern or trend and inferring the trend will continue. Although there is no certainty the trend will continue, the assumption is it will. Therefore, inductive reasoning is, *"Based on this trend, this is probably true."*
- **Abductive reasoning** is similar to inductive reasoning since conclusions are based on probabilities or "guessing." Therefore, abductive reasoning is, "*Because this is probably true, then this may also be true."*
- **Analogical reasoning** is a method of processing information that relies on an analogy to compare the similarities between two specific entities; those similarities are then used to draw a conclusion—the more similarities between the entities, the stronger the argument.

Note. Of the four types of reasoning, only deductive reasoning results in a conclusion that is always true. However, during the conduct of intelligence analysis, this statement can be misleading. During operations, there are few situations in which both a rule is always true and there is adequate collection on the threat to apply deductive reasoning with certainty.

Even in the best of circumstances, inductive, abductive, and analogical reasonings cannot produce conclusions that are certain. All of the types of reasoning rely on accurate information, clear thinking, and freedom from personal bias and group thinking.

B-18. Figure B-2 provides hypothetical examples for each type of reasoning. The examples are based on a peer threat with multiple divisions. The threat designates its divisions as first-tier, second-tier, or third-tier based on their equipment, end strength, and ability to conduct complicated operations. Effective execution of a relief-in-place is very complicated.

Deductive Reasoning	*Inductive Reasoning*	*Abductive Reasoning*	*Analogical Reasoning*
General Rule ↓ Specific Conclusion (always true)	**Specific Observations** ↓ General Conclusion (probably true)	**Incomplete Observations** ↓ Best Prediction (may be true)	**Incomplete Observations** ↓ Possible Prediction (may be true) (Requires Further Analysis)
P1: All first-tier divisions are capable of conducting an effective relief-in-place. **P2:** The 87th Tank Division is designated as a first-tier division. **Conclusion:** The 87th Tank Division is capable of conducting an effective relief-in-place.	**P1:** The 87th Tank Division is designated as a first-tier division. **P2:** The 87th Tank Division is capable of conducting an effective relief-in-place. **Conclusion:** All first-tier divisions are capable of conducting an effective relief-in-place.	**P1:** All first-tier divisions are capable of conducting an effective relief-in-place. **P2:** The 87th Tank Division is capable of conducting an effective relief-in-place. **Conclusion:** The 87th Tank Division is designated as a first-tier division.	**Similarities:** The 46th Tank Division has key leaders who all received exceptional ratings throughout their career; the division is manned at 90% strength. **Similarities:** The 87th Tank Division has key leaders who all received exceptional ratings throughout their career; the division is manned at 90% strength. **P3:** The 46th Tank Division is designated as a first-tier division. **Conclusion:** The 87th Tank Division is designated as a first-tier division.
P premise			

Figure B-2. Types of reasoning examples

AVOIDING ANALYTICAL PITFALLS, TO INCLUDE OVERCOMING BIASES

B-19. Intelligence analysts involved in analyzing complex situations and making conclusions are prone to the influences that shape and mold their view of the world and their ability to reason. These influences are referred to as analytical pitfalls. Critical thinking assists analysts in recognizing these pitfalls in their analysis and the analysis performed by others. Logic fallacies and biases are two general categories of analytical pitfalls.

LOGIC FALLACIES

B-20. Logic fallacies are errors in the reasoning process caused by the failure to apply sound logic. Although usually committed unintentionally, these fallacies are sometimes used deliberately to persuade, convince, or deceive. An analyst must be able to recognize logic fallacies so a false line of reasoning will not distract them and lead to poor conclusions. This appendix discusses the fallacies of relevance, omission, and assumption.

Fallacies of Relevance

B-21. Fallacies of relevance appeal to evidence or examples that are irrelevant to the argument at hand:

- **Appeal to force ("argumentum ad baculum" or the "might-makes-right" fallacy):** This argument uses force, the threat of force, or some other unpleasant backlash to make the audience accept a conclusion. It commonly appears as a last resort when evidence or rational arguments fail to convince. Logically, this consideration has nothing to do with the merits of the points under consideration.
- **Genetic fallacy:** The genetic fallacy is the claim that, because an idea, product, or person must be wrong because of its origin. For example, "That car cannot possibly be any good! It was made outside of the United States!" Or, "Why should I listen to her argument? She comes from California, and we all know those people are not critical thinkers." This type of fallacy is closely related to the fallacy of argumentum ad hominem, below.

- **Argumentum ad hominem (literally "argument to the man"; also called "poisoning the well" and "personal attack"):** This fallacy seeks to discount evidence before it is presented, most often by discrediting the source. For example, an ardent spokesman against the value of strategic bombing states, "You cannot trust that man's testimony regarding the effectiveness of strategic bombing; he's employed by the Air Force." The speaker is trying to discredit contrary evidence by creating the specific impression that the testimony is biased because the testifier represents a certain organization. There are two subcategories:
  - ***Abusive:*** To argue that proposals, assertions, or arguments must be false or dangerous because of an irrational psychological transference with the originator.
  - ***Circumstantial:*** To argue that opponents should accept or refute an argument only because of circumstances in their lives is a fallacy. If one is an environmentalist, suggesting that this environmentalist should not accept hunting because to do so would be incompatible with environmentalism is a circumstantial fallacy. The opponent's special circumstances do not affect the truth or untruth of a specific contention. The speaker or writer must find additional evidence beyond that to make a strong case.
- **Argumentum ad populum ("argument to the people"):** This fallacy uses an appeal to popular assent, often by arousing the feelings and enthusiasm of the multitude rather than building an argument. It is a favorite device with the propagandist, the demagogue, and the advertiser. There are three basic approaches:
  - ***Bandwagon approach:*** "Everybody is doing it." This argumentum ad populum asserts that, since the majority of people believes an argument or chooses a particular COA, the argument must be true or the COA must be the best one. For instance, "Over a million people purchased that phone rather than a competing phone; all those people cannot be wrong. That company must make the best phones." Popular acceptance of any argument does not prove it to be valid.
  - ***Patriotic approach:*** This argument asserts that a certain stance is true or correct because it is somehow patriotic, and that those who disagree are somehow unpatriotic. It overlaps with pathos and argumentum ad hominem to a certain extent. The best way to spot it is to look for emotionally charged terms like Americanism, rugged individualism, motherhood, patriotism, or godless communism, for example, "A true American would never use this approach," or, "A truly free man will exercise his American right to drink beer, since beer belongs in this great country of ours."
  - ***Snob approach:*** This type of argumentum ad populum does not assert "everybody is doing it," but rather that "all the best people are doing it." For instance, "The top analysts at the Central Intelligence Agency agree that my analytic approach is correct." The implication is that anyone who fails to recognize the truth of the analyst's assertion is not an equal to the "top analysts of the Central Intelligence Agency," and thus has no right to question the analytical conclusions.
- **Appeal to tradition (argumentum ad traditio [also referred to as argumentum ad antiquitatem]):** This line of thought asserts that a premise must be true because people have always believed it or done it. Alternatively, it may conclude that the premise has always worked in the past and will thus always work in the future.

Fallacies of Omission

B-22. Fallacies of omission occur when an analyst leaves out necessary material in a conclusion or inference. Some fallacies of omission include oversimplification, composition, division, post hoc, false dilemma, hasty generalization, and special pleading:

- **Oversimplification** is a generality that fails to adequately account for all the complex conditions bearing on a problem. Oversimplification results when one or more of the complex conditions pertaining to a certain situation is omitted and includes ignoring facts, using generalities, and/or applying an inadequately qualified generalization to a specific case. For example, an ordnance specialist inspecting a captured, hand-carried, surface-to-air missile launcher concludes that the threat has no effective low-level air defense. The assessment is based on the fact that the weapons system is equipped with antiquated guidance mechanisms. The ordnance specialist's conclusion omits the following considerations:

  - That this piece of equipment may not be the threat's only low-level air defense weapon.
  - That the launcher may have been planted by the threat to give a misleading picture of the threat's true capabilities and deceive weapons experts.
  - That the threat abandoned the launcher because it was ineffective and more capable systems were available.
- **Fallacy of composition** is committed when a conclusion is drawn about a whole based on the features of parts of that whole when, in fact, no justification is provided for that conclusion. For example, during a battle with an ethnic militia, a single detainee was captured. This detainee was suffering from malnutrition and low morale. It was noted that the detainee was equipped with a semiautomatic weapon of World War II vintage. After a brief interrogation, the intelligence analyst reported the threat militia recently engaged was starving, diseased, and poorly armed. The intelligence analyst failed to consider that—
  - The detainee may have been captured because the detainee was too sick to keep up with the rest of the unit.
  - The weapon of early vintage did not necessarily make it ineffective.
  - Few captured detainees have high morale; in fact, low morale could just as easily result from being captured as it could contribute to being captured.
- **Fallacy of division** is committed when a person infers that what is true of a whole must also be true of the parts of that whole. For example, members of the threat guard's brigade had never surrendered in previous combat. After a recent engagement, a detainee stated it was a member of the guard brigade. The interrogator doubted the detainee's statement because personnel from that brigade never surrender.
- **Fallacy of post hoc ergo propter hoc** (after this, therefore because of this) is consideration of other factors that might have accounted for the same result that are omitted. Post hoc fallacies often occur when trying to establish cause and effect. For example, an aircraft equipped with a new jamming pod was not fired on while flying over threat-controlled territory. It was concluded that, since the aircraft was not intercepted or fired upon, the jamming pod was extremely effective in suppressing threat electronic systems. The conclusion may or may not account for the aircraft not being attacked. Other considerations include—
  - The threat was obtaining electronic intelligence on this new pod.
  - The threat recently relocated several surface-to-air missile units and did not want to reveal their new positions.
- **False dilemma** (also known as black-and-white thinking) is a fallacy in which a person omits consideration of more than two alternatives when in fact there are more than two alternatives. For example, an S-2 reports to the commanding officer that the threat only has the capability to either defend in place or retreat. The S-2 committed the fallacy of false dilemma by failing to anticipate or ignoring that the threat could attack if it were willing to accept high casualties, withdraw to an alternate defensive position, or conduct a delaying action.
- **Hasty generalizations** are conclusions drawn from samples that are too few or from samples that are not truly representative of the population. For example, after interrogating a detainee, the interrogation officer reports the threat's morale as extremely low and that surrender is imminent. In this case, the interrogator is making a hasty generalization because the sample population considered, one detainee, is too small.
- **Special pleading** is a fallacy in which the writer creates a universal principle, then insists that the principle does not for some reason apply to the issue at hand. For instance, "John Doe claimed to be psychic, but when his 'abilities' were tested under proper scientific conditions, they magically disappeared. John explained this saying that one had to have faith in his abilities for them to work."

Fallacies of Assumption

B-23. Fallacies of assumption implicitly or explicitly involve assumptions that may or may not be true. Some fallacies of assumption include begging the question, stating hypotheses contrary to fact, and misusing analogies:

- **Begging the question** (also known as circular reasoning) is a fallacy in which the conclusion occurs as one of the premises.
  - It is an attempt to support a statement by simply repeating the statement in different and stronger terms. For example, a particular group wants democracy. America is a democratic nation. Therefore, that group will accept American-style democracy.
  - When asked why the enemy was not pinned down by fire, the platoon leader replied, "Our suppressive fire was inadequate." The fallacy in this response is that by definition suppressive fire pins down the enemy or is intended to pin him down. Since the platoon failed to pin down the enemy, the inadequacy of this fire was self-evident.
- **Stating hypotheses contrary to fact** occurs when someone states decisively what would have happened had circumstances been different. Such fallacies involve assumptions that are either faulty or simply cannot be proven. For example, the statement, "If we had not supported Castro in his revolutionary days, Cuba would be democratic today" is contrary to fact. Besides being a gross oversimplification, the assumption made in the statement cannot be verified.
- **Misusing analogies** occurs when one generalizes indiscriminately from analogy to real world. One method for weakening an analogous argument is by citing a counter-analogy. Analogies are strong tools that can impart understanding in a complex issue. In the absence of other evidence, intelligence analysts may reason from analogy. Such reasoning assumes that the characteristics and circumstances of the object or event being looked at are similar to the object or event in the analogy.

B-24. The strength of a conclusion drawn from similar situations is proportional to the degree of similarity between the situations. The danger in reasoning from analogy is assuming that because objects, events, or situations are alike in certain aspects, they are alike in all aspects. Conclusions drawn from analogies are inappropriately used when they are accepted as evidence of proof. Situations may often be similar in certain aspects, but not in others. A counter-analogy weakens the original analogy by citing other comparisons that can be made on the same basis.

BIASES

B-25. A subjective viewpoint, bias indicates a preconceived notion about someone or something. Biases generally have a detrimental impact on intelligence analysis because they obscure the true nature of the information. Intelligence analysts must be able to recognize cultural, organizational, personal, and cognitive biases and be aware of the potential influence they can have on judgment.

Cultural Bias

B-26. Americans see the world in a certain way. The inability to see things through the eyes of someone from another country or culture is cultural bias. Biases interfere with the analyst's ability to think the way a threat commander might think or to give policymakers informed advice on the likely reaction of foreign governments to U.S. policy. Also known as mirror imaging, cultural bias attributes someone else's intentions, actions, or reactions to the same kind of logic, cultural values, and thought processes as the individual analyzing the situation. Although cultural bias is difficult to avoid, the following measures can lessen its impact:

- Locate individuals who understand the culture:
  - Include them in the intelligence analysis process.
  - Ask their opinion about likely responses to friendly actions.
  - Take care when using their opinions since they may be subject to biases regarding ethnic groups or cultures in the region and their knowledge may be dated or inaccurate.
- Locate regional experts, such as foreign and regional area officers, who have lived or traveled through the area and are somewhat conversant regarding the culture. Assess the quality of the information provided against the level of knowledge and experience the individual has for that culture or region.

Organizational Bias

B-27. Most organizations have specific policy goals or preconceived ideas. Analysis conducted within these organizations may not be as objective as the same type of analysis done outside the organization. Groupthink and best case are organizational biases that can significantly skew internal analysis.

- **Groupthink.** This bias occurs when a judgment is unconsciously altered because of exposure to selective information and common viewpoints held among individuals. Involving people outside the organization in the analysis can help identify and correct this bias.
- **Best case.** This bias occurs when an analyst presents good news or bad news in the most optimistic light. The judgment is deliberately altered to provide only the information the commander wants to hear. Analysts can avoid this bias by having the moral courage to tell the commander the whole story, good and bad.

A Useful Tool in Logic: Occam's Razor

The term “Occam's Razor” comes from a misspelling of the name William of Ockham. Ockham was a brilliant theologian, philosopher, and logician in the medieval period. One of his rules of thumb has become a standard guideline for thinking through issues logically. Occam's Razor is the principle that, if two competing theories explain a single phenomenon, and they both generally reach the same conclusion, and they are both equally persuasive and convincing, and they both explain the problem or situation satisfactorily, the logician should always pick the less complex one. The one with the fewer number of moving parts, so to speak, is most likely to be correct. The idea is always to cut out extra unnecessary bits, hence the name "razor." An example will help illustrate this.

Suppose you come home and discover that your dog has escaped from the kennel and chewed large chunks out of the couch. Two possible theories occur to you:

- Theory one is that you forgot to latch the kennel door, and the dog pressed against it and opened it, and then the dog was free to run around the inside of the house. This explanation requires two entities (you and the dog) and two actions (you forgetting to lock the kennel door and the dog pressing against the door).
- Theory two is that some unknown person skilled at picking locks managed to disable the front door, then came inside the house, set the dog free from the kennel, then snuck out again covering up any sign of his presence and then relocked the door, leaving the dog free inside to run amok in the house. This theory requires three entities (you, the dog, and the lock-picking intruder) and several actions (picking the lock, entering the house, releasing the dog, hiding the evidence, relocking the door). It also requires us to come up with a plausible motivation for the intruder-a motivation that is absent at this point.

  Either theory would be an adequate and plausible explanation. Both explain the same phenomenon (the escaped dog) and both employ the same theory of how, for example, that the latch was opened somehow, as opposed to some farfetched theory.

  Which theory is most likely correct? If you do not find evidence like strange fingerprints or human footprints or missing possessions to support theory two, William of Ockham would say that the simpler solution (theory one) is most likely to be correct in this case. The first solution only involves two parts-two entities and two actions.

On the other hand, the second theory requires at least five parts-you, the dog, a hypothetical unknown intruder, some plausible motivation, and various actions. It is needlessly complex. Occam's basic rule was: "Thou shalt not multiply extra entities unnecessarily," or to phrase it in modern terms: "Don't speculate about extra hypothetical components if you can find an explanation that is equally plausible without them. "All things being equal, the simpler theory is more likely to be correct.

Personal Bias

B-28. Personal bias is the tendency to base assessments on personal beliefs. This can cause the rejection of valid arguments that conflict with these beliefs. A racially or religiously prejudiced person may reject arguments because of the source. A person with strong political views may discount every argument from another political group.

B-29. There are several types of personal bias. Three common biases exhibited by analysts are—

- **Confirmation bias.** This bias causes analysts to undervalue or ignore evidence contradicting an early judgment and value evidence that tends to confirm already held assessments.
- **Assimilation bias.** This bias involves the modification and elaboration of new information to fit prior conceptions or hypotheses. The bias is toward confirming a preconceived answer.
- **Anchoring bias.** This bias involves the use, often unwitting, of arbitrary values in decision making, including the use of conclusions developed by others.

Cognitive Bias

B-30. The intelligence analyst evaluates information from a variety of sources. The degree of reliability, completeness, and consistency varies from source to source and even from report to report. This variance often creates doubt about the reliability of some sources. Cognitive biases that affect the analyst are—

- **Vividness.** Clear and concise or vivid information has a greater impact on analytical thinking than abstract and vague information. A clear piece of information is held in higher regard than a vague piece of information that may be more accurate. Analysts must consider that an enemy may use deception to portray vivid facts, situations, and capabilities that they want the friendly intelligence effort to believe.
- **Absence of evidence.** Lack of information is the analyst's most common problem, especially in the tactical environment. Analysts must do their best with limited information and avoid holding back intelligence because it is inconclusive. To avoid this bias, the analyst should—
  - Realize that information will be missing.
  - Identify areas where information is lacking and consider alternative conclusions.
  - Adapt or adjust judgments as more information becomes available.
  - Consider whether a lack of information is normal in those areas or whether the absence of information itself is an indicator.
- **Oversensitivity to consistency.** Consistent evidence is a major factor for confidence in the analyst’s judgment. Information may be consistent because it is appropriate, or it may be consistent because it is redundant, is from a small or biased sample, or is the result of the enemy's deception efforts. When making judgments based on consistent evidence, the analyst must—
  - Be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.
  - Be alert for circular reporting, which is intelligence already obtained by the unit that is then reformatted by other units and intelligence organizations, modified slightly, and disseminated back to the unit. This is a common problem; particularly in digital units, where large volumes of information are being processed. It helps to know, to the degree possible, the original source for all intelligence to ensure that a circular report is not used as evidence to confirm an intelligence estimate or conclusion.
- **Persistence on impressions.** When evidence is received, there is a tendency to think of connections that explain the evidence. Impressions are based on these connections. Although the evidence eventually may be discredited, the connection remains and so do the impressions.
- **Dependency on memory.** The ability to recall past events influences judgment concerning future events. Since memory is more readily available, it is easy to rely on memory instead of seeking new information to support analysis.
- **Acceptance of new intelligence.** Often new intelligence is viewed subjectively; either valued as having more value or less value than current intelligence.

HISTORICAL VIGNETTE

B-31. Analytic skills enable analysts to examine situations critically and without bias. This assists them in better identifying and analyzing enemy deception operations. Adversaries and enemy forces induce deception to maintain an analyst's preexisting belief rather than to deceive the analyst and change the analyst's preexisting belief. In the following historical vignette, the German Army in World War II successfully used the Allies' biases against them to launch one of the largest surprise attacks of the war—the Ardennes Offensive, better known as the Battle of the Bulge. The German Army used mirror imaging (see paragraphs 6-29 through 6-31) and other deception techniques to its advantage. The vignette also depicts intelligence failures in applying analytic skills, such critical and creative thinking, leading up to the German attack.

Intelligence Failure: Battle of the Bulge

On 16 December 1944, the German's launched a counteroffensive in the Ardennes region. The objective was to seize the port of Antwerp, isolating Allied forces, cutting supplies, and creating internal tensions between the Allies—possibly inducing a forced peace between Great Britain, the United States, and Germany.

In early December, the Allies were on the offense and total victory was in sight. German forces were pushed as far west as the Maginot Line on the Western Front as Russia continued its attack in the East. Reports of German troop attrition and plane and tank fuel shortages led Allied belief that Germany no longer had the will or resources to fight. The German Army reinforced this Allied belief against the Allies by naming the Ardennes counteroffensive, *WACHT AM RHEIN* or *Watch on the Rhine*, giving a defensive appearance to the operation. Adolf Hitler chose Field Marshal von Rundstedt, one of his top generals, to command the western forces. Because of Rundstedt's military experience and character, Allied intelligence staffs concluded the German main effort would indeed be the defense in the North. The Allies also believed the Ardennes' terrain was unfavorable for a German attack despite the German Army's attack through this terrain against the French in 1940.

The American VIII Corps' defense of the Ardennes was sparse, with little fighting expected in the region. This area was used to rotate troops in and out from the front lines for rest and refit. When intelligence reporting indicated German troop movement to the east of VIII Corps and the Ardennes, it was assessed the German's were using the Ardennes to stage reserves for the northern defense. The Allies relied on Ultra, signals intelligence intercepts of German communications, above other intelligence sources at the time because the intercepts came from the German's themselves. Hitler ordered radio silence fearing that intelligence of the operation would leak to the Allies. Ultra did not indicate a major offensive in the Ardennes from lack of further intercepts in the region.

Allied commanders and intelligence staffs viewed an attack through the Ardennes as highly unlikely although other intelligence reporting at the time may have described a contradictory enemy COA. Reporting included German requests for reconnaissance of routes and bridges in the Ardennes. Local populace also reported a buildup of engineering and bridging equipment nearby. Newly captured prisoners of war revealed secret plans for an offense coming through the Ardennes. The Allies intercepted German orders asking for English-speaking volunteers with American accents. These reports and others did not indicate a German military that was beaten and defeated.

During the months leading to the surprise attack, Germany was able to mass roughly 30 divisions opposite the American VIII Corps. On 16 December 1944, Germany launched an attack on unsuspecting American defenders, resulting in 75,000 American casualties with 19,000 killed in action. Although the Battle of the Bulge ended in an Allied victory and was the last major offensive of the German Army, the German counteroffensive is known as one of the biggest military intelligence failures of World War II.

This page intentionally left blank.

Appendix C

Analytic Standards and Analysis Validation

INTELLIGENCE COMMUNITY ANALYTIC STANDARDS

C-1. During intelligence analysis, the conclusions reached should also adhere to analytic standards, such as those established by the Director of National Intelligence in ICD 203. This directive establishes the analytic standards that govern the production and evaluation of national intelligence analysis to meet the highest standards of integrity and rigorous analytic thinking. The ICD 203 Intelligence Community Analytic Standards act as guidelines and goals for analysts and leaders throughout the intelligence community who strive for excellence in their analytical practices and products. The following identify and describe the five ICD 203 Intelligence Community Analytic Standards, including the nine analytic tradecraft standards:

- **Objective:** Analysts must perform their functions with objectivity and awareness of their own assumptions and reasoning. They must employ reasoning techniques and practical mechanisms that reveal and mitigate bias. Analysts should be alert to the influences of existing analytical positions or judgments and must consider alternative perspectives and contrary information. Analysis should not be unduly constrained by previous judgments when new developments indicate a modification is necessary.
- **Independent of political consideration:** Analytical assessments must not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint. Analytical judgments must not be influenced by the force of preference for a particular policy.
- **Timely:** Analysis must be disseminated in time for it to be actionable. Analytical elements must be continually aware of events of intelligence interest and of intelligence requirements and priorities in order to provide useful analysis at the right time.
- **Based on all available sources of intelligence information:** Analysis should be informed by all relevant information available. Analytical elements should identify and address critical information gaps and work with collection managers and data providers to develop access and collection strategies.
- **Implement and exhibit the analytic tradecraft standards:** See paragraphs C-3 through C-14.

ANALYSIS VALIDATION

C-2. Intelligence analysis and the resultant judgments are incomplete without the estimative language that provides both the probability that an event will occur and the confidence level of the analyst making this assessment. Analysts employ the analytic tradecraft standards to assess probabilities and confidence levels and the actions associated with analytical rigor to draw accurate conclusions.

ANALYTIC TRADECRAFT STANDARDS

C-3. Intelligence analysts exhibit and implement the nine analytic tradecraft standards, one of the five ICD 203 Intelligence Community Analytic Standards. Specifically, they—

- Properly describe the quality and credibility of all underlying sources, information, and methodologies.
- Properly express and explain uncertainties associated with major analytical judgments.
- Properly distinguish between underlying intelligence information and analysts' assumptions and judgments.
- Incorporate analysis of alternatives.
- Demonstrate customer relevance and address implications.

- Use clear and logical argumentation.
- Explain change to or consistency of analytical judgments.
- Make accurate judgments and assessments.
- Incorporate effective visual information where appropriate.

Properly Describe the Quality and Credibility of All Underlying Sources, Information, and Methodologies

C-4. Analytical products should include all underlying sources, information, and methodologies from which analytical judgments are based. Factors affecting source quality and credibility should be described using source descriptors in accordance with ICD 206, *Sourcing Requirements for Disseminated Analytic Products*. Such factors can include accuracy and completeness, possible denial and deception, age and continued currency of information, and technical elements of collection, as well as source access, validation, motivation, possible bias, or expertise. Source summary statements, described in ICD 206, should be used to provide a holistic assessment of the strengths or vulnerabilities in the source base and explain which sources are most important to key analytical judgments.

Properly Express and Explain Uncertainties Associated with Major Analytical Judgments

C-5. Analysts must properly express and explain uncertainties associated with any major analytical judgment. When briefing their analytical results, analysts, at a basic level, must be able to assess the likelihood of an event happening, expressed by using estimative language. Then, they must express their confidence level—high, moderate, or low—in that assessment. (See figure C-1.) For intelligence analysts to reach a high level of confidence in the accuracy of their analytical assessment, they must apply the actions of high analytical rigor found in table C-1 on page C-5.

Expressions of Likelihood	Almost no chance	Very unlikely	Unlikely	Roughly even chance	Likely	Very likely	Almost certain
	Remote	Highly improbable	Improbable	Roughly even odds	Probable	Highly probable	Nearly certain
Probability	01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%
Confidence Levels	Low				Moderate		High

Figure C-1. Estimative language: expressions of likelihood

Note. For expressions of likelihood, analysts are strongly encouraged not to mix terms from the different rows. Additionally, commanders are all different and their individual acceptance of the various probability and confidence levels may be different than those of previous commanders.

Assessing the Likelihood of an Event Happening

C-6. Phrases (such as *we judge*, *we assess*, and *we estimate*) commonly used to convey analytical assessments and judgments, are not facts, proofs, or knowledge. Intelligence analysts use estimative language, shown in figure C-1, to convey their assessment of the probability or likelihood of an event and the level of confidence ascribed to the judgment.

Expressing Confidence in Assessments

C-7. Confidence levels express the strength of the assessment given the reasoning, methodologies, gaps, and assumptions; the number, quality, and diversity of sources; and the potential for deception. (See figure C-1.) To avoid confusion, assessment language and confidence levels are no longer combined in the same sentence. Confidence levels are ascribed using high, moderate, and low levels of confidence in analytical assessments:

- **High confidence level.** High confidence generally indicates that sound reasoning and/or methodologies have been applied; no linchpin assumptions have been made; no critical gaps relevant to the issue are evident; consistent evidence from a variety of independent sources supports the judgment; the potential for deception is low; the body of reporting is not consistent with a plausible alternative; and/or the nature of the issue allows one to render a solid judgment. A *high confidence judgment*, however, is not a fact or a certainty, and such judgments still carry a risk of being inaccurate.
- **Moderate confidence level.** Moderate confidence generally indicates that potentially critical assumptions are used to fill gaps; some inconsistencies exist, but the preponderance of evidence supports the judgment; the information is credibly sourced and plausible but is not of sufficient quality or is not sufficiently corroborated to warrant high confidence; moderate potential for deception exists; and/or the body of reporting leaves open the possibility of a plausible alternative explanation of events.
- **Low confidence level.** Low confidence generally indicates that key assumptions have been used to fill critical gaps; significant inconsistencies or questions exist regarding the evidence; the information is fragmented or uncorroborated or is of questionable credibility and/or plausibility; high potential for deception exists; and/or the body of reporting supports an alternative explanation of events.

Properly Distinguish Between Underlying Intelligence Information and Analysts' Assumptions and Judgments

C-8. Analytical products should clearly distinguish statements that convey underlying intelligence information used in analysis from statements that convey assumptions or judgments. *Assumptions* are suppositions used to frame or support an argument; assumptions affect analytical interpretation of underlying intelligence information. *Judgments* are conclusions based on underlying intelligence information, analysis, and assumptions. Products should state assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps. Products should explain the implications for judgments if assumptions prove to be incorrect. As appropriate, products should also identify indicators that, if detected, would alter judgments.

Incorporate Analysis of Alternatives

C-9. *Analysis of alternatives* is the systematic evaluation of differing hypotheses to explain events or phenomena, explore near-term outcomes, and imagine possible futures to mitigate surprise and risk. Analytical products should identify and assess plausible alternative hypotheses. This is particularly important when major judgments must contend with significant uncertainties, or complexity, such as forecasting future trends, or when low probability events could produce high-impact results. In discussing alternatives, products should address factors such as associated assumptions, likelihood, or implications related to Army forces. Products should also identify indicators that, if detected, would affect the likelihood of identified alternatives.

Demonstrate Relevance and Address Implications

C-10. Analytical products should provide information and insight on issues relevant to the commanders and address the implications of the information and analysis they provide. Products should add value by addressing prospects, context, threats, or factors affecting opportunities for action.

Use Clear and Logical Argumentation

C-11. Analytical products should present a clear main analytical conclusion up front. Products containing multiple judgments should have a main analytical conclusion that is drawn collectively from those judgments. All analytical judgments should be effectively supported by relevant intelligence information and coherent reasoning. Products should be internally consistent and acknowledge significant supporting and contrary information affecting judgments.

Explain Change To or Consistency Of Analytical Judgments

C-12. Analysts should state how their major judgments on a topic are consistent with or represent a change from those in previously published analysis or represent initial coverage of a topic. Products need not be lengthy or detailed in explaining change or consistency. They should avoid using reused or unoriginal language and should make clear how new information or different reasoning led to the judgments expressed in them. Recurrent products should note any changes in judgments; absent changes, recurrent products need not confirm consistency with previous editions. Significant differences in analytical judgment, such as between two intelligence community analytical elements, should be fully considered and brought to the attention of customers.

Make Accurate Judgments and Assessments

C-13. Analytical products should apply expertise and logic to make the most accurate judgments and assessments possible, based on the information available and known information gaps. In doing so, analytical products should present all judgments that would be useful to commanders and should include difficult judgments in order to minimize the risk of being wrong. Inherent to the concept of accuracy is that the analytical conclusion that the analyst presents to the commander should be the one the analyst intended to send. Therefore, analytical products should express judgments as clearly and precisely as possible, reducing ambiguity by addressing the likelihood, timing, and nature of the outcome or development.

Incorporate Effective Visual Presentations When Feasible

C-14. Analysts should present intelligence in a visual format to clarify an analytical conclusion and to complement or enhance the presentation of intelligence and analysis. In particular, visual presentations should be used when information or concepts, such as spatial or temporal relationships, can be conveyed better in graphic form, such as tables, flow charts, and images coupled with written text. Visual presentations may range from a plain display of intelligence information to interactive displays for complex issues and analytical concepts. Visual presentations should always be clear and pertinent to the product's subject. Analytical content in a visual format should also adhere to other analytic tradecraft standards.

ANALYTICAL RIGOR

C-15. *Analytical rigor* is the application of precise and exacting standards to better understand and draw conclusions based on careful consideration or investigation. There are eight primary action-metrics that lead to analytical rigor. When analysts combine these action-metrics with the intelligence analysis process, they can determine the analytical sufficiency of their conclusions. (See table C-1.)

Table C-1. Analytical actions and levels of rigor

Analytical rigor actions	*Levels of analytical rigor*		
	Low rigor	*Moderate rigor*	*High rigor*
Consider alternative hypotheses: Hypothesis exploration describes the extent to which multiple hypotheses were considered in explaining data.	• Little to no consideration of alternatives to primary or initial hypotheses. • Interpretation of ambiguous or conflicting data such that they are compatible with existing beliefs. • Fixation or knowledge shielding behaviors.	• Some consideration of how data could support alternative hypotheses. • An unbalanced focus on a probable hypothesis or a lack of commitment to any particular hypothesis.	• Significant generation and consideration of alternative explanations via the direct evaluation of specific hypotheses. • Incorporation of "outside" perspectives in generating hypotheses. • Evolution and broadening of hypothesis set beyond an initial framing. • Ongoing revision of hypotheses as new data are collected.
Evaluate depth of research: Information search relates to the depth and breadth of the search process used in collecting data.	• Failure to go beyond routine and readily available data sources. • Reliance on a single source type or on data that are far removed from original sources. • Dependence upon “pushed” information, rather than on actively collected information. • Use of stale or dated source data.	• Collection from multiple data types or reliance on proximal sources to support key findings. • Some active information seeking.	• Collection of data from multiple source types in addition to the use of proximal sources for all critical inferences. • Exhaustive and detailed exploration of data in the relevant sample space. • Active approach to information to information collection
Validate information accuracy: Information validation details the levels at which information sources are corroborated and cross-validated.	• General acceptance of information at face value, with little or no clear embellishment of underlying veracity. • Lack of convergent evidence. • Poor tracking and citation of original sources of collected data.	• Use of heuristics to support judgments of source integrity. For example, relying on sources that have previously proven to be consistently accurate. • A few “key” high-quality documents are relied on heavily. • Recognizes and highlights inconsistencies between sources.	• Systematic and explicit processes employed to verify information and to distinguish facts from judgments. • Seeks out multiple, independent sources of converging evidence. • Concerned both with consistency between sources and with validity and credibility within a given source.
Examine source bias: Stance analysis is the evaluation of data with the goal of identifying the stance or perspective of the source and placing it into a broader context of understanding.	• Little consideration of the views and motivations of source data authors. • Recognition of only clearly biased sources or sources that reflect a well-defined position on an issue.	• Perspectives and motivations of authors are considered and assessed to some extent. • Incorporates basic strategies to compare perspectives of different sources. For instance, by dividing issues into “for” or “against” positions.	• Involves significant research into, or leverages a preexisting knowledge of, the backgrounds and views of key players and thought leaders. • May involve more formal assessments of data sources, such as faction analysis, social network analysis, or deception analysis.

Table C-1. Analytical actions and levels of rigor (*continued*)

Analytical rigor actions	*Levels of analytical rigor*		
	Low rigor	*Moderate rigor*	*High rigor*
Scrutinize strength of analysis: Sensitivity analysis considers the extent to which the analyst considers and understands the assumptions and limitations of their analysis.	• Explanations are appropriate and valid at a surface level. • Little consideration of critical "what if?" questions, such as, "What if a given data source turns out to be unreliable?" or "What if a key prediction does not transpire as anticipated?"	• Considers whether being wrong about some inferences would influence the overall best explanation for the data. • Identifies the boundaries of applicability for an analyzed information.	• Goes beyond simple identification to specify the strength of explanations and assessments in the event that individual supporting evidence or hypotheses were to prove invalid or unreliable. • Specifies limitations of the analysis, noting the most vulnerable explanations or predictions on which the analysis is at risk of erring.
Amalgamate information: Information synthesis refers to how far beyond simply collecting and listing data an analyst went in their process.	• Little insight with regard to how the analysis relates to the broader analytical context or to more long-term concerns. • Lack of selectivity, with the inclusion of data figures that are disconnected from the key arguments or central issues. • Extensive use of lists or the restatement of material copied directly from other sources with little interpretation.	• Explicit, though perhaps not systematic, efforts to develop the analysis within a broader framework of understanding. • Depiction of events in context and framing of key issues in terms of tradeoff dimensions and interactions. • Provides insight beyond what is available in the collected data.	• Extracted and integrated information in terms of relationships rather than components and with a thorough consideration of diverse interpretations of relevant data. • Reconceptualization of the original task, employing cross-checks on abstractions. • Performed by individuals who are "reflexive" in that they are attentive to the ways in which their cognitive processes may have hindered effective synthesis.
Incorporate expert input: Specialist collaboration describes the degree to which an analyst incorporates the perspectives of domain experts into their assessments.	• Minimal direct collaboration with experts. • Little if an on-topic, "outside" expertise is accessed or sought out directly.	• Involves some direct interaction with experts, though usually via readily available specialists. • Expertise is drawn from within preexisting personal or organizational networks.	• Independent experts in key content areas are identified and consulted. • Efforts to go beyond a "core network" of contacts to seek out domain-relevant experts, with additional resources and "political capital" potentially expended to gain access to such specialist expertise.
Assess breadth of collaboration: Explanation critique is a different form of collaboration that captures how many different perspectives were incorporated in examining the primary hypotheses.	• Few if any instances of alternative or "outside" criticisms being considered. • Reliance on preexisting channels of critiquing, primarily supervisory.	• Brings alternative perspectives to bear in critiquing the overall intelligence analysis process. • Leverages personal or organizational contacts to examine analytical reasoning. For example, peer analysts or proxy decision makers.	• Familiar as well as independent perspectives have examined the chain of analytical reasoning, explicitly identifying which inferences are stronger and weaker. • Use of formal techniques, such as devil's advocacy or team A/team B (see chapter 6, to challenge and vet hypotheses and explanations. • Expenditure of capital, political or otherwise, in critiquing the intelligence analysis process.

Appendix D

Threat Considerations During Large-Scale Ground Combat Operations

OVERVIEW

D-1. 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 (ADP 3-0). 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.

D-2. Intelligence analysts must be proficient in understanding the threat to ensure they provide quality products and recommendations to commanders and staffs. They should continuously strive to be experts on threat doctrine, capabilities, and equipment. Threat doctrine provides the guidelines a threat often follows or tries to follow during military operations; threat tactics are derived from threat doctrine. Many peer threats require their forces to follow threat doctrine and do not allow these forces to exercise the initiative. Identifying *how* and *when* a threat follows threat doctrine is key to developing COAs. Intelligence analysts must seek the most current (by nation) threat doctrine, capabilities, and equipment from the various U.S. intelligence agencies: Defense Intelligence Agency, NGIC, INSCOM, and several of the DOD organizations responsible for maintaining national threat databases and assessments.

D-3. After mission receipt, analysts should have a basic knowledge of the fundamental maneuver tactics and the combat equipment related to the warfighting functions, which are used to generate threat combat power and access joint and multinational capabilities. Setting the conditions begins with generate intelligence knowledge. Databases and threat signatures developed during generate intelligence knowledge assist in assessing threat capabilities and vulnerabilities during IPB. This information facilitates decision making during the MDMP and provides a common understanding of how friendly forces may gain a position of relative advantage across multiple domains.

D-4. During mission analysis and IPB, analysts reference current intelligence holdings to develop the initial intelligence estimate of the threat situation for the warning order produced during the MDMP. An understanding of the current threat situation enables analysts to recognize potential threat vulnerabilities, which will be developed further during IPB.

D-5. During large-scale ground combat operations, analysts apply their knowledge of threat doctrine, capabilities, and equipment to the OE in order to assess the threat. While maintaining an accurate intelligence threat assessment during combat operations, analysts must be able to—

- **Confirm or deny analytical predictions.** Analysts identify whether or not the threat's actions are consistent with the analytical assessment (for example, validation of the most likely and most dangerous threat COAs).
- **Update the situation template, event template and matrix, and running estimate.** Analysts should recognize the threat's balance of risk and opportunity to create and maintain the conditions necessary to seize, retain, and exploit the threat initiative and achieve decisive results.
- **Assist the commander and staff to update planning.** Analysts continually update the situation template and running estimate to reflect current operations in order to identify windows of opportunity to seize, retain, and exploit the initiative to shape the OE.

THREAT ANALYSIS BY WARFIGHTING FUNCTION

D-6. Analysts must have a detailed knowledge of threat doctrine and capabilities to portray how the threat will conduct operations in a given environment. During the war-gaming step of the MDMP, analysts apply their knowledge of threat doctrine and capabilities. This knowledge enables the staff to determine the threat's likely reaction to friendly COAs and assists the staff in refining the plan recommended to the commander.

D-7. The analysis and predicted implementation of threat doctrine and capabilities must be as accurate and detailed as possible because its inclusion in IPB drives planning. During IPB, this analysis assists the S-2 and S-3 in identifying additional planning considerations and potential operational windows of opportunity for the commander to exploit. Categorizing potential threat capabilities and requirements by warfighting function is a basic way of analyzing the threat. A peer threat force commander is likely to have similar requirements as the Army force commander's requirements. Therefore, categorizing threat elements by warfighting function enables analysts to efficiently convey and commanders and staffs to easily understand threat requirements. Determining the threat's likely requirements assists in determining the threat force commander's likely decision points.

D-8. Intelligence analysts apply techniques and tools to assist them in identifying likely threat requirements, categorized by warfighting function. (See table D-1.) After identifying threat requirements, the S-2 and S-3 collaborate to determine how best to influence the threat's decision-making process.

Table D-1. Threat analysis by warfighting function example

Threat element	*Threat requirements*	*Considerations*	*Support to future friendly operations*
Command and control	Commander's critical information requirements	What must threat commander know to meet the end state?	Provide EEFIs for protection and security.
	CP positioning	How is the threat arrayed on the battlefield?	• Contribute information to the threat overlay. • Provide potential NAIs.
		Does the terrain favor the location of the CPs?	• Identify key terrain. • Identify natural defensive terrain.
		Where are the LOCs that connect CPs across the AO?	Identify AAs
	Commander's location	Which CP has the best defensive posture?	Identify natural defensive terrain.
		What security measures are emplaced at the location?	Identify obstacles for maneuver elements.
		What weapons systems are colocated with the commander?	Develop targets.
	Succession of command	Which personalities would be able to continue operations?	Develop targets.
	Communications guidance	How does the threat communicate throughout the AO?	• Refine the collection plan. • Assess the threat's operations security. • Identify possible bypass routes.
Intelligence	Most likely COA/Most dangerous COA	How much influence can friendly forces apply on the threat?	Identify the threat threshold that would force commitment to a decisive operation.
	Key terrain	What terrain would be advantageous to the threat's mission?	• Develop NAIs. • Identify potential objectives for seizure.
	Weather	What effect will certain weather have on threat operations?	Refine threat COAs.
	Information gaps	What does the threat not know about friendly forces?	• Refine collection plans. • Identify potential threat priority intelligence requirements.
	Intelligence collection guidance	What capabilities is the threat employing to collect information?	• Develop counterreconnaissance plans. • Develop operational security guidelines.

Table D-1. Threat analysis by warfighting function example (*continued*)

Threat element	*Threat requirements*	*Considerations*	*Support to future friendly operations*
Movement and maneuver	Commander's intent	What is the end state the commander is attempting to achieve?	Develop COA criteria.
	Task and purpose of subordinate units	Do projected threat COAs support the threat commander's intent?	COA development
	Task organization	What is the threat command structure?	Develop targets.
	Forms of maneuver	How does the threat conduct specific operations?	Develop threat TTP.
	Reserve composition, mission, priorities, and control measures	How many personnel does the threat have in reserve?	Identify the overall threat strength.
		What is the threat commander's threshold for committing reserve forces onto the battlefield?	Develop COA criteria.
		How will reserve forces operate?	COA development
Fires	• Task and purpose of lethal and nonlethal fires • Schemes of fire	Do projected lethal and nonlethal fires in COAs support the threat commander's intent?	COA development
		What lethal and nonlethal fires capabilities can the threat use?	Develop threat TTP.
		What is the location of fires systems?	Develop NAIs.
		Where would the threat emplace observers?	Develop NAIs.
	Special munitions	Does the threat possess any special munitions?	Adjust planning considerations.
		How much special munitions does the threat possess?	Anticipate potential resupply points.
Protection	Protection priorities	What structures or locations require additional protection?	Refine the collection plan.
		What is the significance of the structures or locations to the threat commander?	Develop high-value targets.
	Terrain factors	Does any terrain provide protection for the threat?	Identify obstacles for maneuver elements.
		What LOCs will the threat prioritize for protection?	• Identify possible AAs. • Develop ways to restrict threat freedom of maneuver.
Sustainment	Sustainment priorities—manning, fueling, fixing, arming, moving the force, and sustaining Soldiers and systems	How will the threat conduct resupply operations?	Develop threat TTP.
		How will the threat refuel vehicles?	• Identify potential LOAs. • Identify AAs. • Identify LOCs for collection.
	Construction of facilities and installations	What types of systems will be needed to degrade threat facilities?	• Identify threat vulnerabilities. • Provide accurate recommendations to friendly capabilities.
	Anticipated requirements of classes III (fuel), IV (fortification), V (ammunition)	How often will the threat require a resupply?	Identify potential threat battle rhythm.

AA avenue of approach
AO area of operations
COA course of action
CP command post
EEFI essential element of friendly information
LOA limit of advance
LOC line of communications
NAI named area of interest
TTP tactics, techniques, and procedures

THREAT EQUIPMENT

D-9. The strengths, vulnerabilities, and functionality of a threat's equipment influence that threat's tactics. Analysts should conduct basic threat equipment analysis combined with threat doctrine for accurate threat capability assessments. Analysis results assist in understanding the threat's ability to employ its capabilities. Understanding the strengths and vulnerabilities of threat equipment by warfighting function assists analysts in identifying key factors about the threat, such as how the threat's equipment status may affect its ability to fight based on threat doctrine, or whether an enemy can go on the offensive, and if so, how far can the enemy advance based on its logistic support. From those factors, analysts can further identify limits of advance and determine the threat's likely objectives. Table D-2, while not all inclusive, provides one way to assist analysts in identifying key factors to consider during large-scale ground combat.

Note. Understanding equipment strengths and vulnerabilities may encompass more than one warfighting function because the equipment may have multiple capabilities. For example, an armored reconnaissance vehicle can fall under the movement and maneuver, intelligence, and protection warfighting functions, as indicated in table D-2, based on its capabilities. In this instance, it is important for analysts to analyze the specific role of the vehicle or unit in order to explain its strengths and vulnerabilities.

Table D-2. Analyst considerations based on threat equipment capabilities

Equipment	*Threat element*	*Description*	*Considerations*	*Strengths and vulnerabilities*
BRM-3K/Kredo 1 (modified BRM for reconnaissance)	**Movement and maneuver**	**Range:** Frag-HE 4000 m (day) 1200–1500 m (night passive sight) 3000 m+ (night-active sight); 4000 m (antiaircraft)	Threat has not been observed conducting night training in 18 months.	• Vehicle can outrange 25-mm bushmaster during daylight hours. • It is unlikely the threat will be proficient on night scopes, providing the advantage to friendly forces.
		Speed: Max road: 70 km/hour Max off-road: 45 km/hour Average cross-country: 35 km/hour Max swim: 10 km/hour **Range:** 600 km (highway)	Open terrain exists throughout the area of operations.	Vehicle will have minimally restricted movement throughout the area of operations.
	Intelligence	• 2-3-m mast with a Kredo-1 radar system • Catherine 2d generation thermal sight extends night range to 5-7 km • 1D22 laser target designator ranges to 7 km	Division capable of detecting radar within 10 seconds of activation.	Threat uses radar to spot targets and call for fire, then quickly transitions to a new location to prevent being targeted.
			Laser designators will enable the threat to send locations rapidly for indirect fires.	When within 7 km of the corps disruption zone and templated reconnaissance positions, units are at an increased risk for indirect fire attack.
	Protection	Six smoke grenade launchers, vehicle engine exhaust systems	Division has reported critical shortages of smoke canisters for the past year.	It is unlikely that smoke will be used for obscuring positions and movement.
		CBRN-automatic overpressure system	Not applicable	Not applicable
		30-355 mm-turret armor (front glacis)	Not applicable	Direct fires from 25 mm or higher are required to penetrate the turret. Tracks are susceptible to .50 caliber direct fire and above for mobility kill.

CBRN chemical, biological, radiological, and nuclear
km kilometer
m meter
mm millimeter

D-10. In-depth analysis of threat equipment assists in nominating equipment critical to the success of the threat's mission. This information assists analysts in nominating HVTs and HPTs for targeting and the S-2 and S-3 in recommending PIRs to the commander. Additionally, it provides friendly forces the ability to exploit threat vulnerabilities by creating defeat mechanisms.

Appendix E
Intelligence Production

OVERVIEW

E-1. The fundamental requirement of intelligence analysis is providing timely, accurate, reliable, and predictive intelligence assessments about the threat and OE to the commander and staff. Therefore, intelligence production requires the dissemination of reports and presentations to support operations. These reports involve various updates to IPB and collection management templates and matrices.

Notes. The development of production and dissemination software in current automation systems enhances intelligence production. DCGS-A and other operational systems must be identified and a location or internet protocol address provided to find maps, overlays, templates, charts, and other analytic techniques and tools.

This appendix contains specific collection requirements and instructions. Unit-level SOP information should not be repeated in the intelligence annex.

INTELLIGENCE PRODUCTS

E-2. The intelligence products described in this appendix are organized based on the following:

- Threat and OE analysis reports.
- Current intelligence reports.
- Supplemental analytical reports.
- Analytical assessments that support orders and briefings.

THREAT AND OPERATIONAL ENVIRONMENT ANALYSIS REPORTS

E-3. The intelligence estimate, intelligence running estimate, and Annex B (Intelligence) to the operation order (OPORD) each maintain an analytical assessment of threat forces' strengths, vulnerabilities, tactics, composition, disposition, training, equipment, and personnel, as well as other OE considerations before, during, and after operations (revision of the original estimate).

Annex B (Intelligence) to the Operation Order

E-4. Commanders and staffs use Annex B (Intelligence) to describe how intelligence supports the concept of operations described in the base plan or order. (See figure E-1 on page E-2.) The purpose of Annex B (Intelligence) is to provide detailed information and intelligence on the characteristics of the OE and to direct intelligence activities. (For more information, see FM 6-0.)

[CLASSIFICATION]

ANNEX B (INTELLIGENCE) to OPERATION ORDER 001

(U) References:

(a) (U) Maps. See base order.

(b) (U) ADP 2-0, FM 2-0, FM 6-0.

(U) Time Zone Used Throughout the Order: *Identify the appropriate time zone.*

1. (U) Situation.

a. (U) Area of Interest. *Describe the area of interest.*

b. (U) Area of Operations (AO). *Describe the AO.*

(1) (U) Terrain. See Tab A (Terrain) to Appendix 1 (Intelligence Estimate) to this annex.

(2) (U) Weather. See Tab B (Weather) to Appendix 1 (Intelligence Estimate) to this annex.

c. (U) Enemy Forces. See Appendix 1 (Intelligence Estimate) to this annex.

d. (U) Friendly Forces. See Annex A (Task Organization).

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. See Annex V (Interagency Coordination).

f. (U) Civil Considerations. See Tab C (Civil Considerations) to Appendix 1 (Intelligence Estimate) to this annex and Annex K (Civil Affairs Operation).

g. (U) Attachments and Detachments. See Annex A (Task Organization).

2. (U) Mission. *Restate the unit's mission*.

3. (U) Execution.

a. (U) Scheme of Intelligence Support. *Describe the intelligence unit's roles and responsibilities in relation to the operation and define priorities of support to subordinate units.*

b. (U) Tasks to Subordinate Units.

(1) (U) *Perform intelligence preparation of the battlefield and situation development, as well as provide analytic support to targeting, information-related activities, protection, and civil affairs operations.*

(2) (U) *Conduct information collection. See Annex L (Information Collection) for specific requirements.*

(3) (U) *Support stability operations, such as Noncombatant Evacuation Operations and foreign humanitarian assistance.*

c. (U) Counterintelligence. See Appendix 2 (Counterintelligence) to this annex.

d. (U) Coordinating Instructions.

(1) (U) Requirements.

(a) (U) Priority Intelligence Requirements (PIRs).

1. (U) PIR #1. *Identify all PIRs in relation to the operation.*
2. (U) PIR #2.
3. (U) PIR #3.

(b) (U) Friendly Force Information Requirements. See base order.

(c) (U) Request for Information (RFI). *Describe the process for handling RFIs.*

(2) (U) Measures for Handling Personnel, Documents, and Materiel.

(a) (U) Prisoners of War, Deserters, Repatriates, Inhabitants, and Other Persons.

(b) (U) Captured Documents and Materiel.

(c) (U) Documents or Equipment Required.

[page number]
[CLASSIFICATION]

Figure E-1. Annex B (Intelligence) to the operation order example

[CLASSIFICATION]

ANNEX B (INTELLIGENCE) to OPERATION ORDER 001

(3) (U) Distribution of Intelligence Products.

(a) (U) *Describe requirements and the process for dissemination of products to and from subordinate units.*

(b) (U) *Subordinate units will submit a daily graphic intelligence summary (GRINTSUM) covering 24 hours (0001L - 2400L) NLT 0600L. The GRINTSUM must include a summary of all significant activities within subordinate units' AOs, a current near-term assessment of the AO, and a rollup of all reporting across every intelligence discipline (signals intelligence, human intelligence, and any interrogation summaries) originating in the AO.*

3. (U) Sustainment. See Annex F (Sustainment).

4. (U) Command and Signal.

a. (U) Command.

(1) (U) Location of Key Intelligence Leaders. *The division G-2 will be colocated with the division commander during all phases of the operation.*

(2) (U) Intelligence Liaison Requirements. *The division G-2 does not require intelligence liaison personnel from subordinate units. Subordinate units' organic liaison officer can execute intelligence liaison duties.*

b. (U) Control.

(1) (U) Command Posts (CPs). *The division main CP is located in the vicinity of military grid reference system (MGRS) 12A BC 1234 5678. The division main CP in the vicinity of MGRS 12A BC 2345 6789.*

(2) (U) Intelligence Coordination Line. See Annex L (Information Collection).

c. (U) Signal. See Annex H (Signal).

ACKNOWLEDGE:

COMMANDER
BG

OFFICIAL:

DEBORD
G-2

ATTACHMENTS:
Appendix 1–Intelligence Estimate
Appendix 2–Counterintelligence
Appendix 3–Signals Intelligence
Appendix 4–Human Intelligence
Appendix 5–Geospatial Intelligence
Appendix 6–Measurement and Signature Intelligence
Appendix 7–Open-Source Intelligence

[page number]
[CLASSIFICATION]

Figure E-1. Annex B (Intelligence) to the operation order example (*continued*)

Intelligence Estimate

E-5. An *intelligence estimate* is the appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view of determining the courses of action open to the enemy or adversary and the order of probability of their adoption (JP 2-0). Since intelligence analysts will have performed IPB to support the commander's MDMP effort and likely participated in a thorough staff war-gaming effort to validate friendly and threat COAs, the intelligence estimate is a version of the staff planning effort and part of the larger OPORD. (See figure E-2 on page E-4.)

E-6. The intelligence staff develops and maintains the intelligence estimate to disseminate information and intelligence that define the threat COA along with the requirements to determine the adoption of a COA. The assessments in the intelligence estimate of COA development, including threat strengths, compositions, dispositions, and vulnerabilities, form the basis for future intelligence analytical requirements.

[CLASSIFICATION]

APPENDIX 1 (INTELLIGENCE ESTIMATE) to ANNEX B (INTELLIGENCE) OPERATION ORDER 001

(U) References:
(a) (U) Maps. See base order.
(b) (U) ADP 2-0, FM 2-0, FM 6-0, ATP 2-01.3, World Equipment Guide (2016).

(U) Time Zone Used Throughout the Order: *Identify the appropriate time zone.*

1. (U) Situation.
a. (U) Area of Interest. See Exhibit 1 to Tab A.
b. (U) Area of Operations. See Exhibit 2 to Tab A.
(1) (U) Terrain. See Tab A (Terrain) to this appendix.
(2) (U) Weather. See to Tab B (Weather) to this appendix.
c. (U) Enemy Forces.
(1) (U) Composition. *The Operational Strategic Command-South (OSC-S) comprises four division tactical groups and one Reserve Component unit*.
(2) (U) Disposition. *The OSC-S underwent intense collective maneuver training before advancing south*.
(3) (U) Capability.
(a) (U) *OSC-S regular formations maintain an overall 80% operational readiness rate*.
(4) (U) Enemy Courses of Action (ECOAs). See Exhibit 3 (ECOA Sketch) to Tab D (Intelligence Preparation of the Battlefield-Products) to this appendix.
(a) (U) ECOA 1.
(b) (U) ECOA 2.
c. (U) Friendly Forces. See Annex A (Task Organization).
d. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. See Annex V (Interagency Coordination).
e. (U) Civil Considerations. See Tab C (Civil Considerations) to this appendix.
f. (U) Attachments and Detachments. See Annex B (Intelligence).
g. (U) Assumptions. See Annex B (Intelligence).
2. (U) Mission. See Annex B (Intelligence).
3. (U) Execution. See Annex B (Intelligence).
4. (U) Sustainment. See Annex B (Intelligence).
5. (U) Command and Signal. See Annex B (Intelligence).

ACKNOWLEDGE:

COMMANDER
BG

OFFICIAL:

DEBORD
G-2

ATTACHMENTS:
Tab A–Terrain
Tab B–Weather
Tab C–Civil Considerations
Tab D–Intelligence Preparation of the Battlefield-Products

[CLASSIFICATION]

Figure E-2. Appendix 1 (Intelligence Estimate) example

Intelligence Running Estimate

E-7. Effective plans and successful execution hinge on accurate and current running estimates. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if the planned future operations are supportable (ADP 5-0). Failure to maintain accurate running estimates may lead to errors or omissions that result in flawed plans or bad decisions during execution. Each staff element is responsible for updating its portion of the running estimate as the operation unfolds.

E-8. The intelligence running estimate enables the intelligence operational officer/noncommissioned officer to continually update the commander on the mission execution from the intelligence perspective. Unlike other intelligence products, the intelligence running estimate combines both the analysis of friendly and allied forces' intelligence activities to support current operations.

E-9. Figure E-3 illustrates an example intelligence running estimate. The analysis focuses on current threat activities, strengths, and assessed intent/objectives to provide the commander and associated reporting requirements with a consistent summary of the threat. As the operation progresses, the collaborative effort may involve further analysis of the terrain and weather, monitoring the flow of displaced persons on the battlefield as inhibitors to friendly force maneuverability, and, when necessary, additional security requirements.

Note. In the highly volatile large-scale ground combat environment, the intelligence operational officer along with the all-source intelligence analyst are likely to maintain the running estimate.

[CLASSIFICATION]

INTELLIGENCE RUNNING ESTIMATE NUMBER___

(U) DATE-TIME GROUP:

(U) REFERENCES: Maps, charts, or other documents.

1. **(U) MISSION:** The commander determines the unit's mission.
2. **(U) AREA OF OPERATIONS (AO):** Describe the existing situation in the AO based on:
   a. **Terrain.** How terrain affects a functional area's capabilities.
   b. **Civil Considerations.** Description of areas, structures, capabilities, organizations, people, and events.
   c. **Weather.** How weather affects friendly and threat warfighting function capabilities.
3. **(U)ENEMY SITUATION:** Summary of each threat characteristic that can influence mission accomplishment:
   a. **Composition.**
   b. **Disposition.** Geographic location of threat elements and how they are deployed or employed.
   c. **Strength.** Committed forces, reinforcements, air, and chemical, biological, radiological, nuclear, and high-yield explosive weapons.
   d. **Tactics and Training.** Strategy, methods of operations, doctrine, tactics, and training.
   e. **Sustainment.** Procurement, maintenance, distribution, and materiel replacement.
   f. **Operational Effectiveness.** Threat morale, weapons effectiveness, equipment readiness, leadership, and personnel.
   g. **Intelligence.** Estimate of the threat's intelligence collection capability.
   h. **Communications.** The threat's communications modes.
   i. **Other.**
4. **(U) ENEMY CAPABILITIES:** In conventional operations:
   a. **State Enemy's Capabilities.** *What*, *where*, *when*, and in what *strength* for each capability.
   b. **State Enemy's Limitations.** Cause and effect of each limitation.
   c. **Analysis and Discussion.** Effect of capabilities on terrain, civil considerations, weather.
5. **(U) CONCLUSIONS:** Conclusions based on information and analysis about the total effects of the AO on threat operations.

ACKNOWLEDGE: [Designated Staff Officer's Name and Designation]
OFFICIAL: [Authenticator's Name and Position]

[CLASSIFICATION]

Figure E-3. Intelligence running estimate example

CURRENT INTELLIGENCE REPORTS

E-10. Current intelligence reports address the current reporting of threat activities on the battlefield. The goal is to provide the commander with predictive analysis of the threat's intentions for future operations based on what conditions occurred by either threat or friendly actions during the past reporting period. This requires extensive intelligence analytical rigor in assessing threat activities and vigilance to the friendly scheme of maneuver.

Intelligence Summary

E-11. The intelligence summary (also known as INTSUM) is a periodic publication of the G-2/S-2 assessment of the threat situation on the battlefield. It provides the commander with context to support decision making based on the G-2/S-2's interpretation and conclusions about the threat, terrain and weather, and civil considerations over a designated period of time. This is typically identified in unit SOPs and in associated OPORD reporting instructions. The intelligence summary also provides COA updates based on the current situation. Unit SOPs designate the command's format for preparing and disseminating an intelligence summary. At a minimum, the intelligence summary should contain the paragraphs and subparagraphs as shown in figure E-4.

[CLASSIFICATION]

INTELLIGENCE SUMMARY (INTSUM) NUMBER____

(U) References: Maps, charts, overlays, and other relevant documents are available at internet protocol address.

(U) Time Zone Used Throughout the Order: ZULU

1. (U) WEATHER. The weather occurring within the operational environment (OE) will affect friendly and threat warfighting capabilities. This assessment is based on the weather officer and intelligence analyst's evaluation of the impact of specific environment conditions on friendly and threat forces. Normally, current and future weather conditions are displayed as far out as five days.

2. (U) SITUATION HIGHLIGHTS. A summary of the OE situation as it has evolved over the reporting period. Highlighted subparagraphs are as follows:

a. **Air:** Highlights of the current air situation. When in conflict with a threat possessing a capable air force, it is critical to the commander to identify whether or not friendly air power has achieved control of the operational airspace. This includes aircraft and air defense interlocking measures.

b. **Land:** Highlights of the current ground situation, usually divided by area of operations. If there are three divisions forming, the forward battle area along with a corps consolidation area and multiple division consolidation areas, then the land portion can be divided in that manner. Additionally, the main effort is often annotated first followed by the secondary and then any guerrilla or insurgent activities in the consolidation areas.

c. **Maritime:** Highlights of the current maritime situation. Maritime operations are as critical as air lift and air supremacy.

d. **Space:** Highlights of the current space situation. Space operations, including space weather, is critical to all operations whether the threat is capable of operating in this domain.

e. **Cyberspace:** Highlights of the current cyberspace situation. Cyberspace operations are critical to all operations whether the threat is capable of operating in this domain.

f. **Information Environment:** Highlights of the current information environment situation.

g. **Electromagnetic Spectrum:** Highlights of the current electromagnetic spectrum situation.

h. **Civil or Other Considerations:** Highlights of the current civil situation. Knowledge of the civilian population and civilian authorities/government is critical to the commander's situational understanding.

[CLASSIFICATION]

Figure E-4. Intelligence summary example

[CLASSIFICATION]

3. (U) SUMMARY OF THE ENEMY SITUATION. Each subparagraph of the threat situation is oriented on the commander's priority intelligence requirements (PIRs) and other information requirements as the basis for the analysis and assessment. The subparagraphs are as follows:

a. **Land:** The analysis of the land situation must include threat and possible insurgent activities detected during the INTSUM reporting period. Each echelon should publish at least one INTSUM daily, but it is likely that brigade and below commands in the forward combat zones will publish an INTSUM every 12 hours and in some missions even sooner. Based on the echelon, it is important for the analysis to consider terrain, weather, and the threat composition and disposition over the next 12 or more hours of combat. If in the consolidation area, the assessment must focus on the friendly forces' ability to support the forward battle with supplies and reinforcements as needed.

b. **Air:** The analysis of the air and air defense situation must focus on the threat air capability to gain or retain control of the air domain. Even when the threat air power is near depletion, ground air defense and even artillery or missile threats may still have a direct impact on friendly air operations—fixed or rotary wing.

c. **Maritime:** The analysis of the maritime situation must focus on the threat naval capability to gain or retain control of the maritime domain. This includes the ability of the threat maritime assets to support threat ground operations within distance of the sea.

d. **Other Domains:** Advise the commander of the other domains in which the threat may have opportunities to deny, impede, or disrupt friendly operations.

e. **Other:** The battlefield will be congested before, during, and after engagements. Any other considerations that answer PIRs or other requirements may enable the commander's decision making.

4. (U) UNIT ASSESSMENT. In each subparagraph, provide an analysis of current and possibly future threat courses of actions (COAs). All discussions of threat COAs must match what has been identified in the military decision-making process effort. If the threat COA has changed since that time, the G-2/S-2 should update the commander and staff to ensure the INTSUM is not the first notification. The subparagraphs are as follows:

a. **Most Likely COA:**

b. **Most Dangerous COA:**

c. **Other:** Other is reserved for other likely developments in civil considerations or a reiteration of pending serve weather.

5. (U) ENEMY MOVEMENT DURING THE REPORTING PERIOD. Provide all-source intelligence analysts a way to present various forms of identifying major threat units (including at least two levels below that of the reporting command) and coordinates to the last known positions. The information may be presented in written form, on a spreadsheet, or as a graphic summary, which should include where in DCGS-A other intelligence organizations may find this information.

6. (U) PIRs. Provide the commander's PIR list and, when possible, identify which PIRs have been answered. PIRs that have not been answered require explanations as to why they have yet to be answered.

7. (U) REPORTS AND DISTRIBUTION. Provide key reporting and distribution instructions from each echelon as well as reporting guidance from subordinate units. This includes the dissemination of reports, summaries, and dissemination requirements from subordinate echelon reporting. The Army uses DSCG-A and each echelon publishes associated procedures for the exchange/publication of various threat databases and reporting. Also provide authentication of the report.

[CLASSIFICATION]

Figure E-4. Intelligence summary example (*continued*)

Graphic Intelligence Summary

E-12. The graphic intelligence summary (also known as GRINTSUM) can be included with the intelligence summary or disseminated as a separate analytical report. It is a graphical representation of the intelligence summary, with emphasis on the threat forces location compared to friendly forces' location. The graphic intelligence summary also includes current PIRs and a summary of threat activities. (See figure E-5 on page E-8.) Since the emphasis of a graphic intelligence summary is graphical, most of the written details should be captured in the intelligence summary or an accompanying report.

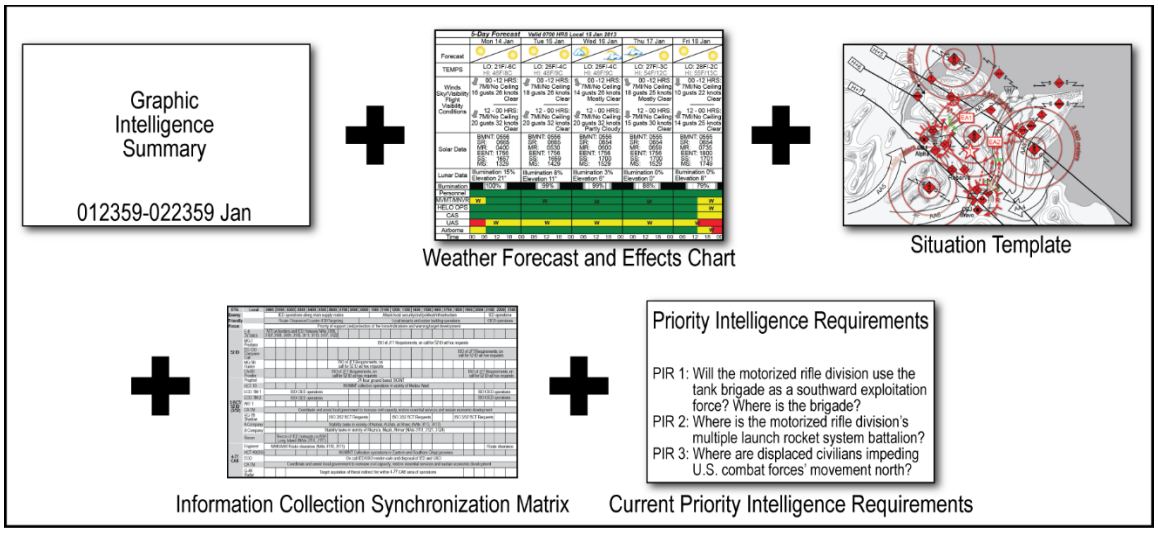


Figure E-5. Graphic intelligence summary example

E-13. There are challenges with using the graphic intelligence summary:

- The size of the graphical portrayal of the OE is often driven by critical facts about the threat that must be shown. Therefore, it is advisable to begin with a general OE map and zoom in on key areas. Ensure the written assessment includes the necessary details by either referencing the accompanying intelligence summary or other report or including the details in the Notes page of a PowerPoint slide.
- The file size must follow the commander's guidance or unit SOPs. Typically, the graphic intelligence summary is one or two graphics (PowerPoint slides) and limited in bit size for ease in emailing and posting on unit web portals. In a tactical large-scale ground combat environment, a brigade or lower command may be unable to send or receive a megabit plus-size file.

Intelligence Report

E-14. The intelligence report (also known as INTREP) demonstrates the importance of intelligence analysis. It is a standardized report, typically one page, used to establish a near current-threat operational standpoint. It points to the threat's responses to friendly actions and the battlefield environment. Intelligence reports may also highlight time-sensitive critical activities that require corroboration with other units and higher echelons. An intelligence report's basic information requirements describe *who*, *what*, *when*, *where*, *why,* and *how* facts in order to provide a conclusion. (See figure E-6.) There is no established timeline for disseminating an intelligence report. Some units may publish one or two daily, while others may publish 15 or 20 reports daily, depending on the activity level of engaging threat forces.

[CLASSIFICATION]

INTELLIGENCE REPORT NUMBER____

(U) References: Maps, charts, overlays, and other relevant documents used to create the intelligence report.

(U) Time Zone Used Throughout the Order: Applicable time zone during the time or reporting.

(U) Commander's Priority Intelligence Requirement: The applicable priority intelligence requirement to which the intelligence report is related.
(U) Summary of Activity: Brief discussion of the threat's general situation or activities, covering the *who*, *what*, *when*, *where*, *why*, and *how*, which support the analyst's conclusion.
(U) Authentication: Authentication by and instructions on handling and destroying.

[CLASSIFICATION]

Figure E-6. Intelligence report example

SUPPLEMENTAL ANALYTICAL REPORTS

E-15. Supplemental analytical reports, such as the periodic intelligence and supplementary intelligence reports, do not fall into a predetermined dissemination timeline. Periodic intelligence reports and supplementary intelligence reports follow a similar format, designated by a senior operational intelligence officer and staff. These reports allow for expanded analytical efforts, providing assessments of a technical or historical comparative nature. However, once the analysis begins to shape an assessment of threat intentions or capabilities, the urgency for releasing these analytical reports may increase.

Periodic Intelligence Report

E-16. The periodic intelligence report (also known as PERINTREP) is a summary of the intelligence situation that covers a longer period than the intelligence summary. (See figure E-7.) It is a means of disseminating detailed information and intelligence, including threat losses, morale, assessed strength, tactics, equipment, and combat effectiveness.

E-17. The periodic intelligence report includes but is not limited to sketches, overlays, marked maps or graphics, and annexes, providing a written and visual representation of the information and/or intelligence. The report is disseminated through the most suitable means based on its volume and urgency.

[CLASSIFICATION]

PERIODIC INTELLIGENCE REPORT NUMBER_____

(U) Period Covered: Date and time to date and time.

(U) References: Maps or charts.

(U) Disposal Instructions: If applicable.

(U) GENERAL ENEMY SITUATION. Briefly summarize threat operations during the period. Furnish amplifying details in the paragraphs that follow and in appropriate annexes or both. Also provide brief highlights of the threat situation and the significance of the threat's major activities, including marked changes in morale, strength, tactics, equipment, and combat effectiveness. Data that is lengthy or can conveniently be shown graphically is presented in annexes.

(U) ENEMY ACTIVITIES. Provide, in conjunction with the paragraphs that follow, details of the situation summarized in paragraph 1. Maximum use of sketches, overlays, marked maps or graphics, and annexes provide written and visual representations of the information and/or intelligence. Omit subparagraphs when appropriate intelligence is not available or is adequately covered by other portions of this report.

(U) ENEMY ORDER OF BATTLE. As appropriate, provide the threat order of battle in the following subparagraphs:

a. **Composition and Disposition.** Include land (airborne, artillery, rocket/missiles, air defense) air, maritime, space, cyberspace, information environment, and the electromagnetic spectrum.
b. **Strength.** Personnel and equipment/weapon losses.
    1. Losses (Killed in Action, Wounded in Action, and Captured).
    2. Assessed or Known Battle Damage Assessment.
    3. Key Personalities and Morale if Known.
    4. Current Strength.
c. **Tactics and Training.**
d. **New Tactics, Weapons, and Equipment.**
e. **Combat Service Support.**
f. **Combat Effectiveness.**
g. **Miscellaneous Details.**
    1. Civil.
    2. Communications (Electronics and Telecommunications).
    3. Electronic Warfare.
    4. Counterintelligence (Sabotage or Espionage).

[page number]

[CLASSIFICATION]

Figure E-7. Periodic intelligence report example

[CLASSIFICATION]

(U) OTHER INTELLIGENCE. Provide a detailed summary of the findings of other intelligence such as technical reports, interrogations, and/or document translations.

a. Technical intelligence summary includes detailed analysis of captured military equipment, communications devices, and can include explosive reports. While this information may not provide current information on the threat situation, it details enemy tactics, techniques, and procedures; new or modified equipment details, and critical information on improvised explosives. Most of the technical information comes from the Department of Defense and the national analysis from the Army's National Ground Intelligence Center.
b. Enemy prisoner of war interrogation reports from human intelligence teams provide key information about the threat forces' leadership, strength, and other details to support future cross-cuing efforts.
c. Translation of captured enemy documents provides similar details of threat capabilities, possible information on supplies, communications securities, and other key military operational details.
d. Additional details on weather and climate summaries.

(U) WEATHER. Provide an update on the impact of weather on future operations. Weather graphics can be presented in the annex as necessary.

(U) TERRAIN. Provide an update on the impact of terrain on future operations. If necessary, use annexes to provide special maps, overlays, and electronic data.

(U) ANALYSIS AND DISCUSSION. List and briefly discuss threat capabilities and vulnerabilities based on the information revealed. The conclusions present the commander's assessment of the most probable courses of actions available to the threat, probability of their adoption, and vulnerabilities that are exploitable by own, higher, adjacent, or lower commanders.

a. Enemy Capabilities.
b. Enemy Vulnerabilities.
c. Conclusions.

(U) REPORTS AND DISTRIBUTION. Provide key reporting and distribution instructions from each echelon as well as reporting guidance from subordinate units. Include the dissemination of reports, summaries, and dissemination requirements from the subordinate echelon's reporting. The Army uses DSCG-A, and each echelon publishes associated procedures for the exchange/publication of various threat databases and reporting. Also provide authentication of the report.

[page number]
[CLASSIFICATION]

Figure E-7. Periodic intelligence report example (*continued*)

Supplementary Intelligence Report

E-18. The supplementary intelligence report (also known as SUPINTREP) is a comprehensive analysis of one or more specific subjects, typically the result of a request or to support a particular operation. This report is formatted similarly to a periodic intelligence report, but it addresses analysis over an extended period of time. Typically, the detailed analysis is from an accumulation of national assessments of threat actions, tactics, and doctrine identified during combat—normally a post-combat review. Maximum use of sketches, photos, overlays, marked maps or graphics, and annexes provides a written and visual representation of the information and/or intelligence. The supplementary intelligence report is disseminated based on the intelligence it contains and the commander's requirements.

E-19. Specific reports may pertain to but are not limited to the following:

- Technical intelligence summary includes detailed analysis of captured military equipment, communications devices, and can include post-explosive reports.
- Enemy prisoner of war interrogation reports from tactical to national sources.
- Translation of captured enemy documents (DOMEX).
- Cyberspace security updates.
- Medical or environmental hazards.
- Changes to civil political and other civilian authorities.

ANALYTICAL ASSESSMENTS THAT SUPPORT ORDERS AND BRIEFINGS

E-20. In addition to designated intelligence production requirements, the intelligence staff also provides analytical assessments to orders, briefings, and staff events, as described in FM 6-0. (See table E-1.) Normally, the intelligence analysis identifies the current threat situation and assessed threat capabilities (often tied to a threat COA); the same information exists in the intelligence summary, intelligence report, and intelligence running estimate. For intelligence analysts, the commander, and often the key staff officer, defines the requirement and may provide additional detailed requirements in unit SOPs.

Table E-1. Support to orders and briefings

Orders			
Reports	***Echelon***	***Dissemination timeline***	***General description***
Operations summary	All	Daily	The commander provides to higher, adjacent, and lower a daily (or twice daily) operations summary that includes an intelligence assessment of threat forces' actions, intent, and assessed strength.
Operation order	All	As needed	The operation order is the same as the intelligence estimate identified in the operation order as Annex B (Intelligence).
Warning order	All	As needed	The G-2/S-2 provides a summary update to paragraph 1.c *Enemy Forces* to the warning order.
Fragmentary order	All	As needed	The G-2/S-2 provides a summary of the threat activity to paragraph 1 *Situation* and as the mission requires to paragraph 3 *Execution*.
Staff briefings			
Briefing	***Echelon***	***Dissemination timeline***	***General description***
Battle update brief	All	Daily	The G-2/S-2 provides an assessment of the threat forces and identifies collection opportunities or requirements to answer the commander's priority intelligence requirement (PIR).
Military decision-making process (MDMP)	All	As needed	The G-2/S-2 provides intelligence analysts to support the planning and war-gaming efforts associated with the commander's MDMP requirements. Normally, the intelligence analysis is in the form of the intelligence preparation of the battlefield steps.
Operations and intelligence brief	All	Likely daily	The G-2/S-2 provides an assessment of the threat forces and identifies collection opportunities or requirements to answer the commander's PIR.
Targeting board	All	As needed	The G-2/S-2 provides an assessment of the threat actions in the high-payoff target and high-value target criteria established by the commander. (See appendix F for more details on intelligence analysis support to targeting.)
After action report	All	As needed	The after action report is a method of capturing lessons learned or, in some cases, identifying what caused a friendly action to occur. In specific cases, the G-2/S-2 may be required to provide a summary assessment of the threat actions that caused a friendly action. (See FM 6-0.)
G-2/S-2 division or corps/battalion or brigade intelligence staff officer			

This page intentionally left blank.

Appendix F

Intelligence Support to Targeting

OVERVIEW

F-1. The targeting effort is cyclical and closely tied to combat assessments. Targeting is a complex and multidiscipline effort that requires coordinated interaction among many command and staff elements. The functional element necessary for effective collaboration is represented in the targeting working group. Intelligence analysts perform a number of critical tasks as part of this working group and the overall targeting effort. (See ATP 3-60 for more information on targeting.)

TARGETING GUIDELINES

F-2. The threat presents a large number of targets that must be engaged with available information collection assets and attack assets. The targeting process assesses the benefits and the costs of engaging various targets in order to achieve the desired end state. Adhering to the five targeting guidelines should increase the probability of creating desired effects while diminishing undesired or adverse collateral effects:

- Targeting focuses on achieving the commander's objectives.
- Targeting seeks to create specific desired effects through lethal and nonlethal actions.
- Targeting directs lethal and nonlethal actions to create desired effects.
- Targeting is a fundamental task of the fires warfighting function that encompasses many disciplines and requires participation from many staff elements and components.
- Targeting creates effects systematically.

TARGETING GUIDANCE AND CATEGORIES

F-3. The commander's targeting guidance must be articulated clearly and simply to enhance understanding. The guidance must be clearly understood by all warfighting functions, especially by the intelligence staff. Targeting guidance must focus on essential threat capabilities and functions that interfere with the achievement of friendly objectives.

F-4. The commander's targeting guidance describes the desired effects to be generated by fires, physical attack, cyberspace electromagnetic activities, and other information-related capabilities against threat operations. Targeting enables the commander, through various lethal and nonlethal capabilities, the ability to produce the desired effects. Capabilities associated with one desired effect may also contribute to other effects. For example, delay can result from disrupting, diverting, or destroying threat capabilities or targets. Intelligence personnel should understand and only use the 14 terms used in ATP 3-60 to describe desired effects:

- Deceive.
- Defeat.
- Degrade.
- Delay.
- Deny.
- Destroy.
- Destruction.
- Disrupt.
- Divert.
- Exploitation.
- Interdict.
- Neutralize.
- Neutralization.
- Suppress.

F-5. To effectively target the threat, friendly forces use deliberate and dynamic targeting. Deliberate targeting prosecutes planned targets, while dynamic targeting prosecutes targets of opportunity and changes to planned targets. During both categories of targeting, friendly forces may prosecute normal, time-sensitive, and sensitive targets.

TARGETING METHODOLOGY

F-6. The targeting methodology organizes the efforts of the commander and staff to accomplish key targeting requirements. This methodology is referred to as the *decide*, *detect*, *deliver*, and *assess* methodology. The methodology assists the commander and staff in deciding which targets must be acquired and engaged and in developing options to engage those targets. Options can be lethal or nonlethal, organic, or supporting assets at all levels as listed—maneuver, electronic attack, psychological, attack aircraft, surface-to-surface fires, air to surface, other information-related capabilities, or a combination of these operations.

F-7. The *decide*, *detect*, *deliver*, and *assess* methodology is an integral part of the MDMP. During the MDMP, targeting becomes more focused based on the commander's guidance and intent. A very important part of targeting is identifying potential fratricide situations and the necessary coordination measures to positively manage and control the attack of targets. These measures are incorporated in the coordinating instructions and appropriate annexes of the operation plan or OPORD.

DECIDE

F-8. The *decide* function of the targeting methodology provides the overall focus and sets priorities for information collection and attack planning. It is the most important targeting function and requires close interaction between the intelligence, plans, operations, and fires cells, and the servicing judge advocate. This step draws heavily on the staff's knowledge of the threat, a detailed IPB (which occurs simultaneously), and a continuous assessment of the situation. Targeting priorities are addressed for each phase or critical event of an operation. The decisions made are reflected in visual products as follows:

- **HPT list.** The *high-payoff target list* is a prioritized list of high-payoff targets by phase of the operation (FM 3-09). 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). An HPT is an HVT that must be acquired and successfully engaged for the success of the friendly commander's mission. A *high-value target* is a target the enemy commander requires for the successful completion of the mission (JP 3-60).
- **Information collection plan.** The information collection plan focuses the collection effort to answer PIRs and other significant requirements. If an HPT is not designated as a PIR, it must still be supported by collection. The information collection plan usually supports the acquisition of more HPTs. (See ATP 2-01.)
- **Target selection standard matrices.** These matrices address accuracy or other specific criteria requiring compliance before targets can be attacked.
- **Attack guidance matrix.** The *attack guidance matrix* is a targeting product approved by the commander, which addresses the how and when targets are engaged and the desired effects (ATP 3-60).

Intelligence Preparation of the Battlefield

F-9. In the same manner that targeting involves coordinated interactions among the commander and entire staff, IPB involves the active participation of the entire staff. The interactions between intelligence personnel and fires personnel are important during the IPB process. (For more information on staff collaboration during IPB, see ATP 2-01.3.) Many of the IPB products significantly influence or are brought forward into the targeting effort. These products assist in target value analysis and war gaming. Some examples of important IPB products include—

- The modified combined obstacle overlay.
- Civil considerations (ASCOPE) products.
- Weather effects products.

- Threat models with recommended HVTs.
- Situation templates with threat time phase lines.
- Event templates and matrices, which have named areas of interest (NAIs).

Target Value Analysis and War Gaming

F-10. From the coordination and work performed during the IPB effort, the targeting working group, especially the intelligence staff and targeting officer, perform target value analysis that yields HVT lists (which may include high-value individual lists) for a specific threat COA. Target value analysis continues the detailed analysis of relevant threat factors, including doctrine, tactics, equipment, capabilities, and expected actions for a specific threat COA. The target value analysis process identifies HVT sets associated with critical threat functions.

F-11. Target spreadsheets (or target folders, as appropriate) identify an HVT compared to a type of operation. Target spreadsheets give detailed targeting information for each HVT, which is used during IPB and war gaming. The intelligence staff and targeting officer collaborate to develop and maintain the target spreadsheet.

F-12. The targeting working group develops HVTs for lethal and nonlethal targeting. For nonlethal targeting, there is no limit on how creative and flexible the working group can be when focusing targeting requirements to support the commander's guidance. In certain circumstances, an HVT may not be focused on a certain geographic area.

F-13. The following assists in identifying and evaluating HVTs:

- Identify HVTs from threat models, situation templates with time phase lines, existing intelligence studies, database evaluations, patrol debriefs, and reporting. The following provide useful information:
  - A review of threat tactics, techniques, and procedures.
  - Previous threat operations.
  - Understanding the threat's objective, tasks, purpose, and intent.
- Identify assets that are key to executing the primary operation 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.
- 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 HVTs varies over the course of an operation. Identify and annotate changes in value by phase of the operation. The following are additional considerations:
  - Use all available intelligence sources (for example, patrol debriefs, reporting) to update and refine the threat models.
  - Categorize the updates to reach a conclusion concerning the threat's operations, capabilities, and vulnerabilities.

F-14. HVTs are finalized and prioritized during war gaming. The staff analyzes and identifies those HVTs that must be attacked to ensure mission success. Additionally, the staff analyzes all implications of attacking those HVTs and possible threat counteractions. Those critical HVTs that the staff confirms as acquired and attacked are nominated as HPTs. Then, the staff groups HPTs into a list, associating the HPTs to a specific point in the battle. The completed HPT list is submitted to the commander for approval.

F-15. During war gaming, the commander and staff identify the best places to attack an HPT. These places are known as target areas of interest (TAIs). A TAI is a point or area where the commander can acquire and engage HPTs. The shape of a TAI reflects the type of threat, target, and weapon system that will engage the target.

F-16. The staff may need to develop additional NAIs to support TAIs. NAIs for nonlethal targets may include religious buildings, places of worship, and shrines that are important to assessing key civil considerations (ASCOPE). Decision points or decision time phase lines are used to ensure the decision to engage or not to engage occurs at the proper time. Decision points and TAIs are recorded on the decision support template.

F-17. A thorough war gaming effort ensures the staff sets the foundation for a successful targeting effort. The purpose of war gaming includes building staff running estimates and developing the scheme of maneuver, scheme of fires, and decision support template. The process also synchronizes the attack guidance matrix with the decision support template and ensures the information collection plan supports all HPTs.

Target Selection

F-18. Target selection depends on the ability to acquire the target. The collection manager must be closely involved in ensuring information collection on HPTs is carefully synchronized into the information collection plan. This task includes breaking HPTs into subsets, when necessary; developing adequate collection tasks; and considering the use of cueing, collection redundancy, and sensor mix during the development of the information collection synchronization matrix. (See ATP 2-01 for more information.)

High-Payoff Target List

F-19. Once prioritized, targets are placed on the HPT list and approved by the commander. Figure F-1 provides an example of an HPT list. The list identifies HPTs by operational phase or specific time windows and order of priority. Other considerations include—

- The sequence or order or appearance.
- The ability to detect, identify, classify, locate, and track the target.
- The degree of accuracy of the acquisition system.
- The ability to engage the target.
- The ability to achieve the desired effects based on the attack guidance.

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 F-1. High-payoff target list example

Target Selection Standards

F-20. Target selection standards are criteria applied to threat activity and used to decide whether the activity is a target. There are two target selection standard categories:

- Targets, which meet accuracy and timeliness requirements for engagement.
- Suspected targets, which must be confirmed before any engagement.

F-21. Target selection standards are based on the threat's activity and available weapon system. The following elements are used to develop the standards:

- Weapon system target location accuracy requirements (target location error).
- Size of threat activity.
- Status of the activity (moving or stationary).
- Timeliness of the information.

F-22. The BCT can develop target selection standards based on anticipated threat characteristics and template threat activities. Different target selection standards may exist for a given threat activity based on different attack systems. For example, a threat artillery battery may have a 150-meter target location error criterion for attack by cannon artillery and a one-kilometer requirement for attack helicopters. The fires cell develops target selection standards in conjunction with the intelligence cell. Units may develop their own worksheet format. Intelligence analysts use the standards to quickly determine targets from combat information and pass the targets to the fires cell.

F-23. The fires cell uses target selection standards to identify targets for attack. Certain situations require the systems to identify friendly and neutral from threats before approval to engage in lethal fire. HPTs that comply with the criteria are tracked until they are attacked in accordance with the attack guidance matrix. Target locations that do not comply with the standards are confirmed before attacked.

F-24. Target selection standards can be depicted in a matrix. Figure F-2 is an example of a target selection standard matrix. Although not shown in figure F-2, it may include a column that lists each friendly information collection system that forwards targets directly to the fires cell or fires direction center. The effects of terrain and weather on information collection assets and threat equipment are considered. While target selection standards are developed specific to the situation, the greatest emphasis is on considering the threat situation, possibility of threat deception, and the reliability of the source or agency that is reporting.

High-Payoff Target	*Timeliness*	*Accuracy*
2S3	30 minutes	500 meters
M-46	30 minutes	500 meters
Air and missile defense	15 minutes	500 meters
Command posts	3 hours	500 meters
Ammunition	6 hours	1 kilometer
Maneuver	1 hour	150 meters

Figure F-2. Example target selection standard matrix

Attack Guidance

F-25. Analyzing target vulnerabilities and the effect an attack has on threat operations within the context of the commander's targeting guidance allows the staff to propose the most efficient available engagement option. During war gaming, decision points linked to events, areas (NAIs and TAIs), or points within the AO are developed. These decision points cue command decisions and staff actions when a tactical activity is needed.

F-26. Based on the commander's guidance, the targeting team recommends target engagement in terms of the effects of fire and attack options. The intelligence staff must understand the definitions of and nuances for each of the 14 terms used to describe desired effects. Desired effects are then translated into automation system values to more effectively engage targets.

F-27. Deciding on which attack system to use occurs simultaneously as deciding when to acquire and attack the target. When deciding to attack by two different means, such as electronic warfare and combat air operations, coordination is required. Coordination requirements are recorded during the war game.

F-28. The commander, with recommendations from the targeting working group, approves the attack guidance, which is more than the attack guidance matrix. The attack guidance details the following:

- An updated prioritized HPT list.
- When, how, and the desired effects of engagement.
- Special instructions.
- BDA requirements.

F-29. This information is developed during the war game. Attack guidance is provided to weapon systems managers via the attack guidance matrix, which, at a minimum, includes—

- Specific HPTs.
- Timing of engagement.
- How targets are engaged.
- Desired effects.
- Remarks, including restrictions.

Target Development

F-30. *Target development* is the systematic examination of potential targets and their components, individual targets, and even elements of targets to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objective (JP 3-60). This analysis includes deconfliction, aim point recommendations, target materials production, and collateral damage estimation. Target development generally results in products such as target folders, information collection requirements, and target briefs. Detailed analysis should characterize the function, criticality, and vulnerabilities of each target, linking targets back to targeting objectives and measures of effectiveness. Target development includes target vetting and target validation.

Note. Although target development is discussed under *detect* in ATP 3-60, for this publication, it is more useful to discuss this step under *decide*.

Target Vetting

F-31. *Vetting* is a part of target development that assesses the accuracy of the supporting intelligence to targeting (JP 3-60). Vetting establishes a reasonable level of confidence in a target's designated functional characterization. The BCT intelligence cell accomplishes this by reviewing all target data for accuracy. At a minimum, the assessment includes at a review of target identification, significance, collateral damage estimation, geospatial or location issues, impact on the threat or friendly forces, impact of not conducting operations on the target, environmental sensitivity, and intelligence gain or loss concerns. Vetting does not include an assessment of compliance with the law of war or rules of engagement.

Target Validation

F-32. *Validation* is a part of target development that ensures all candidate targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of war and rules of engagement (JP 3-60). Targets are validated against multinational concerns during some operations. Target vetting and validation should recur as new intelligence is collected or the situation changes. Target validation is performed by targeting personnel, in coordination with planners, servicing judge advocate, and other experts, as required. (See ATP 3-60 for a list of useful target validation questions.)

DETECT

F-33. As much as possible, the procedures and supporting products that are used during the *detect* function should be developed during the *decide* function. However, the targeting team must periodically update decisions made during the *decide* function concerning IPB products, HPT lists, target synchronization matrices, attack guidance matrices, the information collection plan, and the OPORD. Updating these products can occur throughout the *detect*, *deliver*, and *assess* functions of the targeting methodology.

F-34. Based on targeting priorities, the targeting working group establishes target detection and tracking priorities. Target tracking is inherent in target detection. The fires cell provides the intelligence cell with the degree of accuracy required and dwell time for a target to be eligible for engagement. Then the collection manager can match those requirements to the target location error of the information collection asset.

F-35. Execution of the information collection plan begins as early as possible during planning and continues all the way through the *assess* function and even helps transition operations into the next mission. The execution of the information collection plan to answer targeting information requirements is central to the *detect* function. Targets are detected by using the appropriate information collection assets. ATP 3-60 discusses this effort as detection procedures.

F-36. The *detect* function comprises target detection and additional target development, when necessary. The current operations integration cell is the primary cell responsible for directing the execution of the information collection effort to detect HPTs identified in the *decide* function. The intelligence cell (with the current operations integration cell) must focus their intelligence analysis efforts to support both situation development and the targeting effort. Therefore, close coordination between the intelligence cell and the fire support element is critical. Key staff members in this effort include the G-3/S-3, G-2/S-2, information

operations officer, field artillery intelligence officer (when staffed), targeting officer, and fire support coordinator/officer.

F-37. When detecting a planned HPT, the information is quickly disseminated to the field artillery intelligence officer to determine if the target is an HPT, the target's priority, and if the target complies with target selection standards. To ensure the target information is disseminated quickly, the field artillery intelligence officer should be located in the intelligence cell with communications to the fires cell. If the target is an HPT, the field artillery intelligence officer coordinates with the intelligence cell and disseminates the target directly to the fires cell or fire support element. If the commander approves the target, it is transferred to a firing unit.

F-38. In those cases, where the situation dictates the development of a new HPT or when the staff assesses a significant change to an existing HPT, subsequent target development must occur. When subsequent target development is necessary, the targeting information is forwarded for intelligence analysis and the target development process must occur quickly. Upon identifying a target specified for attack, analysts pass the target to the fire support element. The fire support element executes the attack against the target.

DELIVER

F-39. The *deliver* function executes the target attack guidance and supports the commander's plan once HPTs have been located and identified. Target engagement requires several decisions and actions, which are grouped into tactical and technical decisions.

Tactical Decisions

F-40. Tactical decisions are made based on the analysis that was accomplished during target development. Tactical decisions reconfirm or determine the—

- Time of the engagement.
- Desired effect, degree of damage, or both.
- Delivery system to be used through weaponeering and collateral damage estimation.

Time of Engagement and Desired Effect

F-41. Time of engagement and the desired effect that will be achieved on the target are critical considerations. The commander needs to weigh the operational risk of tactical patience balanced against the immediacy of the planned action in the attack guidance matrix. As the operation evolves, the commander may decide to change the time of engagement or the desired effect on a particular HPT. When a target is a target of opportunity, then the commander and staff must quickly decide on the desired effects.

Delivery System

F-42. This step builds on the analysis performed during target development and includes weaponeering and collateral damage estimation. If the target was already planned, then this step starts with determining if the delivery means is available and still the best weapon or means for the engagement. When the target is a target of opportunity then some analysis is necessary to work through completion of a quick target development.

F-43. *Weaponeering* is the process of determining the specific means required to create a desired effect on a given target (JP 3-60). As much as possible, weaponeering should be planned during the plan function during target development. Weaponeering considers munitions delivery error and accuracy, damage mechanisms and criteria, probability of kill, weapon reliability, and trajectory. Targeting personnel quantify the expected results of fires against targets to produce the desired effects. ATP 3-60 provides a general weaponeering process that can be adapted as needed.

F-44. Collateral damage estimation builds on target validation to assist the commander and unit in staying within the law of war and rules of engagement. Failure to observe these obligations can be very significant to operations and considered a law of war violation. The staff has the responsibility to mitigate unintended or incidental risk of death, injury, or damage according to the law of war and rules of engagement as described in ATP 3-60.

Technical Decisions

F-45. Once the tactical decisions have been made, the G-3/S-3 directs the appropriate unit to engage the target. The fires cell provides the asset or system manager with selected time of engagement, desired effects, and any special restraints or requests for particular munitions types.

F-46. The asset or system manager (for example, field artillery battalion S-3, air liaison officer, or brigade naval gunfire officer) determines if the system can meet the requirements. The fires cell is notified when a delivery system or asset is unable to meet the requirements. In those cases, the fires cell must decide if the selected delivery asset or system should engage the target under a different criterion or if a different delivery asset or system should be used.

ASSESS

F-47. The *assess* function of the targeting methodology is nested in the overall continuous assessment of operations within the operations process. Assessment is directly tied to the commander's decisions throughout the planning, preparation, and execution of operations. Planning for assessment identifies key aspects of the operation that the commander directs be closely monitored, and where the commander wants to make the decisions. Commanders and staffs consider assessment ways, means, and measures. ADP 5-0 discusses overall operational assessment, including measures of effectiveness, measures of performance, and indicators. Intelligence plays a major role in operational assessment.

F-48. Intelligence also plays a major role in assessment as a part of the targeting methodology. The assess function of the targeting methodology is performed through combat assessment. *Combat assessment* is the determination of the effectiveness of force employment during military operations (JP 3-60). Combat assessment comprises three elements:

- BDA.
- Munitions effectiveness assessment.
- Reengagement recommendation.

F-49. Together, BDA and munitions effectiveness assessment provide the commander and staff with an assessment of the effects achieved against targets and whether the targeting guidance was met. Based on this information, the staff can recommend reengagement when necessary.

Battle Damage Assessment

F-50. *Battle damage assessment* is the estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force (JP 3-0). The staff determines how combat assessment relates to specific targets by completing BDA. Producing BDA is primarily an intelligence cell responsibility but requires coordination across the staff, similarly to IPB and most steps of intelligence support to targeting. BDA requirements should be captured as PIRs or as similar high-priority information collection requirements. BDA provides—

- Commanders with an assessment of the target's mission effectiveness, overall status, capabilities (whether full or partial), and likely reactions or any change to their intent. This assists the staff in determining if the engagement is meeting the targeting guidance and is critical to any recommendation to reengage the target.
- Important analysis used to conduct quick target development and decide on the allocation or redirection of assets or weapon systems for any reengagement.

F-51. BDA has three components (see table F-1):

- **Physical damage assessment.** The staff estimates the extent of physical damage to a target based on observed or interpreted damage. It is a post-attack target analysis coordinated among all units.
- **Functional damage assessment.** All-source intelligence analysts assess the remaining functional or operational capability of the threat. The assessment focuses on measurable effects and estimates the threat's ability to reorganize or find alternative means to continue operations. The targeting cell and staff integrate analysis with external sources to determine if the commander's intent for fires has been met.

- **Target system assessment.** The staff conducts a broad assessment of the overall impact and effectiveness of all types of engagement against an entire target system capability (for example, threat air defense artillery systems). All-source intelligence analysts assist the staff in assessing the threat's combat effectiveness or major threat subordinate elements or capabilities needed to accomplish a threat mission. This is a relatively permanent assessment (compared to functional damage assessment) that can be used for more than one mission.

Table F-1. Battle damage assessment components

Component	*Description*
Physical damage assessment	• Quantitative physical damage from munitions blast, fragmentation, or fire. • Based on observed or interpreted damage.
Functional damage assessment	• Estimates the effects on the target's capability to perform its mission. • Assessment based on all-source intelligence. • Includes a time estimate required to reconstitute or replace the target. • Temporary assessment—compared to a target system assessment—used for specific missions.
Target system assessment	• The overall effect on an entire target system's capability. • Applicable against a threat's combat effectiveness. • May address significant subdivisions of a target. • A more permanent assessment.

F-52. BDA requirements for specific HPTs are determined during the *decide* function. Often information collection assets can answer either target development and target acquisition requirements or BDA, but not both types of requirements. An asset used for BDA may be unavailable for target development and target acquisition requirements. The intelligence cell receives, processes, and disseminates results that are analyzed based on desired effects to the targeting team attack.

F-53. The targeting team should consider the following BDA principles:

- BDA should measure what is important to commanders, not make important what is easily measurable.
- BDA should be objective. When receiving a BDA product from another echelon, the conclusions should be verified (time permitting) to identify and resolve discrepancies among BDA analysts at different headquarters.
- The degree of reliability and credibility of BDA relies largely on information collection assets. The quantity and quality of information collection assets influence whether the assessment is highly reliable (concrete, quantifiable, and precise) or has low reliability (estimation). Effective BDA uses more than one source to verify each conclusion.

F-54. BDA is more than determining the number of casualties or the amount of equipment destroyed. The targeting team can use other information such as—

- Whether the targets are moving or hardening in response to the attack.
- Changes in deception efforts and techniques.
- Whether the damage achieved is affecting the threat's combat effectiveness as expected.

F-55. Units may choose to use BDA charts. Figures F-3 and F-4 on page F-10 display two techniques for creating these charts. Figure F-3 is based on the threat's organization; figure F-4 is based on the BDA reported at locations within the AO. Units may choose to use figure F-4 when conducting offensive operations because it provides the commander and staff with an estimation of threat strength at a specific location.

F-56. BDA may simply be compiled information about a particular target or area (for example, the area's cessation of fires). If BDA is developed, the targeting team gives the collection management team and operations cell adequate warning to task information collection units and prepare and orient intelligence collection systems to the right target at the right time. BDA outcomes may result in changed plans and earlier decisions. The targeting team periodically updates earlier decisions during the *decide* function concerning IPB products, HPT lists, target selection standards, attack guidance matrices, collection management tools, and operation plans or OPORDs.

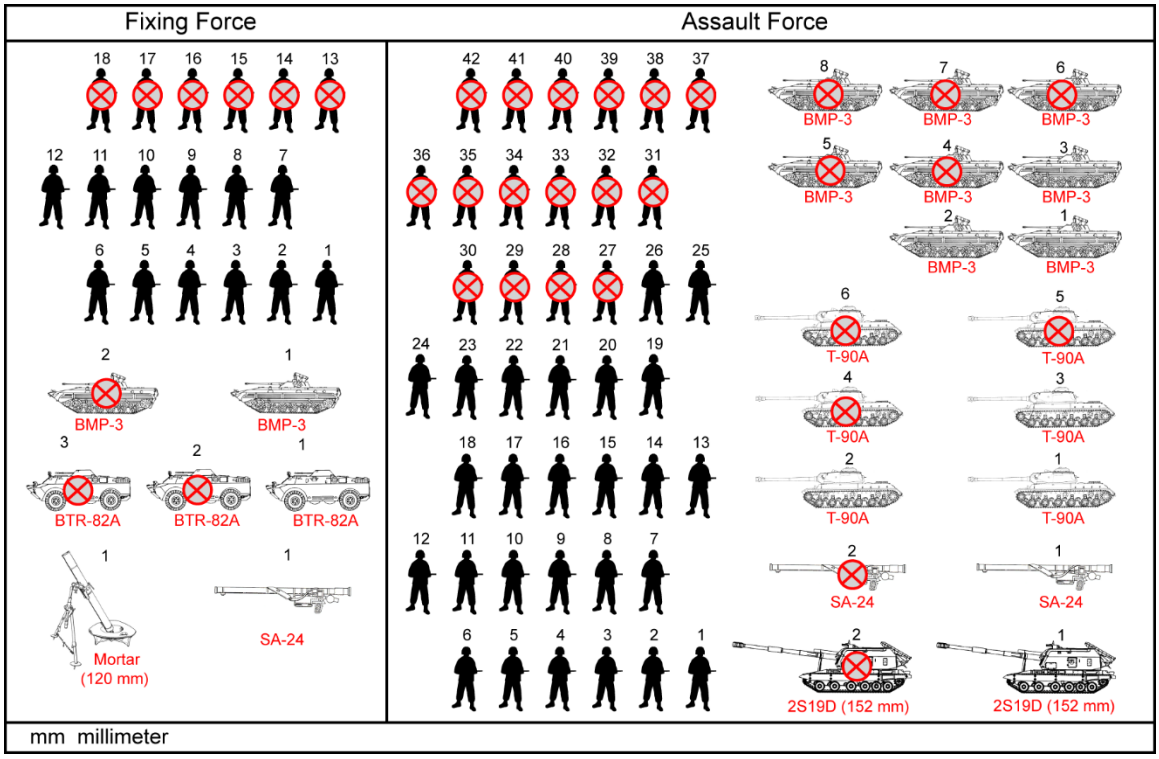


Figure F-3. Battle damage assessment chart (based on threat organization)

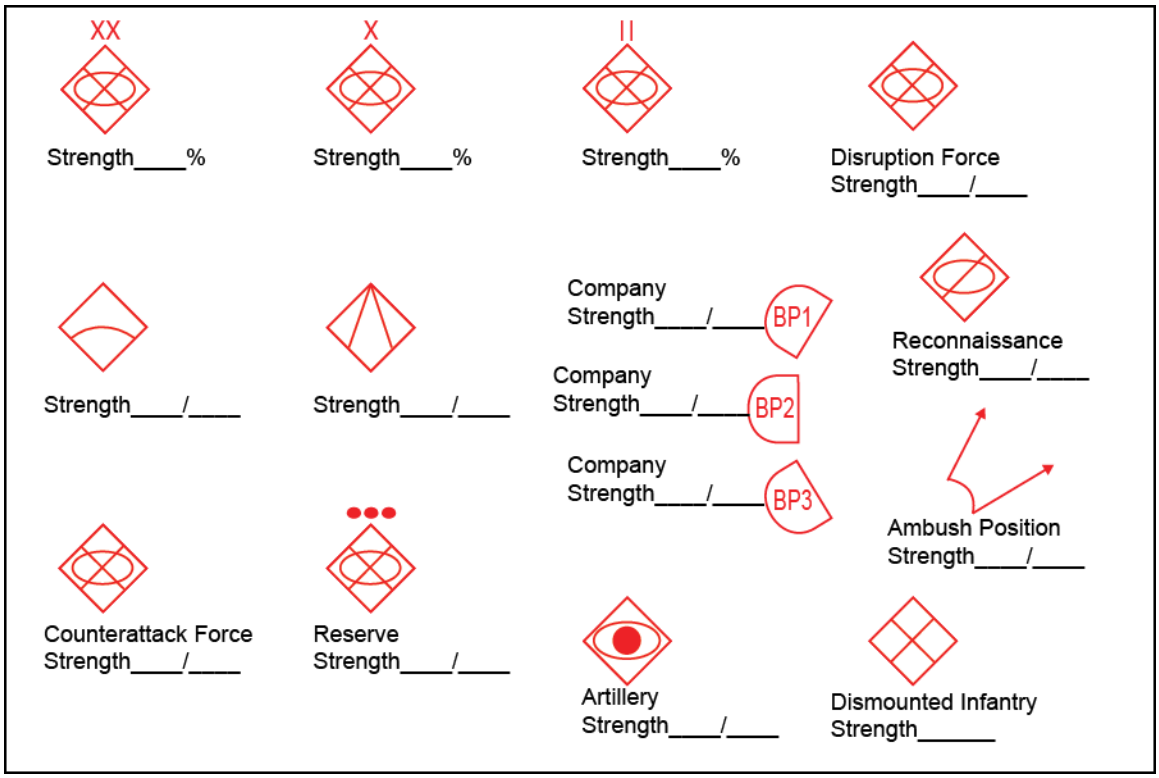


Figure F-4. Battle damage assessment chart (based on location)

Munitions Effectiveness Assessment

F-57. The intelligence cell is not normally involved in the munitions effectiveness assessment but should track them to better understand the unit targeting effort. The G-3/S-3, in coordination with the fires cell and targeting working group, conducts the munitions effectiveness assessment concurrent with BDA. The munitions effectiveness assessment focuses on the munitions effectiveness of the specific threat weapons or other types of systems. The fires cell uses specific weaponeering software. Then the G-3/S-3 and fires cell conducts the munitions effectiveness assessment to increase the effectiveness of the targeting methodology, tactics, weapon systems, munitions, and weapon delivery patterns. Based on the assessment, the targeting working group may recommend modifying the commander's guidance about the unit basic load, required supply rate, and controlled supply rate.

Reengagement Recommendation

F-58. Unlike the munitions effectiveness assessment, the intelligence cell is involved in a reengagement recommendation. When delivery of fires does not achieve a predecided effect or reach a preset BDA criterion, a decision from the commander is necessary. The targeting team and current operations cell must assess the operational risk associated with reengaging or not reengaging an HPT. Based on the BDA and munitions effectiveness assessment, the G-2/S-2, in conjunction with the fire support coordinator and G-3/S-3, considers to what degree the targeting objective has been achieved and makes a recommendation to the commander. Reengagement and other recommendations should address objectives relative to targets, target critical elements, target systems, threat combats for strength, and friendly maneuver.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ACE	analysis and control element
ACH	analysis of competing hypotheses
ADP	Army doctrine publication
AO	area of operations
AR	Army regulation
ART	Army tactical task
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
BCT	brigade combat team
BDA	battle damage assessment
CFA	critical factors analysis
COA	course of action
DCGS-A	Distributed Common Ground System-Army
DOD	Department of Defense
DOMEX	document and media exploitation
FEBA	forward edge of the battle area
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
HAC	human intelligence analysis cell
HPT	high-payoff target
HUMINT	human intelligence
HVT	high-value target
IADS	integrated air defense system
ICD	intelligence community directive
INSCOM	U.S. Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
JP	joint publication
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MLRS	multiple launch rocket system

NAI	named area of interest
NGIC	National Ground Intelligence Center
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (military aspects of terrain)
OE	operational environment
OPORD	operation order
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
SOP	standard operating procedure
TAI	target area of interest
U.S.	United States

SECTION II – TERMS

Army special operations forces

Those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. (JP 3-05)

attack guidance matrix

A targeting product approved by the commander, which addresses the how and when targets are engaged and the desired effects. (ATP 3-60)

battle damage assessment

The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force. (JP 3-0)

combat assessment

The determination of the effectiveness of force employment during military operations. (JP 3-60)

combat information

Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 2-01)

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 objective(s). (JP 5-0)

critical requirement

An essential condition, resource, or 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)

defensive operation

An operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations. (ADP 3-0)

fusion

(Army) Consolidating, combining, and correlating information together. (ADP 2-0)

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-payoff target list

A prioritized list of high-payoff targets by phase of the operation. (FM 3-09)

high-value target

A target the enemy commander requires for the successful completion of the mission. (JP 3-60)

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

In the context of decision making, data that has been organized and processed in order to provide context for further analysis. (ADP 6-0)

information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

intelligence analysis

The process by which collected information is evaluated and intgrated with existing information to facilitate intelligence production. (ADP 2-0)

intelligence estimate

The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view of determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 2-0)

knowledge

In the context of decision making, information that has been analyzed and evaluated for operational implications. (ADP 6-0)

large-scale combat operations

Extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives. (ADP 3-0)

large-scale ground combat operations

Sustained combat operations involving multiple corps and divisions. (ADP 3-0)

military decision-making process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

offensive operation

An operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers. (ADP 3-0)

operational level of warfare

The level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. (JP 3-0)

relevant information

All information of importance to the commander and staff in the exercise of command and control. (ADP 6-0)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if the planned future operations are supportable. (ADP 5-0)

stability operation

An operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADP 3-0)

strategic level of warfare

The level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. (JP 3-0)

tactical level of warfare

The level of warfare at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. (JP 3-0)

target development

The systematic examination of potential targets and their components, individual targets, and even elements of targets to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objective. (JP 3-60)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

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. (ADP 3-0)

validation

A part of target development that ensures all candidate targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of war and rules of engagement. (JP 3-60)

vetting

A part of target development that assesses the accuracy of the supporting intelligence to targeting. (JP 3-60)

weaponeering

The process of determining the specific means required to create a desired effect on a given target. (JP 3-60)

References

All URLs accessed on 19 November 2019.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. November 2019.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

ADP 2-0. *Intelligence*. 31 July 2019.

ADP 3-0. *Operations*. 31 July 2019.

ATP 2-01. *Plan Requirements and Assess Collection*. 19 August 2014.

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 01 March 2019.

FM 1-02.1. *Operational Terms*. 21 November 2019.

FM 2-0. *Intelligence*. 06 July 2018.

FM 3-0. *Operations*. 06 October 2017.

JP 3-60. *Joint Targeting*. 28 September 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/Doctrine/.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 05 July 2017.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-01. *Countering Air and Missile Threats.* 21 April 2017.

JP 3-05. *Special Operations*. 16 July 2014.

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-15.1. *Counter-Improvised Explosive Device Activities*. 17 July 2018.

JP 5-0. *Joint Planning*. 16 June 2017.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/.

ADP 3-05. *Army Special Operations*. 31 July 2019.

ADP 3-07. *Stability*. 31 July 2019.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 4-0. *Sustainment*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-0. *Mission Command: Command and Control of Army Forces.* 31 July 2019.

AR 380-28. *Army Sensitive Compartmented Information Security Program*. 13 August 2018.

ATP 2-19.1. *(U) Echelons Above Corps Intelligence Organizations (S).* 17 December 2015.

ATP 2-19.3. *Corps and Division Intelligence Techniques*. 26 March 2015.

ATP 2-19.4. *Brigade Combat Team Intelligence Techniques*. 10 February 2015.

ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)*. 11 December 2015.

ATP 2-22.6-2. *(U) Signals Intelligence Volume II: Reference Guide*. 20 June 2017.

ATP 2-22.9. *Open-Source Intelligence*. 15 August 2019.

ATP 2-22.82. *Biometrics-Enabled Intelligence (U)*. 02 November 2015.

ATP 2-91.8. *Techniques for Document and Media Exploitation*. 05 May 2015.

ATP 3-11.36. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Planning*. 24 September 2018.

ATP 3-11.37. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Reconnaissance and Surveillance*. 25 March 2013.

ATP 3-21.51. *Subterranean Operations*. 01 November 2019.

ATP 3-39.10. *Police Operations*. 26 January 2015.

ATP 3-39.20. *Police Intelligence Operations*. 13 May 2019.

ATP 3-39.30. *Security and Mobility Support*. 30 October 2014.

ATP 3-60. *Targeting*. 07 May 2015.

ATP 3-90.4. *Combined Arms Mobility*. 08 March 2016.

ATP 3-90.8. *Combined Arms Countermobility Operations*. 17 September 2014.

ATP 3-90.37. *Countering Improvised Explosive Devices*. 29 July 2014.

ATP 4-32. *Explosive Ordnance Disposal (EOD) Operations*. 30 September 2013.

ATP 4-32.1. *Explosive Ordnance Disposal (EOD) Group and Battalion Headquarters Operations*. 24 January 2017.

ATP 5-0.1. *Army Design Methodology*. 01 July 2015.

FM 2-22.3. *Human Intelligence Collector Operations*. 06 September 2006.

FM 3-01. *U.S. Army Air and Missile Defense Operations*. 02 November 2015.

FM 3-04. *Army Aviation*. 29 July 2015.

FM 3-09. *Field Artillery Operations and Fire Support*. 04 April 2014.

FM 3-11. *Chemical, Biological, Radiological, and Nuclear Operations*. 23 May 2019.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

FM 3-13. *Information Operations.* 06 December 2016.

FM 3-14. *Army Space Operations*. 30 October 2019.

FM 3-34. *Engineer Operations*. 02 April 2014.

FM 3-39. *Military Police Operations*. 09 April 2019.

FM 3-53. *Military Information Support Operations*. 04 January 2013.

FM 3-55. *Information Collection*. 03 May 2013.

FM 3-57. *Civil Affairs Operations*. 17 April 2019.

FM 3-63. *Detainee Operations*. 28 April 2014.

FM 4-02. *Army Health System*. 26 August 2013.

FM 6-0. *Commander and Staff Organization and Operation*s. 05 May 2014.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27. *The Commander's Handbook on the Law of Land Warfare*. 07 August 2019.

OTHER PUBLICATIONS

ICD 203. *Analytic Standards.* 02 January 2015. Available online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

ICD 206. *Sourcing Requirements for Disseminated Analytic Products*. 22 January 2015. Available online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

+SOURCES USED

Defense Intelligence Agency. *Analytic Design: Analytic Tradecraft Guidance from the DI Research Director*. Available by contacting the DI Analytic Development Office via email at DIA_Tradecraft@coe.ic.gov.

Mackinder, Halford John. *The Geographical Pivot of History*. 1904. Available online: https://archive.org/download/The-geographical-pivot-of-history.

Mahan, Alfred Thayer. *The Influence of Sea Power upon History, 1660-1783*. 1890. Boston, MA: Little, Brown and Company.

United States Army in World War II. The European Theater of Operations: The Ardennes: Battle of the Bulge. Available online: https://history.army.mil/books/wwii/7-8/7-8_cont.htm.

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.

A

abductive reasoning. *See* reasoning, types of.

ACH. *See* contrarian structured analytic techniques.

action-metrics. *See* analysis validation.

activities matrix. *See* tool.

all-source analysis, 1-7, 1-10–1-14

all-source analytical element, 1-7, 1-8, 1-10, 1-13, 1-34

all-source analytical task, 3-1–3-5
- generate intelligence knowledge, 3-1, 3-2, 3-6
- perform IPB, 3-1, 3-2, 3-8
- perform situation development, 3-1, 3-2, 3-12, 3-13
- provide intelligence support to information operations, 3-16
- provide intelligence support to targeting, 3-14, 3-15
- provide warnings, 3-1, 3-2, 3-10, 3-11

all-source production, 1-10–1-14

analogical reasoning. *See* reasoning, types of.

analysis,1-1, 1-2. *See also* intelligence analysis; threat.

analysis, across the echelons, 1-33, 1-34, 7-3, 7-4
- battalion, 1-7, 2-6, 2-8, 2-22, 7-2, 7-11
- BCT, 1-7, 1-8, 2-6, 2-8, 2-15, 2-18, 7-10, 8-3, 8-5, F-22, F-31
- corps, 1-7, 1-14, 3-4, 6-23, 7-4, 7-8, 8-3, 8-10, 8-11
- division, 1-7, 2-6, 2-8, 2-15, 2-18, 4-7, 7-9, 8-8, 8-9
- national and joint, 7-5
- theater army, 1-7, 3-4, 7-6–7-8

analysis of competing hypotheses. *See* ACH.

analysis validation
- analytic tradecraft standards, C-2–C-14
- analytical rigor, 2-17, 2-18, B-4, C-2, C-15 (table C-1, action-metrics), E-10

analytic design
- collaboration during, 9-12
- managing long-term analytical assessments, 9-2, 9-4, 9-13
- results of, 9-13

analytic design, steps of, 9-4
- step 1, frame the question/issue, 9-5
- step 2, review and assess knowledge, 9-6
- step 3, review resources, 9-7
- step 4, select the analytic approach/methodology and plan project, 9-8
- step 5, develop knowledge, 9-9
- step 6, perform analysis, 9-10
- step 7, evaluate analysis, 9-11, 9-13

analytic problem, 2-8, 5-15, 6-19
- familiarity with, 2-10
- framing of, 2-5, 9-15 (table 9-1)
- solving, 4-6

analytic standards, 1-27, C-1

analytic technique. *See also* structured analytic techniques.
- using, 2-9, 2-16

analytic tradecraft standards, 1-27 (figure 1-4), 2-2. *See also* analysis validation.

analytical judgments, 5-37, 6-6 (table 6-2), C-1
- change to/consistency of, C-12
- confidence in/credibility in, 5-32, 5-38 (table 5-11), C-3–C-5

analytical judgments (*continued*)
- forming, 2-5, 4-3, 5-27

+analytical pitfalls, 1-26, 2-1
- avoiding, B-19
- biases, B-25–B-30
- logic fallacies, B-20–B-24

analytical rigor. *See* analysis validation.

Army design methodology, 3-2, 9-5, 9-14

Army strategic roles, 1-35, 5-38, 7-1. *See also* intelligence requirements.
- shape OEs, 1-45
- prevent conflict, 1-45
- prevail in large-scale ground combat, 1-37
- consolidate gains, 1-45

association matrix. *See* tool.

automation systems, 1-11, 4-7, E-1, F-26
- DCGS-A, 4-7, A-4, A-5, E-1

B

basic structured analytic techniques, 5-1, 5-2
- chronologies, 5-1, 5-7-5-10
- event mapping 5-1, 5-24–5-26
- event tree 5-1, 5-22, 5-23
- link analysis, 5-1, 5-18–5-21
- matrices, 5-1, 5-11–5-14
- sorting, 5-1, 5-3–5-6
- weighted ranking, 5-1, 5-15–5-17

+basic thinking abilities, 1-16, 4-1, B-13
- information ordering, 1-16, B-14
- pattern recognition, 1-16, B-15
- reasoning, 1-16, B-2, B-16–B-18

battalion level. *See* analysis, across the echelons.

battle damage assessment (BDA), A-4, F-50–F-56

Entries are by paragraph number unless indicated otherwise.

BCT level. *See* analysis, across the echelons.

bias. *See also* analytical pitfalls.
 assimilation and confirmation biases, 5-33

brainstorming. *See* imaginative structured analytic techniques.

brigade combat team. *See* BCT.

C

collaboration, 1-25, 1-26
 across the echelons, 1-33, 1-43
 between intelligence analysis and collection management, 1-30, 1-32
 during the analytic design process, 9-12

collection management, A-1
 and intelligence support to targeting, 3-15, F-56
 in relation to intelligence analysis, 1-28–1-32
 performed by functional elements, 7-12

combat information. *See* information.

complementary intelligence capability
 as a single-source intelligence capability, 1-7, 1-9

conclusion, accurate. *See* analysis validation, analytical rigor.

confidence level
 assessing, 2-17
 expressing, C-7

contrarian structured analytic techniques, 6-1, 6-2
 ACH, 6-2–6-5, 6-16
 devil's advocacy, 4-7, 6-2, 6-6–6-9, C-15 (table C-1)
 high-impact/low-probability analysis, 6-2, 6-11–6-14, 6-18
 team A/team B, 4-7, 6-2, 6-9, 6-10, C-15 (table C-1)

convergent thinking. *See* imaginative structured analytic techniques, brainstorming.

corps level. *See* analysis, across the echelons.

+creative thinking, 1-16, 2-1, 4-1, B-6–B-8, B-12, B-31

critical capability. *See* imaginative structured analytic techniques, functional analysis.

critical factors analysis (CFA). *See* imaginative structured analytic techniques, functional analysis.

critical requirement. *See* imaginative structured analytic techniques, functional analysis.

+critical thinking, 1-16, 2-1, 1-24, 1-26, 4-1, B-6–B-12, B-31

critical vulnerability. *See* imaginative structured analytic techniques, functional analysis.

D

DCGS-A. *See* automation systems.

deductive reasoning. *See* reasoning, types of.

defensive operations. *See* large-scale ground combat operations.

diagnostic structured analytic techniques, 5-27
 indicators/signposts of change 5-27, 5-36–5-39
 key assumptions check 5-27–5-31
 quality of information check 5-27, 5-32–5-35

Distributed Common Ground System-Army. *See* DCGS-A.

divergent thinking. *See* imaginative structured analytic techniques, brainstorming.

division level. *See* analysis, across the echelons.

E

echelons, 1-31, 1-43. *See also* analysis, across the echelons.
 and multi-domain operations, 8-1
 and the analytical focus, 8-3

F

fallacies. *See* analytical pitfalls.

fight for intelligence, 1-37, 1-42
 during large-scale ground combat operations, 1-39, 8-3

functional analysis, 3-6. *See also* imaginative structured analytic techniques.

fusion (as part of all-source analysis and production), 1-11

G

generate intelligence knowledge, 1-45 (table 1-2), 9-14
 as an all-source analytical task. *See* all-source analytical task.
 tasks, 3-7
 to assess the threat, D-3

H

high-payoff target list, F-8, F-19

hypothesis, 2-7, 2-17
 ACH, 6-2–6-5, 6-16
 alternative, 6-7, 9-12, 9-13, C-9
 comparing, 6-9, 6-10
 generating, 2-5, 4-3, 5-3 (table 5-1), 5-4, 5-38, 6-12, 6-16
 reviewing, 5-23–5-26
 validating, 2-18

I

identity intelligence, 1-9, 3-5, 7-5. *See also* intelligence, categories of.

imaginative structured analytic techniques, 6-19
 brainstorming, 6-19–6-22
 functional analysis, 6-19, 6-23–6-25
 outside-in thinking 6-19, 6-26–6-28
 red hat/team analysis, 6-19, 6-29–6-31

indicator, F-47
 defined, 3-11
 threat, 1-31, 3-13

inductive reasoning. *See* reasoning, types of.

Entries are by paragraph number unless indicated otherwise.

information, 1-1
  accuracy, 2-7, 2-12–2-16
  combat information, 1-14, 1-37 (table 1-1), 2-12, F-22
  corroboration of, 1-13, 2-12, 2-13, 2-16, C-7
  refining. *See* fusion.
  relevancy, 2-8, 2-12
  relevant information, 2-4, 2-9
  reliability, 2-7, 2-12–2-16
information collection 1-4, 1-28, 1-29, 1-31, 1-37, B-2
information collection plan, F-8
information operations. *See* all-source analytical task.
information ordering. *See* basic thinking abilities.
INSCOM, 7-5, D-2
intelligence
  categories of, 2-19
  support to information operations, 3-16
  support to targeting, 3-14, 3-15
intelligence analysis
  as discussed in ADP 2-0, 1-6, 1-7
  automation support, A-1–A-3
  comprises, 1-7
  conducting, 1-15, 1-16
  crosswalking with analytic design, 9-14, 9-15
  defined, 1-3
  effective analysis, six aspects of, 1-16–1-27
  facilitating situational understanding, 1-12, 1-44, 2-19, A-2
  large-scale ground combat operations, effect on, 1-37, 1-39
  support to functional elements, 7-12
  unique aspects of, 1-5
intelligence analysis process, 2-1–2-3, 2-6
  analyze phase, 2-4, 2-9–2-15, 8-6 (table 8-1), 8-9 (table 8-2), 8-11 (table 8-3)
  and long-term analytical assessment, 9-3
  integrate phase, 2-4, 2-16–2-18, 8-6 (table 8-1), 8-9 (table 8-2), 8-11 (table 8-3)
intelligence analysis process (*continued*)
  produce phase, 2-4, 2-19–2-22, 8-6 (table 8-1), 8-9 (table 8-2), 8-11 (table 8-3)
  screen phase, 2-4, 2-7, 2-8, 8-6 (table 8-1)
intelligence analyst. *See also* analytical judgments.
  and mission-specific requirements, 7-12
  avoiding analytical pitfalls. *See* analytical pitfalls.
  challenges, 1-4, 1-17, 1-18, 1-37
  doctrinal concepts, understanding of, 1-39
  employing analytic tradecraft standards, C-2
  +intelligence analytical skills, B-2–B-5
  understanding the threat, D-2
intelligence architecture, 1-34
Intelligence Community Directive (ICD) 203. *See* analytic standards.
Intelligence Community Directive (ICD) 206, C-4
intelligence discipline
  as a single-source intelligence capability, 1-7, 1-9
intelligence preparation of the battlefield. *See* IPB.
intelligence product, 2-19, 2-20, E-2
  analytical support to orders and briefings, E-20
  Annex B (Intelligence) to the operation order, E-3, E-4
  graphic intelligence summary, E-12, E-13
  intelligence estimate, E-3, E-5, E-6
  intelligence report, E-14
  intelligence running estimate, E-3, E-7–E-9
  intelligence summary, E-11
  periodic intelligence report, E-15–E-17
  supplementary intelligence report, E-15, E-18, E-19
intelligence requirements (associated with the Army strategic roles), 7-13
  shape OEs, 7-14
  prevent conflict, 7-15
  prevail in large-scale ground combat, 7-16–7-20
  consolidate gains, 7-21–7-26
intelligence warfighting function, 1-3, 1-30, 3-2, 7-3, 7-17, A-4
IPB, 3-7, 9-14
  and targeting, F-9
  as an all-source analytical task. *See* all-source analytical task.
  assessing the threat, D-3, D-4
  performed by functional elements, 7-12
  situation development and, 3-12, 3-13
  steps of, 3-9

K

knowledge, defined, 1-1

L

large-scale combat operations, defined, 1-36
large-scale ground combat operations, 1-35–1-37, 7-2. *See also* Army strategic role; fight for intelligence; intelligence requirements.
  and consolidating gains, 7-22
  and the threat, D-1–D-5
  defensive operations in, 7-17, 7-19, 7-20
  offensive operations in, 7-17, 7-18
levels of warfare, 7-4
  operational, 1-27, 1-38, 3-4, 7-4, 8-4, 8-10, 8-11, 9-1
  strategic, 1-38, 2-13, 3-4, 7-4, 9-1
  tactical, 1-14, 1-27, 1-38, 2-13, 7-4, 8-4–8-11
link analysis. *See* basic structured analytic techniques.
link diagram. *See* tool.

Entries are by paragraph number unless indicated otherwise.

long-term analytical assessment, 3-4
described, 9-1, 9-3
managing. *See* analytic design.

M

MDMP, 3-2, D-3
and analytical support, 3-8, 3-9
employing, 9-14
input to, 6-30

method (pertaining to analysis), 4-2

military decision-making process. *See* MDMP.

multi-domain operations, 1-39, 1-44, 8-1, 8-11 (table 8-3)

N

National Ground Intelligence Center (NGIC), 1-7, 7-4, 7-5, D-2

national to tactical intelligence, 1-25

O

OE
assessing the threat, D-5
intelligence assessments about, E-1, E-3
relevent aspects of, 3-12
shaping, 3-2, 4-4. *See also* Army strategic role; intelligence requirements.
visualizing, 1-2, 3-1, 3-8, 9-15 (table 9-1)

offensive operations. *See* large-scale ground combat operations.

operational art, 1-39

operational environment. *See* OE.

operational framework, 1-39

operational level of warfare. *See* levels of warfare.

P

pattern analysis plot sheet. *See* tool.

pattern recognition. *See* basic thinking abilities.

peer threat, 1-38, 1-44, 1-45 (table 1-2), 8-3, D-1, D-2, D-7
countering information collection, 1-37

PIR, 2-6, 2-8, 2-22
answering, 2-21, 4-4, 7-3
information relevant to, 2-7
understanding, 2-5

position of relative advantage, 1-39, 1-42, 1-43, 3-2

priority intelligence requirement. *See* PIR.

R

+reasoning, 1-16, B-13, B-16
types of, B-17, B-18
using, 2-9, 2-16

relevant information. *See* information.

S

single-source analysis, 1-7–1-9

single-source analytical elements, 1-7, 1-8

situation development, 8-2
as an all-source analytical task. *See* all-source analytical task.

situational understanding. *See* intelligence analysis.

stability operations, 7-21, 7-23–7-26

strategic level of warfare. *See* levels of warfare.

structured analytic techniques. *See also* basic structured analytic techniques; contrarian structured analytic techniques; diagnosic, structured analytic techniques; imaginative structured analytic techniques.
applying, 4-3–4-7

T

tactical level of warfare. *See* levels of warfare.

target detection. *See* targeting methodology, detect.

target development, F-30–F-32

target value analysis, F-10–F-17

targeting. F-1–F-4. *See also* all-source analytical task.

targeting methodology, F-6, F-7
decide, F-8–F-32
detect, F-33–F-38
deliver, F-39–F-46
assess, F-47–F-58

technique (pertaining to analysis), 4-2

theater army level. *See* analysis, across the echelons.

threat
analysis by warfighting function, D-6–D-8
and analysis, 1-3, 3-13
and critical factors analysis (CFA), 6-23–6-25
and large-scale ground combat operations, D-1–D-5
categorizing and understanding, 6-29–6-31
defined, D-1
equipment, D-9, D-10
intelligence assessments, about, E-1, E-3

threat intentions matrix. *See* tool.

time event chart.*See* tool.

timeline. *See* tool.

tool (pertaining to analysis), 4-2
activities matrix, 5-11, 5-21
association matrix, 5-11, 5-21
link diagram, 5-21
pattern analysis plot sheet, 5-5, 5-6
threat intentions matrix, 5-11, 5-14
time event chart, 5-10
timeline, 5-9

U

U.S. Army Intelligence and Security Command. *See* INSCOM.

W

warning intelligence, 1-45 (table 1-2). *See also* intelligence, categories of.
as an all-source analytical task. *See* all-source analytical task.

window of opportunity, 1-39, 1-42, 1-43

ATP 2-33.4, C1

30 May 2025

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2514301

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.