MCWP 2-12 -- 23 Jul 99
(Coordinating Draft)

MAGTF INTELLIGENCE ANALYSIS AND PRODUCTION

U.S. Marine Corps

PCN ??? ?????? ??

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

__ ___ 1999

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations,* provide the doctrine and higher order tactics, techniques, and procedures for intelligence operations. MCWP 2-12, *MAGTF Intelligence Analysis and Production,* complements and expands upon this information by detailing doctrine, tactics, techniques, and procedures for the conduct of intelligence analysis and production in support of the Marine air-ground task force (MAGTF). The primary target audience of this publication is intelligence personnel responsible for the planning and execution of intelligence analysis and production operations. Personnel who provide support to this and all users of intelligence and intelligence products should also read this publication.

MCWP 2-12 describes aspects of MAGTF intelligence analysis and production operations and activities including doctrinal fundamentals, the nature of analytical thinking, intelligence preparation of the battlespace, intelligence support to targeting, command and control, communications and information systems support, intelligence products and formats, planning, execution, and training. MCWP 2-12 provides the information needed by Marines to understand, plan, and execute intelligence analysis and production operations in support of the MAGTF.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

JOHN E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: ??? ?????? ??

MCWP 2-12
MAGTF INTELLIGENCE ANALYSIS AND PRODUCTION

TABLE OF CONTENTS

		PAGE
	Foreword	i
	Table of Contents	ii

CHAPTER 1 - Fundamentals

1001	Purpose	1-1
1002	Definitions	1-1
1003	Overview of Intelligence Analysis and Production	1-2
1004	Intelligence Analysis and Production Relative to Operations and C2	1-9
1005	Responsibilities for Analysis and Production	1-10

CHAPTER 2 - Filtering, Recording and Evaluating

2001	Principles	2-1
2002	Filtering	2-2
2003	Recording	2-3
2004	Evaluation	2-14

CHAPTER 3 - Analytical Thinking

3001	Analytical Framework	3-1
3002	Analytic Problem Solving	3-3
3003	Pitfalls of Analysis	3-11
3004	Intelligence Analysis and Decisionmaking	3-19

CHAPTER 4 - Intelligence Preparation of the Battlespace

4001	Concept	4-1
4002	Process	4-1
4003	Output	4-26

CHAPTER 5 - Analysis of the Battlespace

5000	Purpose	5-1
5001	Responsibility	5-1
5002	Preparation	5-2
5003	Characteristics of the Battlespace	5-2

5004 Climatological/Weather Characteristics of the Battlespace 5-20
5005 Infrastruture Characteristics of the Battlespace 5-26
5006 Analysis of Political, Economic, and Sociological Factors 5-33

CHAPTER 6 - Threat Analysis

6001 Overview 6-1
6002 Threat Order of Battle 6-1
6003 Developing a Threat Model 6-7
6004 Determining Threat Courses of Action 6-12
6005 Evaluate, Prioritize, and Develop the Courses of Action 6-16
6006 Key Elements of the the Course of Action 6-22
6007 Other Analytical Techniques 6-24

CHAPTER 7 - Target Development and Battle Damage Assessment

7001 Overview 7-1
7002 The Targeting Cycle 7-2
7003 Target Development 7-3
7004 Target Systems Analysis 7-5
7005 Target Analysis Products 7-9
7006 Target/Objective Studies 7-10
7007 Battle Damage Assessment 7-11

CHAPTER 8 - Intelligence Production

8001 Overview 8-1
8002 Principles 8-2
8003 Production Cycle 8-3
8004 Production Management 8-5
8005 Intelligence Products 8-7
8006 Intelligence Production in the MAGTF 8-9
8007 External Production Support 8-11

CHAPTER 9 - Analysis and Production Cell

9001 General 9-1
9002 Mission 9-2
9003 Capabilities 9-2
9004 Organization 9-3
9005 Supporting Organizations 9-5
9006 Concept of Employment 9-11
9007 Communications and Information Systems 9-15

CHAPTER 10 - Analysis and Production in MAGTF Operations

10001	Overview	10-1
10002	Analysis and Production in Operational Maneuver from the Sea	10-1
10003	Intelligence Analysis and Production in Sustained Operations Ashore	10-4
10004	Intelligence Analysis and Production in Military Operations Other Than War	10-5
10005	Intelligence Analysis and Production in Joint Operations	10-10
10006	Intelligence Analysis and Production in Combined Operations	10-12
10007	Pre-Crisis (Peacetime) Analysis and Production	10-15
10008	Analysis and Production During the Warning/Deployment Phase	10-21
10009	Analysis and Production During Execution	10-23

APPENDICES

A	Glossary	A-1
B	References	B-1
C	Intelligence Estimate Format	C-1
D	Weather Critical Values	D-1
E	Tactical Indicators	E-1
F	BDA Report Format	F-1
G	Intelligence Summary Format	G-1
H	Intelligence Report Format	H-1
I	Intelligence Information Brief Format	I-1
J	Production Requirement/Request for Intelligence Format	J-1

LIST OF FIGURES

1-1	Intelligence Cycle	1-3
1-2	Information Hierarchy and the Intelligence Cycle	1-4
1-3	Intelligence Support to Planning and Decisionmaking	1-10
2-1	Example of an Intelligence Journal Page	2-5
2-2	Sample Unit Workbook Page	2-9
2-3	Example of an Order of Battle Overlay	2-10
2-4	Example Order of Battle Record (STANAG 2077)	2-11
4-1	Examining the Battlespace	4-3
4-2	Weather Effects Matrix	4-10
4-3	Doctrinal Template	4-13
4-4	Threat Model with Type High Value Targets Matrix	4-15
4-5	Combining Doctrine and Battlespace Effects to Develop Threat Courses of Action	4-18
4-6	Example of a Situation Template	4-20
4-7	Develop the Event Template by Comparing and Contrasting NAIs and Indicators Associated with Each Course of Action	4-22
4-8	Event Matrix	4-23
5-1	Group Mobility Corridors to Form Avenues of Approach	5-11
5-2	Weather Forecast Graphic	5-25
5-3	Weather Effects Matrix	5-26
6-1	Example Using Text or a Matrix to Describe the Conduct of the Course of Action	6-9
6-2	Threat Synchronization Matrix	6-10
6-3	Target Value Matrix	6-12
6-4	Situation Template Emphasizing High Value Targets	6-19

LIST OF FIGURES (cont.)

6-5	Situation Template with HVTs and TPLs	6-20
6-6	Synthesizing the Event Template	6-23
6-7	Event Matrix	6-23
6-8	Coordinates Register	6-32
6-9	Pattern Analysis Plot Sheet	6-33
6-10	Activities Matrix	6-34
6-11	Association Matrix	6-35
6-12	Link Diagram	6-36
6-13	Analyzing a PIR Using METT-T	6-37
7-1	Joint Targeting Cycle and D3A	7-2
7-2	Target System, Components, and Elements	7-6
7-3	Phase I BDA/FDA Information Flow	7-12
7-4	Phase II BDA/FDA Information Flow	7-13
7-5	Phase III BDA/TSA Information Flow	7-14
8-1	Intelligence Production Requirements Flow	8-18
8-2	DOD Production Requirements Process	8-19
9-1	Intelligence Battalion Organization	9-1
9-2	Definition of *Staff Cognizance*	9-6
9-3	Imagery Intelligence Platoon Organization	9-7
9-4	Marine Corps Imagery Support Unit Organization	9-8
9-5	Topographic Platoon Organization	9-9
9-6	CI/HUMINT Company Organization	9-10
9-7	MEF CE's Combat Intelligence Center and Intelligence Battalion's Intelligence Operations Center Key Elements	9-11
9-8	Intelligence Battalion's Intelligence Operations Center Organization and Functions	9-12
9-9	Senior Intelligence Staff Officers Relationships and Intelligence Production Support Flow	9-13
9-10	Senior MEF Intelligence Staff Officers' and Intelligence and Reconnaissance Unit Commanders' Responsibilities, Roles and Tasks	9-14
9-11	MEF Intelligence Processing, Analysis, Production, and Dissemination Communications and Information Systems Architecture	9-17

TABLE

9-1	Analysis & Production Company Tactical Organization and Support	9-4
D-1	Weather Critical Values Chart	D-2

Chapter 1

FUNDAMENTALS

1001. Purpose

The focus of this doctrinal publication is the analysis and production phase of the intelligence cycle. A fundamental responsibility of MAGTF intelligence is to provide decisionmakers at all levels of command the fullest possible understanding of the battlespace. This encompasses a sophisticated knowledge of the environment, both physical and political/economic/cultural, and the threat in the area of operations. This knowledge is developed through the execution of the intelligence analysis and production function. This manual provides direction for the conduct of this function. It outlines the purpose, responsibilities, organization, and tactics, techniques, and procedures pertinent to MAGTF intelligence analysis and production. The procedures detailed are applicable to the full spectrum of MAGTF operational and tactical employment and provide the basis for the training of all personnel involved in the conduct of intelligence analysis and production.

1002. Definitions

a. Intelligence. The knowledge about the enemy and surrounding environment needed to support decisionmaking. This knowledge results from the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat . (MCRP 5-12C)

b. All-Source Intelligence. Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (Joint Pub 1-02)

c. Information. Unevaluated material of every description that may be used in the production of intelligence. Information is derived from the processing of raw data, i.e. bits or bytes of data received from a sensor or direct human observer. Information used to generate intelligence is commonly drawn from three types of data:

(1) Intelligence Data. Data derived from assets primarily dedicated to intelligence collection: imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCWP 2-1)

(2) Sensor Data. Data derived from sensors whose primary mission is surveillance or target acquisition: air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

(3) Combat Data. Data derived from reporting by operational units. (MCRP 5-12C)

d. Priority Intelligence Requirement (PIR). Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking (Joint Pub 1-02). An intelligence requirement associated with a decision that will critically affect the overall success of the command's mission (MCRP 5-12C).

e. Intelligence Requirement (IR). Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence (Joint Pub 1-02) In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions (MCRP 5-12C)**.**

f. Processing and Exploitation. The conversion of collected information into a form suitable to the production of intelligence. Largely a technical function, processing and exploitation converts data into an understandable form and enhances its presentation. (MCWP 2-1)

g. Analysis. The sifting and sorting of evaluated information to isolate significant elements with respect to the mission and operations of the command. (MCWP 2-1)

h. Production. The conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production is a process of synthesis -- the most important action in developing usable intelligence for the commander. (MCWP 2-1)

1003. Overview of Intelligence Analysis and Production

a. Analysis and Production and the Intelligence Functions. In providing support to the commander, MAGTF intelligence organizations carry out six specific intelligence functions: support the commander's estimate, development the situation, provide indications and warning, and support force protection, targeting, and combat assessment. Integral to all these functions is analysis and production. In each case, data is synthesized into intelligence which provides a portion of the knowledge from which the commander can reach an acceptable level of understanding and then act upon it. The objective is to answer the all-important question: *"What effect does all this have on our ability to accomplish the mission?"* The focus and form of the intelligence created may vary according to the function, but common to all is the process of analysis and production from which that intelligence is derived.

b. Analysis and Production within the Intelligence Cycle. Analysis and production is the fourth step in the six-step intelligence cycle (see figure 1-1). It is this step that converts data into intelligence and creates *knowledge* (see figure 1-2). Without analysis and production commanders would be confronted with a tremendous mass of random data, instead of the

knowledge needed for the planning and execution of operations. Analysis and production itself encompasses a series of steps which begin with the receipt of processed information and end with the completion of an intelligence product that is ready for dissemination. Those steps are:

- **Filtering.** The discarding of irrelevant or repetitive information prior to its entering the production process.

- **Recording.** The reduction of information to writing or some other graphical representation and the arranging of that information into groups of related items.

- **Evaluating.** Determining the pertinence, reliability, and accuracy of information.

- **Analyzing.** The process in which information is analyzed and synthesized to predict possible outcomes.

- **Product Preparation.** Incorporating the developed intelligence into an appropriate product -- text reports and studies, graphics, overlays, or combinations -- for dissemination.

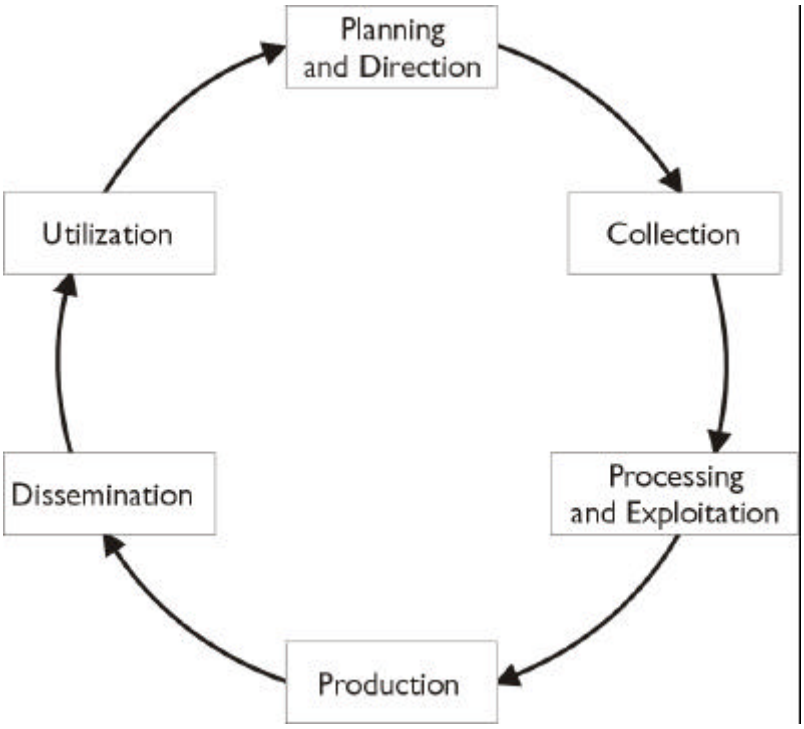

Figure 1-1. Intelligence Cycle

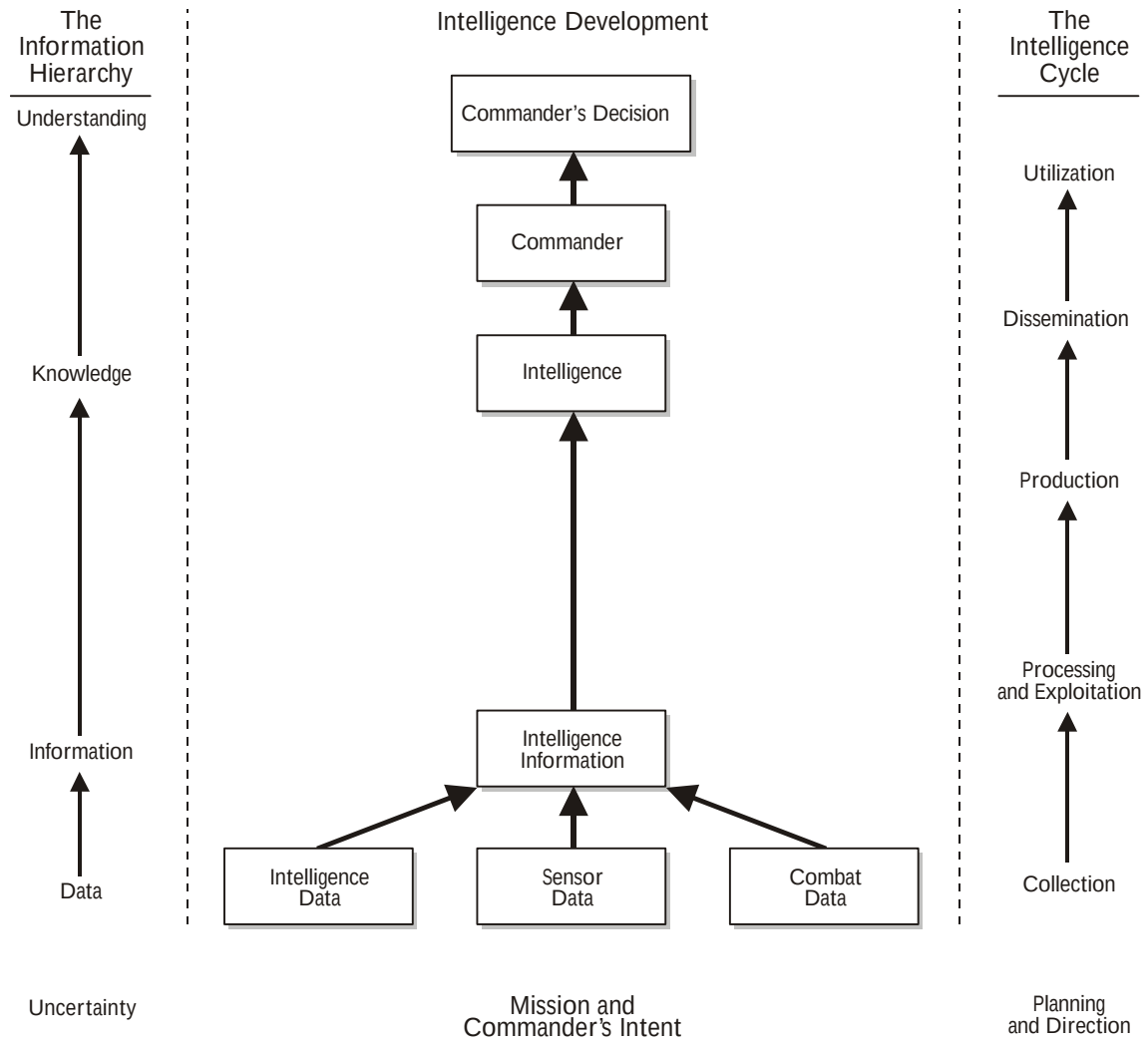

Figure 1-2. Information Hierarchy and the Intelligence Cycle

Analysis and production can be extremely simple or incredibly complex. At one extreme, comprehensive and detailed intelligence studies are required to support the planning of a MEF in a major regional contingency (MRC); at the other, simple and direct answers to rapidly changing questions are needed to support the ongoing battle at the battalion level. For this reason, we distinguish between two types of production: ***deliberate production*** and ***immediate production***. ***Deliberate production*** makes full use of all available information to provide a complete and extensive product that satisfies non-time sensitive IRs. ***Immediate production*** identifies information that has direct application in current operations; this information is subjected to a compressed version of the production process and the resulting product is rapidly disseminated to those affected. There is no clear boundary between deliberate and immediate production, however, deliberate production normally supports the ***planning*** of operations while immediate production is associated with mission ***execution***. The basic methodology for both types of

production is the same. What differs is the amount of time that can be used in developing the finished intelligence products and the degree of detail provided in those products. In any situation, *the critical consideration is providing timely, accurate, and relevant intelligence to commanders and planners, and not just information*. The intelligence must deliver knowledge, in context, in time, and be in a form for utilization in the decisionmaking process.

c. Processing and Exploitation. Processing and exploitation is the third step of the intelligence cycle and immediately precedes production. Processing and exploitation is the conversion of collected information into a form suitable for the production of intelligence. Largely a technical function, processing and exploitation converts data into an understandable form and enhances its presentation. Examples of processing and exploitation include film processing, document translation, and signals intercept. Processing is frequently not a discrete function, but is accomplished during collection or production. Some data requires minimal processing; it is collected in a form already suitable for analysis or processing takes place automatically during collection. Other types of data require extensive processing which can effect the timeliness and accuracy of the resulting information. Because processing and production are often accomplished by the same organization, for example in the radio battalion's operations control and analysis center (OCAC) or by intelligence battalion's (intel bn) imagery intelligence platoon (IIP), production management generally encompasses any processing functions that are required to convert raw data into a usable format.

d. Preparation for Analysis. The first four steps of the analysis and production phase involve preparing information for analysis. The objective is to discard information not pertinent to the situation, organize and document the information in a manner which facilitates analysis, and assess the quality of the individual elements of information to determine the reliability and importance of each report or piece of information. The steps used to prepare information for analysis are: **filtering, recording, and evaluating**. In deliberate production, comprehensive and detailed procedures are often employed to accomplish these steps. The complexity of these procedures increases with the level of command, scope of the operation, and number of agencies/elements participating in the production process. However, it is important to note that filtering, recording, or evaluation systems are *tools* to support the analytical effort, **not** an end unto themselves. Intelligence personnel must be thoroughly familiar with the methodology being employed in preparing information for analysis to ensure that the pertinent information is available to the right analyst when needed. In immediate production, a central node or individual-- normally the intelligence watch in the combat operations center (COC) -- makes a rapid assessment of each piece of incoming information to determine its pertinence and evaluate its reliability and accuracy. This evaluation is based on the situational awareness of the intelligence watch personnel, i.e. their knowledge and understanding of the enemy situation, the current intelligence estimate, and ongoing and planned friendly operations and IRs. The watch performs the minimal collating and recording necessary to permit an immediate tactical analysis to be completed and judgments made. Simultaneous with or upon completion of immediate production, the information is entered into the formal recording and evaluation system for further use in deliberate production. At lower tactical echelons the entire process, from receipt of information to dissemination and utilization, can take a matter of seconds or minutes. Efficient organization,

established standing operating procedures (SOP), and individual and unit training are key components of effective preparation for, and conduct of, analysis and production.

e. Analysis. Intelligence analysis is the heart of the analysis and production phase. Analysis is a process in which data/information is related and applied to an existing situation in order to provide determination of possible outcomes. It involves sifting and sorting evaluated information to isolate significant elements with respect to the mission of the command, determining the significance of the information relative to information and intelligence already known, and drawing deductions about the probable meaning of the evaluated information. The purpose of intelligence analysis is to provide the commander with the knowledge of the battlespace and the threat required for planning and execution of combat operations. Intelligence analysts seek to *lessen* the uncertainty facing a commander, thereby permitting him to make decisions, focus his combat power on courses of action that maximize his opportunity for success.

(1) Framework. The analysis framework used by intelligence analysts is described as: **analysis, synthesis, and estimation**. This framework provides a disciplined approach to gathering and understanding information, and a means for the analyst to place information in context and relate it to planned or ongoing operations.

(a) Analysis. Good analysis begins with a clear understanding of the unit's mission, the commander's intent, and the commander's IRs. All information is viewed in relation to those elements. Analysis divides the battlespace into component parts in order to isolate and define the individual elements of significant information. Rather than attempt to understand the mass of information he is confronted with all at once, the analyst first breaks the situation down into single pieces or smaller groups of information. The division of the battlespace may be based upon physical dimensions (length, depth, width, altitude), time, threat force structure (divisions, wings, groups, task forces, etc.), battlefield activities (C2, air defense, fire support, etc.), or any characteristic that facilitates understanding by the individual analyst and satisfying the needs of the MAGTF. Once the situation is broken down, key elements are identified which enable the analyst to formulate hypotheses, make deductions from those hypotheses, and reach conclusions. As they are received, individual pieces of new information are compared to the existing situation to determine if they relate to any of the key elements already identified and to assess the impact of the new information on the current intelligence estimate. Effective analysis requires judgment, a thorough knowledge of military operations, the characteristics of the battlespace, the friendly situation and IRs, and the threat situation to include the current situation, doctrine, and past practices.

(b) Synthesis. Synthesis is the piecing of information into a coherent, meaningful picture of the battlespace. It is based on the ongoing or previous analysis of separate information and events taking place within the area of operations. Relationships between individual significant pieces of information are identified and integrated with the existing picture of the battlespace to provide a new image of the situation. Synthesis enables the intelligence analyst to see the battlespace as a coherent whole and rapidly discern emerging patterns in either environmental conditions or enemy activity.

(c) Estimation. Estimation is the step in the analytical process which determines a threat's capabilities, intent, probable courses of action, and likely reactions to friendly operations. Building upon the image developed during analysis and synthesis, the analyst applies his knowledge and judgment to deduce the likely results of the patterns of activity he has identified. **Estimation is not guessing and it is not predicting**; instead, it is based on detailed study of a particular tactical situation, experience, and the application of specific tools and methodologies. **Estimation is the bottom line of the whole analytical process**. Intelligence must do more than just describe the current conditions; it must present an image of future possibilities. While intelligence cannot provide absolute certainty, well-founded estimates can reduce the uncertainty facing the commander, thereby facilitating the planning and execution of successful MAGTF operations.

(2) Intelligence Preparation of the Battlespace. IPB is a systematic, continuous process of analyzing the threat and environment in a specific geographic area as an aid to decisionmaking. It is the primary analytical methodology used to produce intelligence in support of staff estimates and the planning, decision, execution, and assessment (PDE&A) cycle.

(a) Methodology. IPB is a continuous process consisting of the following four steps (see Chapter 4 for a detailed discussion of IPB methodology):

- **Define the battlespace environment** - This step identifies the scope and focus of the IPB effort. In this step three key factors are determined. First, the characteristics of the battlespace which can influence friendly and threat operations are pinpointed for in-depth study. These may include, but are not limited to, terrain, weather, logistical infrastructure, and demographics. Second, the limits of the study are established based on the mission, characteristics of the battlespace, and nature of the threat. The command's area of operations (AO) is usually defined, thus the area of interest (AOI) is the focus of definition. In cases where an AO has not been assigned, the G-2/S-2 works with the G-3/S-3 to develop a recommendation for the commander's approval. With the battlespace defined, the third step is to identify gaps in current intelligence holdings relative to that battlespace, the mission, and the threat. Those identified gaps become the basis for the command's initial intelligence requirements and begin to define the intelligence collection, production and dissemination plans. Defining the battlespace environment provides necessary direction for the entire intelligence process and is a prerequisite to successful IPB.

- **Describe the battlespace effects -** Step 2 evaluates the ***effects*** of the environment with which both sides must contend. It identifies the limitations and opportunities the environment offers on the potential operations of both friendly and enemy forces. This assessment always includes an examination of the terrain and the weather, but will also include all other environmental factors which can influence the conduct of operations. Depending upon the specific type of operation, these characteristics may include: local infrastructure, mass communications, politics, economics, demographics, and sociology.

- **Evaluate the threat -** In step 3, all aspects of the threat or potential threats are analyzed to determine threat force capabilities. A detailed examination of the threat is used to develop threat models which accurately portray how threat forces normally execute operations and how they have reacted to similar situations in the past. The threat model should identify capabilities, strengths, limitations, the enemy center(s) of gravity, and critical vulnerabilities. When facing a well-known threat, this step can draw on historical data bases and well developed threat models. When operating against a new or less well-known threat, intelligence data bases and threat models will need to be rapidly developed concurrently.

- **Determine threat COAs -** The final step synthesizes the results of the previous steps into a meaningful conclusion. The threat models developed in step 3 are integrated with the effects of environment identified in step 2 to determine potential threat courses of action and assess their impact on friendly operations. The courses of action are used to estimate future enemy activity, portray the threat in the wargaming process, and guide intelligence collection and target development efforts. The number of COAs analyzed will depend upon the command echelon and time available, but at minimum will always include the most likely and the most dangerous threat COAs.

(b) Application. IPB provides a means to interpret information and understand the battlespace that can be applied at all levels and in any operational situation. Through the IPB process, information which has been collected and processed is analyzed, synthesized, and used to estimate possible outcomes that can effect mission accomplishment. However, it must be noted that IPB is a tool, not an end unto itself. **There is no one single way to perform IPB.** While the principles and steps of the IPB process remain constant - regardless of the type of mission and size of the intelligence section conducting IPB - the application of the principles may vary in each specific situation. The mission, characteristics of the battlespace, timeline, and resources available will determine the focus and amount of detail included in the IPB process. The IPB conducted by a Marine expeditionary force (MEF) during contingency planning for a MRC differs considerably in scope, detail, and the key elements which are studied in comparison to the effort done by a Marine expeditionary unit (special operations capable) (MEU[SOC]) in preparation for a short-notice NEO.

(c) Results. The IPB process develops tailored, mission focused knowledge-based intelligence which is incorporated into a variety of intelligence products. IPB emphasizes providing intelligence in the form of graphics and images, formats that help the commander rapidly visualize, absorb, and apply the intelligence in his decisionmaking process. A number of "standard" overlays and graphics are associated with the IPB process, however, it is important to note that each situation is unique, and that the type of products generated as a result of IPB will vary considerably based upon the size of the unit, time available, the IRs and characteristics of the mission and area or operations. A modified combined obstacle overlay (MCOO) and threat doctrinal template that support conventional operations may be of limited use in a military operations other than war (MOOTW) mission.

f. Product Preparation. Product preparation involves translating the results of analysis into usable intelligence products that are timely, accurate and tailored to both the unit and its mission. The analyst must strive to provide knowledge that the decisionmaker can easily and quickly visualize and absorb. To the greatest extent possible, that knowledge should be presented in the form of coherent, meaningful images that are easily assimilated by commanders rather than in accumulated lists or texts. A series of standard intelligence products are used to support MAGTF operations. Standard production formats facilitate rapid preparation, mutual support between intelligence sections, ease of dissemination, and, most importantly, familiarity for the user. The baseline production formats provided in this manual can be tailored to meet the requirements of any operational situation. The standard all-source intelligence products prepared within the MAGTF are:

- IPB graphics, matrices, and charts
- The MAGTF contingency intelligence study
- The intelligence estimate
- The target/objective study
- The intelligence summary (INTSUM)
- The intelligence report (INTREP)

1004. Intelligence Analysis and Production Relative to Operations and C2

Intelligence is inseparable from operations. Intelligence drives operations by **shaping** the planning and execution of operations; intelligence provides a menu of factors that the commander will consider when making a decision. It is the analytical and production effort that identifies these factors and presents them to the decisionmaker in a form that enables them to understand the battlespace, place intelligence in context, and utilize the product to carry out successful operations. Analysis and production shapes operations by:

- Identifying potential advantages offered by the environment.
- Defining the limitations imposed by the environment.
- Locating and assessing enemy strengths to be avoided.
- Determining enemy vulnerabilities to be exploited.
- Providing an estimate of likely enemy actions and reactions based on reasoned analysis, synthesis, and judgment

Intelligence and operations must be linked throughout the PDE&A cycle at all command echelons. The PDE&A cycle provides the framework for the implementation of command and control (C2). The principal aim of C2 is to enhance the commander's ability to make sound and timely decisions. Whether the analytical or intuitive approach to decisionmaking is used, intelligence analysis and production aids the commander by reducing uncertainty. Deliberate intelligence production shapes the plan and provides the knowledge that facilitates execution. (See figure 1-3.) Immediate intelligence production identifies changes in the situation that modify the plan or trigger decisions during execution of the operation. Intelligence production provides the basis for assessing the effectiveness of current operations. At the same time, operations drives the analysis and production effort. The mission and commander's intent focus the initial IPB, while the potential courses of action, the concept of operations, the future planning effort, and all IRs determine the scope and content of the production process. Intelligence production is not an end unto itself; intelligence must be relevant to the mission and used to satisfy specific operational and tactical IRs.

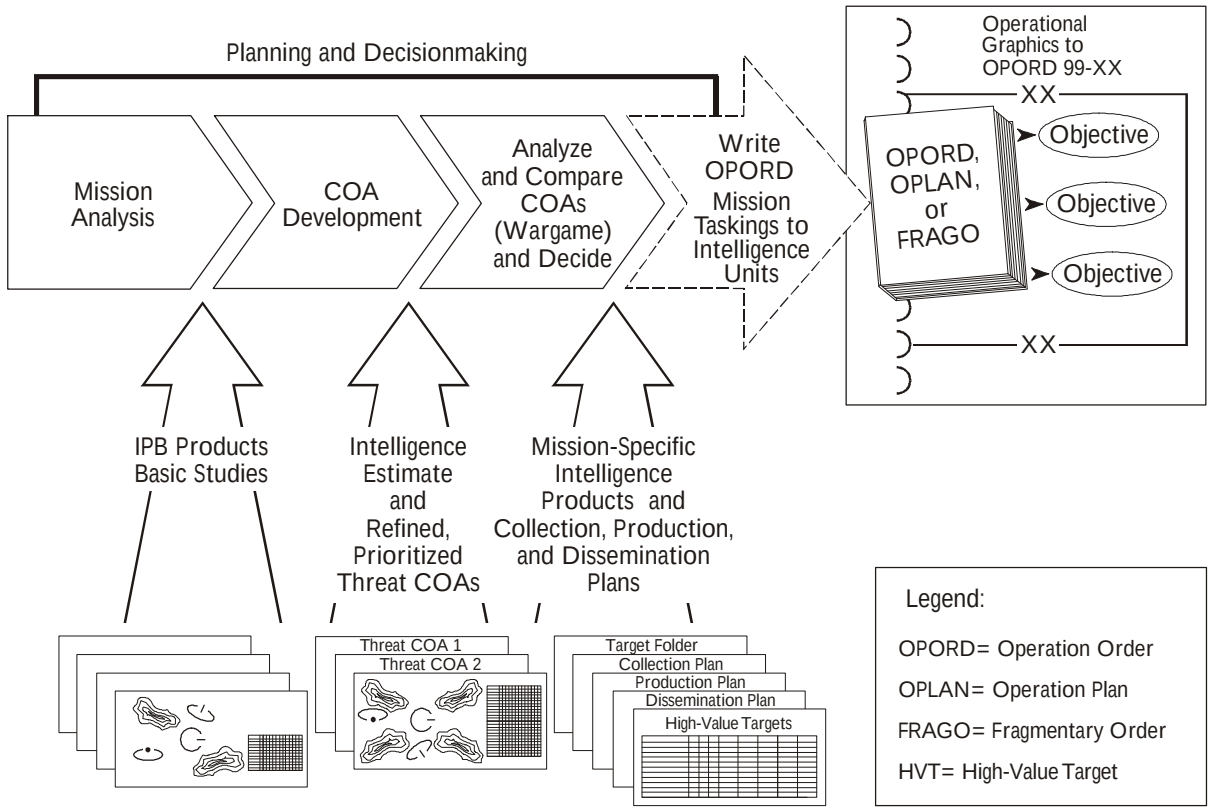

Figure 1-3. Intelligence Support to Planning and Decisionmaking

1005. Responsibilities for Analysis and Production

a. The Commander. Intelligence is an inherent and essential responsibility of command. The commander must be involved personally in the conduct of intelligence activities, providing guidance, supervision, judgment, and authority to ensure a timely and useful product is developed.

The commander's participation in intelligence analysis and production encompasses the following specific responsibilities:

- **Focus the Analytical & Production Effort -** The commander must give guidance and direction to ensure that the intelligence developed through analysis and production satisfies his requirements. His statement of intent and approval of the command's PIRs focus the analytical and production effort. In addition, he should supervise the process to ensure that it is responding to his (and his subordinate commanders) intent and intelligence needs, providing direction in specifics such as the scope of the IPB effort, preferred product formats, and priorities among his subordinates' production requirements.

- **Participate in the Analytical Process -** The commander must understand and participate in the analytical process. Since intelligence analysis is always based on incomplete information and involves assumptions and judgments, the resulting product will never provide absolute certainty. The commander must understand and scrutinize the process, making his own analysis of intelligence operations and resulting products in order to determine its operational impact and overall effectiveness.

- **Evaluate the Product -** The commander must provide timely and specific constructive feedback to his intelligence officer, supporting intelligence battalion commander, and all analysis and production elements. He should identify where the intelligence provided met his expectations and where and how it fell short. Key areas to evaluate include product content, presentation, and timeliness. Meaningful evaluation of the analytical and production effort provides the basis for its continual improvement.

b. Principal Staff Officers. Like the commander, the other principal staff officers play an important role in intelligence analysis and production. Through development of focused intelligence requirements, and recommending which should be PIRs, they assist in directing the intelligence analysis and production effort. They can also assist the analytical effort by making available to the intelligence section the wide range of skills and backgrounds resident within their staff sections. A tremendous synergism can be achieved when task-organized, multidisciplinary teams of intelligence analysts and other occupational specialties are formed to analyze a very specific issue. Likewise, a key component to effective wargaming is a red cell which has experts in various warfighting functions thinking and fighting like the threat. Most importantly, however, principal staff officers must use the intelligence products, evaluate their worth and effectiveness, and provide constructive feedback.

c. The Unit Intelligence Officer. The intelligence officer manages the intelligence effort for the commander, implementing activities that execute the intelligence analysis and production function for the command. In order to effectively carry out his responsibilities, the intelligence officer must be a full participant in the commander's decisionmaking process. Understanding the scope and rationale behind decisions enables the intelligence officer to anticipate future requirements and properly focus the analysis and production effort. Key responsibilities of the intelligence officer for analysis and production are:

- Integrate and focus all-source intelligence on PIRs of the commander and subordinate commanders in order to support estimates of the situation, situation development, COA development, planning and decisionmaking.

- Supervise the development and dissemination of all-source intelligence products that are tailored to the units' needs and concepts of operations, and that are provided in time to support planning and decisionmaking.

- Provide a bottom-line analysis to the commander and his staff of enemy capabilities, strengths, and vulnerabilities as well as opportunities and limitations presented by the environment for use in the decisionmaking process.

- Request analysis and production support for requirements which exceed organic capabilities.

- Insure the nature of the analytical effort and the content of the intelligence product is understood and properly utilized in the planning and execution of combat operations.

d. The Organic Intelligence Section. The unit intelligence section supports the commander, the intelligence officer, and the command as a whole through the development of mission-oriented intelligence products. The analytical and production capabilities of organic intelligence sections will vary with the size of the section and level or type of command it supports. However, all intelligence sections (or their supporting intel bn/intel bn detachment) are capable of performing the following analysis and production tasks:

- Conduct mission-focused IPB analysis and production for the unit's AO and AOI.

- Develop and maintain a comprehensive intelligence estimate.

- Tailor intelligence products produced at all levels to meet specific unit requirements.

- Maintain an accurate all-source picture of the enemy situation in the AO and AOI.

- Prepare target analysis and target intelligence products.

- Provide intelligence operational linkage and communications and information system connectivity with higher, adjacent, supporting and subordinate analytical elements.

With the exception of the MEF intel bn and the Division and Marine aircraft wing (MAW) G-2 sections, organic intelligence sections have a limited capability to perform deliberate production. Prior to the execution phase of an operation, the majority of their effort is devoted to tailoring products developed by dedicated external production elements. However, all intelligence sections produce IPB analysis and intelligence estimates to meet the needs of their commands. During the

conduct of combat operations, organic intelligence sections focus on immediate production and the generation of mission-specific intelligence products such as the target/objective area study. Dependent on the situation and mission, direct support teams (DSTs) may be assigned from the MEF or MSC to augment and enhance the organic analysis and production capabilities of a subordinate unit.

e. Analysis and Production Company (A&P Co), Intelligence Battalion. The A&P Co is the primary all-source analysis and production element of the MEF. The A&P Co is an organic unit within the intel bn and is composed of an IIP, a topographic platoon (topo plt), an all-source fusion center, and two direct support teams (DST). The A&P Co is in general support of the MAGTF and will provide direct support teams to MAGTF subordinate elements, as required. The A&P Co performs the following tasks:

- Assists the intelligence battalion commander with planning, developing and directing the MAGTF intelligence production plan and its integration with the collection and dissemination plans.

- Provides and maintains centralized all-source analysis and production in support of the entire MAGTF within the MAGTF analysis and production cell.

- Maintains an all-source picture of the threat situation for the entire MAGTF AO and AOI.

- Provides geographic intelligence (GEOINT) and geospatial information and services (GI&S) to MAGTFs and other commands as directed and overall C2 of the topo plt.

- Provides imagery analysis and imagery intelligence (IMINT) production support for MAGTFs and other commands as directed and overall C2 of the IIP.

- Provides task-organized, trained and equipped detachments to assist MAGTFs or other designated commands in the processing, exploitation, evaluation, integration, analysis, interpretation, production, and dissemination of all-source intelligence. This includes intelligence DSTs with enhanced intelligence planning, analytical, production and dissemination capabilities that can be either attached to or placed in direct support (DS) of MEF major subordinate commands (MSC) or other MAGTFs.

Although the A&P company is a subordinate element of the MEF intel bn, as the MAGTF's only dedicated production element, the company responds to the IRs of the **entire force.** The MAGTF G-2, through intel bn commander in his role as the intelligence support coordinator (ISC), establishes the A&P company's analytical and production priorities based upon the MAGTF's mission, commander's intent, PIRs, the current and projected enemy situation, and ongoing planning for future operations. The primary focus of the A&P Co is deliberate production. In the garrison or pre-crisis environment, the A&P Co's main function is to conduct IPB of potential contingency areas in order to produce MAGTF contingency intelligence studies. During operations and exercises, the A&P Co develops intelligence to support future operations,

deliberate targeting, and development of the key target/objective area studies. A detailed discussion of the A&P Co organization, functions, and employment is provided in Chapter 9.

Chapter 2

FILTERING, RECORDING, AND EVALUATING

2001. Principles

The production phase of the intelligence cycle begins with receipt of data, information, or intelligence previously developed or obtained from outside the command. Successful production depends upon the careful and thorough preparation of the incoming data, information, and intelligence for analysis. This preparation may overlap with the processing and exploitation phase and encompasses the first three steps of the production phase: filtering, recording, and evaluating. The following principals are employed when preparing information for analysis:

a. Identify Information of Immediate Tactical Value. Every piece of data, information, or intelligence received must be assessed to determine its tactical value and how it affects current operations. Particular attention must be paid to possible “alarms,” “triggers” and high payoff targets (HPT) which are defined by, and tied to, the command’s PIRs, decision support tools, and targeting priorities. If the information is relevant to ongoing operations, immediate production is initiated. The information is rapidly evaluated, analyzed, and disseminated for use by the commander and staff, subordinate and other effected units.

b. Eliminate Redundant and Irrelevant Data Early in Processing. Each item received must be scrutinized to determine its pertinence to the unit's intelligence requirements. The incoming flow of data, information and intelligence must be filtered for relevance to the mission, area of interest, and timeliness as well as redundancy. The objective is to ensure the intelligence analyst is getting everything that is useful to the analytical process while not being overwhelmed with unnecessary information or repetitive reporting.

c. Identify Relevance to Ongoing Production. An important aspect of preparing an item for analysis is determining its impact on the ongoing intelligence production effort. The process should identify how the data, information, or intelligence received contributes to ongoing production in order to determine who should get the information, how urgent the information is, and in what format the information should be provided.

d. Develop and Practice Standing Operating Procedures. Much time and effort can be saved if SOPs for handling information are employed. Standard methodologies for filtering, collating, recording, and evaluating increase the speed at which incoming items are prepared for analysis, provide consistency in the way information is handled, and enhance comprehension of personnel performing these functions as well as the analysts receiving the incoming items. Once SOPs are developed, it is critical that all personnel are trained in and understand the use of these procedures.

e. Employ Reliable and Accessible Recording Tools. Recording is not an end to itself and should never be permitted to interfere with timely analysis, production, dissemination, and utilization of intelligence. However, effective analysis depends in part on the ability to access, recall, and manipulate the stream of all-source data, information, and intelligence flowing into the command. Recording methods should be simple and flexible. Analysts must able to access information when they need it, and receive the information in a form that facilitates understanding and rapid integration with other data, information, or intelligence. The widespread use of automated information systems has enhanced the speed and utility of intelligence recording tools, but care must be used when employing automated information systems (AIS) to ensure the necessary reliability and accessibility is built into the systems and associated backup procedures.

2002. Filtering

Filtering is the discarding of irrelevant or repetitive information prior to its entering the analysis and production process. Current and emerging collection, communications, and intelligence AIS' provide access to a vast quantity of raw data, processed information, and finished intelligence; there is significant potential for information overload of intelligence sections and personnel. An effective filtering system is essential for managing the flow of data, information and intelligence into the unit's intelligence processing/production system.

a. Filtering Criteria. Before being entered into the production process, the relevance of each item to the unit's intelligence requirements must be assessed. Material determined not to apply is discarded without further handling. The following criteria are used in making these assessments:

- Subject Matter -- the content of the data/report must be related in some way to the unit's IRs. Information that has no bearing on the IRs is discarded, unless some potential use or impact of the information on future requirements can be anticipated.

- Location -- the event detailed in the data/report must have occurred within the unit's area of operations or area of interest.

- Time of Occurrence -- the report should have continuing significance, i.e. not relate information overtaken by events. For example, reports of impending air or missile strikes may be received after the strike has begun; such reports are discarded unless they contain new or specific details that may be of analytical importance.

- Redundancy -- multiple reports relating to the same data or event are often received. Reports that repeat the initial information without adding significant additional data or analysis should be discarded.

The unit intelligence officer, ISC, A&P cell OIC, or intelligence COC watch officer establish basic criteria for filtering. It is critical that the filtering criteria be reviewed on a regular basis and

updated to reflect changes in intelligence requirements, the area of interest, and timeliness of information needed.

b . Methodology. Filtering should occur as early as possible in the information processing system. Despite the fielding of automated intelligence systems, such as the Marine Corps' intelligence analysis system (IAS) and the technical control and analysis center (TCAC), often filtering is still largely a manual process. Voice reports, translated documents, images, finished intelligence documents from higher echelons, etc. must still be reviewed by a human and filtered. For machine-readable formatted messages, automated intelligence systems can be a significant tool in the filtering process.

(1) Manual Filtering. Most intelligence sections establish a central point for the receipt and distribution of all incoming intelligence and reconnaissance reports; this is normally the intelligence watch within the COC or the surveillance and reconnaissance cell (SARC). The watch examines each piece of data, information, and intelligence received, compares the content to the filtering criteria, and decides whether to discard the report. Personnel performing the filtering function must be familiar with the production process, understand the filtering criteria-- in particular the unit's intelligence requirements -- have situational awareness, and exercise sound judgment. Intelligence sections should incorporate instruction and practical application in filtering as part of their regular training and exercise programs.

(2) Automated Filtering. Systems such as the IAS can automatically filter incoming messages according to specified parameters such as location, time, and type of report. IAS can also speed the process by correlating incoming information to existing units tracks within the data base. For this automatic function to occur, however, data fields in the formatted messages dealing with location and unit name or identification must be filled or the system will hold the message for manual correlation. Once again, automated systems are a **tool** to assist the analyst, not replace them. To be most effective, the system operator must continually review the filtering parameters and assess if the system is filtering the information effectively. As with strictly manual filtering, IAS operators must be familiar with the unit's intelligence requirements, have situational awareness, and exercise sound judgment.

2003. Recording

a. Purpose. Recording is the reduction of information to writing or some other graphical representation and the arranging of this information into groups of related items. Recording is performed so all items of information can be observed as an integrated picture and studied in relation to each other. Recording information makes evaluation and analysis easier and facilitates preparation of intelligence products by drawing together all available information on a specific subject. It also provides a record of events for post-operation study of the enemy and area of operations.

b. Methodology. Some form of recording is performed by intelligence sections at all levels, and normally involves:

- Registering all incoming information.

- Logging, map or chart marking, filing and indexing, or entering information in the data base of an automated system.

- Maintaining a system designed for rapid and efficient operations by the intelligence section.

At lower levels of command echelons, especially during mobile operations, recording may be no more than the maintenance of a log and marked map, while at a higher command echelons, recording will rely more heavily on automated information systems, electronic data bases, and visual display units. However, no matter what method is adopted , the fullest use should be made of graphic means of recording, i.e., maps, overlays, graphs, charts, which make it possible to visualize and absorb the maximum amount of information in the shortest possible time. The indexing and categorizing of subject matter in a recording system must be related to the projected area, scope and nature of the operations and must be based on:

- The commander's PIRs and all other Irs.

- The anticipated volume of information and frequency of reports at peak periods, i.e., information flow.

The recording means used must be adequate to handle the volume of information and intelligence received and to serve the needs of those who must have access to it. Means and techniques of recording must permit timely dissemination of information and intelligence. In the past, most recording was manually generated either on a map, journal, or status board. Today, automated data processing and information systems such as IAS are the most common recording devices. There are formats and programs available to handle intelligence journals, files, records. Data bases can be updated automatically, and that data recalled and displayed in the form of overlays. Office automation software allows the rapid creation of charts and graphs, the annotation and manipulation of images, and the rapid assembly of words and text.

c. Intelligence Recording Tools. Whether operating in a manual or automated environment, the most common types of recording tools utilized by the intelligence analyst are the intelligence journal, enemy situation map, intelligence workbook, order of battle/analyst files, and target files.

(1) Intelligence Journal. The intelligence journal is an official, permanent, and chronological record of reports and messages that have been received and transmitted, important events that have occurred, and actions taken in response. For each item entered, the journal normally contains a journal entry number; the time the information was sent, received, or noted; the date/time group of the message sent or received; originating agency or addressee; a brief description of the item; and disposition of the information. The journal entry number assigned to an incoming message is recorded on the message itself, and messages are filed in the journal file in the numerical order of the journal entries. The journal, besides providing a brief chronological

account of events, serves as an index to the journal file. The journal covers a stated period, normally 24 hours (see figure 2-1).

INTELLIGENCE SECTION JOURNAL

PAGE NO. 1 | NO. OF PAGES 1

ORGANIZATION OR INSTALLATION: 1st MARDIV

LOCATION: BURGEW, GE (LA567275)

PERIOD COVERED — FROM: HOUR 0001, DATE 07 DEC 80 — TO: HOUR 2400, DATE 07 DEC 80

ITEM NO.	TIME IN	TIME OUT	INCIDENTS, MESSAGES, ORDERS, ETC.	ACTION TAKEN	INL
1	0001		Journal opened 0001		BW
2	0030		5th MAR:Company team A patrol reported		
			enemy supply dump vicinity LA888912.	Map, S3, Cdr	BW
3		0035	ALL UNITS: Execute alternate challenge	CO, Staff, units	DT
			password. Primary compromised at 0700045.		
4	0200		5th MAR:Follow-up to item 2. Search	CO, S3	DT
			results: 12XAT mines, 30,000 rounds 7.62		
			ammunition, 6 rolls barbed wire, all destroy-		
			ed in place.		
65	2400		Journal closed 2400		
			SUMMARY		
			No enemy contact during period, but one		
			enemy ammunition dump destroyed.		

TYPED NAME AND GRADE OF OFFICER OR OFFICIAL ON DUTY: SAMUEL A. MORRIS, CAPT, COC Intel Watch Off

SIGNATURE: SAM

SAMPLE

Figure 2-1. Example of Intelligence Journal Page

(2) Enemy Situation Map

(a) Purpose. The enemy situation map is the primary analytical tool at all command echelons. During fast-moving combat operations, particularly at lower levels, it is often the only recording device used. It is a temporary graphic display of current enemy dispositions, major enemy activities, and other pertinent intelligence and information. By presenting this in

relation to each other, it helps with interpretation, analysis, and decisionmaking. It helps dissemination by permitting the ready transfer of intelligence concerning all enemy forces capable of interfering with the mission of the unit concerned.

(b) Methodology. The enemy situation map should cover enough area to facilitate the conduct of current operations and also the planning of future operations. A large MAGTF, such as a MEF, will normally require three enemy situation maps of different scales:

- Large-scale tactical map (approx 1:50,000) for current ground operations.

- Medium-scale operational map (approx 1:250,000) covering the AO and portions of the AI to record deep enemy installations (airfields, missile sites) and enemy forces that can affect friendly operations.

- Small-scale strategic map (approx 1:1,000,000 or smaller) to cover entire MAGTF AI and beyond.

At lower echelons, one map may suffice. The scale used is dependent on the mission and threat. The map scale(s) to be used should be decided between the G-2/S-2 and the G-3/S-3 during step one of the IPB process (Defining the Battlespace). Often, a combined G-2/G-3 map is used to conserve space in the COC or other C2 cells. If separate intelligence and operations maps are maintained, acetate overlays must be readily interchangeable between maps.

The information displayed on the situation map must be tailored to the mission, nature of the threat or enemy, terrain, the command echelon being supported, the unit's IRs, and force protection and targeting priorities. Generally, enemy maneuver units are posted which are two echelons below that of the friendly unit. Enemy units, regardless of size, in our rear areas are always posted because of the amount of damage they can inflict on C2 and sustainment. The situation map reflects enemy unit identification, disposition, and boundaries; significant terrain and infrastructure features; and the locations of obstacles (manmade or natural).

When plotting enemy activities and dispositions, indicate the latest time when the activity was observed or the disposition was confirmed. All information must be posted using standard military symbols and abbreviations (see FM 101-5-1/MCRP 5-2A, *Operational Terms and Graphics*, for standard symbology). Explain any deviations from these symbols in the marginal data on the map or overlay. Of course, all maps and overlays must be clearly marked with the appropriate classification.

Information is posted on the situation map as it is received and removed promptly when no longer current, since omissions or outdated information may result in erroneous evaluations, interpretation, and decisions. On a hard copy situation map, separate flaps of acetate can be used to record different types of information, reducing overcrowding. Also, to reduce overcrowding, a number or letter system can be used to record significant events or activity. The letter or number is marked at the appropriate location on the map where the activity occurred. On a board or marginal area alongside the map, the same letter or number is recorded along with a notation as to

the activity observed. Use a numbering system that is easily cross-indexed to the journal or message file for a complete report.

(c) Automation. The automated functions of the IAS and other intelligence information systems greatly assists the maintenance of an enemy situation map. Different scale views of the battlefield can be obtained by zooming in and out through various maps. The number, size, and types of enemy units displayed can be changed quickly by the operator to enhance the visualization of the information. Information concerning last report, location, etc., can be called up by clicking on the unit of interest. Electronic "overlays" can be forwarded to other IAS users or to systems such as TCO for display. Information can be easily displayed for briefings using large-screen displays. With robust communications connectivity, a "common picture of the battlespace" can be shared in near-real time with users at separate locations. Some limitations, however, are available communications bandwidth and the size and quality of the information in the data base. Consideration must be given to developing manual and electronic back-ups in the event of catastrophic failure of the system.

(3) Intelligence Workbook. The intelligence workbook is used to record incoming information by subject for ready reference and comparison. It primarily aids in determining the meaning and significance of related items of information. This facilitates further processing, production, and dissemination, particularly the preparation of intelligence summaries and reports. There is no prescribed format for the workbook, however, the most common format is to organize the book according to the various topics in the intelligence summary (see appendix C.) As information is received, it is recorded in one or more parts of the workbook based on its content. For example, a report concerning a newly identified enemy armor unit could be recorded under the section for "New Units" as well as in the section for "Armor." For each entry, reference should be made to the journal entry number for the source report, the time of the event or observation, the location, and a brief extract of the information applicable to that section of the workbook. Maintaining the workbook can be a manpower and time-intensive effort, but if properly done it can be a powerful tool for analysis. The IAS has the ability to parse portions of incoming messages into numerous sections of an electronic data base/workbook simultaneously, based on the operator's selections. Employed properly, this capability can significantly streamline the maintenance of an intelligence workbook

(4) Order of Battle (OOB) Files. OOB files include information and intelligence on the identification, strength, command structure, and disposition of personnel, units, and equipment of any military force. OOB information, along with other information on the threat, terrain and weather, is a key element in the creation of finished intelligence products such as IPB, estimates, and BDA.

OOB can be maintained on threat, allied, and neutral or third party forces. It can be subdivided further into ground order of battle (GOB), air order of battle (AOB), naval order of battle (NOB), electronic order of battle (EOB), weapons of mass destruction (WMD), and other categories tailored to the unit's needs. The amount of subdividing and level of detail maintained in each subdivision depends on the command level where the analysis takes place, the type of threat forces that can influence friendly operations, the mission assigned, and the AOR. A MEF

conducting an amphibious operation may have need to maintain information on all types of forces. Conversely, a battalion or squadron operating as part of sustained operations ashore may focus on those OOB types that most affect them (GOB, AOB), while relying on higher, adjacent, supporting or other service commands in the theater to provide detailed OOB for other types if required (WMD, EOB, NOB, etc.). For each type of OOB, there are specific factors such as composition, strength tactics, training, etc. that are evaluated (see Chapter 6, *Threat Analysis*, for a detailed discussion of each factor). Again, defining what types of OOB will be tracked, the level of detail, and in what geographic area is part of step one (*Defining the Battlespace*) of IPB.

At lower command echelons, OOB analysis is generally more focused, less detailed, immediate in nature, and performed by the unit's intelligence personnel as part of their general duties. At higher levels, particularly at a MEF or MAGTF CE , one or more analysts may be assigned to each type of OOB. At these levels, OOB information normally becomes voluminous in a short period of time. In organizing this information, OOB analysts must maintain extensive and systematic compilations and filing systems. Specific items of information and intelligence must be located on short notice and incorporated into comprehensive reports or analyses. Regardless of the level of command, there are several typical OOB tools which may be utilized, as appropriate, by analysts at the tactical intelligence level. They include:

(a) Unit Workbook. The format for the unit workbook depends entirely on the structure of the enemy force being monitored. It consists of a collection of unit worksheets arranged by type of unit or in numerical sequence. Analysts with OOB baseline documents at their disposal may use them as unit workbooks by inserting additional pages as new information is received. Normally, the parent unit listed on the unit worksheet is equivalent in size to the level of command performing the analysis. Records are normally maintained on units one level above and two levels below, however, this can be modified based on the situation. Unit OOB details are noted in the remarks column. Items such as reports of branch insignia, number and types of weapons, and statements of local residents are entered in this column in abbreviated form. The date and the source of information are recorded for each entry (see figure 2-2.)

Parent Unit _____

SUBORDINATE UNITS	CITY	COORDINATES	INSTL	PERSONALITIES	ID OR CODE NO	REMARKS
Div Hq	Stein	PV818147	1 and 3	Commander COL Crechin		EPW no 26, Captured 2 Feb 68
96 Mech Rifle Regt	Delitach	PU820934	4	Commander COL Kursheve	16181	Document Captured 19 Mar 68
145 Mech Rifle Regt	Ellenburg	PU852961	2	LTC Shrenko	16182	Deserter 21 Mar 68
3d Bn	Gladbach	PV891024	1			Gladbach residents rpt battalion subordinate to Hqs in Ellenburg, 3 Feb 68
43 Med Tk Regt	Linburg	PV863106	3	Commander COL Reshvic		Agent Report 26 May 68
358 Trans-Bn	Lehrt	PV825158	1		16195	OB Bank

Figure 2-2. Sample Unit Workbook Page

(b) OOB Situation Overlay. This is a graphic portrayal of current enemy OOB, either confirmed or unconfirmed. It shows identification and disposition of enemy units and any other information which will assist in developing the enemy OOB. Enemy units down to and including two echelons below the analyst's own level of command are plotted. As with the enemy situation map, standard symbols should be used per FM 101-5/MCRP5-2A. Peculiarities of enemy organizations, the tactical situation, and time and personnel available will determine what will be plotted or omitted on OOB maps. The time and date of the information are entered below each plotted symbol. A caption box on the OOB situation map is an annotation containing information which helps to explain the OOB situation. Although any number of caption boxes may be used, normally three types are necessary: strength, unlocated units, and legend. At lower tactical echelons, the OOB situation overlay and the enemy situation map may be combined for simplicity. At higher echelons, separate types of OOB may be maintained on overlays by the applicable analyst near their work area, with a composite OOB overlay used on the enemy situation map and for briefings (see figure 2-3.) As previously discussed, the IAS allows the rapid generation of tailored electronic overlays based on available database information.

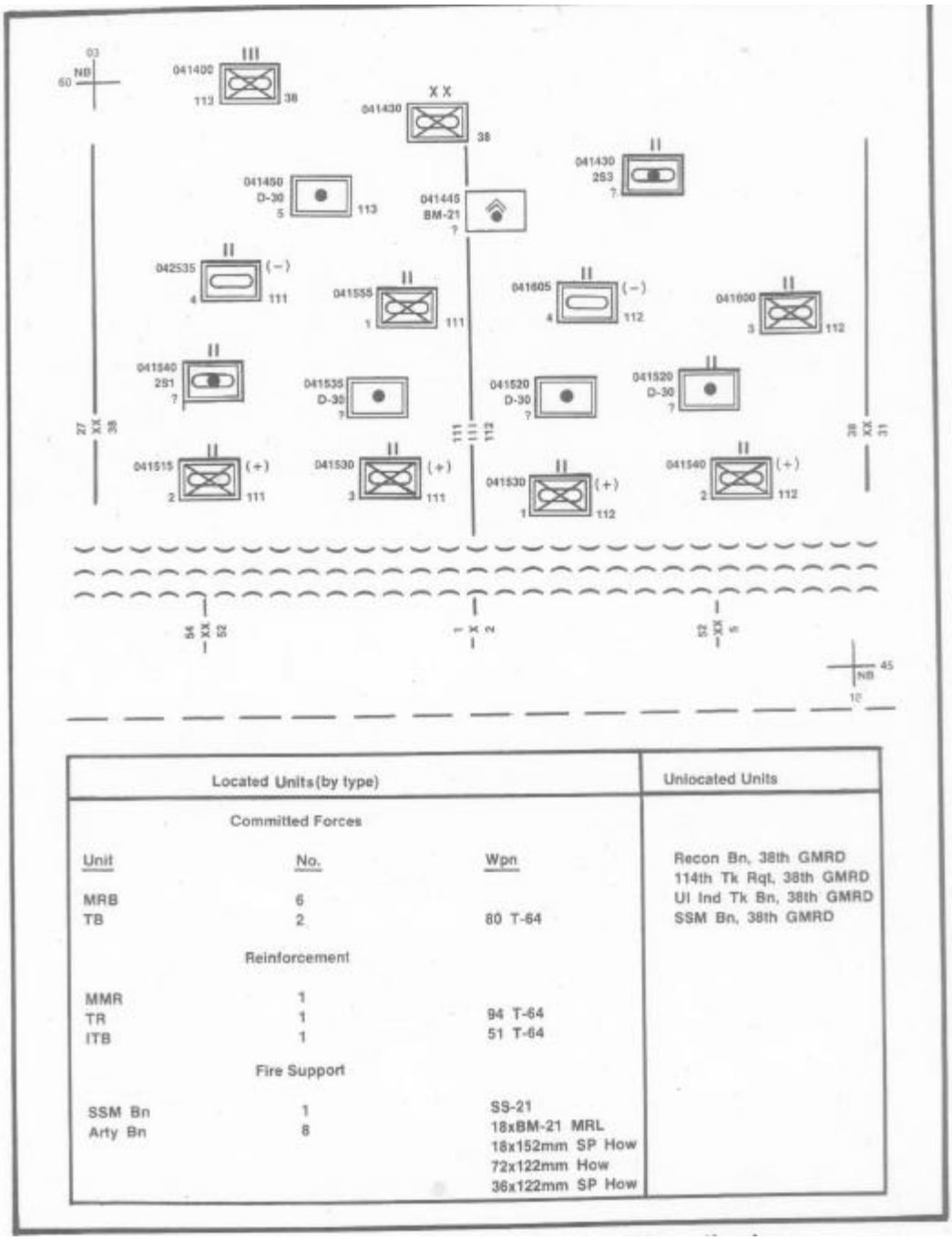

Figure 2-3. Example OOB Overlay

(c) OOB Record (STANAG 2077). OOB record files are used to maintain accurate and complete data on units. OOB records can be maintained at all echelons as necessary. Normally, one record will be maintained on each threat unit in a position to affect current or future operations (see figures 2-4.)

OOB RECORD

PARENT FORMATION									
Service		Formation or Unit name		Alternative Name		Role		Superior Formation	
HQ Location Name		HQ Location Coordinates		Combat Effectiveness		Allegiance		Commander's Last Name	

SUBORDINATE FORMATIONS/UNITS									
Serial Number	Subordinate Unit or Formation Name	Location Coordinates	Role	Signature Equipment	Equipment Quantity	Commander's Last Name	Personnel Strength	Combat Effectiveness	Record Date/Update
Record Evaluation and Source					Remarks				

Figure 2-4. Example OOB Record (STANAG 2077)

The OOB record contains the following minimum information:

- Service (branch of armed forces to which unit belongs, including paramilitary and insurgent).
- Formation or unit name (name or title by which the unit is know).
- Alternative name (unofficial popular name).
- Role (principal function of the unit i.e., command, combat, combat service support, etc.).
- Superior formation (immediate senior formation or unit).
- HQ location name (nearest identifiable town or village).
- HQ location coordinates (UTM and latitude/longitude).
- Combat effectiveness assessment (ability to perform intended mission or function expressed is a percentage).
- Allegiance (entity or country to which unit owes its loyalty).
- Commander's last name.
- Subordinate formations/units:
  - Serial number.
  - Subordinate unit name.
  - Location coordinates (UTM and latitude/longitude).
  - Role.
  - Signature equipment (particular equipment which might identify the unit).
  - Equipment quantity (number of signature equipment in the unit).
  - Commander's last name.
  - Personnel strength (assessed strength).
  - Combat effectiveness.

- Record date/update (date of information or last time record was updated whichever is later).

- Record evaluation and source (listing, if appropriate, of source and reliability as well as validity of the information).

- Remarks (unit history, insignia, etc.).

(d) Personality File. Personality data on designated categories of individuals are recorded. Information on key figures can be of significant value in establishing an opponent's *intent.*

(e) Military Installation File. This file contains all information that has been collected on each installation to include the number and types of buildings and their capacities, personnel uniforms and insignia, and major items of equipment. Maps, town plans, or sketches supplement this file by showing the location of each installation within the city.

(f) Organizational Chart. Depicts the complete organization of all units, from the highest type headquarters to the lowest unit, including personnel and major weapons strengths. Principal weapons and equipment charts may be prepared to supplement organizational charts.

(g) Strength Worksheet. Used to maintain a running numerical tabulation of the enemy's personnel and equipment strengths. This information is recorded on committed units, fire support units, and reinforcements. This may be combined with OOB cards or other unit files. See Chapter 7, *Target Development and Battle Damage Assessment*, for a detailed discussion of combat strength assessment.

(5) Target Files

(a) Target Intelligence Files. Target intelligence files are developed selectively and aggressively to include the targets which, when attacked, will have an effect on the enemy. These files consist of the following information:

- Location. Geographic and UTM coordinates. Desired locational accuracy is within 10 meters.

- Altitude. Meters or feet above sea level of that point of ground on which the target is located.

- Description. Type, shape, attitude, dispersion, and composition.

- Vulnerability. Assessed vulnerability of target to ordnance delivery. Includes construction, degree of protection, and dependence of the target on component parts.

- Recovery Time. Accurate assessment of the time required for the enemy to replace or return the target to active or usable status.

- Accessibility. Location of a target with respect to other terrain or cultural features which may limit the direction or angle of attack.

- Importance. Estimate of how the enemy would be affected by damage to that target.

(b) Target Card Files. These files are comprised of sets of cards, each card containing a target serial number and certain information concerning a specific target. These cards serve as a basis for the preparation of the target list and target bulletins. They are prepared not only for all targets currently in the target list, but also for potential targets which are not listed. Target cards will be prepared and maintained on unlisted targets so that if units change their status, they can be added to the target list without delay. Complete target card files are maintained by all commands who will, at some phase of the operation, exercise control of the target list.

(6) Tools Automation. As previously discussed, the IAS provides an automated means to employ the recording tools discussed above. Taking a subset of an existing data base produced at the national and theater level (currently the modernized integrated data base, or MIDB), and when attached to appropriate communications, the IAS can automatically receive, filter, parse, collate, update, and display threat-related data. That data can be manipulated to provide the functionality of the intelligence journal, enemy situation map, workbook, OOB overlays, OOB files, and target files. Desktop applications software can be used to generate spread sheets for strength tabulations and other types of files.

2004. Evaluation

a. Purpose. In evaluating information, the intelligence section determines its **relevance,** the **reliability** of its source, and its **accuracy**. Evaluating information in this manner is important to analysis by determining the relative value of any given piece of information. It is also critical to determining whether **immediate** or **deliberate** production and dissemination should be performed.

b. Relevance. As each item of information is received, it is examined immediately for its relevance by area, time, and content. The information must be evaluated for intelligence value, urgency, and who needs to see it. Generally, information relating to the AO or AOI is relevant. Information that is not relevant is not processed further. Urgent information is disseminated immediately to those who need it. Information which is not of an urgent nature is usually fully evaluated and interpreted with the resulting intelligence disseminated later.

c. Reliability. Both the source of the information and the agency which collected it are evaluated for reliability. The principal basis for judging the reliability of a source or agency (other than MAGTF units), is previous experience with the source. Criteria for evaluating MAGTF unit reliability include a knowledge of their training, experience and past performance. The

headquarters closest to the source or agency is ordinarily the best judge of its reliability. Consequently, a higher headquarters normally accepts the reliability evaluation of the reporting headquarters.

d. Accuracy. Accuracy involves the probable truth of the information. An indication of accuracy of an item of information may be revealed by considering the degree that that information appears to be true, based purely on logic. Its accuracy is evaluated on the consistency of the information within itself and with other information, particularly information known to be true; and whether the information is confirmed or corroborated by reports from other sources or agencies. The most reliable method of judging accuracy is comparison with other information obtained through other collection sources and agencies. A marked difference in the evaluation of the accuracy of information may occur between higher and lower echelons. Higher echelons have access to more sources of information and intelligence than lower echelons, thus providing more opportunity to confirm, corroborate, or refute the accuracy of reported data. Regardless of the source, the accuracy of each report or piece of information should be reevaluated at each echelon. Although information received from higher headquarters has normally been processed, evaluated and interpreted, the information may be old. New information not available at the time the higher headquarters made its assessment may alter the accuracy.

e. Evaluation Rating System. A technique for evaluating the reliability and accuracy of information is determined by using a standard system in accordance with STANAG 2022. A letter is used to show the evaluation of reliability and a numeral to show the evaluation of accuracy. Evaluation of the reliability of the source is shown as follows:

A - Completely reliable

B - Usually reliable

C - Fairly reliable

D - Not usually reliable

E - Unreliable

F - Reliability cannot be judged

A rating of **A** is assigned under only the most unusual circumstances. For example, this evaluation may be given when it is known that the source has experience and extensive background with the type of information reported. A rating of **B** indicates a source of known integrity. A rating of **F** is assigned when there is no basis for estimating the reliability of the source. Agencies are ordinarily rated **A, B, or C**. However, when the source and the collecting/reporting agency are evaluated differently, only the lower degree of reliability is indicated.

The credibility of information is indicated as follows:

1 - Confirmed by other sources

2 - Probably true

3 - Possibly true

4 - Doubtfully true

5 - Improbable

6 - Truth cannot be judged

If the information confirms currently held information and it can be stated with certainty that the reported information originates from different source it is be classified as "confirmed by other sources" and is rated **1**. If the information confirms currently held information in total or in essential parts and cannot be "confirmed by other sources", but there is no reason to suspect that the reported information comes from the same source as the information already available, it will be classified as "probably true" and will be given the rating **2**. If the investigation reveals that the reported facts, on which no further information is yet available, are compatible with the previously observed behavior of the target, or if the known background of a person leads to the deduction that he might have acted as reported, the information received will be classified as "possibly true" and will be given the rating **3**. Reported but unconfirmed information, which contradicts estimates or the known behavior of the target, will be classified as "doubtful" and will be given the rating **4** if this information cannot be disproved by available facts. Reported information which is not confirmed by available data and contradicts the experience previously assumed to be reliable with regard to a target or issue is classified as "improbable" and will be given the rating **5**. The same classification is given to reported information that contradicts existing data on a subject originally given a rating **1 or 2**. If the investigation of a report reveals that a basis for a rating **1 to 5** is not given, the reported information will be classified as "truth cannot be judged" and will be given the rating **6**. The statement "truth cannot be judged" is always preferred over the inaccurate use of ratings **1 to 5.** If there is no sound basis for ratings **1 to 5** because of the complete absence of other information on the same target, the rating **6** has to be given.

Although both letters and numerals are used to indicate the evaluation of an item of information, they are independent of each other. A completely reliable agency may report information obtained from a completely reliable source which, on the basis of other information is judged to be improbable. In such a case, the evaluation of the information is **A-5**. A source known to be unreliable may provide raw information that is accepted as credible information, when confirmed by reliable sources. In this case, a report is evaluated **E-1.** A report evaluated **F-6** may be accurate and should not be arbitrarily discarded.

Evaluation ratings are most valuable when information is disseminated to higher, adjacent, or lower units. Each item of information in a report should contain an evaluation to aid the recipient in understanding its significance.

Chapter 3

ANALYTICAL THINKING

3001. Analytical Framework

a. Overview. Intelligence analysts seek to enhance the understanding of the commander and staff in order to reduce uncertainty, limit risk, and support planning and decisionmaking. Through analysis, information is transformed into knowledge. By applying judgment to knowledge we achieve understanding, and with understanding of the present we can anticipate the future. This basic framework--**analyze**, **synthesize**, and **estimate**--is at the heart of intelligence analysis and intelligence support to decsionmaking. To achieve the goal of enhanced understanding for the commander, intelligence analysts must understand how decisionmaking occurs, the forms of reasoning, and the pitfalls often associated with analysis. At a minimum, the analyst must:

- Know the commander's mission, intent, and guidance.
- Understand the battlefield framework which includes the area of operations, area of influence, the battlespace, and battlefield organization.
- Understand information management.
- Understand friendly and threat doctrine and tactics.
- Develop PIRs and IRs geared to answer or provide additional information on a threat's capabilities, vulnerabilities, intentions, and courses of action (COA).
- Understand how to use analytical tools, i.e., IPB, automated intelligence systems, databases, I&W, situation development, targeting, and order of battle factors.
- Relate information to the six intelligence functions and METT-T (mission, enemy, terrain and weather, troops and support available, and time available).

b. Analysis. Analysis is a process for commanders and analysts to determine IRs, study information and available intelligence, and determine a threat's capabilities, vulnerabilities, intentions and COAs against friendly operations and systems. The scope and objective of analysis is to take a commander's area of operations (AO) and dissect it for pertinent information. Analysis in its simplest terms requires a whole-- whether it is a geographic region or a subject -- to be broken down into bits and pieces of information and then evaluated for its significance. To turn collected or raw information into useful intelligence, analysts must actively compare it to known friendly capabilities, intentions, and the commanders PIRs. Analysis starts with the

commander defining his battlespace area and PIRs. Analysts can then focus on the area of operations and prioritize all IRs, query intelligence data bases, determine gaps, and leverage collection and production assets in order to ultimately determine a threat's capabilities, vulnerabilities, and intentions. Analysis considers the implications of the battlespace and its constituent parts in terms of depth, width, height, time, and both friendly and threat commanders' IRs and decision cycles.

c. Synthesis. Synthesis is the piecing of information into a coherent, meaningful picture; creating a *whole* from many parts. It is based on the ongoing or previous analysis of separate information and events taking place within a given area. More than simply pulling together information, synthesis determines the relationships that exist among that information. It allows commanders and analysts to see the battlespace as a coherent whole and rapidly discern emerging patterns and indicators. It is from the synthesized picture that we can estimate future threat actions and discern intent. Without synthesis, estimating threat capabilities, vulnerabilities, and intentions cannot occur.

d. Estimation. Estimation is the step in the analytical process that seeks to address future outcomes and probabilities. It is the last step and the bottom line of the analytical process. Building upon the picture developed during analysis and synthesis, the analyst applies experience and judgment to deduce the likely results of patterns of activity he has identified. Estimation is not guessing, but instead is the sound application of reason and logic against known information. The intelligence analyst must base estimates on solid analysis using specific tools and methodologies.

In conventional analysis, the analyst examines, assesses and compares bits and pieces of information, and synthesizes findings into an intelligence product. These products normally reflect an adversaries capabilities and vulnerabilities. Estimation goes one step further, as the objective is not just to establish capabilities, but also determine the threat's intentions and probable COAs. In short, the analyst tries to surmise what the threat intends to do and how this will affect friendly forces.

Estimation is the most challenging element of intelligence analysis and involves a high degree of risk. The intelligence analyst must stretch his or her intellectual resources to the limit to conduct effective estimative analysis. Because the analyst is dealing with a thinking enemy and is subject to all the chance and probabilities inherent to conflict, intelligence estimates will often be wrong. The goal is not to achieve perfection and certainty, but to provide the best estimate possible given the information at hand and the needs of the commander.

EXAMPLE
Information from aerial reconnaissance indicates the movement of approximately 31 moving target indicators (MTIs). The MTI location and time is annotated on a mission report. Based on this report the analyst will conduct several mental functions (**analysis)**, attempt to fuse this information into what is happening in the battlespace, and predict intentions. What steps are taken.
* The MTIs location is plotted on a situation map with the date time group annotated.
* Once plotted the analyst looks for any relationships to previously reported units in the area. If the answer is no, what must be done to find out the who, what, where, and why questions.
* If there is a relationship, we can probably determine what type of unit it is (tanks, armored personnel carriers, etc.). Additionally, the direction of movement is now determined, along with the unit's speed, normally determined as the MTIs pass through named areas of interest.
* With this information the analyst now looks at the bigger picture: does the movement indicate where they will be committed? Is this part of the threat's main effort? Specifically, the analyst is trying to synthesize what this information really means.
* Through the combination of analysis, adjunct information, and seeing what it means overall (**synthesis**), the analyst is now prepared to state the threat's intentions (**estimate**). The estimate, in this case, should specify what the equipment is, the unit designator, speed of march, and when they can be attacked. It is answering the "when," in this case, that is the estimate.

3002. Analytic Problem Solving

At its base, intelligence analysis involves the application of reason and logic to solve problems, with "problems" being defined as what effects will the weather, terrain, and threat have on friendly operations, both current and future. There are several analytical theories, terms, and processes used in problem solving. The ones most commonly used by military intelligence analysts are discussed below. This is not intended to be a checklist, which if followed will result in perfect analysis. Instead, it is intended to educate the intelligence analyst in the mental processes that can and should occur when conducting analysis. It is important to remember that the entire analyze-synthesize-estimate process may occur mentally within a matter of seconds during fast-paced tactical operations. At higher levels, the process may be more involved, with more time available to rigorously apply the techniques that follow.

a. Analytical Theories

(1). Proposition or Premise. Most theories begin with a proposition or premise, which is a statement that may or may not be true. A common example of a proposition is, "An enemy company is defending at NAI #13." When the analyst first creates this mental proposition he is at the *"I wonder if..."* stage of analysis. Because he does not yet know if the statement is

true or false, the proposition is typically rephrased as a question. For example, "Is there an enemy company defending at NAI 13?"

Propositions can be detailed or abstract. The question regarding the enemy presence at NAI 13 is an example of a detailed proposition. A more abstract proposition might be, *"Is the enemy main effort going to be along the landing beaches south of Churchhill?"* This proposition is abstract because no one single observation will confirm or deny it. Instead, multiple collection assets would be used to report on detailed propositions that would then allow the analyst to discern or "infer" the enemy's main effort.

(2). Observable and Inferable. It is important to understand the distinction between observable and inferable. A single collection asset "observes" detailed propositions in a single report. Abstract propositions, however, can only be "inferred" by the analysis of a set of detailed propositions from multiple reports. In military intelligence, the term for a detailed proposition is a **specific information requirement (SIR)**. The doctrinal term for an abstract proposition is an **IR**. Critical abstract propositions can be designated by the commander as **PIRs**. SIRs are normally generated by the intelligence staff to subdivide an IR or PIR into more detailed propositions that can then by addressed through integrated intelligence operation -- collection, production and dissemination -- planning.

The relationship between any two propositions allows an intelligence analyst to make inferences and analyze large amounts of information to produce intelligence (analytical conclusions). This relationship, in its most basic form, is "proposition X *causes* proposition Y." The same relationship can also be expressed as "from the observance of proposition Y, we can infer proposition X."

Example

An example of this relationship is the existence of a regimental artillery group (RAG) at NAI 14 will cause the existence of certain air defense assets in and around NAI 14. In its restated form, from the observance of certain air defense assets in and around NAI 14, we can infer the existence of a RAG at NAI 14.

We also, however, have to take into account the *probability* of each relationship. For example, the types of air defense assets normally associated with the RAG may also protect a logistics support area (LSA) or command post (CP). Hence it is more accurate to state that from the *observance* of a certain type of air defense near NAI 14 we can infer there is a 50 percent probability of a RAG, a 40 percent probability it contains an LSA, and a 10 percent probability that it contains a CP.

(3). A Priori. The probabilities, in the absence of any other information, are called *a priori*. In practice the *a priori* described above are rarely assessed in isolation of any other information. However, in practice we typically possess more information than what is contained in a single report. This leads to the use of a *conditional* probability. An example of this situation states *a priori* of the enemy commander choosing to concentrate his main effort along

avenue of approach number 1 (AA-1) may be 66 percent. The *conditional* probability, however, of the main effort along AA-1 might be 25 percent given that we have observed an unusually large number of combat vehicles on AA-2.

(4). Certainty and Fuzziness. Propositions have varying degrees of both certainty and fuzziness. Certainty is the degree of belief in something. An example of certainty is, *"I personally saw an enemy company at NAI-13, and we have six corroborating reports."* A less certain proposition would be, "HUMINT has a semi-reliable source that claims there is a company at NAI-13, and we have no other reports on the subject."

Fuzziness is the measure of how well the known information matches the desired information. An example of a non-fuzzy proposition is, "Our patrol reports the exact number of enemy soldiers and equipment for an enemy company." A fuzzy proposition would be, "Our patrol reports about half the number of men and equipment of an enemy company, so this could be an augmented platoon, two under-strength platoons, or and extremely weak company."

b. Applied Logic. Typically, intelligence deals with obscure data, few facts, and severe time constraints. As such the ability to apply formal logic in intelligence analysis can be limited. Nevertheless, there are areas of applied logic that are most relevant to intelligence analysis.

(1). Facts, Opinions, Inferences, and Source Reliability. In its most basic form, analysis involves drawing reliable conclusions, based on facts, opinions, and inferences. As information is received it is categorized as either *fact* or *opinion*. From these facts and opinions analysts then make certain *inferences* or conclusions.

(a) Facts. A fact is a statement that has been demonstrated to be true. As an example, it is a fact that you are reading this statement. Given a preference, an analyst will always choose to work with facts. Unfortunately, facts are not always available. In the absence of facts, opinions may be used. Combining available facts and expert judgments, analysts attempt to piece together a picture of the battlefield and the commander's battlespace. When presenting the resulting conclusions, it is important to distinguish between what is fact and what is opinion. As former Chairman of the JCS General Colin Powell once said, "Tell me what you know, tell me what you don't know, tell me what you think...and always distinguish which is which."

(b) Opinions. When facts are unavailable, an analyst might use *opinions*. An opinion is what someone believes to be true. In using opinions in place of facts, it is well to remember that unlike facts, opinions may or may not be true. Sometimes opinions are uttered as statements of fact and often they reflect value judgments. A value judgment is an expression of the "goodness" or "badness" of something. A value judgment is an expression of personal taste, reference, worthiness, merit, quality, excellence, or bias. For example, "ELINT is a far more reliable source of intelligence than HUMINT." In this case, the speaker is making an evaluation or generalization and commenting on how they perceive reality. Analysts must use extra caution when basing conclusions on opinions.

(c) Inferences. Inferences are conclusions drawn from facts, opinions, or other inferences. Noting foliage that appeared discolored in contrast to surrounding foliage, an image interpreter concludes that the area being looked at contains a camouflaged position. Based on expert knowledge of imagery, he has *inferred* the presence of a camouflage position from the *fact* of discolored foliage. Such inferences may serve as input for subsequent problems; in this case determining what is camouflaged at that particular location. It is important to remember that inferences are estimative conclusions. Inferences are particularly important in determining a threat commander's *intent.* Unless the threat commander announces it, intent can only be established by inference. Such inferences are based on facts developed through the continual study of an adversary's doctrine, tactics, and capabilities. Whenever possible, inferences should be drawn from facts, or a mixture of facts and opinion. Conclusions drawn from opinions alone are prone to be wrong and should not carry the same weight as those drawn from facts.

(d) Source Reliability. When evaluating information, analysts are especially concerned with the reliability of the source. Reliability relates to the accuracy and credibility of the information being reported. Normally, analysts expect a highly reliable source to provide accurate information. It must be remembered, however, that even highly reliable humans sources have limitations, and reliable electronic sources may be spoofed. Thus, even information reported from reliable sources should be compared with other facts before being classified as fact itself (see Chapter 2 for a detailed discussion of evaluating sources and information).

(2). Reasoning. This logic deals with the mental process that is brought to bear on facts, opinions, and inferences. Analysts solve problems through reasoning. There are two types of reasoning: *deductive* and *inductive*.

(a) Deductive Reasoning. Deductive reasoning is the process of reasoning from general cases to specific cases. It is the drawing of conclusions from one or more propositions or premises. A proposition or premise is a combination of evidence and *assumptions* which, when combined, lay the foundation for an argument, hypothesis or conclusion. For example, the statement, *"Air strikes and naval bombardment always precede an amphibious landing,"* is a proposition based on an assumption. Propositions may or may not be true; in the case of the statement above, not all amphibious landings have been preceded by preparatory fires. In order for deduction to be used effectively intelligence analysts must make certain their propositions are true, and their reasoning is correct or valid. When an inference or conclusion is said to be valid, it means that the conclusion or inference must necessarily follow the proposition(s). Conclusions can also be unreliable if the propositions are false. What makes a conclusion unreliable is that the validity of the proposition has not been established.

EXAMPLE: Deductive Reasoning
A Naval intelligence analyst is given a report about an unidentified submarine transiting the Polar ice cap. The analyst reasons:
(1) The ability to transit under the ice cap requires long submerged endurance.
(2) The only submarines with adequate endurance are nuclear-powered.
(3) Therefore, The unidentified submarine is nuclear-powered. In this case the analyst reasoned from a general type (submarines) to a specific type (nuclear-powered). He used *deductive* reasoning.

In the example the propositions are stated as facts. However, depending on the time of year, the Polar ice cap can be transited on the surface. Furthermore, the second proposition, although stated as a fact, assumes that the threat has not developed any high-endurance power sources other than nuclear energy. As a result, the conclusion, although valid, is unreliable. In order to be reliable, a conclusion must be drawn from valid and true propositions. If a deductive argument is valid, and if the propositions of that argument are true, then the conclusion of that argument must also be true.

EXAMPLE #2: Deductive Reasoning
During a field training exercise, reconnaissance elements are able to photograph OPFOR tanks in defilade positions. The photos show a main gun tube with a 125mm bore and three track return rollers. Four types of threat tanks are equipped with the 125mm gun (T-64, T-72, T-80, and T-90) but only two have three track return rollers (T-72 and T-90). Since the T-90 was not replicated in this exercise, the analysts conclude that friendly forces will be engaging T-72 tanks. In this case the reasoning went from the general (125mm gun and three return rollers) to the specific (the T-72, which was the only tank with both characteristics replicated in the exercise). The argument is valid and the propositions forming the argument are true, so the conclusion of the argument must also be true.

(b) Inductive Reasoning. The second type of reasoning is inductive reasoning. It is the process of arriving at conclusions based on evaluating facts or inferences.

EXAMPLE: Inductive Reasoning
The following reports reach an intelligence agency regarding the actions of two adversarial countries:
-- Country X is massing armor and artillery along the border of Country Y.
-- Country X has also blockaded sea-lanes used by both countries.
-- Finally, Country X has imposed wartime restrictions on its civilian population.
From these reports, analysts *infer* that hostilities between the two countries are imminent. The analysts are using inductive reasoning.

Induction goes beyond the facts or observations to a statement that has not yet been (or cannot be) verified. Since only verified data can be called reliable, conclusions drawn inductively are somewhat unreliable.

EXAMPLE #2: Inductive Reasoning
An intelligence analyst is given the following information about a Coalition armored vehicle:
(1) Fact #1: Five road wheels and four return rollers.
(2) Fact #2: Armament which included a single 73mm gun, one coaxial and two hull-mounted 7.62mm machineguns, and a single SAGGER anti-tank missile mounted on the barrel of the 73mm gun.
(3) Fact #3: Crew of four with three passengers
(4) Inference #1: A maximum speed *estimated* to be 80kph.

From these characteristics the analyst inferred that the reported vehicle was a Russian-made BMD. Since he reasoned from a number of separate facts or inferences to arrive at a conclusion he used inductive reasoning.

The strength of an inductive argument depends on how probable it is that the conclusion would be true if the premises or propositions were true. Inductive arguments are characterized as being "strong" or "weak" vice "valid" and "invalid". Arguments are made strong by:

- The number of instances cited in the propositions.
- The number of propositions that confirm the conclusion.
- The closer in time the occurrences are to the conclusion.
- Dissimilarities in the evidence which still support the conclusion.

Very often propositions used in deduction are arrived at inductively and vice versa.

EXAMPLE #3: Deduction and Induction
Major proposition: The massing of troops along a border is a prelude to war.

Minor proposition: A country is known to have massed troops along the border.

Conclusion: This country is about to initiate war with its neighbor.

At first glance, the deductive argument shown above might seem acceptable. A closer look will show, however, that a major weakness of the argument is that the major proposition is not always true. In certain instances, troops could be massed for internal security, exercises, or a show of

force. The major proposition--derived from inductive reasoning--by itself is an ambiguous signal. Assuming the propositions are true, and assuming the analyst reasoned validly, we can say the conclusion the analyst reached is valid. An analyst may reason correctly, but from data that is incorrect, thus arriving at conclusions that are not true.

(3) Tests of Truth. Both inductive and deductive reasoning involve determining the "truth" of propositions. There are three basic tests of truth which intelligence analysts may employ.

(a) Correspondence Test of Truth. An analyst studying an information report notices that all presented information is the result of firsthand observation. Knowing the source to be professionally competent, the analyst assumes that every statement in the report corresponds to reality. The theory that "truth" is a statement that corresponds to reality is known as the *Correspondence Test of Truth*.

EXAMPLE: Correspondence Test of Truth
Pilots returning from an interdiction mission claim three tanks destroyed. The squadron S2 chief interrogated each pilot separately and all gave substantially the same report.

Assuming the pilots' claims are accurate, then it would reflect reality. By reporting BDA of three tanks probably destroyed, the S2 chief is adhering to the *Correspondence Test of Truth*.

Despite the fact that all pilots of one flight claimed three tanks destroyed, the MAGTF commander wants more supporting evidence. The MAGTF G2 plans a UAV mission over the area where the tanks were reported hit to provide confirmation. Both the commander and the G2 are placing more credibility in visual evidence because it is believed to be more objective and less prone to human error. This ignores the fact that video requires interpretation, and this interpretation involves a degree of subjectivity.

All images must be interpreted by humans. When humans interpret images they use subjective judgment. One of the weaknesses of the *Correspondence Test of Truth* is that observations are required to establish "truth." Invariably, these observations must themselves be tested by other observations.

The UAV tape revealed three badly damaged tanks in defilade positions. The MAGTF BDA analyst now considers the UAV report along with the pilot debriefs, and based on this information reports three tanks confirmed damaged.

In the above example, the "truth" was how well statements or other evidence corresponded to reality. To test the degree of correspondence, observations are required. These observations themselves must be tested by additional observations. The chief criterion in observations is objectivity. Greater objectivity can be attained by using a mix of collection assets. Analysts naturally place more confidence in one source or system than another. In the case of the UAV verses the pilot reporting, the UAV's loiter time and ability to observe the target from multiple

aspects gave the information derived greater credibility than the information from the pilot who may have only had a fleeting glimpse of the target while trying to egress. When a variety of sensors tend to corroborate each other, confidence in the conclusions increases (probably destroyed to confirmed damaged).

The *Correspondence Test of Truth* requires observations to test whether or not, and to what extent, statements correspond to reality. One problem with this theory in practice is that seldom does the threat permit direct observations; in fact, the threat often goes to great lengths to prevent direct observations or to deceive those observations made.

(b) Coherence Test of Truth. Where direct access to the threat is denied, the *Coherence Test of Truth* becomes necessary. The coherence theory refers to how consistent different pieces of information are in relation to each other. An analyst considering a new piece of information which corroborates what he already knows would place more credibility in the new information and the conclusions drawn from it. Unlike the *Correspondence Test of Truth*, where observations are used to validate statements, the *Coherence Test of Truth* uses *consistency* with other ideas or facts to validate statements.

EXAMPLE: Coherence Test of Truth
In the latter part of September, the CINC J2 staff considered the following information:
(1) The ACME coalition countries normally conclude a training cycle with a large-scale combined exercise (historical record).
(2) Visitors to Coyote land reported being denied access to certain areas in the vicinity of Road Runner, in western Tunnel province. (This report has been confirmed)
(3) Reports indicate certain infantry, armor and engineer units from Tasmania, Elmer Land, and Chickenhawk have moved from their garrison locations. (Reports unconfirmed)
(4) All commercial air traffic to Road Runner will be restricted for a period of two weeks, starting 01 October. (Report confirmed)

The intelligence staff concluded that this year's ACME exercise would take place in or near Road Runner, Tunnel province, during the period 01 to 14 October. Although no one piece of information pointed directly to this conclusion, all pieces of information seemed consistent with each other as well as to the conclusion.

Intelligence rarely works entirely in the realm of theory. Usually there is some factual basis for most inferences or conclusions. It is proper to consider the *Coherence Test of Truth* as supplementing the *Correspondence Test of Truth*.

(c) Pragmatic Test of Truth. The *Pragmatic Test of Truth* proposes that a given statement is true if it works in practice.

EXAMPLE: Pragmatic Test of Truth
Prior to the Battle of Cape Esperance in World War II, Admiral Norman Scott organized his task force into a long, single column. He believed this "line-ahead" formation would be the most effective against the night tactics practiced by Japanese units. In the ensuing battle, Scott sank two Japanese destroyers and severely damaged two cruisers. After the battle, Admiral Scott concluded the "line-ahead" formation was indeed effective and when combined with his radar-controlled fire control systems he could master any night battle. Admiral Scott believed the results of the battle supported his original theory regarding the effectiveness of the line-ahead formation.

While a practical tool, the *Pragmatic Test of Truth* has some significant weaknesses. First, the results may only appear to justify the means used to achieve them. Second, the successful outcome cannot necessarily be attributed to the means used to achieve it because other factors may have produced the same outcome. In the Admiral Scott example, the use of radar-controlled guns may have produced the same result no matter what formation used. Lastly, an unsuccessful outcome does not necessarily imply that the means used were unsound; again, other unknown factors may have contributed to the unsuccessful outcome.

3003. Pitfalls of Analysis

The application of logic and reasoning is a human, mental process. Despite our best efforts, as humans we are subject to numerous influences which shape and mold our view of the world and our ability to reason about it. Intelligence analysts involved in discerning facts, inferences, and conclusions, are prone to the same errors, which will be collectively referred to as *pitfalls of analysis*. It is important for analysts to be able recognize these pitfalls--both in relation to their own analysis and the analysis performed by others--in an effort to minimize their impact. Analytical pitfalls may be grouped into two general categories: *logical fallacies* and *biases*.

a. Logical Fallacies. Logical fallacies are errors in the reasoning process caused by the failure to apply sound logic. Though usually committed accidentally, they are sometimes used deliberately to persuade, convince or deceive. Logical fallacies may be broken into two categories: *omission* and *assumption*.

(1) Omission. Fallacies of *omission* leave out something important. The argument may omit a consideration of many cases; it may omit a consideration of a hypothesis that would account for the same conclusion; or it may omit something unfavorable to the argument. Fallacies of *omission* can occur in many forms.

(a) Oversimplification. Oversimplification is a generality that fails to adequately account for all the complex conditions bearing on a problem.

EXAMPLE: Oversimplification
"The M1A1 tank won the Gulf War." This statement ignores the fact that the M1A1 tank was only one of many weapons used during the Gulf War.

Oversimplification includes ignoring facts, using generalities, and applying an inadequately qualified generalization to a specific case. Oversimplification results when one or more of the complex conditions pertaining to a certain situation are omitted.

EXAMPLE: Oversimplification #2
An ordnance specialist inspecting a captured hand-carried, surface-to-air missile launcher concludes that the threat has no effective low-level air defense. His assessment is based on the fact that the launcher is equipped with antiquated guidance mechanisms.

The ordnance specialist's conclusion omits the following considerations:

- That the launcher was "planted" by the threat to give a misleading picture of their true capabilities.
- That the threat abandoned the launcher because it was ineffective and more capable systems were available.
- The weapon may have been deliberately doctored to mislead weapons experts.
- Other weapons such as anti-aircraft artillery, small arms, etc., can be very effective in some situations.

(b) Hasty Generalization. *Hasty generalizations* are conclusions drawn from samples that are too few or from samples that are not truly representative.

EXAMPLE: Hasty Generalization
After interrogating an enemy prisoner of war (EPW), the interrogation officer reports the threat's morale as extremely low and that capitulation is imminent.

In this case, the interrogator is making a *hasty generalization* because the sample population considered (one EPW) is too small.

(c) Composition. The fallacy of *composition* is erroneously reasoning from the properties of a single entity to properties of a group.

EXAMPLE: Composition
During a skirmish with a Viet Cong battalion, a single EPW was captured. This EPW was suffering from malaria and malnutrition and his morale was obviously low. It was noted that he was equipped with a semi-automatic weapon of WWII vintage. After a brief interrogation, the intelligence analyst reported the enemy battalion recently engaged was starving, diseased, and poorly armed.

Remarks: What the intelligence analyst failed to consider was that--

- Perhaps a reason only one prisoner was captured was because he was too sick to keep up with the rest of the battalion.
- Because the weapon was of early vintage did not necessarily make it ineffective.
- Few captured prisoners have high morale; in fact, low morale could just as easily result from being captured as it could contribute to being captured.

In this example, besides falling prey to *hasty generalization*, the analyst has also demonstrated the fallacy of *composition* by applying the properties of a single prisoner to an entire enemy unit.

(d) Division. The opposite of *composition*, the fallacy of *division* erroneously assumes that the characteristics of a group exist in every member of that group.

EXAMPLE: Division
Members of the threat's Guards Brigade had never surrendered in previous combat. After a recent engagement, an EPW stated he was a member of the Guard's Brigade. The interrogator doubted the EPW's statements because personnel from that Brigade never surrender.

In this example, the interrogator committed the error of *division* by assuming that since no Guard's Brigade personnel had ever surrendered, the EPW could not be from that Brigade. The analyst took the characteristics of a *unit* and uniformly applied them to every member of that unit. There are rarely absolutes, and there are exceptions to most rules.

(e) Special Pleading. In *special pleading*, only one side of an argument is presented.

EXAMPLE: Special Pleading
At the conclusion of a staff study, the staff members--all proponents of the proposed COA--are directed to list the pros and cons of the proposal.
Arguments for the proposal:

- Job requires little to no increase in manpower
- Can save the government $2 million dollars
- Minimum risk to personnel
- Equipment readily available
- Little special training required

Arguments against: None.

By omitting arguments against, the staff committed the fallacy of *special pleading*. This fallacy also arises when the many interacting forces that give rise to a situation (cause and effect) are ignored.

(f) Post Hoc. In the fallacy of *post hoc* ergo *propter hoc* (before the event, therefore caused the event), consideration of other factors which might have accounted for the same result are omitted. *Post hoc* fallacies often occur when trying to establish cause and effect.

EXAMPLE: Post Hoc
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.

(g) False Dilemma. The fallacy of the *false dilemma* omits consideration of more than two alternatives.

EXAMPLE: False Dilemma #1
"Either we attack at dawn or the enemy will be too strong."

The two words that generally warn of a potential false dilemma fallacy are *either* and *or*. False dilemmas are closely related to the fallacy of the *excluded middle*. Both fallacies ignore or exclude consideration of options other than two extreme positions. False dilemmas are fallacies because middle alternatives are excluded.

EXAMPLE: False Dilemma #2
An S2 reports to his commanding officer that the "...enemy has only the capability to either defend in place or retreat."

The S2 has committed the fallacy of *false dilemma* because he has failed to anticipate or is ignoring other considerations, namely:

- That the enemy could attack if they were willing to accept high casualties.
- That the enemy could withdraw to an alternate defensive position.
- That the enemy could conduct a delaying action.

(2) Assumption. Fallacies of assumption relate to *begging the question* (also referred to as *circular reasoning*), *stating hypotheses contrary to fact*, *"poisoning the well,"* and *misusing analogies*. All of these fallacies implicitly or explicitly involve assumptions, which may or may not be true.

(a) Begging the Question. This is a fallacy that occurs when a speaker *assumes* he is giving a legitimate response to a question, when in fact he may be merely rephrasing the question.

EXAMPLE: Begging the Question #1
A platoon leader, when asked why he was unable to pin down the enemy by fire, replied that, "Our suppressive fire was inadequate."

The fallacy in this response is that suppressive fire, by definition, is fire that pins down the enemy or is intended to pin him down; the inadequacy of this fire was self-evident, since the platoon failed to pin down the threat.

EXAMPLE: Begging the Question #2
(Pilot to debriefing officer:) "In response to your questions about whether or not all of my bombs landed on target, I'd like to say that as soon as I completed my pass there were two large secondary explosions."

The pilot begs the question by shifting attention from the primary issue to a secondary one. His response did not address the question he was asked.

(b) Stating Hypotheses Contrary to Fact. This fallacy occurs when someone states decisively what would have happened had circumstances been different. Such fallacies involve assumptions which are either faulty or simply cannot be proven or verified.

EXAMPLE: Hypotheses Contrary to Fact
"If we had not supported Castro in his revolutionary days, Cuba would be safe for democracy today."

Besides being a gross oversimplification, the assumption made in the statement cannot be verified.

(c) "Poisoning The Well." This fallacy involves seeking to discount evidence before it is presented, most often by discrediting the source.

EXAMPLE: Poisoning the Well #1
An ardent spokesman against the value of strategic bombing states, "You can't trust that man's testimony regarding the effectiveness of strategic bombing; he's employed by the Air Force."

The specific impression the speaker is trying to create is that the testimony is necessarily biased because the testifier represents a certain organization. He seeks to discredit contrary evidence by making the *assumption* that the testifier is biased.

EXAMPLE: Poisoning the Well #2
One intelligence analyst says to another engaged in pilot debriefs, "Be careful with this man. It's his first mission."

Again, the effect of this statement is that it intends to discredit evidence before it is presented. It pleads against the circumstances of the subject with the *assumption* that the pilot's lack of experience will result in bad information.

(d) Misusing Analogies. Analogies are strong tools that can be used to impart understanding in relation to 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. The strength of a conclusion drawn from analogy is proportional to the degree of similarity between two objects or events. The danger in reasoning from analogy is assuming that because objects, events, or situations are alike in certain aspects, they are alike in all.

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. When one generalizes indiscriminately from analogy to real world, this is misusing analogies. One method for weakening an analogous argument is by citing a counter-analogy. A counter-analogy weakens the original analogy by citing other comparisons that can be made on the same basis.

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

Despite its powerful imagery, the analogy used by Sir Winston Churchill was misused by trying to attribute animal characteristics (soft belly) to an inanimate object (the Axis).

b. Biases. If a single term best describes the factors that interfere with successful analytic thinking, that term would be *bias*. A bias is a subjective viewpoint. It indicates a preconceived notion about someone or something. It is important to recognize biases and be aware of the potential influence they can have on judgment. Biases can have a positive influence on analysis. With a lack of information, a preconceived notion can give the analyst a starting point for thinking about a situation. However, biases generally have a detrimental impact because they obscure the true nature of the information. The analyst needs to recognize several categories of biases so that he isn't misled or does not draw the wrong conclusions during the analysis process. Biases can be cultural, organizational, personal, and cognitive (perception).

(1) Cultural Biases. As Americans we 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*. It interferes with our ability to think the way an enemy commander might think, or to give informed advice to policymakers on the likely reaction of foreign governments to American policy. Cultural bias is also known as *mirror-imaging*, or attributing someone else's intentions, actions, or reactions to the same kind of logic, cultural values, and thought processes that characterize ourselves.

It is difficult to avoid cultural bias, but some measures can be taken to lessen its impact. The best method is to locate individuals who were born or raised within that country or culture and either include them within the analytical process, or ask their opinion about likely responses to friendly actions. Care must be taken to not put total faith in their opinions, since they themselves may be

subject to biases regarding different ethnic groups or cultures in the region. Likewise, their knowledge of a particular society may be dated and no longer accurate.

Another balance against cultural bias is to locate regional experts such as foreign area officers (FAO) and regional area officers (RAO), who have lived or traveled through the area and are somewhat conversant regarding the culture. Again, the quality of the information provided must be assessed against the level of knowledge and experience that individual has for that culture or region.

(2) Organizational Biases. Most organizations have specific policy goals or preconceived ideas. Any analysis done within these organizations may not be as objective as the same type of analysis done outside the organization. Some of the problems that occur from a subjective internal analysis range from unconsciously altering a judgment because of exposure to selective information and common viewpoints held among individuals (group-think), to deliberately altering a judgment to provide the commander with only what he wants to hear (Best Case). Best case is where the analyst presents only good news, or couches bad news in the most optimistic light so as not to anger the commander. Group-think can be combated by involving people outside the organization in the analysis. Best Case can only be avoided by having the moral courage to tell the commander the whole story; good and bad.

(3) Personal Biases. Personal biases stem from past experiences. If a thought pattern previously led to success, the analyst tends to continue to follow this pattern. Even if the situations have nothing in common, the tendency to follow the methods that were successful in the past is very strong.

(4) Cognitive Biases. The all-source intelligence analyst evaluates information from a variety of sources (HUMINT, SIGINT, IMINT, open source, etc.). Each source has strengths and weaknesses. 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. The cognitive biases that will give the analyst the most problems are vividness, absence of evidence, oversensitivity to consistency, persistence of impressions based on discredited evidence, and availability.

(a) Vividness. Clear and concise information has a greater impact on thinking than abstract and vague information. Even if the vague piece of information has more value as evidence, the tendency is to disregard it more readily than a clear piece of information would be disregarded.

(b) Absence of Evidence. Lack of information is by far the most common problem, especially in the tactical environment. The analyst must do the best he can with limited information and avoid holding back information because it is inconclusive -- it rarely is. The analyst must realize that information will be missing. He should identify areas where information is lacking and consider alternative hypotheses; judgments can be adapted or adjusted as more information becomes available. Also, he should consider whether a lack of information is normal in those areas or whether the absence of information itself is an indicator.

(c) Oversensitivity to Consistency. Consistent evidence will be a major factor for confidence in the analyst's judgment. On the one hand, consistent information is appropriate. On the other hand, information may be consistent because it's redundant, or it may be coming from a small or biased sample. The analyst needs to consider if the evidence represents the total potentially available information. If it does not, or if it is not known, then the confidence level should be low, regardless of the consistency. The analyst must be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.

(d) Persistence of Impressions Based on Discredited Evidence. Whenever evidence is received, there is a tendency to think of connections that explain the evidence. Impressions are based on these connections. Though the evidence eventually may be discredited, the connection still remains, and so do the impressions.

(e) Availability. The ability to recall past events influences judgment concerning future events. Since memory is more readily available, hence more acceptable, it is easy to rely upon memory instead of seeking a proper sample to predict events.

3004. Intelligence Analysis and Decisionmaking

One principal aim of intelligence analysis is to allow the commander to make timely and informed decisions. The commander’s ability to make decisions is always influenced by uncertainty and time. All decisions must be made in the face of uncertainty. Theoretically, we can reduce uncertainty by gaining more information, but any such decrease in uncertainty occurs at the expense of time. Ultimately, it is not so much the amount of information that matters, but the right elements of information available at the right time and place.

a. Analytical Decisionmaking. There are two basic approaches to decisionmaking: analytical and intuitive. In analytical decisionmaking, several options for solving the problem at hand are identified, studied, and compared to arrive at the best solution. The basic idea is that comparing multiple options concurrently will produce the optimal solution. As a result, analytical decisionmaking tends to be methodical and time-consuming. Theoretically, reasoning power matters more than experience.

b. Intuitive Decisionmaking. In intuitive decsionmaking, the commander assesses the situation in an effort to recognize a pattern; once a pattern is identified, experience and judgment guide the commander in evaluating the key elements of the problem and rapidly determining a satisfactory solution. The intuitive approach focuses on situation assessment instead of on the comparison of multiple options. Intuitive decisionmaking aims at “satificing,” finding the first solution which will satisfactorily solve the problem, rather than on optimizing, as the analytical approach attempts to do. Because it does not involve comparing multiple options, intuitive decisionmaking is generally much faster than analytical decisionmaking.

c. Intelligence Analysis and Decisionmaking. Each approach has strengths and weaknesses; although conceptually distinct, the two are rarely mutually exclusive in practice.

Intelligence supports both approaches. Intelligence supports analytical decisionmaking by helping to identify the options available and provide the framework (in the form of estimates and studies focused on the threat and key factors of the battlespace) for analysis and comparisons of those options. Intelligence supports intuitive decisionmaking by providing the knowledge that helps the commander to recognize emerging patterns. The process of intelligence analysis itself employs both analytical and intuitive decsionmaking to arrive at the conclusions presented to the commander. The IPB process, particularly if all the various types of products are prepared in detail, is a distinctly analytical process. The decision support template (DST) derived from the IPB process, however, is a tool that facilitates intuitive decisionmaking. Generally, the analytical approach conforms well to the pre-hostility or contingency planning phase, while the intuitive model is usually more appropriate during execution of tactical operations. The challenge for the intelligence analyst is knowing how much and what kinds of information the commander requires. Too much information may only confuse an intuitive decsisionmaker, and his information requirements will change continually. Too little information for an analytical decisionmaker may result in procrastination and the continual demand for more. The key to overcoming these challenges is a solid understanding of the commander, constant interaction through training and exercises, and a well developed process for identifying information requirements.

Chapter 4

INTELLIGENCE PREPARATION OF THE BATTLESPACE

4001. Concept

Intelligence preparation of the battlespace (IPB) is an analytical tool and process that is utilized to help understand the enemy, weather, terrain and other aspects of the environment, and the options and impact it presents to both friendly and threat forces. It is a systematic, continuous process of analyzing the threat and environment in a specific geographic area to determine and evaluate threat capabilities, vulnerabilities, and probable courses of action. It is designed to support staff estimates, planning and decisionmaking. The results of IPB are incorporated into the intelligence estimate, but more importantly, it provides knowledge-based intelligence that can be visualized and absorbed by decisionmakers. The IPB process emphasizes providing intelligence in the form of graphics and images -- formats that help the commander rapidly visualize, assimilate, and apply the intelligence in the decisionmaking process. The use of graphics to display intelligence increases the commander's ability to discern patterns as they are emerging and conduct recognitional or intuitive decision making, thereby increasing operational tempo.

4002. Process

The principles and steps of the IPB process remain constant regardless of the type of mission or size of staff section conducting IPB. The steps are:

- Define the battlespace environment
- Describe the battlespace effects
- Evaluate the threat
- Determine threat COAs

The application of these principles, however, varies with each specific situation. There is no one right way to do IPB. IPB requirements for a humanitarian assistance operation will significantly differ from combat operations against a conventional armed force. A given unit or staff section does not always prepare all IPB products in every situation. Determining which products to prepare and identifying their relative priority depends on the factors of METT-T and command guidance. IPB is an interactive process. Operations and intelligence must have a common focus

to successfully apply the IPB process (see FM 34-130/FMFRP 3-23-2, *Intelligence Preparation of the Battlefield*,[1] for a detailed discussion of the IPB process).

a. Step 1-- Define the Battlespace Environment. The first step is to identify for further analysis specific features of the environment or activities within it, and the physical space where they exist, that may influence available friendly and enemy COAs and the commander's decisions. This step consists of the following:

- Identify significant characteristics of the environment.
- Identify the limits of the command's AO and battlespace.
- Establish the limits of the AOI.
- Identify the amount of detail required and feasible within the time available for IPB.
- Evaluate existing data bases and identify intelligence gaps.
- Collect the material and intelligence required to conduct the remainder of IPB.

(1) Identify Significant Characteristics of the Environment. Characteristics of the battlespace environment that will influence the commander's decisions or affect the COAs available to your own force or the threat are of special significance. During a humanitarian assistance operation, for example, the location and activities of civilian relief organizations might be a significant characteristic of the battlespace. During support to counter-drug operations, significant characteristics might include production of narcotics or trading of weapons. During a conventional war, typical characteristics include location and activities of enemy reserves, reinforcements, and long range fire support. When identifying significant characteristics of the battlespace, consider threat forces and all other aspects of the environment that may have an effect on accomplishing the unit's mission. Depending on the situation, these might include:

- Geography, terrain, and weather of the area.
- Population demographics (ethnic groups, religious groups, age distribution, income groups).
- Political or socio-economic factors, including the role of clans, tribes, gangs, etc.
- Infrastructures, such as transportation or telecommunications.
- Rules of engagement (ROE) or legal restrictions such as international treaties or agreements.

---

[1] FM 34-130/FMFRP 3-23-2 is now under revision with an estimated publication date during 2000. Upon approval it will be designated and retitled as MCRP 2-12A, *Intelligence Preparation of the Battlespace*.

- Threat forces and their capabilities, in general terms, to include paramilitary and unconventional forces.

Initially, examine each characteristic only in general terms to identify those of significance to the command and its mission. Further evaluation of each characteristic takes place during later steps of the IPB process. Identifying the significant characteristics of the battlespace environment helps establish the geographical limits of the AOI and directs analytical efforts in steps 2 and 3 of the IPB process. It also helps identify gaps in the type of information and intelligence required to complete the IPB process and answer the PIRs and IRs (see Figure 4-1.).

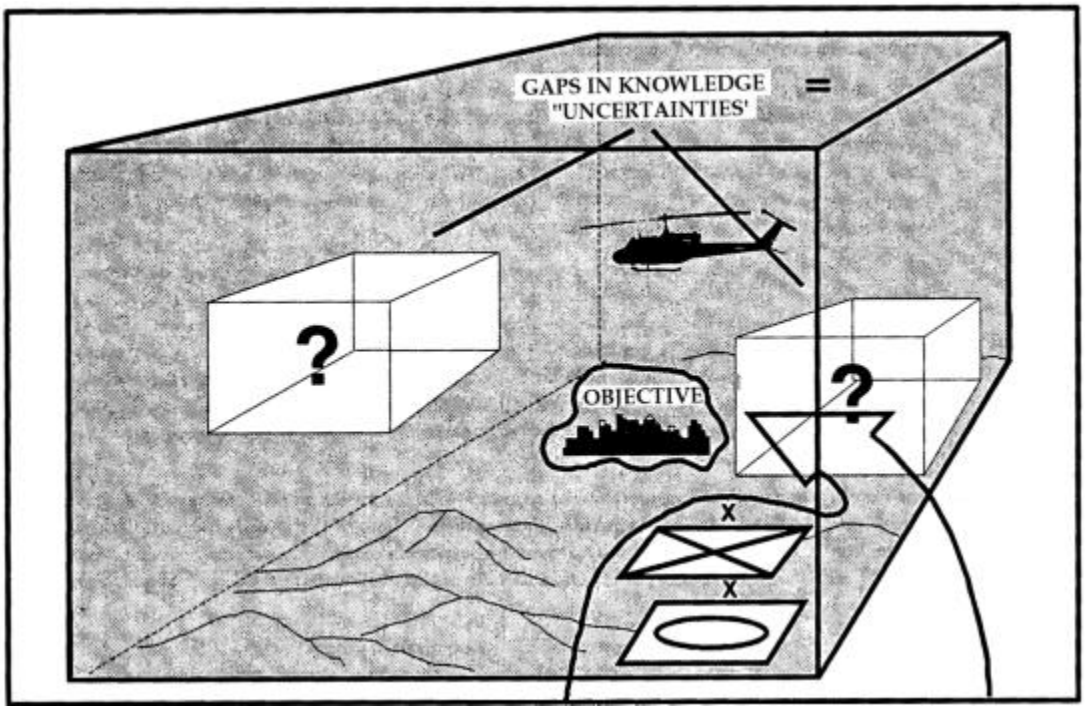

Figure 4-1. Examining the Battlespace

(2) Identify the Limits of the Command's AO and Battlespace. The **area of operations (AO)** represents an area in which the authority and responsibility for the conduct of operations has been assigned to a commander. The limits of the AO are normally the boundaries specified in the OPORD or execute order from higher headquarters that define the command's mission.

- The **area of influence** is the geographical area where a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command and control (C2). The area of may well extend beyond the area of operations based on the range of organic or supporting weapon systems.

- The **area of interest (AOI)** is selected by the commander based on the estimate of the situation. The dimensions are not constrained by the organic ability to acquire

information on that area. The AOI must extend, in as irregular a shape and as far as needed, in all directions to safeguard the command from surprise. The AOI must be viewed in four dimensions: width, depth, height or airspace, and time.

- The **battlespace** is all aspects of air, surface, subsurface, land, space, and the electromagnetic spectrum which encompass the area of operations, the area of influence, and the area of interest.

(3) Establish the Limits of the AOI. The AOI is the geographical area from which information and intelligence are required to permit planning or successful conduct of the command's operation. The command's AOI is generally larger than its AO. The limits of the AOI include each of the characteristics of the battlespace environment identified as exerting an influence on available COAs or command decisions.

Base the limits of the AOI on the ability of the threat to project power or move forces into the AO. Consider the geographical locations of other activities or characteristics of the environment which might influence COAs or the commander's decision and consider changes in the command's battlespace as a result of maneuver.

AOIs can be divided up into several components, such as ground, air, or political. The air AOI, for example, is usually larger than the ground AOI and would only relate when the projection of air power is of interest. For the air AOI, include a consideration of altitude. When conducting air defense related IPB, the AOI should extend upwards to the maximum service ceiling of the threat's aircraft. When conducting aviation related IPB, the AOI should extend to the maximum service ceiling of friendly aircraft or the maximum effective altitude of threat air defense systems, whichever is greater. Although various AOI may be developed separately, at some point you must consider them as an integrated whole.

One of the primary considerations in establishing the limits of the AOI is time. Base the time limit not only on the threat's mobility, both ground and air, but also the amount of time needed to accomplish the friendly mission. For missions of relatively short duration, such as the evacuation of noncombatants or raids, the AOI usually includes only immediate, direct threats to mission accomplishment and may be relatively small. A helicopter raid where the MAGTF has air superiority might have an AOI that includes only air defense systems within the range of the engagement area and the air routes to and from. Some long term missions, such as peacekeeping, will result in an extensive AOI that considers many political and economic factors as well as conventional military factors.

Since the limits of the AOI are based on threats to mission accomplishment rather than strictly terrain considerations, they might cross into neutral countries. If developments in a neutral country might influence the accomplishment of the unit's mission, then include that country within the AOI.

(4) Identify the Amount of Detail Required and Feasible Within the Time Available. The time available for completion of the IPB process may not permit the luxury of

conducting each step in detail. The focus must be on the parts of IPB that are most important to the commander in planning and executing his mission. Identifying the amount of detail required avoids wasting time on developing more detail than necessary in each step of the process. For example, the situation may not require an analysis of all threat forces within the AOI. Perhaps only selected areas within the command's AO require detailed analysis due to assigned mission or other factors of METT-T. Some geographical areas or threat forces within the AO may require only a summary type evaluation of their effects or capabilities.

(5) Evaluate Existing Intelligence Data Bases and Identify Intelligence Gaps. Not all the intelligence and information required to evaluate the effects of each characteristic of the battlespace and each threat force will be available in a current data base. This is especially true of the majority of countries where the MAGTF may potentially conduct operations in the future. Identifying the intelligence gaps early allows the ability to initiate action to collect the intelligence required to fill them, to perform necessary production, and then disseminate in a timely manner resulting intelligence products to all needing them.

Identify and prioritize the intelligence gaps in current holdings, using the commander's PIRs and intent to set the priorities. Identify any gaps which cannot be filled within the time allowed for IPB and inform the commander and operators so that reasonable assumptions can be formulated.

(6) Collect the Required Intelligence and Materials. Initiate collection or requests for intelligence to fill the gaps to the level of detail required to conduct IPB. Include collection against all identified significant characteristics of the battlespace, not just threat forces, in priority order.

Initiate action on identified intelligence production requirements (IPR) and continuously update the IPB products as additional intelligence is received. Inform the commander as you confirm assumptions made during the initial mission analysis and IPB process. If any assumptions are proven invalid, re-examine the evaluations and decisions on which they were based.

Ideally, intelligence operations enable the analyst to develop the estimates of the battlespace and the threat that match the actual situation. In reality, intelligence will never eliminate all the unknown aspects or uncertainties which concern a commander and his staff. Be prepared to fill in the gaps with reasonable assumptions and estimates.

b. Step 2-- Describe the Battlespace Effects. The second step is to determine how the battlespace environment affects both threat and friendly operations. The evaluation begins with an analysis of the existing and projected conditions of the battlespace environment, then it determines their effects on friendly and threat operations and broad COAs.[2] The specific steps include:

---

[2] See MCWP 2-12.1, *Geographic Intelligence*, for additional information regarding analysis of the battlespace environment.

- Analyze the battlespace environment:

  -- Terrain analysis

  -- Weather analysis

  -- Analysis of other characteristics of the battlespace

- Describe the battlespace effects on threat and friendly capabilities and broad COAs.

(1) Analyze the Battlespace Environment. The degree of detail in the analysis will vary depending on the area of the battlespace environment being evaluated. Generally, the AO is evaluated in more detail than the AOI. Additionally, the focus will vary throughout each area. For example, rear areas within the AO may require a different focus than areas near the main battle area. The battlespace is not homogeneous. Certain areas, or sub-sectors, will affect various types of operations to varying degrees. During the evaluation, identify areas that favor each type of operation. Include the traditional operations (offense and defense) as well as the operations associated with any METT-T specific factors (such as force protection and peace enforcement).

(a) Terrain Analysis. The best terrain analysis is based on a reconnaissance of the AO and AOI. Identify gaps in knowledge of the terrain which a map analysis cannot satisfy. Use the gaps identified to guide reconnaissance planning and focus on areas most important to the commander and his mission.

The intel bn's topo plt usually conducts the major portion of the terrain and hydrographic analysis and development of supporting geographic intelligence (GEOINT) products. They can also receive support from Army topographic units operating as part of or in support of the joint force. Topographic personnel work closely with weather personnel and weather analysts to ensure that terrain analysis incorporates the effects of current and projected weather events.

The National Imagery and Mapping Agency (NIMA) produces specialized maps, overlays, and automated data bases to aid in map based evaluations. The tactical terrain analysis data base (TTADB) consists of selected terrain information which can be exploited by terrain analysts to satisfy military requirements and is limited to those natural and man-made features of tactical military significance. Specialized NIMA products address such factors as:

- Cross-country mobility.

- Transportation systems (road and bridge information).

- Vegetation type and distribution.

- Surface drainage and configuration.

- Surface materials (soils).

- Ground water.

- Obstacles.

Ensure that the terrain analysis includes the effects of weather on the military aspects of the terrain. Consider the existing situation as well as conditions forecasted to occur during mission execution. Also consider that terrain analysis is a continuous process. Changes to the battlespace environment may change the evaluations of its effects that result from terrain analysis. Express the results of evaluating the terrain's effects by identifying areas of the battlespace that favor, disfavor, or do not affect each broad COA. Conclusions about the effects of terrain are reached through two sub-steps: analysis of the military aspects of the terrain; and evaluation of the terrain's effects on military operations.

((1)) Analyze the Military Aspects of the Terrain. Terrain analysis consists of an evaluation of the military aspects of the battlespace's terrain to determine its effects on military capabilities. The military aspects of terrain are:

- **Key Terrain** - Any locality or area (natural or manmade) the seizure, retention, or control of which affords a marked advantage to either combatant.

- **Observation and Fields of Fire** - Observation is the ability to see the threat either visually or through the use of surveillance devices. Fields of fire are that area that a weapon may effectively cover with fire from a given position.

- **Cover and Concealment** - Cover is the protection from the effects of direct and indirect. Concealment is protection from observation. Cover and/or concealment can be provided by ditches, caves, river banks, folds in the ground, shell craters, buildings, walls, embankments, woods, underbrush and other natural or manmade features.

- **Obstacles** - Any natural or manmade feature that stops, impedes, slows or diverts military movement.

- **Avenues of Approach and Mobility Corridors (Ground/Air)** - Avenues of approach (AA) are air or ground routes of an attacking force of a given size leading to its objectives or to key terrain in its path. Mobility corridors are areas where a force will be canalized due to terrain restrictions. A mobility corridor itself is relatively free of obstacles and wide enough to allow maneuver of tactical formations, allowing military forces to capitalize on the principles of mass and speed. When grouped together mobility corridors constitute an AA. Based on all previous terrain analysis, the analyst determines how the terrain will allow maneuver to objectives. Aircraft also use air AA, both rotary and fixed wing. There are both friendly and threat AAs. To determine avenues you must first know where the threat wants to get to.

((2)) Evaluate the Terrain's Effects on Military Operations. Evaluate the terrain's effects on friendly and threat offensive and defensive COAs by identifying the areas along each avenue of approach best suited for use as potential:

- **Engagement areas and ambush sites** - Using the results of evaluating concealment and cover, identify areas where maneuvering forces are vulnerable to fires. Consider weapons ranges, missile flight times, and the likely speed of maneuvering forces. If the unit is attacking, these are areas where it will be vulnerable to threat fires. If the unit is defending, these are potential engagement areas.

- **Battle positions** - Identify concealed and covered positions that offer observation and fields of fire into potential engagement areas. If your command is defending, they are potential defensive positions. If your command is attacking, they provide a start point for determining possible threat COAs. They might also be used by friendly attacking forces to block enemy counterattacks.

- **Immediate or intermediate objectives** - Identify any areas or terrain features that dominate the avenues of approach or assigned objective areas. These will usually correspond to areas already identified as key terrain. As time permits, or situation requires, also identify potential assembly and dispersal areas, observation posts, artillery and air defense positions, landing zones (LZ) and drop zones (DZ), etc.

The terrain rarely favors one type of operation throughout the width, breadth and height of the battlespace. Within a given area certain sub-sectors will affect various operations to varying degrees. Based on the location and nature of the potential engagement areas, battle positions, and so forth, determine which areas of the battlespace favor each broad COA, such as attack or defend.

Consider all these factors when analyzing terrain, but always focus on the ones of most relevance to the specific situation and needs of the commander. Evaluate them in any order that best supports your analysis. Terrain analysis is not an end product of the IPB process. It is the means to determine which friendly COAs can best exploit the opportunities the terrain provides and how the terrain affects the threat's available COAs. One of the most effective graphic products that will aid the staff in the completion of their own estimates and plans is to construct a Modified Combined Obstacle Overlay (MCOO). A more detailed discussion of Terrain Analysis is covered in Chapter 5, *Analysis of the Battlespace*.

(b) Weather Analysis. Although commanders have no control over weather, they can take advantage of it or minimize its effects through planning. During the weather analysis step, weather is analyzed in detail to determine how it affects friendly and enemy capabilities to move, shoot, and communicate. Terrain and weather are inseparable factors of tactical intelligence and must be integrated. Weather forecasts and assessments contribute to intelligence and must be considered when the commander develops his courses of action. The type and amount of weather support needed for a particular mission is situational, depending on the type of mission, forces involved, the terrain, and the enemy.

There are two subsets to accomplishing weather analysis: analyze the military aspects of weather; and evaluate the weather's effects on military operations. Weather analysis is covered in more detail in Chapter 5, *Analysis of the Battlespace*. (See also MCWP 3-35.7, *MAGTF Meteorological and Oceanographic Support*.)

((1)) Analyze the Military Aspects of Weather. There are 5 military aspects of weather:

- **Temperature and Humidity -** At extremes, affects the operation of equipment and efficiency of personnel. As temperature and humidity increase, air density decreases which may affect aircraft payloads. These may require the use of special equipment for personnel.

- **Precipitation** - Affects soil trafficability, visibility, personnel effectiveness and the functioning of some weapons and equipment, particularly electro-optical devices. Heavy snow will degrade the effects of munitions, while a combination of precipitation and low temperatures may degrade air operations.

- **Wind -** Winds of sufficient speed can reduce the combat effectiveness of a force downwind as the result of blowing dust, smoke, sand, or precipitation. The upwind force usually has better visibility and are more favorably positioned for NBC operations. Strong winds and turbulence limit airborne and aviation operations.

- **Visibility -** Poor visibility is beneficial to offensive and retrograde operations. In the offense, it conceals the concentration of maneuver forces, thus enhancing the possibility of achieving surprise. Low visibility hinders the defense because cohesion and control become difficult to maintain, reconnaissance and surveillance are impeded, and target acquisition is less accurate. Visibility is affected by all aspects of weather and must be evaluated in those terms.

- **Clouds -** Cloud cover affects ground operations by limiting illumination and the solar heating of targets. Heavy cloud cover can degrade many target acquisition systems, the use of infrared-guided artillery, and general aviation operations.

((2)) Evaluate the Weather's Effects on Military Operations. Weather has both direct and indirect effects on military operations. Examples of indirect effects are:

- Temperature inversions might cause some battle positions to be more at risk to the effects of chemical warfare than others due to their altitude.

- Local conditions of visibility, such as fog, might make some potential engagement areas more attractive than others.

- Hot, dry weather might force a unit to consider water sources as key terrain.

Evaluation of the direct effects of weather begins by establishing critical values for each military aspects of weather's effects on personnel, specific types of equipment, and the various s types of military operations the command may be required to perform. Once set, these critical values are used as the metric for determining specific effects of local weather on both friendly and enemy operations. The results of the analysis are best displayed graphically, as shown in Figure 4-2.

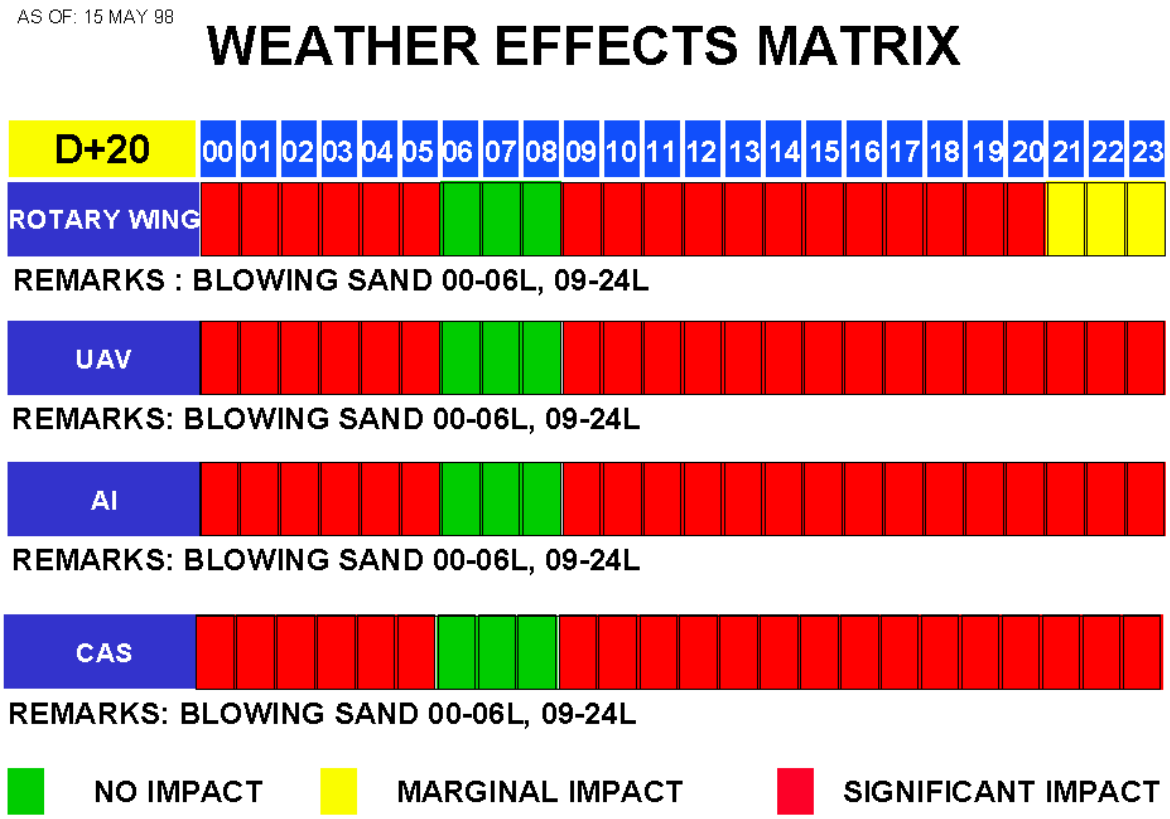

Figure 4-2. Weather Effects Matrix

(c) Analysis of Other Characteristics of the Battlespace. Other characteristics include all aspects of the battlespace environment that affect friendly and threat COAs not already incorporated into terrain and weather analysis. For example, an S-2 may report that religious considerations will make cordon and search operations on Wednesdays difficult to execute since the local population will be praying at the same time we are trying to conduct the search. Some examples of characteristics to consider include:

- Logistics infrastructure - land use patterns, sources of potable water, bulk fuel storage, natural resources, industries and technologies, and chemical and nuclear facilities.

- Population demographics - living conditions, cultural distinctions, religious beliefs, political grievances, political affiliation, and education levels.

- Economics.

- Politics - local, regional, and international (treaties, agreements, and legal restrictions; includes unofficial systems such as gangs).

Although the effects of other characteristics will usually be discussed in text or matrix form, wherever possible always attempt to use graphics. Examples of graphic depictions would include an overlay showing areas most vulnerable to insurgent activity, based on demographic distribution; or an overlay showing high value target in the logistics infrastructure.

(2) Describe the Battlespace Effects on Threat and Friendly Capabilities and Broad Courses of Action. Combine the evaluation of the effects of terrain, weather, and other characteristics of the battlespace into one integrated product. Do not focus on factors that lead to your conclusions. Instead, focus on the total environment's effects on COAs available to both friendly and threat forces. For friendly forces, this can be accomplished as follows:

- Prior to development of friendly COAs:

  -- Provide the evaluated and prioritized set of AAs to the operations officer/planning staff to facilitate the designation of axis of advance, direction of attack, or zone of attack for each subordinate unit (offensive operations).

  -- Provide the sets of defensible terrain along threat AAs to facilitate the development of strongpoints, battle positions, or sectors for each subordinate unit (defense and retrograde).

  -- Identify periods when weather conditions will optimize the use of friendly target acquisition and aviation operations to facilitate the timing of particular operations.

- After the development of friendly COAs, provide evaluation of how each COA does or does not utilize the opportunities the battlespace provides.

When addressing effects on threat COAs, a good technique is to view capabilities from the perspective of the threat's S-2 and S-3 who must recommend a set of COAs to their commander. Your evaluation of the battlespace effects on the threat must be tailored to the specific threat you are facing, keeping in mind that weather and terrain may effect threat weapon systems, vehicles, and even personnel differently than your own. It is important that operations and planning staffs are aware and understand these differences to avoid assumptions that the battlespace will affect both forces equally. Remember that other characteristics may influence threat actions more than

weather and terrain, and their cultural biases may cause them to view legal, political, economic, and demographic issues in an entirely different manner than U.S. personnel would.

The bottom line is to evaluate the battlespace completely from the perspective of the threat. Express this evaluation in terms of COAs, not detailed descriptions of the analytical factors that led to the conclusions. Focus the commander by relating specific threat activities in both time and space. Be prepared to back your conclusions with the detailed analysis performed in the preceding steps.

Final conclusions from the description of the battlespace environment should be communicated in written reports such as the analysis of the AO or intelligence estimate. Graphic products developed during the analysis and evaluation should be disseminated to the staff and other commands for utilization in their own IPB and planning efforts.

c. Step 3-- Evaluate the Threat. The third step is to determine the threat force capabilities and the doctrinal principles, tactics, techniques, and procedures it has historically used. This involves a detailed study of their composition, tactical doctrine, procedures, weapons and equipment, and supporting systems. Here the intelligence section determines threat capabilities and how the threat operates relative to doctrine and training or how he would fight if not restricted by weather and terrain. The specific steps include:

- Update or create threat models.

  -- Convert threat doctrine or patterns of operation to graphics (doctrinal templates).

  -- Describe in words the threat's tactics and options.

  -- Identify COGs.

  -- Identify high value targets (HVT).

- Identify threat capabilities.

(1) Update or Create Threat Models. Threat models depict how threat forces prefer to conduct operations under ideal conditions. They are based on the threat's normal or "doctrinal" organization, equipment, tactics, techniques, and procedures. Threat models result from a detailed study of the threat force. Ideally, threat models are constructed prior to deployment. Threat models consist of three parts: Doctrinal templates, a description of preferred tactics and options, and identification of HVTs.

(a) Doctrinal Templates. Doctrinal templates illustrate the deployment pattern and disposition preferred by the threat's normal tactics when not constrained by the effects of the battlespace environment. They are usually scaled graphic depictions of threat dispositions for a particular type of standard operation, such as a battalion moving to contact or an insurgent ambush. Figure 4-3 shows one such doctrinal template.

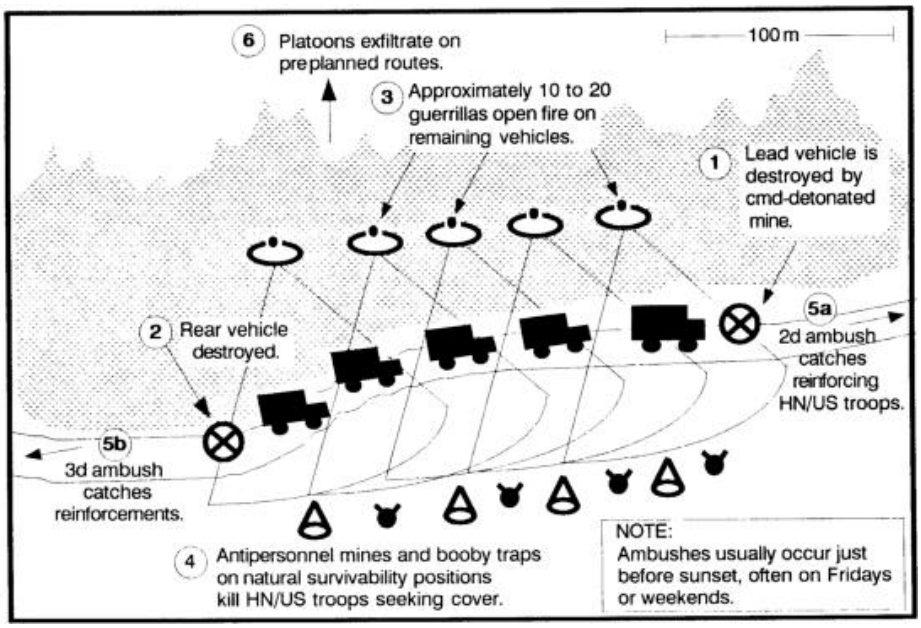

Figure 4-3 Doctrinal Template

Doctrinal templates are constructed through an analysis of intelligence data bases and an evaluation of the threat's past operations. The analysis should focus on patterns in task organization, timing, distances, relative locations, groupings, and use of terrain and weather. Some doctrinal templates consider the threat force as a whole, while others focus on a single battlefield function like intelligence or fires. Above all, doctrinal templates must be tailored to the needs of the unit or staff section creating them.

(b) Description of Tactics and Options. The threat model includes a description of the threat's preferred tactics. It addresses the operations of the major units or elements portrayed on the template and the activities of different battlefield functions. It also contains a listing or description of the options available to the threat should the operation fail (branches), or subsequent operations if it succeeds (sequels). Even if the threat's preferred tactics can be depicted graphically, the threat model includes a description. This allows the template to become more than a "snapshot in time" of the operation being depicted. It aids in mentally wargaming the operation over its duration during the development of threat COAs and situation templates. The description should address typical timelines and phases of the operation, points where units transition from one formation to another, decision criteria (if known) and how each battlefield function contributes to the operation's success. This analysis of the individual role of battlefield functions, related in time and space, will aid in the later identification of (HVTs) and high pay-off targets (HPT).

(c) Identification of Center(s) of Gravity. COGs are those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. A COG is a key source of strength without which an enemy cannot function. COGs may exist at the strategic, operational, and tactical levels and its is against

these COGs that military operations are usually directed. While knowledge of a threat's COGs at all levels is useful, the analyst should focus on the COGs appropriate to the level of operations which their friendly force is concerned with. At this stage of the IPB process, the identification of COGs is an initial assessment. Later in Step 4, as specific threat COAs are developed, a corresponding assessment of COGs will be made for each specific COA. Often COGs will also be identified as HVTs.

(d) Critical Vulnerabilities. Of all the vulnerabilities we might choose to exploit, some are more critical to the enemy than others. Some may contribute significantly to the enemy's downfall while others may lead only to minimal gains. Therefore, we focus our efforts against a CV, a vulnerability that, if exploited, will do the most significant damage to the enemy's ability to resist us.

(e) Identification of Type HVTs. Assets that the threat commander requires for the successful completion of the mission depicted and described on the template are HVTs. Identify HVT's from an evaluation of the data base, the doctrinal template, its supporting narrative, and the use of tactical judgment. Develop the initial list of HVTs by mentally wargaming and thinking through the operation to identify those assets that are critical to the operation's success, particularly at critical junctures or phases. Identify assets which are key to executing the primary operation, particularly those that are key to satisfying decision criteria. Determine how the threat might react to the loss of an HVT; consider his ability to substitute other assets or modify his plan to compensate. Examples of type HVTs include: C2, intelligence, fire support, communications and information systems, air defenses, engineers, and logistics/CSS. After identifying the set of HVTs, rank order them with regard to their relative worth to the threat's operation. An HVTs value usually varies over the course of an operation, so identify changes of value by phase. As key assets are identified, they should be grouped into one of the 13 categories used to develop target sets, thus facilitating the development of targeting strategies. Figure 4-4 shows a threat model with type HVTs identified. As always, tailor IPB products to your command's needs by concentrating on HVTs that are important to your mission.

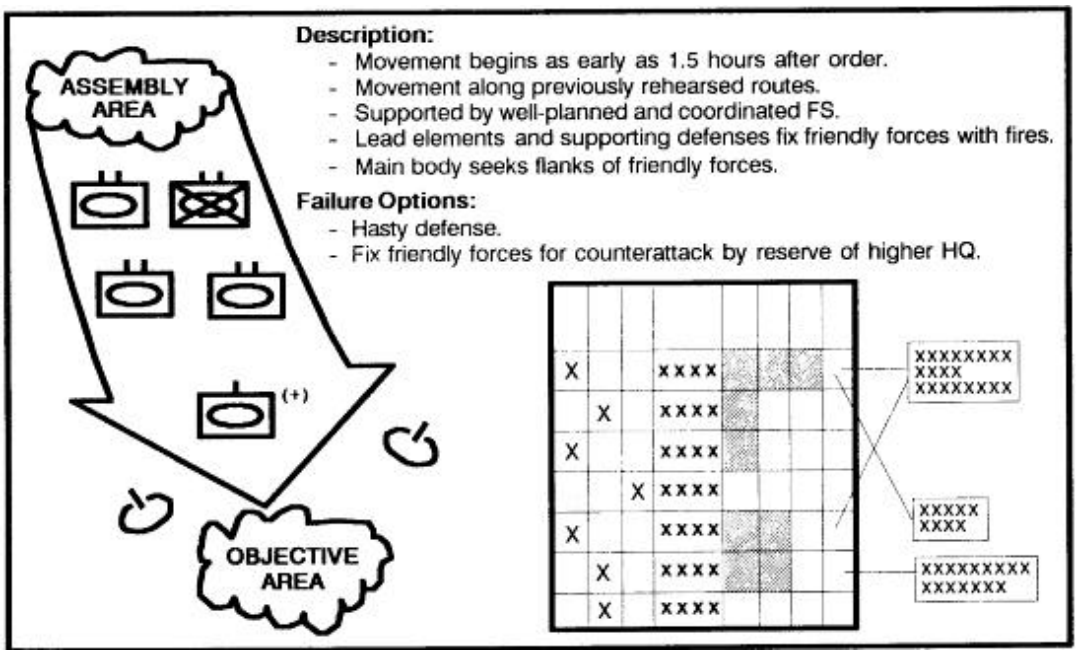

Figure 4-4. Threat Model with Type High Value Targets Matrix

(2) Identify Threat Capabilities. Threat capabilities are the broad COAs and supporting operations which the threat can take to influence the accomplishment of the friendly mission. They take the form of statements, such as:

- "The enemy has the ability to insert up to 2 battalions of infantry in a single lift operation."
- "The enemy can establish a prepared defense by 14 May."
- "The demonstrators can effectively block traffic at up to 7 different intersections in our zone."

There are generally four tactical COAs open to military forces in conventional operations:

- Attack.
- Defend.
- Reinforce.
- Conduct a retrograde.

Each of these broad COAs can be divided into a variety of more specific COAs. For example, an attack may be an envelopment, a penetration, or other variations of an attack. A retrograde

movement may be a delaying action, a withdrawal, or a retirement. Other capabilities include support to broad COAs or specific types of operations. Examples of these types of capabilities are:

- Deception operations.
- Riverine operations.
- Psychological operations.
- Intelligence operations.
- Use of NBC weapons.
- Espionage, sabotage, subversive, and terrorist operations.

At other levels of war and during operations other than war, you will consider other types of operations and broad COAs. In any case, start with the developed threat models and consider the threat's ability to conduct each operation based on the current situation. Most situations will not present the threat with the ideal conditions envisioned by his doctrine. He may be understrength in equipment or personnel, short of logistics support, lacking air support, or his troops may be inexperienced or poorly trained. All factors related to the current situation must be taken into account when determining threat capabilities. Do not limit the threat models and evaluation of capabilities strictly to military forces. During a NEO for instance, demonstrators and rioters may be as much a threat as military forces.

d. Step 4-- Determine Threat Courses of Action. The fourth step is the identification and development of likely threat COAs that will influence the accomplishment of the friendly mission. The specific steps include:

- Identify the threat's likely objectives and desired end state.
- Identify the full set of COAs available to the threat. At a minimum this will include the threat's most likely COA and the COA most dangerous to the friendly force.
- Evaluate and prioritize each COA.
- Develop each COA in the amount of detail time allows.
- Identify initial collection, production and dissemination requirements.

(1) Identify the Threat's Likely Objectives and Desired End State. Start with the threat command at least one level above your own and identify likely objectives and desired end state. As you identify the likely objectives at each level of command, repeat the process for the next subordinate level, working down to at least two levels below your own command.

Ensure that each level's objective will accomplish the likely objectives and desired end state of its parent command(s). In operations other than war, you may be required to start more than one level above your command, perhaps as high as the government or major clan leadership level. Only in rare cases will the analyst have the intelligence needed to state the threat's objectives and desired end state as facts. Instead, they will be usually stated as assumptions. As with all assumptions, ensure they are discussed with the commander and staff, and that they are clearly identified as such. During operations other than war it is important to consider more than the conventional objectives of terrain or friendly forces. This is also true at higher levels of command where the threat's political and economic objectives have a direct influence on his COAs. It is entirely possible that the threat’s intent and objectives may not interfere with the accomplishment of the friendly mission, such as during a NEO or other operations less than war.

(2) Identify the Full Set of COAs Available to the Threat. To ensure that the analyst considers the full set of COAs available to the threat, the following should be considered at a minimum:

- The COAs the threat historical doctrine and TTP indicates appropriate to the current situation and the likely objectives identified. This requires an understanding of the threat's decision making process as well as an appreciation for how he perceives the current situation.

- The threat COAs which could significantly influence the command's mission, even if the threat's doctrine and TTP indicates these as infeasible under current conditions. Consider any indirect or "wildcard" COAs that the threat is capable of executing.

- The threat COAs indicated by recent activities and events. To avoid surprise from an unanticipated COA, consider all possible explanations for the threat's activity in terms of possible COAs.

Consider each subset of COAs independently to avoid forming biases that restrict the analysis and evaluation. Once each subset has been evaluated separately, combine them to eliminate redundancy and minor variations. Compare the consolidated list to threat capabilities identified in step 3 of the IPB process (Evaluate the Threat), and eliminate any COAs which the threat is incapable of executing. Based on the evaluation of the threat's capabilities, select threat models that will accomplish the threat's likely objectives. Examine how the effects of the battlespace from step 2 of the IPB process (Describe the Battlespace's Effects) influence their application as COAs (see figure 4-5).

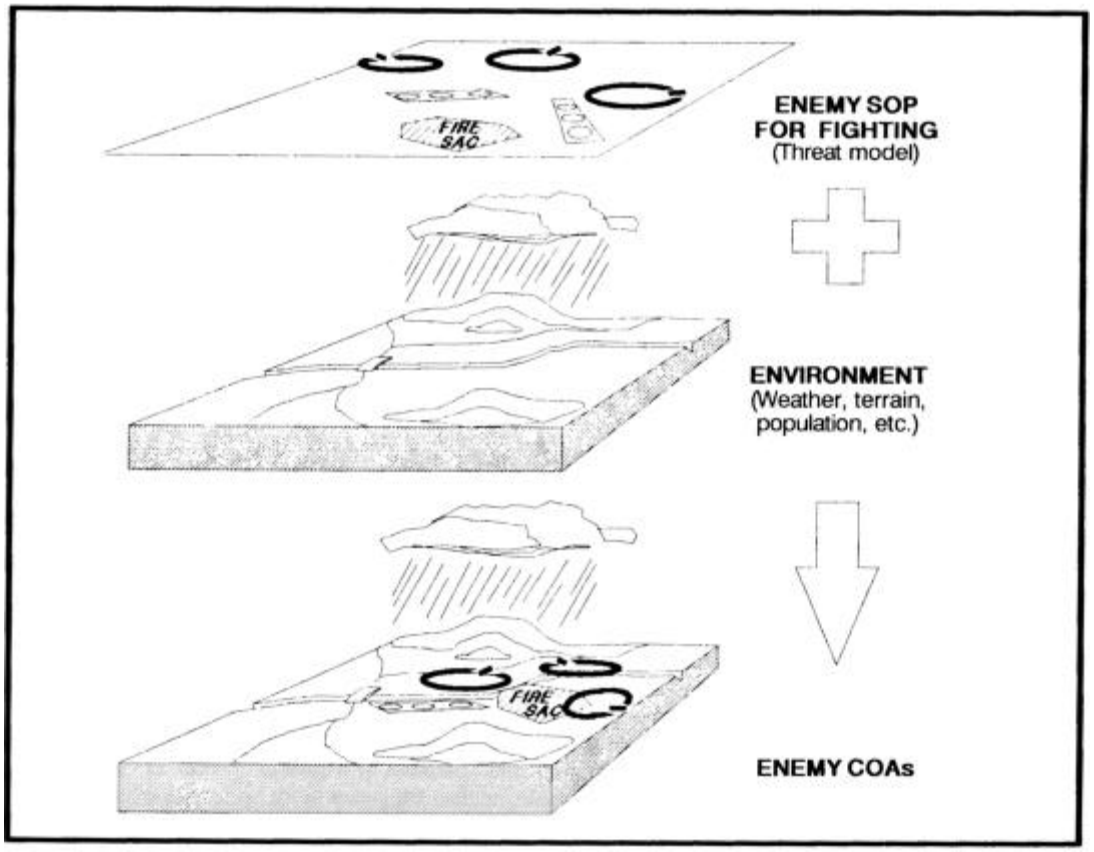

Figure 4-5. Combining Doctrine and Battlespace Effects to Develop Threat COAs

Start with the general COAs open to the threat, such as deliberate attack, hasty attack, defend, and delay. Further define each general COA as a set of specific COAs by integrating the threat models from step 3 with a description of the battelspace's effects from step 2. Each COA identified should meet five criteria: suitability, feasibility, acceptability, uniqueness, and consistency with threat doctrine/TTP and recently observed activities and patterns.

(3) Evaluate and Prioritize each Course of Action. The resulting set of COAs depicts the full set of options available to the threat. Remember that the threat COAs identified are *assumptions* about the threat, *not facts*. However, the commander and his staff still need to develop a plan that is optimized to one of the COAs, while still allowing for contingency options if the threat chooses another COA. Therefore, the analyst must evaluate each COA and prioritize it according to an estimate of likely adoption by the threat. Establish an initial priority list to allow the staff to plan for friendly COAs. Once the commander selects a friendly COA, the list may need to be reprioritized to reflect possible reactions to friendly dispositions and activities.

(4) Develop Each Course of Action in the Amount of Detail Time Allows. Once the complete set of threat COAs has been identified, develop each COA into as much detail as the situation requires and time allows. Base the order in which each COA is developed on its

probability of adoption and the commander's guidance. To ensure completeness, each COA must answer five questions:

- What - the type of operation.
- When - the time the action will begin.
- Where - sectors, zones, axis of attack, etc.
- How - the method by which the threat will employ his assets.
- Why - the objective or end state of the threat.

Consider threat forces available to at least one level of command above your own when developing each COA. For example, a battalion S-2 would consider the COAs available to threat regiments and brigades. This helps account for possible reinforcing forces and the threat higher command's own objectives and intent. Conversely, each COA should provide resolution to two levels of command below your own. Thus our same battalion S-2 would depict missions and actions down to the platoon level.

Each developed threat COA has three parts:

- A situation template.
- A description of the COA, COG(s), CVs and options.
- A listing of HVTs.

(a) Situation Template. Situation templates are graphic depictions of expected threat dispositions should he adopt a particular COA. They usually depict the most critical point in the operation as agreed upon by the G-2/S-2 and G-3/S-3. An analyst may prepare several templates to represent different "snapshots in time" starting with the threat's initial array of forces. These are useful in depicting points where the threat may adopt branches or sequels to the main COA, places where the threat is especially vulnerable, or other key points in the battle such as initial contact with friendly forces. Situation templates are used to support staff wargaming and then develop event templates.

To construct a situation template, begin with the threat model representing the operation under consideration. Overlay the doctrinal template on the products that depict the battlespace environment's effects on operations. The product of choice is the MCOO, but this may vary with the situation. Using judgment and knowledge of the threat's preferred tactics and doctrine as depicted in the threat model, the dispositions portrayed on the doctrinal template are adjusted to account for the battlespace environment's effects. There will be many options available; attempt to view the situation from the point of view of the threat commander when selecting from among them. Check the situation template to ensure that all the threat's major assets have been

accounted for, particularly the locations and activities of the HVTs listed in the threat model. If possible, evaluate time and space factors to develop time phase lines (TPL) depicting threat movement. The TPLs can be refined during wargaming. An example of a situation template is depicted in figure 4-6.

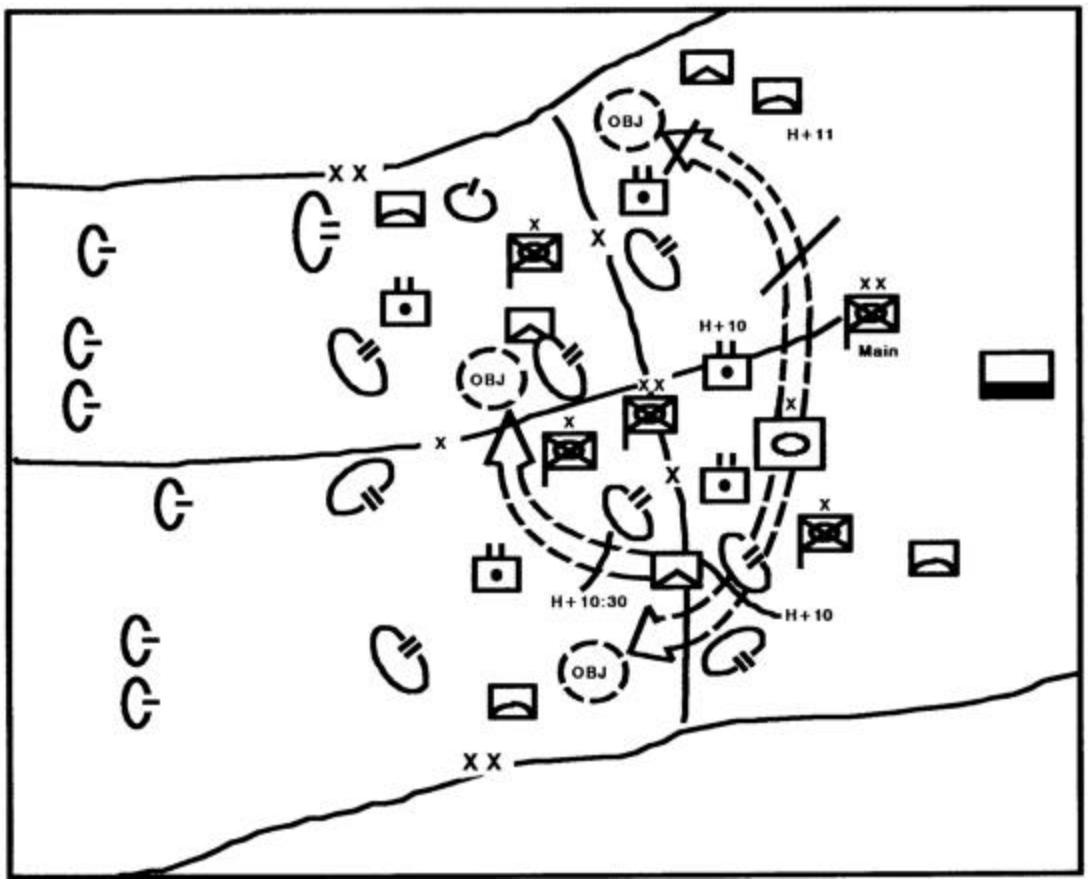

Figure 4-6. Example Situation Template

(b) Description of the COA and Options. This is a description of the activities of the forces depicted on the situation template. It can range from a narrative description to a detailed "synchronization matrix" depicting the activities of each unit and battlefield function in detail. It should address the earliest time the COA can be executed, the threat COG(s), timelines and the phases associated with the COA, and decisions the threat commander will make during execution of the COA and after. In effect the analyst is mentally wargaming the COA and attempting to tie threat actions and decisions to both time and space. This will help when later constructing the event template. Use the COA description to support staff wargaming and to develop the event template and supporting indicators.

(c) High Value Targets (HVTs). As the analyst prepares and mentally wargames the situation template, note how enemy systems provide critical support to the COA. This leads to identification of HVTs. HVTs may themselves be COGs or CVs, or they may be

assets which if destroyed or neutralized may allow us to attack a COG or CV. Use the list of HVTs in the threat model as a guide, but do not be limited by it. Determine the effect on the COA of losing each HVT and identify likely threat responses. The relative worth of each HVT will vary with the specific situation under consideration and over the course of the COAs conduct. Identify the times or phases in the COA when the target is most valuable to the threat commander and make the appropriate notations on the list of HVTs. Transfer the refined and updated list of HVTs to the situation template. The list will support staff wargaming and the targeting process.

Note on the situation template any areas where HVTs must appear or be employed to make the operation successful. Focus on their locations at the times they are most valuable, or just before. These are potential target areas of interest (TAI) and engagement areas (EA) that will then be further refined and used by the G-3/S-3.

(5) Identify Initial Intelligence Collection, Production and Dissemination Requirements. After identifying the set of potential threat COAs the initial challenge is to determine which one he will actually adopt. Initial collection requirements are designed to help answer the challenge. The art of identifying initial intelligence collection requirements (ICR) revolves around predicting specific areas and activities, which, when observed, will reveal which COAs the threat has chosen. The area where the analyst expects key events to occur are designated as named areas of interest (NAI). The activities which reveal the selected COA are called **indicators**. Identified intelligence production requirements (IPR) will support prioritization and planning of necessary intelligence products. Finally, identified intelligence dissemination requirements (IDR) will support prioritization and planning for the eventual dissemination of intelligence products to all commanders and staff sections needing them.

(a) Event Template. The differences between the NAIs, indicators, and TPLs associated with each COA form the basis of the event template. The event template is a guide for collection, reconnaissance and surveillance planning. It depicts where to collect information that will indicate which COA the threat has adopted.

Evaluate each COA to identify its associated NAIs. Mentally wargame execution of the COA and note places where activity must occur if that COA is adopted. Pay particular attention to times and places where the threat's HVTs are employed or enter areas where they can be easily acquired and engaged. These areas will evolve into NAIs in support of targeting. Also consider places where the threat is expected to take certain actions or make certain decisions, such as adoption of a branch plan or execution of a counterattack.

An NAI can be a specific point, a route, or an area. They can match obvious natural terrain features or arbitrary features, such as TPLs or engagement areas. Make them large enough to encompass the activity which serves as the indicator of the threat's COA.

Compare and contrast the NAIs and indicators associated with each COA against the others and identify their differences. Concentrate on the differences that will provide the most reliable indications of adoption of each unique COA. Mark the selected NAIs on the event template. The initial event template focuses only on identifying which of the predicted COAs the threat has

adopted. Later, you will update and further refine the event template and its supporting matrix to support friendly decisions identified during staff wargaming (see figure 4-7).

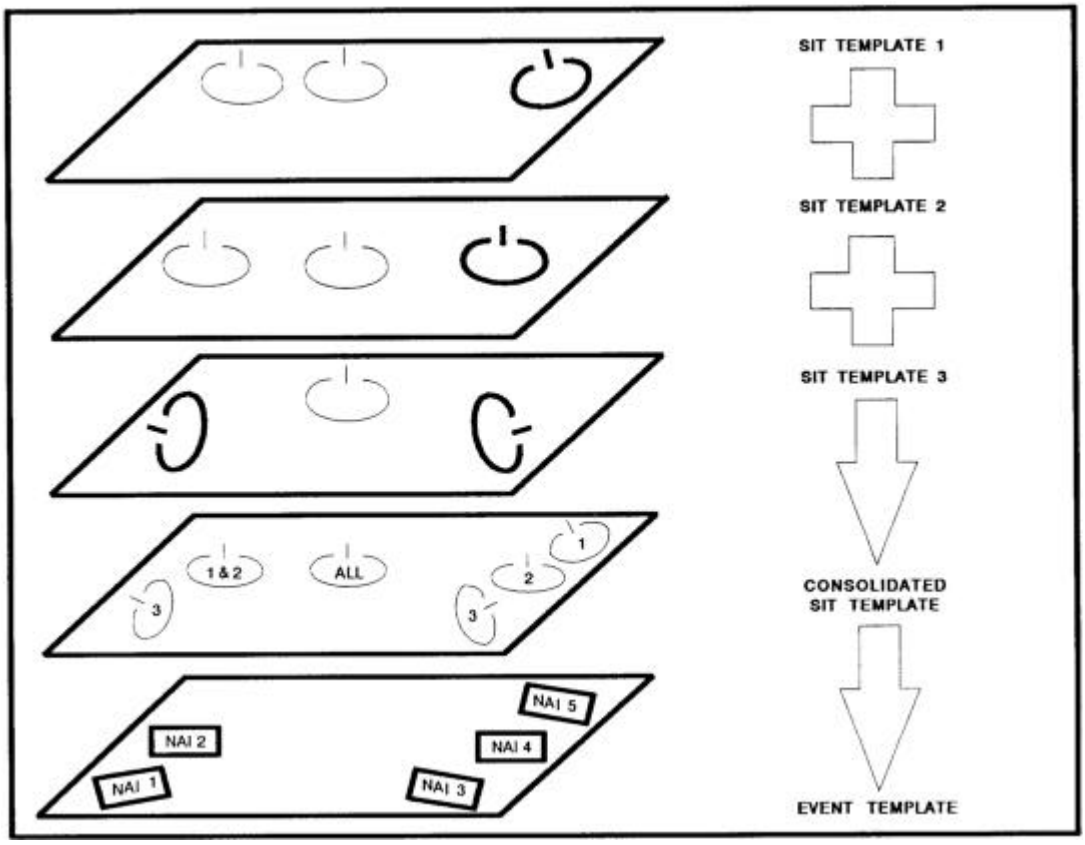

Figure 4-7. Develop the Event Template by Comparing and Contrasting the NAIs and Indicators Associated with each COA

(b) Event Matrix. The event matrix supports the event template by providing details on the type of activity expected in each NAI, the times the NAI is expected to be active, and its relationship to other events on the battlefield. Its primary use is in planning intelligence collection; however, it serves as an aid to situation development as well.

Examine the events associated with each NAI on the event template and restate them in the form of indicators. Enter the indicators into the event matrix along with the times they are most likely to occur. Use the TPLs from the situation template or the description of the COA to establish the expected times in the event matrix. If there is a latest-time-information-of-value (LTIOV) timeline, based on the expected flow of events, record it into the event matrix as a guide for the collection manager (see figure 4-8).

NAI No.	NO EARLIER THAN (HOURS)	NO LATER THAN	INDICATOR
NAI 1	H-7	H-2	Engineer preparation of artillery positions
NAI 1	H-2	H-30min	Artillery occupies firing positions
NAI 1	H-1	H-15min	Artillery commences preparatory fires
NAI 2	H-2	H-1.5	Combat recon patrol conducts route recon
NAI 2	H-1.5	H-30min	Rifle company (+) in march formation

Figure 4-8. Event Matrix

The event template and matrix form the basis for planning integrated collection, production and dissemination strategies, synchronizing intelligence operations with all other friendly operations. They enable the G-2/S-2 to develop precise ICRs, IPRs and IDRs, maximizing the effectiveness of limited resources over extended areas against a vast array of threat targets. In some cases, the event template can be disseminated in the form of a graphic to support intelligence operations planning by other units. Event templating also serves the G-3/S-3 by, among other things, telling him where, when, and what to shoot, jam, deceive, and maneuver against.

e. Decision Support Template (DST). Although not inherently the responsibility of the G-2/S-2 or the formal IPB process, the DST is the capstone product in the staff planning process and the logical conclusion to the IPB. The DST relates time, space and threat actions to assist the commander in determining when decisions need to be made; either to employ fires or maneuver forces. **It does not dictate decisions to the commander**, but instead helps the commander think ahead in the battle to reduce uncertainty and aid in recognitional or intuitive decision making.

The DST is normally developed during COA wargaming as threat and friendly actions are compared in time and space. Unlike the previous products, the DST is a *staff* product prepared under the staff cognizance of the G-3/S-3, reflecting the judgment and expertise of the intelligence, maneuver, fires, CIS, and logistics support staffs. The products developed during IPB-- the threat COA models, the event template, and event matrix --form the basis for and drive wargaming and the development of the DST.

Through event templating, identification was made of those areas on the battlefield where significant events and activities will likely occur and where targets will likely appear. As the wargaming process proceeds, the staff identifies areas where the commander can influence the action through fire and maneuver. These areas are designated TAIs. A TAI is an engagement point or area, usually along a mobility corridor, where the interdiction of threat forces by fires, maneuver or jamming will deprive or reduce a threat capability. It can also cause the threat commander to abandon a particular COA or require the use of unusual support to continue operations. Times and locations where HVTs will appear are particularly suited to become TAIs.

The identification of TAIs is a joint effort between the intelligence, operations and fire support staffs. The intelligence staff identifies the times and places where opportunities present themselves and the effect of interdiction on threat capabilities. The operations and fire support staffs consider the availability of interdiction resources, the effects of interdiction on the accomplishment of the friendly mission, and the priorities for the use of available resources.

Following the selection of TAIs, decision points (DP) are identified. The location of DPs is largely influenced by the availability and capability of friendly fire and maneuver systems; therefore their selection is primarily a G-3/S-3 function, with support from other participants in the planning staff.

DPs identify those battlefield events which may require tactical decisions and when these decisions must be made for the commander to retain available options. Examples of the types of decisions include:

- Commit the reserve
- Surge friendly air support
- Artillery concentrations on TAIs, perhaps in conjunction with electronic attack operations.
- Delivery of scatterable mines
- Shift of the main effort
- Commence the next phase of an operation
- Change the overall mission of a subordinate unit
- Request assistance from higher headquarters

Decisions must be made early enough to ensure that they can be coordinated across all command echelons and implemented in time to achieve the desired results. NAIs must be developed which provide the required indicators in sufficient time and preciseness to allow a timely decision to be made. When placing DPs, consider time for intelligence collection, processing, analysis, production, and dissemination to take place; the time required to prepare and or move friendly assets that will execute the mission; and the activities and movements of the target or threat during the time elapsed between decision and execution.

As the wargaming progresses, a recorder will track decision points, both by time and location, and also develop the synchronization matrix to ensure all battlespace functions are working in harmony toward the same goals. Upon the selection of a friendly COA by the commander, the intelligence staff will then take the associated DPs, NAIs, and TAIs and ensure detailed collection and dissemination plans are developed to support them.

f. The Abbreviated IPB Process. Many of the steps involved in IPB are time, labor and resource intensive. This is especially true at lower tactical echelons where automated systems and personnel support for terrain analysis and other production functions are not always available. Unfortunately, those same echelons generally have less time available for the IPB process. Following are some effective techniques for abbreviating the IPB process.

(1) Work Ahead. The best solution is to complete as much ahead of time as possible. Establish a series of base products, particularly those that deal with the battlespace environment's effects on operations. Keep them updated by periodic review instead of waiting until receipt of a new mission.

Keep data bases on potential threats up to date. As intelligence is received that indicates changes or evolution in threat doctrine, change the threat models to match.

Since most MAGTF units are faced with a number of contingency missions, conduct periodic reviews to ensure that the base IPB products, such as descriptions of the battlespace environment and the threat, are updated regularly.

Become familiar with the support available from higher headquarters, theater intelligence centers, and service agencies such as the Marine Corps Intelligence Activity (MCIA). Know how to get what you need when you need it. Submit Production Requirements (PRs) for information and intelligence products on areas where your unit is most likely to be employed. Think through and develop checklists on how to get support, before, during and after deployment. Finally, maintain awareness of HHQ's plans and priorities for all ICRs, IPRs and IDRs submitted to them.

(2) Focus on Essentials. Consider the general factors of METT-T when starting the IPB effort, particularly the factor of time. Backward plan the IPB effort. Determine how much time you can devote to each step of the IPB process. Ensure that the timeline allows you to properly support the planning and decision making process.

Decide which products you will develop and to what degree of detail. Focus on the products most important to your mission. Rather than fully developing one threat COA at the expense of all others, identify the full range of available COAs. Determine the degree of detail required and then develop all COAs to that level of detail.

Always work in a priority order established by the commander's intent and needs. If the commander is particularly pressed for time, he may specify which COAs he wants to focus on, such as the most likely and the most dangerous. This implies that you first identify all COAs and evaluate them to determine which is the most likely or most dangerous. You abbreviate the IPB process by developing in detail only those the commander has specified.

(3) Stay Objective Oriented. The objective of IPB is to help the commander and his staff make decisions and develop the best possible plans in the time available. This requires models of the range of viable threat COAs that will influence mission accomplishment.

Supporting the finished plan with intelligence requires a good event template and matrix. Everything else is only a means to producing these essentials.

(4) Minimum Essentials. In a pinch you can get by with just a good set of threat models and a good event template and matrix. To save time and materials, you can combine all threat COA model templates and the event template on a single map overlay, or use cartoons and sketches as a map substitute.

If you have not yet described the battlespace environment's effects, work directly from the map or sketch of major terrain features. Start by identifying the set of COAs and briefly comparing them to determine which is most likely and which is most dangerous considering the current situation and your command's mission. Rank the remainder in order of likely adoption.

Begin by developing the most dangerous or most likely threat COA. In the absence of guidance from the commander or G-3/S-3, judgment is the only guide for which to do first. Develop the selected COA to as much detail as the available time allows before turning to the other.

Next, construct an event template that focuses on identifying which of the two COAs the threat has adopted. Then turn to developing the remaining courses of action. Work each COA in the priority order you put them in when evaluating their likelihood of adoption.

As each COA is finished to the determined degree of detail, incorporate NAIs associated with it into the event template. The initial structuring of the collection requirements can actually wait until the staff wargaming. The most important milestone prior to wargaming is to develop the most likely and most dangerous COAs.

If the most likely COA is also the most dangerous COA, develop the second most likely or the second most dangerous COA. **NEVER** take just one COA into wargaming--this is not an acceptable way to abbreviate the IPB or staff planning processes.

The intelligence product that results from this approach is far less than the comprehensive set of products described throughout this chapter. However, the "one-overlay product", when developed to a quality standard and focused on the unit's mission, PIRs and IRs, has repeatedly proven to be effective on the battlefield. This is IPB in its most elementary form, and it proves the strength of the fundamental IPB process.

4003. Output

Throughout the IPB process, various products such as the threat models, threat COAs graphics, and the event template are produced to support staff planning. The graphics developed, particularly the weather and terrain effects graphics, the situational templates and the event template, can be disseminated to assist subordinate units in their own planning. This is particularly useful when the available planning time is limited. The G-3/S-3 may choose to use the decision support template, with friendly tactical control measures added, as the operations graphic for the OPORD. Done correctly, these graphics can provide tremendous volumes of

understanding and knowledge in concise and easily useable forms. At other times, however, additional written products can and should be prepared. This is particularly true for standing OPLANs where a significant amount of time has been available to develop a fine-grained view of the environment and threat. The two products discussed below are the most commonly used, and both are directly derived from the IPB process.

a. Intelligence Estimate

(1) Purpose. In order to facilitate staff planning, the G-2/S-2 prepares the intelligence estimate before the remainder of the staff complete their own estimates if at all possible. The intelligence estimate is the standard means of conveying key basic and current intelligence and relating it to the operational mission. It is a snapshot in time and forms the basis for the facts and assumptions of the decision making process, driving the other staff estimates and the remaining steps of the MCPP. At higher command levels, it provides major portions of the written commander's estimate. The products of IPB are the basis for the intelligence estimate. If the G-2/S-2 lacks the time required to prepare a written estimate, he can usually substitute graphics that depict the results of his IPB evaluations and analysis.

(2) Format. The intelligence estimate has a standardized five paragraph format that easily incorporates the information derived from steps 2, 3, and 4 of the IPB process. It should include a statement that identifies the cutoff time for information and intelligence used in its preparation. A detailed outline for the intelligence estimate format is provided in appendix C. The intelligence estimate should be concise, mission focused, and tailored to the needs of the unit. The utilization of graphics is encouraged and preferred, whenever possible.

(a) Paragraph 1 - Mission. Paragraph 1 concisely restates the command's mission. This should be the same re-stated mission as developed during the mission analysis phase of the MCPP.

(b) Paragraph 2 - Characteristics of the Area of Operations. In paragraph 2, the G-2/S-2 states conditions which exist and indicates the effect of these conditions on enemy capabilities and the assigned mission. It is derived from step 2 of the IPB process (**Describe the Effects of the Battlespace**). The area of operations is usually discussed under nine main subheadings (MOOTW may require a slightly tailored group of subheadings): military geography, hydrography, climate and weather, transportation, civilian telecommunications and media, economics and infrastructure, politics, sociology, and health and medical. The G-2/S-2 considers the amount of information and intelligence available and whether the factors under consideration are important enough to the commander to require detailed treatment. The degree of detail included in the intelligence estimate will depend on the operational situation and the needs of the command in which it is written. Analysis of the area of operations is covered in Chapter 5.

(c) Paragraph 3 - Enemy Military Situation. Paragraph 3 is derived from step 3 of the IPB process (**Evaluate the Threat**) and should include all or most of the data used as the basis for the later analysis of the enemy capabilities. This is primarily a discussion of

what is known about the threat (facts) and the results of the analysis of those facts (assumptions). The enemy military situation is discussed under nine major subheadings (subheadings generally will vary for MOOTW): ground forces, naval forces, air forces, air defense forces, paramilitary and security forces, command and control warfare capability, NBC capabilities, night combat capabilities, and unconventional warfare capabilities. Sufficient information and intelligence must be presented to indicate all general capabilities of the enemy that could affect the mission. However, if it is obvious that these same facts must be repeated in detail in the paragraph which follows, and if exclusion of these facts does not eliminate certain capabilities, then it is permissible to place such facts in the enemy capabilities rather than situation paragraph. Voluminous amounts of data should be considered for inclusion as tabs vice in the body of the estimate. As with paragraph 2, if the threat does not possess a particular type of force, or if that force will have no impact on the mission, that portion should be noted as omitted.

(d) Paragraph 4 - Capabilities and Analysis. Paragraph 4 focuses on those COAs of which the enemy is capable and, if adopted, will affect the accomplishment of the mission. Each threat capability should contain intelligence and other relevant information on what the threat can do, where they can do it, when they can begin and achieve their mission, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering all applicable factors from paragraphs 2 and 3, and attempt to determine and give reasons for the estimated probable adoption by the threat. Examine the threat's capabilities by discussing the factors that favor or militate against its adoption by the threat. The analysis of each capability should also include a discussion of threat strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indicators that point to possible adoption of the capability. Finally, state the estimated effect the threat's adoption of each capability will have on the accomplishment of the friendly mission. The term "capabilities" includes not only the general COAs open to the enemy, such as attack, defense, or withdrawal, but also all the particular COAs possible under each general course of action. These COAs should exactly correspond with the enemy COA models developed in step 4 of the IPB process.

(e) Paragraph 5 - Conclusions and Vulnerabilities. Paragraph 5 is derived from the evaluations made during the IPB process and in paragraphs 2, 3, and 4. It is here that the G-2/S-2 summarizes the effects of the battlespace environment on friendly and enemy COAs, lists the set of probable threat COAs (in order of probability of adoption) based on enemy capabilities in paragraph 4 of the intelligence estimate, and lists the threat's exploitable vulnerabilities. The G-2/S-2 is giving his estimate based on the analysis and synthesis of all available evidence. If the available evidence of enemy activity is not definitive enough to justify an enemy course of action for probable adoption, the intelligence officer selects one based on the characteristics of the area of operations, enemy doctrine, enemy practices, and other available evidence. Conclusions reached on this basis are so indicated to the commander. If the enemy is capable of implementing two or more capabilities simultaneously, that fact should be plainly indicated. This also applies to any combination of the listed capabilities. Where possible, the following five standards should be covered in stating these capabilities:

- What action can occur ?
- Where (in what area) it can occur ?
- In what strength it can be accomplished ?
- When it can occur ?
- From where it can be carried out ?

(f) Tabs. Tabs are utilized to reduce volume in the body of the estimate, but yet still provide detailed data, information and intelligence pertaining to the battlespace and the threat. Appendix C identifies the standard Tabs to a MAGTF intelligence estimate; these can be omitted or added to, however, as the situation requires.

As with the IPB process itself, the intelligence estimate must be tailored to the needs of the command based on METT-T. At times, it simply is not practical to prepare a written estimate. Instead, the intelligence officer may provide a quick, concise, verbal estimate. At higher echelons, estimates supporting standing OPLANs may be so large as to be published as separate documents containing hundreds of pages. In either extreme, they will still follow the basic format outlined above. The bottom line is to provide the commander with the best estimate of what the threat can do, where, and when. The structure of the IPB process and the intelligence estimate format provide the tools for making those determinations. How to apply those tools, and to what level of detail, is part of the art of intelligence analysis.

b. Target/Objective Studies.

(1) Purpose. IPB impacts development through the evaluation of terrain and weather, and the association of threat forces at specific times and locations within the battlespace. Situation, event, and decision support templates identify NAIs. Once identified NAIs can then confirm or deny a threats activities or adoption of a particular COA. Additionally, decision points and target areas of interest (TAI) are identified which require key intelligence that supports either fire or maneuver. From the IPB and wargaming processes, HVTs and HPTs are derived. Target/objective studies are focused, detailed intelligence products which aid in the application of fires or the maneuver of forces against a specific target set or area. These studies can also be utilized by small units, such as MEU(SOC)s, for mission preparation and execution. (See chapter 7 for a detailed discussion of target development and BDA)

(2) Content. Target/Objective studies are graphically oriented and may utilize many of the graphics derived during the IPB process. One such product is a target folder, which contain the following information depending on the specific mission:

- Orientation Graphic

- Time-Distance Graphic

- Weather Forecast

- Hydrographic Forecast and Astronomical Data

- Intelligence Briefing Notes For Mission

- Graphic Intelligence Summary

- Objective Area Graphic Enhancements

  -- Orientation Graphic (10-20 KM around Objective)

  -- Mission Planning Graphic (5 KM around Objective)

  -- Objective Area Graphics

  -- Objective Area Imagery

- Imagery and Graphics of Insertion Points

- SERE Plan

- Challenge and Password

- Mission Specific Data as Required

Chapter 5

ANALYSIS OF THE BATTLESPACE

5000. Purpose

The analysis of the battlespace is a comprehensive study to determine the characteristics and effects of weather, oceanographic, and terrain environmental factors on enemy and friendly operations throughout the commander's AO, and often his AOI as well. It serves as a basis for developing specific friendly COAs and for helping determine enemy capabilities and COAs in commander and staff estimates. This analysis allows the commander and staff to see the battlespace in both spatial (width, depth, height/airspace) and temporal (time) dimensions.

5001. Responsibility

The intelligence officer has staff responsibility for initiating, coordinating, and ensuring completion and dissemination of the analysis of the battlespace. This is accomplished in close coordination with the operations officer and other staff personnel who contribute within their respective warfighting functional areas. The final analysis represents a coordinated staff effort. At the MEF or MAGTF level, typical contributors include the following:

a. Topographic Platoon, A&P Company, Intelligence Battalion. Provides tailored terrain, littoral, and infrastructure studies and factor overlays. Supports integration of weather factors into terrain studies portraying environmental effects. Products are disseminated as graphic tactical decision aids (TDAs) to support IPB and COA development.

b. Staff Weather Officer (SWO), G-2 Division, MEF CE. Provides operational weather forecasts and environmental impact graphics as well as other weather and climatic data to include light and tidal information.

c. All-Source Fusion Cell, A&P Company, Intelligence Battalion. Develops information on sociological, political, economic, technological, and related conditions covering countries of interest. Provides fused , all-source IPB and other intelligence products to support MEF staff planning and decisionmaking.

d. Civil Affairs Officer. Provides information on the civilian personnel, local labor conditions, and capabilities.

e. G-4 Engineer Officer. Assists analysis of routes, potential obstacles and barriers and other information related to mobility and counter mobility.

f. G-3 Psychological Operations Officer. Assists assessment of the local conditions for psychological operations.

5002. Preparation

When possible, the intelligence officer coordinates the development of an analysis of the battlespace based on anticipated missions. On receipt of the warning/execute order, the intelligence officer reevaluates the analysis in terms of the commander's assigned AO and potential AOI. As the operation progresses, changes in mission and the commander's AO and AOI, or receipt of additional or more accurate information will require revision of the analysis. MEF and higher headquarters will normally prepare a detailed written analysis when planning anticipated missions. In the MSCs, the G-2s may prepare a written analysis tailored to the unit's specific mission and intelligence needs. However, in most operations, the geospatial information and services (GI&S) officer, the intelligence battalion commander/ISC, and the A&P cell OIC will use the MEF's analysis supplemented by information of particular importance to the command. Graphic representations of weather and terrain data developed during the IPB are attached as annexes in the tactical study of the terrain covering the MAGTF's AO and AOI.

5003. Characteristics of the Battlespace

The limits of the battlespace are determined for all aspects of air, surface, subsurface, land, space, and the electromagnetic spectrum which can directly or indirectly impact friendly forces. The battlespace generally includes all or most of the AO as well as the AOI. The AOI encompasses that area beyond the AO from which intelligence and information are required to permit planning, decisionmaking, and the successful conduct of operations. Defining the limits of the AO, the AOI, and the battlespace is a joint effort between the operations and intelligence staffs based on the commander's guidance. The AO and AOI are dynamic in nature, and include all interrelated factors capable of affecting a unit's operation. The battlespace is measured in four dimensions: depth, width, height, and time. A battlespace analysis of the AO and AOI evaluates and integrates four environmental dimensions: terrain analysis (land), hydrographic analysis (sea), airspace analysis (air), and climatological analysis (weather). The battlespace analysis study allows the operational commander and staff to fully appreciate the opportunities and limitations afforded by major terrain and oceanographic features, zones of entry, transportation networks, obstacles, and built-up areas within the AO and AOI and fit an operational concept to that environment. The analysis of the characteristics of the battlespace and the preparation of the tactical study of the terrain and other GEOINT products are covered in more detail in MCWP 2-12.1 *Geographic Intelligence*.

a. Terrain Analysis (Land). Terrain analysis is the evaluation of geographic (natural and man-made) features. This evaluation provides information to the planning headquarters including avenues of approach (location and trafficability), zones of entry (deep, close, rear areas), and key or decisive terrain. Much of the detailed work of terrain analysis is done by the A&P company or the its geographic intelligence support teams (GIST) attached to or in direct support of the MSCs, or the

geographic intelligence teams (GIT) attached to a MEU(SOC) CE. Commanders and staff officers must be familiar with the capabilities of these organizations in order to properly direct their work.

(1) Analysis of the Battlespace Environment. The degree of detail in the analysis will vary depending on the area of the battlespace environment. Generally, the evaluation of the AO is more detailed than the AOI. Additionally, the focus will vary throughout each area. For example, rear areas within the AO may require a different focus than areas near or in the main battle area (MBA).

(a) Terrain Analysis. The topo plt and the IIP, A&P company, will conduct the major portion of the terrain analysis production, combining data base information with the results of tactical aerial and ground reconnaissance. Topographic personnel work closely with staff weather officers to ensure their terrain analysis products incorporates the effects of current and projected weather phenomena.

(b) Reconnaissance. The best terrain analysis is based on a reconnaissance of the AO and AOI. Databases are used as a guide for collection, production and dissemination planning and operations, focusing on the areas of most importance to the commander and his mission.

(c) Refresh Requirement. Terrain analysis is a continuous process. Changes in the battlespace environment may change the evaluations of its effects.

(d) Results of evaluation. Express the results of evaluating the terrain's effects by identifying areas of the battlefield that favor, disfavor, or do not effect each broad COA. Conclusions regarding the effects of terrain are reached through a two step process: analysis of the military aspects of the terrain; and evaluation of the terrain's effects on military operations.

(2) Geospatial Factors. Natural terrain factors influence all types of operations and missions. For example, data on the trafficability of soils, the presence of bedrock, as well as the type and density of vegetation is needed when developing cover and concealment, cross-country movement, or other geographic databases. The National Imagery and Mapping Agency (NIMA) produces numerous digital databases that support the development of geospatial factors and geographic classification.

Maps, particularly topographic and geodetic, aerial charts, and facility maps are basic sources of information. Publications containing topographic information include those of geographic societies, engineering and scientific firms, and numerous government intelligence agencies. Libraries, bookstores, and universities are excellent sources.

(a) Surface Configuration. Surface configuration refers to the shape of the earth's land surface. This geographic factor is concerned with the description or representation of mountains, slopes, ravines, embankments, ditches, plowed fields, and rice field dikes which profoundly influence various military operations. This factor is limited only by physical shape, size, and arrangement; it is not concerned whether the feature is man-made or of natural origin. The position of

the earth's surface features combined with their size and shape are used to categorize surface configuration.

Land forms are the physical expression of the land surface. The principal groups of land forms are plains (plateaus), hills, and mountains. Within each of these groups are surface features of a smaller size, such as flat lowlands, and valleys. For geospatial analysis and GEOINT production purposes, major land forms are arbitrarily delimited on the basis of local relief and are classified as follows:

Plains: elevation less than 150 meters (500 feet)

Flat ---------- Less than 15 meters
Undulating ---------- 15 to 50 meters
Gently rolling ------ 50 to 100 meters
Rolling ---------- 100 to 150 meters

Hills: 150 to 600 meters (500 to 2000 feet)

Low ---------- Less than 300 meters
High ---------- 300 to 600 meters

Mountains: more than 600 meters (2000 feet)

Low ---------- 600 to 1500 meters
High ---------- More than 1500 meters

Relief, elevations or irregularities of a land surface are represented on graphics by contours, hypometric tints, shading, spot elevations, hachures, etc. Local relief is the differences in elevation between the different points in a given area.

(b) Hydrologic Features. Hydrology is concerned with the characteristics of surface and subsurface waters. This geographic factor is concerned with the shape, size and distribution of water bodies of all kinds. Temporal variance is a matter of great concern, since these shapes, sizes and distribution change over time. There are also dynamic factors, such as current volume and velocity. These dynamic factors are closely associated with the other geographic factors because many of their characteristics are directly or indirectly influenced by them. Knowledge of the earth's land surface (surface configuration), geologic and soil formations (surface composition), and vegetation will help find and evaluate supplies of water and determine how its occurrence and distribution will affect military operations.

Surface water encompasses all inland waters: streams, rivers and canals, standing bodies of water (lakes and ponds), seasonally or perennially wet areas (swamps and marshes), and glaciers.

Subsurface water, or groundwater, is water located beneath the surface of the earth. Although more difficult to locate and develop than surface water, ground water sources are less susceptible to contamination and may be the only source of water in arid regions.

Wet areas are tracts of seasonally, or perennially, water covered ground areas. These areas are treated separately in the collection of data because information requirements differ from other water bodies, especially in evaluation for cross-country movement.

Most military problems involving water courses (streams, rivers, creeks, canals, etc.) arise from the fact that stream drainage conditions vary not only from place to place but from time to time. Military planners are concerned with the flow and channel characteristics of these water courses and their effect on military operations. Like water courses of which they are normally a part, water bodies (lakes, inland seas, reservoirs, glaciers and snowfields) are involved in the hydrologic and military aspects of surface drainage. They affect the characteristics of surface drainage by storing precipitation and run-off and by retarding or augmenting flood flows. Militarily, they constitute obstacles to cross-country movement or may provide avenues when sufficiently frozen.

(c) Vegetation Features. Vegetation has a significant effect on many types of military operations, and it must be carefully considered in planning operations. Vegetation includes all plant life growing on the surface of the earth, or other flora in or on the water. Vegetation factors are used to evaluate the potential effect of vegetation on movement (both vehicular and foot), concealment, cover, observation, airdrops, and construction. The type of vegetation in an area gives an indication of the climatic conditions, soil, drainage, and water supply. For the purpose of geospatial analysis and GEOINT production, vegetation is grouped into four general types with distinctive characteristics. These include trees, scrub and shrubs, grasses, and crops.

((1)) Trees are defined as perennial woody plants at least 10 feet in height, with single stems and defined crown shapes. A forest is an extensive area covered by trees and may be relatively open, or the trees may grow in close formation so that their crowns touch. Smaller areas covered by trees may be termed woods, groves or woodlots. On military maps, any perennial vegetation high enough to conceal troops or thick enough to be a serious obstacle to free passage is classified as woods or brushwood.

((2)) Scrub includes a variety of trees that have had their growth stunted because of soil or climatic conditions. Scrub growth includes cactus, stunted shrubs, sagebrush, mesquite, and similar plants found in arid or semiarid areas. Shrubs, like trees, are either deciduous or coniferous. Shrubs comprise the undergrowth in open forests; in arid and semiarid areas they are the dominant vegetation. Shrubs normally offer no serious obstacle to movement and provide good concealment from ground observation; however, they may restrict fields of fire.

((3)) Grasses include all kinds of non-woody plants. A grassland is an extensive area where the natural vegetation consists primarily of grasses and forbs (forbs are herbaceous plants, and the dominant type in alpine and certain semi-desert areas). In low latitudes,

grasslands often are termed savannas; in middle latitudes, they are called prairies (tall grass) and steppes (short grass). Grasslands in wet or poorly drained areas are commonly called meadows. For geospatial analysis purposes, grass more than 1 meter (3 feet) high is considered tall, and below that height, short. Grass often improves the trafficability of some soils; very tall grass may also provide concealment for foot troops.

((4)) Field crops constitute the predominant class of cultivated vegetation. Vine crops and orchards are common but not widespread, and tree plantations are found in relatively few areas. The size of cultivated areas ranges from paddy fields covering a quarter of an acre to vast wheat fields extending for thousands of acres. In a densely populated agricultural area where all arable land is used for the crop that brings the highest yield, it may be possible to predict the nature of the soils from information about the predominant crops. Rice, for example, requires fine-textured soils. Other crops generally must have firm, well-drained land. An area of orchards or plantations usually consists of rows of evenly spaced trees, showing evidence of planned planting that can be distinguished on aerial photographs. Usually such an area is free from underbrush and vines. Rice fields are flooded areas surrounded by low dikes or walls. Some crops, such as grain, improve the trafficability of soils while other, such as vineyards, present a tangled maze of poles and wires that are definite obstacles to vehicles and dismounted troops. Wheeled vehicles and some tracked vehicles are unable to cross flooded paddy fields, although they can negotiate them when the fields are drained or frozen.

(d) Surface Materials. This geographic feature is concerned with the composition and physical properties of the materials of the earth's surface. It considers the classification and engineering properties of soil and rock as they apply to military operations and military construction.

Soil is the unconsolidated material that overlies bedrock and is clearly distinguishable from bedrock. It is the accumulation of disintegrated and decayed rock and vegetation. This accumulation can be hundreds of feet thick or it may be absent in given areas. For field identification and classification, soils may be grouped into five principal types: gravel, sand, silt, clay and organic matter. These types seldom exist separately but are found in mixtures of various proportions, each type contributing its characteristics to the mixture. Soils between 15 cm (6 inches) and 2 meters (6 feet) in depth are the most important. Next in importance are the soils from 2 to 6 meters (6 to 20 feet). Soil depth can be measured directly from borrow pits, road cuts, building excavations, and stream banks.

Rock may be defined as the firm or consolidated material of the earth's crust. Bedrock is solid undisturbed rock either exposed at the surface or underlying the soil. The physical and engineering characteristics of rocks are significant factors in military operations, particularly in construction and in locating ground water.

(3) Military Aspects of Terrain. The intelligence officer uses portions of the IPB process to evaluate the battlespace in terms of the military aspects of the terrain. These aspects are key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach and mobility corridors, or KOCOA. KOCOA is not a rigorous analysis and is appropriate to the battalion/squadron and regimental/MAG/CSSD levels. At division, MAW, FSSG, and higher levels

KOCOA is absorbed into the terrain analysis process. KOCOA is not the end product of the IPB process. Rather, it is the means to determine which friendly COAs can best exploit the opportunities the terrain provides and how the terrain affects the threat's available COAs.

(a) Key Terrain. Key terrain is any location or area that the seizure, retention, or control of affords a marked advantage to either combatant. An example of key terrain is a bridge over an unfordable river which gives access to the opposite shore without requiring an assault crossing. Another example is a level clearing in rough terrain which is the only accessible landing field for helicopter operations. A common technique is to depict key terrain on overlays with a large "K" within a circle or curve that encloses and follows the contours of the designated terrain.

In the offense, key terrain features are usually forward of friendly dispositions and are often assigned as objectives. Terrain features in adjacent sectors may be key terrain if their control is necessary for the continuation of the attack or the accomplishment of the mission. If the mission is to destroy threat forces, key terrain may include areas whose seizure helps ensure the required destruction. Terrain which gives the threat effective observation along an axis of friendly advance may be key terrain if the threat must be denied its possession or control.

In the defense, key terrain is usually within the area of operations and within or behind the selected defensive area. Some examples of such key terrain are terrain which gives good observation over avenues of approach (AA) and into the defensive position; terrain which permits the defender to cover an obstacle by fire; and important road junctions or communication centers which affect the use of reserves, sustainment, or lines of communication (LOC).

(b) Observation and Fields of Fire. Observation is the ability to see the threat, either visually or through the use of surveillance devices. Factors that limit or deny observation include concealment and cover. Observation analysis is useful in selecting LZs and DZs, planning helicopter forward area arming and refueling point (FAARP) locations, identifying areas vulnerable to aerial intelligence collection systems, and selecting low-level flight routes and aerial battle positions. A field of fire is the area that a weapon or group of weapons may effectively cover with fire from a given position. Terrain that offers cover limits fields of fire. For example, an ideal field of fire for flat trajectory weapons is an open area in which the threat can be seen and on which he has no protection from the fire of those weapons, out to the weapon's maximum effective range.

Geographic factors that offer good observation and fields of fire generally favors defensive COAs. These factors are usually represented on an overlay with areas of poor observation and fields of fire marked by parallel diagonal lines or crosshatching. The evaluation of observation and fields of fire allows:

Identification of potential EAs (often referred to as "fire sacks" or "kill zones").

Identification of defensible terrain and specific system or equipment positions.

Identification of locations where maneuvering forces are most vulnerable to observation and fires.

(c) Cover and Concealment. Cover is protection from the effects of direct and indirect fires. It can be provided by ditches, caves, river banks, folds in the ground, shell craters, buildings, walls, and embankments. **Concealment** is protection from observation. It can be provided by woods, underbrush, snowdrifts, tall grass, and cultivated vegetation.

Cover and concealment are desirable for both the attack and the defense. Cover and Concealment analysis may be combined into a single overlay crosshatched to depict areas. You can usually use the product developed during the evaluation of observation and fields of fire as a starting point. Use the results of the evaluation to:

Identify and evaluate AAs.

Identify defensible terrain and potential battle positions.

Identify potential assembly and dispersal areas.

(d) Obstacles. Obstacles are any natural or man-made terrain feature that stops, impedes, or diverts military movement. Obstacles to air mobility include features that exceed the aircraft's service ceiling, restrict nap-of-the-earth (NOE) flight or force the aircraft to employ a particular flight profile. An evaluation of obstacles leads to the identification of mobility corridors. This in turn helps identify defensible terrain and AAs. To evaluate obstacles:

Identify pertinent obstacles in the AO.

Determine the effect of each obstacle on the mobility of the evaluated force.

Combine the effects of individual obstacles into an integrated product.

Factors to be considered when evaluating obstacles are: vegetation, surface drainage, surface materials, surface configuration, obstacles, transportation systems (particularly bridge classifications and road conditions), and the effects of actual or projected weather. This evaluation can be done through the preparation of separate overlays for each factor, or by consideration of all factors in one product. Regardless of the method used, this evaluation is then combined into a single product known as the combined obstacles overlay (COO). The COO integrates the evaluations of the various factors into a single product that depicts the battlespace effects on mobility.

The cumulative effects of obstacles are often graphically depicted as areas of terrain classified as **UNRESTRICTED, RESTRICTED,** and **SEVERELY RESTRICTED** (note these terms have replaced the terms, go, slow-go, and no-go). These terms are defined as follows:

UNRESTRICTED: Indicates terrain free of any restrictions to movement. Nothing needs to be done to enhance mobility. UNRESTRICTED terrain for armored or mechanized forces is typically flat to moderately sloping terrain with scattered or widely spaced obstacles such as trees or rocks. UNRESTRICTED terrain allows wide maneuver by the force under consideration.

RESTRICTED: Terrain hinders movement to some degree. Little effort is needed to enhance mobility but units may have difficulty maintaining preferred speeds, moving in combat formations, or transitioning from one formation to another. RESTRICTED terrain slows movement by requiring zigzagging or frequent detours. RESTRICTED terrain for armored or mechanized forces typically consists of moderate to steep slopes or moderate to densely spaced obstacles such as trees, rocks, or buildings. Swamps or rugged terrain are examples of RESTRICTED terrain for dismounted infantry forces. Logistical or rear area movement may be supported by poorly developed road systems. A common and useful technique is to depict RESTRICTED terrain on overlays and sketches by marking the areas with parallel diagonal lines.

SEVERELY RESTRICTED: Terrain severely hinders or slows movement in combat formations unless some effort is made to enhance mobility. This could take the form of committing engineer assets to improving mobility or of deviating from doctrinal tactics, such as moving in column instead of line formations or at speeds much lower than those preferred. SEVERELY RESTRICTED terrain for armored and mechanized forces is typically characterized by steep slopes and large or densely spaced obstacles with little or no supporting roads. A common technique is to depict this type of terrain on overlays and sketches by marking the areas with crosshatched diagonal lines. Other types of SEVERELY RESTRICTED terrain include minefields, unfordable rivers that exceed the vehicle-launched bridge length, and road or railroad embankments. Depict these types of SEVERELY RESTRICTED terrain using the standard symbology contained in FM 101-5-1/MCRP 5-2A. If standard symbology does not exist, such as for unfordable rivers, depict them using wide solid lines, ad hoc symbology, or crosshatching as appropriate. Ensure all non-standard symbolgy is explained in the graphic's legend and is known to all who receive these products.

Terrain mobility classifications are not absolute and reflect the relative effect of terrain on the maneuver of combat formations. They are based on the ability of a force to maneuver in combat formations, usually linear, or to transition from one type of formation to another, as opposed to simply moving through a piece of terrain. It is also possible that local obstacles or "micro-terrain" may restrict movement even in an area which is overall considered UNRESTRICTED. Conversely, identifying an area as SEVERELY RESTRICTED terrain does not imply that movement through that area is impossible, only that it is impractical. Units moving in column along roads generally have little trouble traversing SEVERELY RESTRICTED terrain.

Terrain considered SEVERELY RESTRICTED for one unit may pose no obstructions, or even be favorable to, the mobility of another unit. For example, a dismounted infantry unit could easily negotiate a hilly, forested area that an armor unit might consider SEVERELY RESTRICTED. Similarly, helicopters may consider an area containing several tall towers and numerous high tension wires as

SEVERELY RESTRICTED terrain while the same area would pose little or no difficulties to high performance aircraft operating at higher altitudes. History is replete with examples of forces negotiating terrain classified as impassable by their opponent, thus the classification of terrain must never be taken as absolute.

(e) Avenues of Approach and Mobility Corridors. An **avenue of approach** (AA) is an air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. During offensive operations, the evaluation of AAs leads to a recommendation on the best route to the command's objective and identification of avenues available to the enemy force for withdrawal or the movement of reserves. During the defense, identify AAs that support the threat's offensive capabilities and avenues that support the movement and commitment of friendly reserves. To develop AAs , identify and categorize **mobility corridors**, group corridors to form AAs, evaluate AAs and then prioritize them.

Mobility corridors are areas where a force will be channeled due to terrain constrictions. The mobility corridor itself is relatively free of obstacles and allows military forces to capitalize on the principles of mass and speed. The best mobility corridors use UNRESTRICTED terrain that provides enough space for a force to move in its preferred doctrinal formations while avoiding major obstacles. Mobility corridors usually follow the direction of roads and trails, however, in some parts of the world, the terrain is so difficult that the only mobility corridors available may be through RESTRICTED or even SEVERELY RESTRICTED terrain.

The combined obstacle overlay (COO) is used to identify mobility corridors wide enough to permit maneuver in tactical formations. If friendly and threat forces require mobility corridors of different width, perhaps due to organizational or equipment differences, you may have to conduct two separate evaluations. Identification of mobility corridors requires some knowledge of friendly and threat organizations for combat and preferred tactics. Mobility corridors usually follow the direction of roads and trails.

When identifying mobility corridors factors other than obstacles and mobility must be evaluated. Mobility corridors, like obstacles, are a function of the type and mobility of the force being evaluated. For example, mechanized and armored units generally require large open areas in which to move. Dismounted infantry, and most insurgents and terrorists, are less restricted by the presence of obstacles or hindering terrain and prefer areas that provide concealment and cover. Similarly, the mobility corridor used by a jet aircraft with a minimum operating altitude of 1,000 feet is quite different from that considered by a helicopter with a maximum service ceiling of 10,000 feet.

Once identified, mobility corridors are categorized according to the size or type of force they will accommodate. Mobility corridors are normally identified for forces two echelons below the friendly command, although in situations such as MOOTW this may not apply. In addition, where terrain is restrictive, allowing only relatively small mobility corridors, the evaluation may need to look several echelons below the friendly command.

Group mobility corridors together to form AAs. An AA will normally provide ease of movement and enough width for dispersion of a force large enough to significantly affect the outcome of an operation. AAs are normally identified for a force one echelon below the friendly command. Unlike mobility corridors, AAs may include areas of SEVERELY RESTRICTED terrain since they show only the general area through which a force can move. Depict AAs using the outlines of arrows that encompass the mobility corridors which constitute the avenue. Threat AAs are generally depicted in read, friendly in blue (see figure 5-1).

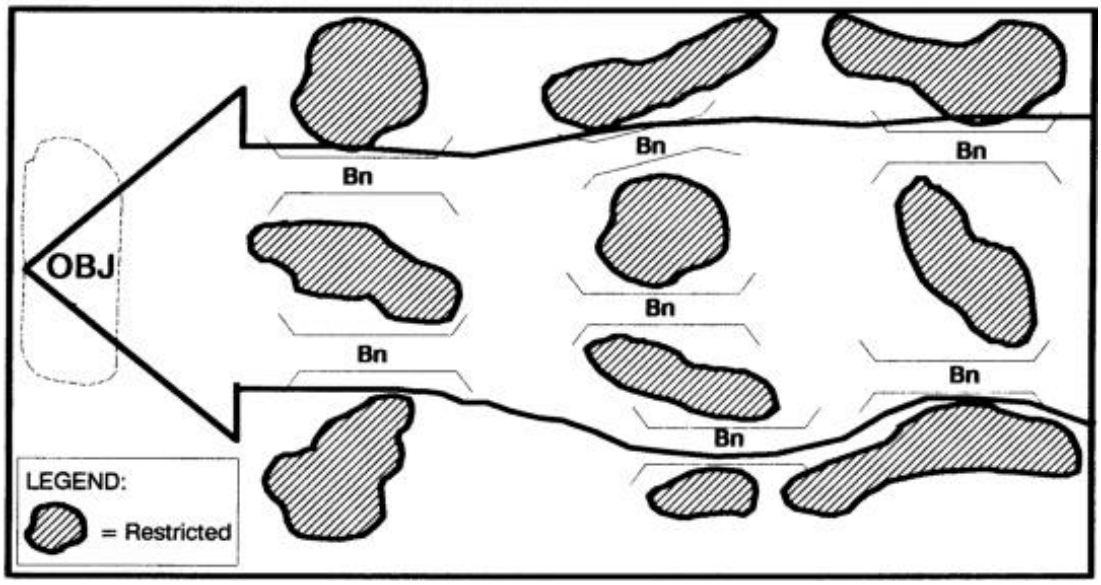

Figure 5-1. Group Mobility Corridors to Form Avenues of Approach

An evaluation of avenues of approach identifies those which best support maneuver capabilities. This evaluation should be a combined effort performed by the intelligence section, the MC&G officer or terrain analysis team, and the operations section. Evaluate them for suitability in terms of:

Access to key terrain and adjacent avenues.

Degree of channalization and ease of movement.

Use of concealment and cover.

Use of observation and fields of fire.

Sustainability.

Directness to the objective.

b. Hydrographic Analysis (Sea). Intelligence of coasts and landing beaches is an important component of studies of world areas containing shorelines, whether they be on the open sea or on inland waters. The coast is, in many places, the first line of resistance in the defense of a country and normally allows only limited maneuver space. Comprehensive analysis of littoral and hydrographic factors worldwide is conducted by the Naval Oceanographic Office (NAVOCEANO) at the Stennis Space Flight Laboratory, Mississippi. Detailed imagery-based beach studies are produced by the Joint Intelligence Center, Pacific (JICPAC); the Atlantic Intelligence Command (AIC); and the Marine Corps Intelligence Activity (MCIA). Graphic and text-based analysis are available both online via INTELINK/INTELINK-S and via request for production validated through the operational chain.

(1) Description and Definitions. Hydrographic analysis and production is an evaluation of coastal regions of the world with regards to their capability to support amphibious operations. In support of Naval ship-to-shore-to hinterland maneuver strategies and concepts, the littoral zone is roughly defined as 60 nautical miles seaward from the high water line, and 60 nautical miles landward from the high water line. The "wet" or hydrographic analysis is subdivided into the offshore, nearshore, and foreshore environments. The "dry" or land analysis is subdivided into the beach and inland or hinterland environments.

Beaches are the most prevalent natural feature of the coastal region. They are accumulations of loose sand, gravel, or boulders that are shaped by waves and currents acting on the shore. Along many lowland coasts, beaches occur as barrier islands that parallel the coast and are separated by a lagoon or bay. For example, barrier islands extend almost the entire length of the East and Gulf coasts of the United States. Along other stretches of coast, beaches are backed by eroding cliffs, or the beach may be totally absent, with high rocky cliffs facing the waves directly.

(2) Hydrographic Conditions

(a) Seas and Surf. Seas are waves which affect amphibious landings and originated in local storms. Swells are waves that have traveled hundreds to several thousands of miles from a distant storm before arriving at the landing site. Regardless of origin, breaking waves (breakers or surf) 4 feet in height normally are considered too high for amphibious assault operations or for logistics over the shore (LOTS). Wave or surf observations for intelligence should cover at least three years and preferably more to permit accurate assessments of monthly or seasonal frequencies. Type of breakers will indicate the type of nearshore bottom over which waves are approaching.

Spilling breakers indicate a gentle sloping bottom, so gentle in fact that the waves lose energy gradually as they approach. Spilling breakers dissipate energy by breaking at the crest only, and it is common to see a number of such breakers existing simultaneously.

Plunging breakers are waves which become totally unstable because of abrupt changes in the bottom over which they approach. These changes may be in the form of a longshore bar or degree of steepness at the shore. In either case the waves break in a rollover, plunging action.

Surging breakers are the least common of all types of breakers. They occur only at very steep nearshore bottoms. This type of wave peaks up near the shoreline but instead of breaking or spilling actually surges up the face of the beach. Surging breakers are significant as indicators of steep nearshore gradient.

(b) Tides. Tides are the alternate rising and falling of the sea caused by the gravitational attraction of the moon and sun. In any given locality the actual tidal range which occurs is the complicated product of various forces including local bottom configuration. The importance tidal phenomena have in amphibious operations is critical and analysts should be aware that the level of the sea is not constant. Therefore, beach widths, hazards, and depths must be related to a specified vertical datum or to the time of day observations were made in order to permit computation of the stage of the tide. The size and configuration of oceanic basins may alter the height and time of the tides. Tidal information for most places on the coasts of the world can be obtained from tide tables published by the U.S. Department of Commerce.

(c) Currents. Currents in the nearshore zone which influence amphibious landing operations may be generally classified as wave-generated currents, tidal currents, or stream currents.

The **wave-generated** currents, caused by the angular breaking of waves on the beach slope and the resultant back rush normal to the beach, results in a littoral current (longshore current) in the nearshore zone, flowing generally parallel with the shoreline. It is found shoreward of the outermost edge of the breaker zone and varies in velocity or force with the force of the waves, their angle of impingement upon the shore, and the steepness of the foreshore. Littoral currents may be insignificant in terms of amphibious operations, or they may be strong enough to cause personnel to lose their footing, to make maneuvering of craft difficult, and to throw landing/assault craft out of control and expose them to broadside attack by the surf. Littoral currents are particularly significant where depths shoreward of the breaker zone are such as to make wading hazardous.

Tidal currents are generally only significant in their effect on amphibious landings in the proximity of tidal inlets, estuaries, river mouths, and similar restricted channels. With large tidal ranges these currents may make the maneuver of landing craft on beaches adjacent to the tidal inlet extremely hazardous.

Currents which extend from rivers into the open sea are frequently of such strength as to affect the maneuver of landing craft near the mouth of such rivers. As in the case of tidal currents, river currents are of significance in amphibious landings only in the proximity of river mouths.

(3) Considerations for beach selection. From a tactical perspective, the ideal beach for an amphibious landing is one with no obstructions in the sea approaches, deep water close inshore, nearshore gradients sufficiently deep for dry-ramp beaching of landing craft and ships, soil composed of firm sand with gentle gradients, small tides, and no currents or surf. The beach terrain should be gently rising, relatively clear, and with a firm surface that has adequate drainage. Flat or gently rising terrain, backed by a coastal range high enough to mask the landing area, is the most desirable for landing

operations. Ideal conditions are rarely found, so suitable areas must be evaluated to determine those that come nearest to the optimum requirements. The following features need to be evaluated to support amphibious operations.

(a) Size. Beaches are measured in kilometers and the size of the beach will determine what size force is capable of being supported. The size of the beach will also define requirements for follow-on logistical forces and establishment of logistical base sites/dumps. The total length of the beach and the usable length (gross length minus portions rendered unsuitable for landing by features such as rock outcroppings, rivers, etc.) must be given. The unsuitable sections of the beach should also be described and plotted. Beach features which might affect movement along the beach should be described and located. It is important to know the widths of beaches that would be available at different stages of the tide particularly the width at low-water stage (maximum width) and at high-water stage (minimum width). When beach widths are quoted, the stage of the tide should be given. Where beach widths vary throughout the length of the beach, the location of major changes in width should be given.

(b) Approaches. Characteristics of water depths are generally given seaward of the 30 meter depth curve and should stress major obstructions and obstacles in the offshore approaches. More detailed analysis and information is provided shoreward from the 30 meter depth curve giving distances and azimuths of obstructions and obstacles from the centerline of the beach. Descriptions will include general approach conditions, specifically noting the presence of shoals, bars, kelp beds, island groups, or exposed rocks.

(c) Gradient. The gradient of the foreshore may be so steep as to prohibit the landing of vehicles from beached craft without use of matting, or it may be so flat as to cause personnel and vehicles to move great distances over exposed areas from boats to cover. The gradient of the high-water zone of the foreshore may be much steeper than the foreshore. If so, the condition is recorded. Information of seasonal changes in gradient, if available, also should be recorded. If backshores are not level, their slope is also necessary. Gradient is normally given as one unit of vertical rise in relation to horizontal distance (such as 1 foot vertical height over 20 feet of horizontal distance = 1:20). Gradient may also be given in percent of slope or degrees of angle if it is clearly indicated.

(d) Hydrographic conditions. Hydrographic conditions shoreward of the 30 meter depth curve should be thoroughly investigated and surveyed if possible. Shallower depths of the surf zone from zero to 30 meters are of primary concern in amphibious operations because it is here that surf is encountered, craft may ground, and troops and vehicles may have to disembark in water. The precision and scope of the surveys should be adequate for accurate location of obstructions, determination of clear boat passages to the beach, location of points of grounding for all types of landing craft, determination of trafficability of bottom materials, selection of suitable beaching places for landing craft and amphibious vehicles, and determining maneuver areas for craft of all types.

(e) Composition. A description of the characteristics of the beach material gives a valuable clue to the slope or gradient of a beach when other information is lacking, as this

gradient is determined chiefly by the size of material and the character of wave action. The depth of beach materials and the nature of subsurface materials is also a valuable indication of beach firmness and trafficability.

(f) Trafficability. The trafficability of a beach is the ability to sustain traffic of troops and vehicles. Trafficability varies greatly with many factors such as moisture content, slope, grain size, compacting, etc. Some general rules on beach firmness follow; however, many factors influence firmness and changes in firmness may occur in short periods of time.

Sandy beaches are more firm when damp. Beach backshores are frequently dry and therefore soft. Sorted pebbles and cobbles are firm as far as bearing capacity is concerned, but they are loose to traction of wheels and tracks of vehicles and provide poor trafficability. Clay is invariably soft when wet, but combinations of clay and sand content may be firm. A mixture of fine to coarse sand tends to be firm. Soft zones are common near the upper level of wave wash at high tide; these soft zones are due to the entrapment of air in pockets under the wet sand. In general, sand beaches exposed to wave action are firmer than beaches of similar material in sheltered locations.

(g) Vegetation. Permanent vegetation normally is absent from beaches. Temporary grasses and herbaceous plants may become sparsely established in seasons of low waves, but eventually are destroyed. Vegetation on a beach is rarely of significance to military operations except for mangrove. Although mangrove normally occurs in sheltered tidal areas having a soft, fine bottom material, they may exist on foreshores which do not experience heavy wave action. Their interlaced roots constitute a barrier to movement.

(h) Obstacles

((1)) Natural. Cusps are more or less evenly spaced ridges or horns of beach material and intervening crescent shaped troughs. The horns trend at right angles to the shoreline, and taper to their point seaward. Cusps present on beaches should be noted. There are several characteristics of this beach feature that may be significant in amphibious landings. Along gravel beaches the cusps may develop very large proportions, rising several feet above adjacent troughs and becoming a serious hindrance to traffic. Cusps are soft, whereas the troughs are usually of the same firmness as the normal beach face.

Beach ridges are essentially continuous mounds or ridges along a beach created by wave action along the upper limits of the beach. They may occur as single ridges or as a series of approximately parallel ridges extending some distance inland. The ridges commonly are 3 to 8 feet in height above mean high tide but have been known to attain a height of 30 feet on pebble beaches. Ridges may consist of sand, pebbles, or gravel (shingle included). In the latter case they may be formidable barriers to movement off the beach. Gravel or shingle ridges are high and loose and are very difficult to traverse.

A **scarp** is a near-vertical face cut into beach materials by a period of erosive wave action. Only those scarps which are cut into the backshore have appreciable permanence because normal wave action will soon eliminate those on or near the foreshore.

A **beach berm** is a nearly horizontal formation of material deposited by wave action. It begins at the limit of normal-wave up rush and extends landward. No berm or one or more berms may exist. Several berms indicate several depositional wave regimes. Where more than one berm exists, they are separated by beach scarps in various stages of deterioration. The seaward margin of a berm is know as the berm crest. Berms are usually dry and soft, but may be firm for a short time when damp.

((2)) Man-made. Groins are structures utilized in the stabilization of a beach. They are long, low, narrow structures extending seaward from the backshore and are intended to entrap water-suspended sand in motion along the shore. Groins are usually built as a system of structures spaced at regular intervals along the beach, therefore they are obstacles to the lateral movement of vehicles, especially along the foreshore of a beach.

Jetties are structures projecting seaward from the shoreline and through the normal surf zone. They are larger and more massive than groins and are used to improve and stabilize inlets and river mouths. They prevent deposition of sand in the channel, regulate the inflow and outflow of tides and river discharge, and protect vessels entering the inlet or river. In order to prevent the movement of sand into the channel and to protect vessels against wave action, jetties must be high enough to protect against expected storm waves.

Bulkheads and **sea walls** are used primarily to protect areas of the coast against heavy storm-wave action. They limit the shoreward movement of destructive waves, but under severe wave action they may cause the removal of sand from the beach by inducing scour at the base of the wall, and by reflected wave energy. During periods of normal wave action the sand may be returned to the beach, but the sea wall or bulkhead has no function in this action. They are solely for the protection of land behind the bulkhead or sea wall. Sea walls and bulkheads may be barriers to troop and vehicular movement from a beach to inland areas. They normally are strongly designed to protect against the highest storm wave which can be expected in that particular locality and therefore could be difficult to break through.

(i) Exits. Uninterrupted movement inland from a beach is necessary to provide direct, rapid support and supply of combat forces and to avoid the creation of lucrative targets of accumulated material and personnel on beaches. However, movement off a beach inland onto favorable terrain in many localities is one of the most difficult aspects of a landing because of the prevalence of bluffs, dunes, swamp, or lagoons close behind beaches. Existing exits are those which require little or no preparation. They may be man-made or natural, roads, ramps, stairs, paths, gullies, dry stream beds, and gaps between dunes. Another characteristic of an exit requiring evaluation is the width. An exit should have a minimum width of 8 feet to permit the passage of vehicles.

(3) Amphibious Operations. Amphibious operations require detailed studies of oceanography, weather, and terrain. A technical discussion of the requirements and preparation of these studies is beyond the scope of this manual. They are covered in greater detail in joint publication 3-02, *Joint Doctrine for Amphibious Operations*, MCWP 2-12.1, *Geographic Intelligence*, the MCWP 3-31 series, and FM 34-81, *Weather Support for Army Tactical Operations*.

c. Airspace Analysis (Air). The modern battlespace must be considered in three dimensions: width, depth, and airspace. Width and depth have traditionally been considered during operations and emphasized in the IPB process. However, the increased friendly force reliance on air support and mobility have dictated that the battlespace be viewed in terms of a third dimension -- airspace.

(1) Description. Before the rise of aviation, the battlespace had always been viewed in terms of square kilometers. Since the addition of the airplane and helicopter to the arsenal of war, the battlespace must now be viewed in terms of cubic kilometers. Airspace itself has no reference points to guide the analyst, and all evidence of air activity is erased seconds after the activity occurs. Airspace analysis must therefore tie air events to time and to the ground. Because of this requirement, it is often difficult to establish NAIs, TAIs, and air operations DPs. It is critical that aircraft maximum service ceilings, minimum operating altitudes for both fixed and rotary-wing aircraft, and the maximum effective ranges of air defense weapons systems be integrated with the terrain into airspace analysis.

(2) Airspace Battlespace Area Evaluation. Evaluation of the third dimension, airspace, is conducted from a different perspective than that done for ground IPB. Terrain and weather have entirely different effects on aviation operations. The third dimension of the battlespace includes the air AO and the air AOI. The air AO, like the ground AO, is the area where the commander is assigned responsibility and authority for military operations. It is identical to the ground AO when considering the placement of ground-based systems, but is limited only by maximum and minimum aircraft operating altitudes and the maximum effective ranges and altitudes of air defense weapons when considering actual airspace. The air AOI includes airspace adjacent to the air AO and extends into enemy airspace. The air AOI is normally much larger than the ground AOI due to the great distances aircraft can cover rapidly. The air AOI extends upward to the maximum service ceiling of enemy aircraft and the maximum effective altitude of enemy air defense weapon systems. The air AOI may also extend as far as enemy airfields and to the maximum range of enemy surface-to-surface missile systems. During the evaluation of the Battlespace, potential locations of LZ, DZ, FAARPs, and forward assembly or expeditionary airfields are identified to pinpoint requirements for further analysis.

(3) Geospatial Analysis Support. Geospatial analysis and GEOINT production in support of air defense, counter-air, and other air-associated operations is significantly different from analysis for ground operations. The analyst is dealing with an environment that extends several thousand meters above ground level (AGL), and with forces whose mobility is limited only by the ability of their equipment. The nature of airspace does not eliminate the need for terrain analysis because aircraft and air defense elements will still attempt to use the terrain to their best advantage. In fact, it is probably accurate to say that third dimension analysis (airspace) relies as much on terrain analysis as does the ground IPB effort. Standard military topographic maps are not normally considered suitable for other

than the most basic airspace analysis. Standard 1:50,000 scale topographic maps are most useful when analyzing the ability of an aircraft to approach, acquire, and engage a target. The analysis of an aircraft's approach (from air base to target vicinity), or of enemy air corridors should be conducted using standard 1:250,000 scale Joint Operations Graphic - Air (JOG-A) specifically designed for this purpose.

As with ground IPB, the intelligence staff receives support from the terrain team during airspace analysis. However, this support must be augmented by personnel from other functional areas with an understanding of the air threat, air defense systems and operations, and close air support (CAS) techniques. Terrain analysis for air operations focuses on the same military aspects of terrain as ground operations. However, the analysis of these aspects is directed first at their effects on airspace operations, and then on their resultant effects on the overall operation.

(a) Key Terrain. Key terrain in airspace analysis is any terrain feature which allows air defense weapons to engage channeled or constrained air or airborne forces. Areas that limit aircraft lateral movement, restrict air maneuver, or have elevations higher than maximum aircraft service ceilings should also be considered key terrain. Other areas which should be considered key terrain include:

Airfields.

LZs and DZs.

Fixed or surveyed air defense weapons and radar sites.

FARRPs.

(b) Observation and Fields of Fire. As with ground operations, observation involves the effects of the terrain on reconnaissance and surveillance, as well as target acquisition. Fields of fire involves the effects of terrain on weapon's effectiveness. In air defense, both counter-air and other air operations are closely related to line of sight (LOS). Ground operations are concerned primarily with horizontal LOS, where air and air-associated operations are primarily concerned with air and ground oblique and vertical LOS.

Both attack aircraft and air defense assets want as much protection as possible from enemy observation, and both require direct LOS to the target. It is, therefore, necessary to analyze airspace regarding the routes which provide the best protection for aircraft entering the target area and those which provide the best fields of fire for the aircraft once it reaches the target area. Similarly, the analysis must consider where air defense assets can best be hidden from observation, and retain good fields of fire against the primary air avenues of approach and mobility corridors.

(c) Concealment and cover. Many of the air-related aspects of concealment and cover have been addressed under observation and fields of fire. Friendly force operations require cover from aerial direct fires, especially antitank fires, and concealment from aerial reconnaissance and

surveillance. Similarly, the enemy will attempt to use terrain to provide cover from direct fires and to conceal their operations from friendly detection.

While not considered as either concealment or cover in the strictest sense, NOE flight enhances both fixed and rotary-wing aircraft survivability. An NOE flight makes the optimum use of available terrain for concealment and cover, and hinders quick countering responses by ground forces and air defense assets.

(d) Obstacles. Normally, three types of obstacles are considered during airspace analysis. They include:

Obstacles to the effective employment of air defense target acquisition or weapon systems.

Obstacles which restrict NOE flight (below 22.8 meters, or 75 feet in height).

Obstacles which force aircraft to employ a particular profile or attack route or to gain excessive altitude (above 22.8 meters in height).

Obstacles to the effective employment of air defense target acquisition or weapons systems include terrain which masks LOS, built-up areas (especially areas with tall buildings), and vegetation. Obstacles which restrict NOE flight include tall trees, radio, television and microwave relay towers, power transmission lines, support towers, smoke and obscurants, and tall buildings. Obstacles that force aircraft to gain excessive altitude or to adopt a particular attack profile or attack route include mountains, large hill masses, built-up areas, and excessively tall trees. Of particular interest are obstacles which restrict lateral movement within the air avenue of approach or mobility corridor. These obstacles have the same effect on aircraft as ground obstacles; that is, channeling movement and restricting evasive action. They often become key terrain for the employment of air defense weapons systems.

(e) Avenues of Approach. Airspace avenues of approach are evaluated by the same criteria as ground avenues of approach. A good air avenue of approach permits maneuver while providing terrain masking from air defense weapon systems. Additional variables considered in analyzing the air avenues of approach include:

Type of aircraft.

Maximum service ceiling of the aircraft.

Attack profile being employed.

Weapon system or expected ordnance.

Type of target to be attacked.

(f) Weather Analysis. Weather aspects (especially temperature, humidity, and cloud cover) also have a significant impact on the ability of aircraft to use a particular avenue of approach. Aviation operations are especially susceptible to the effects of weather. Weather analysis for airspace operations considers the same factors of visibility, wind speed and direction, precipitation, cloud cover and temperature, and humidity as does weather analysis for ground operations.

5004. Climatological/Weather Characteristics of the Battlespace. Commanders cannot control the weather, but must be sensitive to the effects inclement and other weather factors have on personnel, equipment, and mission accomplishment. Weather and visibility conditions create advantages and disadvantages for opposing forces. Commanders and their staffs must acquire weather information about the entire battlespace area and know how to exploit the opportunities the weather offers while minimizing its adverse effects.

a. Description

(1) Interaction of Battlespace Environment Elements. Weather conditions, terrain, battlespace induced contaminants, illumination, oceanographic, and background signatures are some of the primary factors that will be found in a battlespace environment. Paragraph b of this section defines some of the more common weather elements affecting the battlespace. Weather conditions such as wind, precipitation, and cloud cover can impact, or can be influenced by, the other conditions of the battlespace (such as terrain, illumination, etc.). All of these conditions are interdependent and must be considered as a whole.

(2) Weather Effects and Terrain. Terrain features affect such weather elements as visibility, temperature, humidity, precipitation, winds, and cloud cover. The most common example of terrain affecting weather is on the windward side of high terrain, such as mountains, the rainfall rate will be greater than on the leeward (opposite) side. Weather conditions such as temperature, winds, and precipitation have a definite effect on the terrain and can enhance or limit military operations, such as trafficability, water crossing (fording), and first-round accuracy of supporting field artillery fires. The responsibility for determining weather effects on mobility and counter-mobility is given to the topo plt at the MEF level or supporting GISTs at MSC and GITs at MEU(SOC) CE levels. This is done in conjunction with the staff Engineer Officer and weather team or SWO.

b. Common Weather Elements

(1) Temperature. Temperature is the value of heat or cold recorded by a thermometer normally at 6 feet above the ground at the observation site. Temperatures are normally given in both Fahrenheit and Celsius values. Periods of freezing temperatures will increase the trafficability of some soils, while at the same time it may create ice sheets on roads, making movement more difficult. Thawing temperatures may make frozen soils difficult to traverse and may damage roads with poor foundations. The ability of projectiles to penetrate the earth is decreased by frozen soil, but

freezing increases the casualty effect of contact-fused shells. Melting snows may cause floods and in mountain areas result in avalanches. Temperature inversions create an exception to the normal decrease in temperature that occurs with increases in altitude. In a temperature inversion, the air nearest the ground is colder than the overlying air. The lower air remains stable, holding dust and smoke near the ground, reducing visibility and air purity.

(2) Humidity. Humidity is the state of the atmosphere with respect to water vapor content. It is usually expressed as relative or absolute humidity. The effects of humidity on ballistics are important because of the relationship of humidity and density. The amount of water vapor in the air affects the trajectory of projectiles by the influence it has on air temperature and density. Humidity also has an effect on the distance sounds travel, thus affecting listening posts and sound-ranging operations.

(3) Precipitation. Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types. The intensity of precipitation is described as light, moderate, or heavy. Precipitation affects soil trafficability and hence cross-country movement (CCM). In areas of seasonal precipitation, the CCM characteristics of an area may change drastically each season. Seasonal floods may swell or flood streams, making fording and bridging operations difficult or impossible. Snow and sleet hamper movement on roads in winter, often making them impassable in mountainous areas. The snow that accumulates in mountains during the winter months frequently affords a water supply throughout the year to lower, drier regions. Precipitation usually has an adverse effect on visibility and observation, although rain may wash excessive impurities from the air. Rain and snow aid concealment, and may facilitate surprise attacks. Operations of listening posts and many electro-optical systems are often limited by precipitation.

(4) Visibility. Visibility is a measurement of the horizontal distance at the surface or aloft that the unaided human eye can discern a large object or terrain feature. Visibility is reported in meters or fractions of a mile, and is reported as a prevailing value of the visibility in all directions. Thus, a visibility report of 1,600 meters may not reveal that fog is diminishing visibility to 400 meters in the northwest if the observer has good visibility in other directions. However, such an event would typically be carried in the weather observation's remarks section.

(5) Wind Speed and Direction. Wind speed is the measure of the rate of movement of the air past a given point and the direction from which the wind is blowing. A gust is a rapid fluctuation in wind speed with a variation of 10 knots or more between peak and lull. In arid or semiarid areas, strong winds frequently raise large clouds of dust and sand which greatly reduce observation. Similar effects result in snow covered regions, where blowing snow may reduce visibility over wide areas. Observation aircraft and sensors may be grounded entirely during such periods. Winds tend to deflect projectiles from their normal paths, particularly when they are fired at long ranges. The effect that wind will have on a projectile increases with an increase in the velocity of the wind and the size of the projectile. To obtain accuracy in indirect fires, the direction and velocity of the wind must be known in order to apply compensating corrections to firing data. Strong winds hinder amphibious operations by creating high seas which will prevent landing craft from landing or retracting. It will also affect heliborne operations during the ship-to-shore movement phase.

(6) Clouds. Cloud conditions are described by the amount of cloud cover and the height of the base of the cloud above ground level. A cloud ceiling is the height of the lowest broken or overcast layer, and is expressed in feet. A higher layer of several scattered layers of clouds is designated as a cloud ceiling. Daytime cloudiness reduces the amount of heat received from the sun at the earth's surface, slowing down the drying of roads and affecting the trafficability of soils. Extensive night cloudiness prevents the loss of heat from the earth's surface due to radiation cooling and results in higher nighttime temperatures. Cloudiness chiefly affects air operations by limiting aerial observation and reconnaissance.

(7) Atmospheric Pressure. Atmospheric pressure is the pressure exerted by the atmosphere at a given point and measured by a barometer in inches of mercury or in millibars. High pressure altitude is critical to the lift capability of fixed wing aircraft. Density altitude is a place in the atmosphere corresponding to a particular value of air density. High pressure is critical to helicopter operations.

c. Intelligence Preparation of the Battlespace. IPB templates and processes provide an integrated graphic portrayal of enemy doctrine and the effects of weather and terrain within the AO and AOI. Development of IPB products, while still in garrison, based on climatology gives a general idea of what average seasonal weather conditions will be in the AO. Once in the field, terrain and weather analyses in support of the IPB are based on locally updated terrain data bases and the current weather forecast for the AO and the AOI.

d. Climatological/Weather Effects. Weather, climate, and terrain are so interrelated they must be considered together when planning MAGTF operations. Weather elements are capable of drastically altering terrain features and trafficability. Conversely, terrain features exert some influence on local weather. This relationship of weather and terrain must be carefully correlated in terrain studies in order to produce accurate geospatial analysis. Terrain features are affected by such elements as visibility, temperature, humidity, precipitation, winds, clouds, and electrical phenomena. The specific factors described vary with the geographic area, time, and season. Terrain features also influence the climate of an area. A description of the climate of a large area can consider these terrain influences only generally, whereas a description of a small area, such as a single valley, can be quite specific.

The type of operation planned determines the pertinent elements of climatological information, intelligence assessments and products to be furnished. Planning of airborne, amphibious, and other special operations requires knowledge of weather and oceanographic elements of somewhat different emphasis than are normal to ground operations.

The major weather elements affecting tactical operations are restricted visibility, winds, precipitation, cloud cover, temperature, and humidity. Only when the effects of these elements are understood and properly evaluated can the weather factor be judiciously weighed with other essential elements of information.

(1) Effects of Restricted Visibility. Poor visibility normally aids both the ground offense and withdrawal. It restricts visual reconnaissance and surveillance. In the offense, it tends to conceal concentrations and maneuver of friendly forces from the enemy, thus enhancing the possibility of achieving surprise. Poor visibility generally hinders the defense, because defensive cohesion and control are difficult. Target acquisition is less accurate with a consequent decrease in the ability to place aimed fire on the advancing force, although this disadvantage may be partially offset by extensive use of illuminants, radar, sound detection, and thermal/infrared sensing devices. Poor visibility enhances patrol activities and guerrilla operations by masking and screening movement.

(2) Effects of Wind. Wind velocity, both on the surface and aloft, almost invariably favors the upwind force in any type of operation. Chemical and biological weapons will saturate the low-level downwind atmosphere with contaminating aerosols. Wind of sufficient speed reduces the tactical capability of the downwind force by blowing dust, smoke, sand, rain, or snow on personnel and equipment. The upwind force, with the wind at its back, has better forward visibility and can advance easier and faster.

(3) Effects of Precipitation. The primary significance of precipitation is its effect on the state of the ground and trafficability, on the efficiency of personnel, and on visibility. The effects of restricted visibility caused by precipitation are just as important as those caused by airborne particles such as dust or smoke. Rain, snow, and fog mask patrol and guerrilla activities by decreasing the enemy's surveillance and detection capability. Precipitation severely reduces trafficability; it alters the surface condition of different soils to varying extents. A heavy rain may make some types of unsurfaced roads impassable, but have little effect on others. Heavy or prolonged precipitation usually aids the protected defense by limiting the mobility of an offensive force. It can also drastically reduce the efficiency and effectiveness of exposed personnel. On the other hand, precipitation may aid offensive operations by degrading the surveillance capabilities of radar, electro-optical, and infrared devices.

(4) Effect of Clouds. The type and amount of cloud cover, as well as the height of cloud bases and tops, influence ground tactics because they affect the entire range of both friendly and enemy aviation. Extensive cloud cover reduces the effectiveness of air support, and provides a tactical advantage as cloud cover increases, as cloud bases lower, and with the increase of conditions frequently associated with clouds, such as icing, turbulence, and poor visibility aloft. Clouds further affect ground operations because they may limit illumination and visibility. They also determine the types, intensities, and amounts of precipitation. As solar radiation interceptors, clouds tend to reduce extremes of surface temperature.

(5) Effect of Temperature and Humidity. Temperature and humidity affect the density of the air. When temperature and humidity are high, the air will be more dense than when they are low. Thus, the efficiency of all aircraft is reduced in areas of high temperature and high humidity. Although temperature and humidity do not directly favor or disfavor a particular tactical operation, extremes will reduce personnel capabilities and may necessitate a reduction of aircraft payloads. Tactics devised for one climatic zone may require considerable revision if used in another. High temperature and humidity conditions found in the tropics are conducive to growth of dense foliage and

jungles, which drastically affect operations. In temperate climates, cold weather periods create an almost constant need for heated shelter, cause difficulty in constructing fortifications, increase the amount of dependence upon logistical support, and necessitate special clothing, equipment, and combat skills.

(6) Weather Forecast and Weather Effects Matrix. Conduct of the battle within the AO is influenced by the effects of weather. The key is exploiting opportunities offered by weather while reducing or minimizing the adverse effects. The geographical layout of the battlespace is important because the times and distance across the AO and AOI vary with the size, type of unit, and mission. These constraints affect the type of weather forecasts needed in terms of time and area. The duration of the forecast must meet or exceed the planning and execution cycles. Utilizing a the weather forecast graphics (see figure 5-2) and the weather effects matrix (see figure 5-3), critical impacts can quickly be identified and graphically portrayed for a variety of missions. Essential to creating such a matrix are the critical values related to specific types of equipment and operations. Unit intelligence officers, working in conjunction with operations personnel, should develop detailed critical value tables for their units as part of their garrison activities. Those critical values can then be quickly modified and applied to planned operations to determine the impact of weather factors on friendly actions. Appendix D provides an example of weather related critical values.

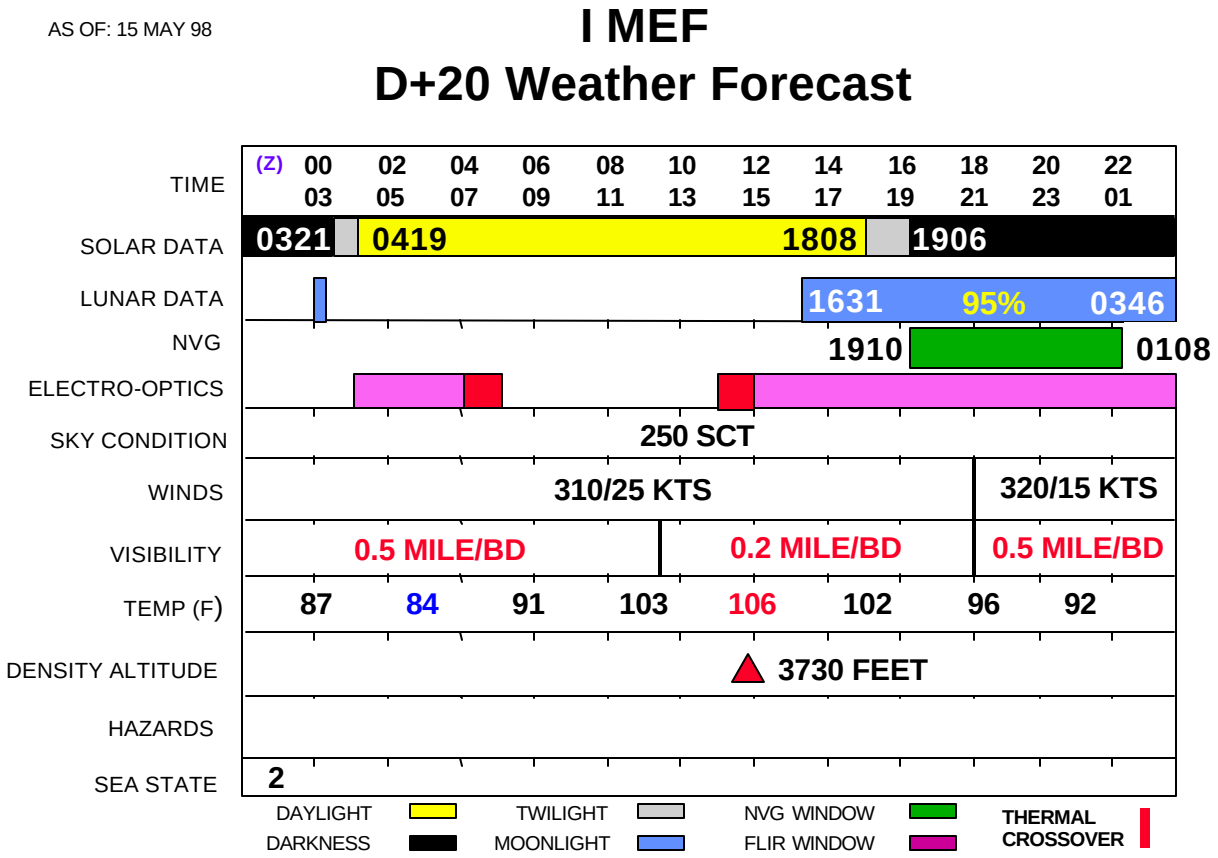

Figure 5-2 Weather Forecast Graphic

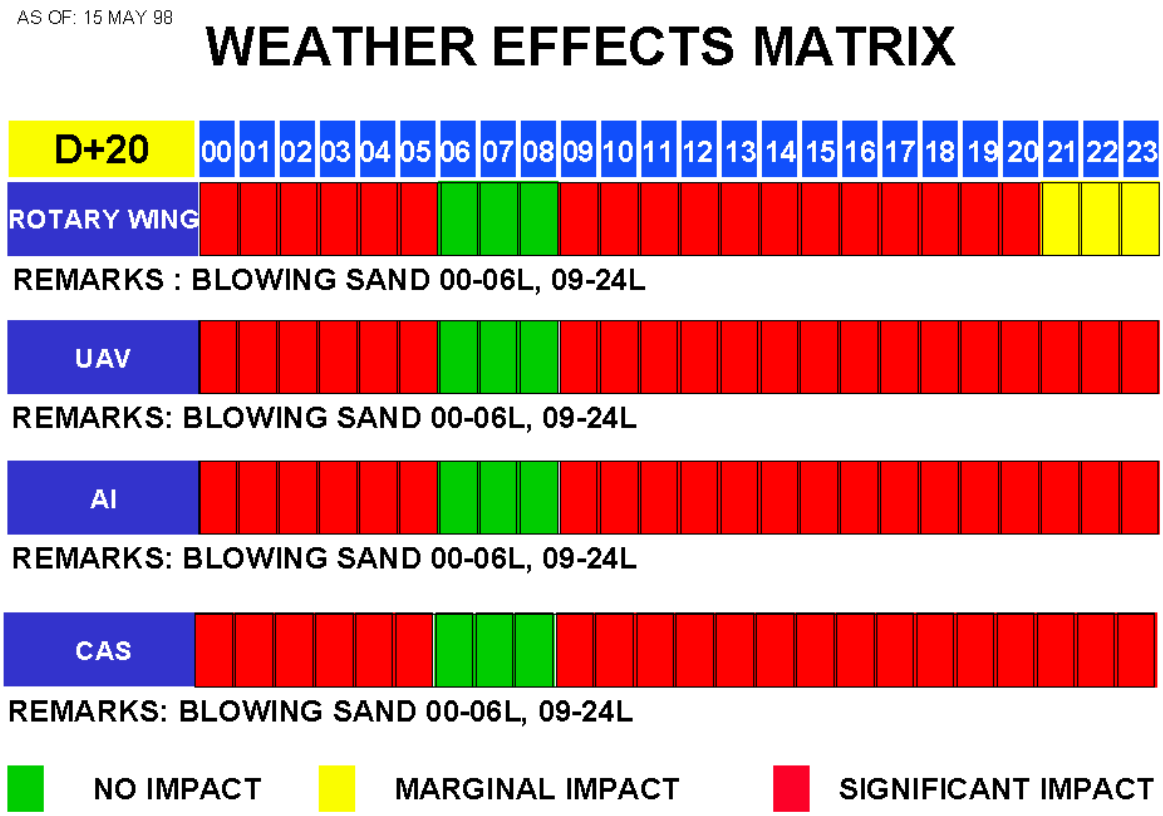

Figure 5-3 Weather Effects Matrix

5005. Infrastructure Characteristics of the Battlespace

a. Overview. The infrastructure of a potential AO is a key element of information, particularly in an expeditionary environment. From points of entry, such as ports and airfields, to transportation systems, economic infrastructure, and social infrastructure, all have an impact on how friendly forces will enter into, move through, and sustain themselves in the AO. Infrastructure also impacts a potential threat's ability to conduct operations to oppose us. The importance of particular facilities will, of course, depend on the units involved and the type of operations envisioned. As with all IPB analysis, the study of a target area's infrastructure must be focused on those factors which are crucial to mission accomplishment. Without such a focus, the intelligence analyst can be quickly overwhelmed with the shear magnitude of the task. Most commands, particularly at the lower tactical levels, do not have the resources to conduct detailed, independent, analysis of infrastructure. Instead, the intelligence staff must be familiar with all sources of infrastructure information that can be rapidly accessed when needed. Infrastructure analysis is performed by theater joint intelligence centers, U.S. Transportation Command, the National Imagery and Mapping Agency, the Defense Intelligence Agency, Service Intelligence Centers such as the National Ground Intelligence Center and the Marine Corps Intelligence Activity, and even non-intelligence organizations such as Marine Corps and Army civil affairs units. Detailed

infrastructure analysis can be resource and time intensive, thus identification of analytical requirements prior to conflict or crisis will help ensure the availability of the information when needed.

One of the primary considerations in planning large-scale operations is the extent and general nature of the transportation network. Planners must consider the entire pattern of transportation facilities. An area with a dense transportation network, for example, is favorable for major offensives. One that is crisscrossed with canals and railroads, but possesses few roads, will limit the use of wheeled vehicles and the maneuver of armor and mechanized infantry. Railroads extending along the axis of advance will assume greater importance than those perpendicular to the axis, and the direction of major highways and waterways assumes equal significance.

b. Transportation System. In preparing intelligence studies, all transportation facilities must be carefully evaluated to determine their effect on the proposed operations. At higher levels of command, each major facility may be the subject of a detailed study by unit intelligence analysts or by external agencies such as theater joint intelligence centers (JIC), TRANSCOM JIC, or the Defense Intelligence Agency.

(1) Highway/Road Network. The term "highway" has a much broader meaning for intelligence purposes than for everyday usage. It includes all types of roads and trails, from multi-lane super highways to ordinary pack trails and footpaths. All associated structures and facilities necessary for movement and for protection of the routes, such as bridges, ferries, snowsheds, tunnels, and fords are considered as integral parts of the highway system. An adequate highway system is a fundamental requirement in the conduct of any major military operation. Military interest in highways of a given area or country covers all physical characteristics of the existing road-track-trail system and the various administrative and operational aspects pertaining to construction and maintenance. Studies should provide information on the existing routes and any major repair or rehabilitation that may be required, as well as information on where new routes will be needed to support a planned operation.

Routes in the combat zone usually need meet only minimum standards, but those in rear areas, especially in the vicinity of water terminals, airfields, and supply installations, must be well surfaced and capable of carrying heavy traffic without excessive maintenance. Operations on a wide front will require a large number of secondary routes in both forward and rear areas. The information presented in a terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation. In addition to the severe abuse given to roads by large volumes of heavy traffic, important bridges, intersections, and narrow defiles are primary targets for enemy interdiction by fires, or unconventional operations. The maintenance of unnecessary routes must be avoided, and the construction of new routes held to a minimum.

(2) Railroad network. The term "railway" includes all fixed property belonging to a line, such as land, permanent way, and facilities necessary for the movement of traffic and protection of the permanent way. It also includes associated bridges, tunnels, snowsheds, galleries, ferries, and other structures. Studies on railroads cover all physical characteristics of the existing system and all available information pertaining to development, construction, and maintenance. The term "physical

characteristics" describes the roadway and all its component parts (roadbed, ballast, track, rails, etc.), its horizontal and vertical alignment, as well as critical features. Information on physical characteristics is necessary for determining capacities and maintenance or rehabilitation requirements of railways.

Railways often constitute the backbone of the transportation system in countries where no complementary road system has been extensively developed. Suitability for mass movement and low susceptibility to weather effects, make them particularly useful for logistics support. Maneuver warfare, with its emphasis on dispersal and the requirement for more and smaller rear installations, also lends importance to secondary and feeder lines. Railways and their associated facilities are highly vulnerable to enemy attack, particularly to sabotage and guerrilla operations. Keeping a railroad in operation requires trained security forces and extensive protective measures.

(3) Port and Harbor Facilities. Information and intelligence on ports, naval bases, and shipyard facilities is essential for estimating their capacities, capabilities, vulnerability, and other items of military significance. Ports are classified on an area rather than worldwide basis, and a principal port in a small maritime nation may be equivalent to a much lesser port in a more extensive port system of another country. In wartime, principal and secondary ports and bases are prime targets for destruction, and the relative importance of minor ports increases.

Only when a harbor has been developed for transacting business between ship and shore does it become part of a port. A port, therefore, normally consists of a harbor plus terminal facilities. Harbors are classified according to location: coastal, bay and estuary, and river harbors. Harbors associated with ports may be natural, improved, or artificial. The great majority of harbors associated with ports are either artificial or improved natural harbors.

(a) Harbor Works. Harbor works, including protective works, are the structures designed to provide shelter, to control water flow, and to regulate erosion for the improvement of the navigability of a harbor. The principal categories and types of structures are breakwaters, jetties, groins, sea walls, bulkheads, dikes, locks, and moles. Harbor works do not include port facilities that are designed specifically for the transfer of cargo and the servicing of ships.

(b) Depths. Depths are an important element in such port topics as harbor, entrance, anchorage, wharves, and dry docks. Depths are computed in terms of established reference planes which are based on, but do not necessarily coincide with, tidal levels. The particular reference plane on which depths on hydrographic charts are based is called chart datum and is defined on the chart. Precise datum are established for most ports and are the basis for soundings. The reference plane should be clearly indicated when depths are reported.

(c) Navigable Fairways. The navigable fairways through the approach and the entrance to the harbor and the harbor itself frequently determine the size of ships that can be accommodated in the port. Any fairway with controlling dimensions that limit the size (draft, length, beam, height above water) of ships that can traverse it should be described in detail. Reports on the experiences of ships with critical dimensions that have entered are most helpful.

(d) Anchorage. Much of the anchorage data can best be shown on large scale charts and plans. All available information of an operational nature should be reported, including anchorage designations and berth assignments by local authorities, normal anchoring practices, and ship experiences.

(4) Airfields. Airfields, whether military or civilian, are closely linked to the nation's transportation system. Airfields are of vital importance during every phase of a military combat situation and the size and features of an airfield determines its combat and reconnaissance capabilities. Geographic studies are concerned with deriving specific information on airfields. Principally, they focus on the type of airfield, its physical dimensions, what the airfield is constructed of, the condition of the field, and the nature of its support facilities.

For the purpose of this publication, the word "airfield" is used in the broadest sense, regardless of the complexity of its supporting facilities. The term is commonly applied to such diverse installations as airbases, airports, airstrips, landing strips, air depots, heliports, helipads, and seaplane stations. An airfield may be serviceable but not occupied. It may be under construction, in partial operation, or in full operation. These factors should be reported when discernible.

(5) Structures and Crossings. Structures and crossings on highways or railways include bridges, culverts, tunnels, galleries, ferries and fords. Also, for the purpose of geographic studies, they include cableways, tramways and other features which may reduce or interrupt the flow of traffic on a transportation route. Bridges and culverts are the structures most frequently encountered; however, any features that may present a potential interdiction is of significance in a military operation. Detailed information on structures and crossings is essential to a battlespace analyst and to an engineer who may be required to repair or restore a structure.

(a) Bridges. Highway and railway bridges and tunnels are vulnerable points on a line of communications. Timely preservation, destruction, or repair of a bridge may be the key to an effective defense or to the successful penetration of an enemy area. A bridge seized intact has great value in offensive operations, since even a small bridge facilitates the movement of forces over a river or stream.

Detailed information, other than length, about bridges cannot be obtained from topographic maps, but measurements from aerial photographs usually permit an approximate determination of the bridge length, width, clearance and height above water. Necessary details concerning a bridge should be obtained from reconnaissance or, if available, from the NIMA produced planning terrain tactical data base (PTTDB). Basic information requirements for a bridge include a summary of its structural characteristics, critical dimensions (length, useable width, overhead clearance), an estimate of capacity, and general conditions.

(b) Tunnels, Galleries, and Snowsheds. Features on a transportation route where it would be relatively easy to block traffic, or that affect the traffic capacity of the road, are

considered to be critical features of the road. Such features include tunnels, snowsheds, galleries, mountain passes, terrain gaps, gorges and defiles, deep cuts, steep grades and sharp curves. Any obstructions to traffic flow which limit the physical dimensions of vehicles utilizing a specific route are important aspects of route studies. Reductions in traveled way widths, such as narrow streets in built up areas, drainage ditches, embankments, and war damage all limit vehicular movement. Underpasses and other covered traveled ways may restrict traffic flow not only as to width but also as to height.

A **tunnel** is an underground section of the route which has been made by cut-and-cover or bored for the passage of a route. It consists of the bore(s), a liner (optional) and portals. Common shapes of tunnel bores are semicircular, elliptical, horseshoe, and square with arched ceiling. Bores may be lined with brick, masonry or concrete or they may be unlined. Some very long tunnels are artificially ventilated by blowers at the portals or in ventilating shafts above the bore. Alignment of tunnels may be straight or curved.

Snowsheds and **Galleries**. Built in rugged, mountainous terrain, these protective structures are not as common as bridges or tunnels. Snowsheds offer protection against snow accumulations as well as drifts and slides on exposed sections of the permanent way. Galleries offer protection against snow and rock avalanches. They may be cut into the side of a cliff and have a natural overhang, or the cover may be a concrete slab, either of which guides the avalanche across the track or road. One side of a gallery is usually open.

Retaining walls are built to support embankments, either on the uphill or downhill side of the roadway. Retaining walls also are necessary where an embankment requires support against the pressure of water.

(c) Ferries. A ferry site is that place where traffic and cargo are conveyed across a river or other water barriers by a vessel called a ferry or ferry boat. Ferry boats or vessels vary widely in physical appearance and capacity depending on the depth, width, and current of the stream, and the characteristics of traffic to be moved. Propulsion of ferries may be by oars, cable and pulleys, poles, stream current (trail and flying ferries), or by steam, gasoline, and diesel engines. Usually, the capacity of a civil ferry boat is expressed in tons and total number of passengers. In addition, it is often assigned a military load classification number. Ferry slips or piers are generally provided on the shore to permit easy loading of passengers, cargo and vehicles. The slips may vary from simple log piers to elaborate terminal buildings. A distinguishing characteristic of a ferry slip is often the floating or adjustable approach ramp which accommodates to variations in ferry deck level. The limiting characteristics of ferry sites includes the width of the water barrier from bank to bank, the distance and time traveled by the ferry boat from one side to the other side, and the depths of the water at each ferry slip. Climatic conditions have a marked effect on ferry operations. Fog and ice substantially reduce the total traffic moving capacity and increase the hazard of the water route. Therefore, data on tide fluctuations, freezing periods, floods, excessive dry spells, and their effects on ferry operation are important considerations. Note that ferry slips are often optimal places for the grounding of displacement landing craft or as exit points for amphibious vehicles.

(d) Fords. A ford is a location in a water barrier (such as a river) where the physical characteristics of the current, bottom, and approaches permit the passage of personnel or vehicles and other equipment under their own propulsion (or assisted) and where their wheels or tracks remain in contact with the bottom. The physical characteristics of a ford include trafficability, approaches, bottom, climatic conditions, current, and low water (or underwater) bridges.

Approaches may be paved with concrete or bituminous surface material but are usually unimproved. The composition of the steam bottom determines its trafficability. In some cases, the natural river bottom of a ford may have been improved to increase load bearing capacity and to reduce the water depth. Improved fords may have gravel or concrete surfacing, layers of sandbags, metal screening or matting, timber or wooden planking. Bottom conditions are determined by checking the stability and composition of the bed. Known and suspected ford sites are key information when assessing the ability of a bridge to be by-passed.

(e) Cableways and Tramways. Cableways, tramways and other facilities of this nature are not usually major factors in a military operation; however, they may be encountered in rugged mountainous regions and beach areas or used as connections between two primary supply routes. Cableways and tramways are always considered obstacles to low flying aircraft.

(6) Inland Waterways. The term inland waterways is applied to the rivers, canals, lakes, and inland seas which are used as avenues of transport. It also includes the inter-coastal waterways, usually running parallel to the coastline of a land mass and sheltered enough to permit the navigation of small vessels. Inland waterways provide an economical form of transportation for bulk supplies, freeing faster modes for shipments of a higher priority. Waterway transport is slow and it is also inflexible since new waterways cannot be constructed during military operations. The depths of rivers and streams used as waterways fluctuate with maximum and minimum rainfall. Streams with fairly direct courses commonly are interrupted by falls and rapids. Streams of low and uniform gradients usually meander and their channels shift constantly, depositing sandbars which are a menace to navigation. Unless ice breaking operations can be conducted, traffic is halted completely during a freezing period. The thaw following a freeze may cause floods. Periods of drought may result in insufficient water for the movement of vessels. The locks, bridges, cuts, dams, and other fixed facilities are vulnerable to enemy action.

c. Utilities. Utilities, services, facilities, and construction resources comprise the essential internal supply systems and installations used to protect and maintain the life of a region or city. Military interest in this field is primarily logistical, although these facilities take on greater importance during urban operations, particularly operations other than war. Although installations, equipment, and services of supply for large concentrations of population can be used by military forces, maximum use of these facilities can be made only if the specific adequacy and quality are known.

(1) Power system/grid. Electricity is essential to the life of modern regions and cities. While other sources of power or light such as gas, coal and water are also used, destruction of electrical

generation and distribution facilities in most cities would bring industrial production and most utilities and services to a halt.

(2) POL facilities. Information on the petroleum and natural gas resources of a nation is significant to any modern military operation. It provides a means for evaluating the capacity of a nation to produce, process and supply fluid or gaseous hydrocarbons for military purposes, and the vulnerability of its economy to attack on its petroleum supply system.

(3) Water. Water is the most extensively used commodity in both urban and rural habitats. Maintaining an adequate supply and controlling the quality of the water are the main functions of an urban water supply system. Data on the adequacy and capacity of a water supply system and the quality of the water is essential for military evaluation of an area.

(4) Telecommunications. Telecommunications refers to all forms of civil and military telecommunications systems, facilities and equipment. It also refers to the related governmental and commercial organizations that regulate and operate the systems. Telecommunications services include telephone, telegraph, teleprinter, facsimile, data transmission, radio broadcast and television.

d. Urban Areas/Population Concentrations

(1) Introduction. The ever-increasing urbanization of the world's population dictates that urban areas will increasingly be the area of operations for both war and operations other than war. Geospatial studies of urban areas are important in the planning of tactical through strategic operations, in targeting, and in planning the logistical support for operations. Knowledge of the characteristics of urban areas is essential to the conduct of civil affairs and in counterintelligence operations. Urban areas are significant as military objectives or targets and as bases of operations. They may be one or a combination of: power centers (political, economic, military); industrial production centers; population centers; transportation centers; service centers (distribution points for fuels, power, water, raw materials, food, manufactured goods); or cultural and scientific centers (seats of thought and learning, and focal points of modern technological developments). Often they will be the focal point for internal ethnic, class, religious, or cultural conflict.

(2) Urban Classification. Urban areas are classified according to size, ranging from small to mega-cities. The classification is generally based on the population size and density, but is also a function of the area encompassed by the city and its immediate suburbs. Cities may also be classified as strategic, secondary, or minor according to their general position in the country's society, economy, and defense establishment. In general, importance in the national economy will be the primary factor; however, location, size, complexity, and specialized function also are significant factors in classifying cities.

An important aspect in the classification of cities is the determination of construction type. Rarely is a city of one type of construction; instead there will be a mixture of everything from shantytowns to

high-rise skyscrapers. The analyst should attempt to determine what the predominant construction type is as well as what percentages of the city are composed of varying types.

(3) Components of Urban Area Intelligence. The complexity of GEOINT studies on urban areas requires its division into several components. Primary factors would include the physical characteristics, building construction type, accessibility, utilities, civil facilities, industrial, military and other important installations. Particularly important are underground facilities such as subways, sewers, underground rivers, utility tunnels, etc. LOS considerations in cities are crucial, thus the urban area must be assessed in three dimensions: ground-level, above ground and below ground. Since urban operations are manpower intensive and generally conducted at very low unit levels, the information required is usually very fine-grained in detail. The MCIA publication *Urban Generic Information Requirements Handbook*, MCIA-1586-005-99, provides a detailed discussion of the components of urban area analysis.

e. Construction Resources

(1) Construction Studies. Studies on construction resources include the data from which estimates can be made concerning a nation's capabilities for the type of construction work comparable to that carried out by the U.S. Army Corps of Engineers. It is also concerned with the problems involved in the construction necessary to support U.S. military operations in a foreign area. It deals with civil works, as well as with construction that is wholly military in nature or that which may influence military construction. Availability of construction materials is key to assessing friendly engineer requirements.

(2) Organizations. To evaluate a nation's construction capabilities, it is necessary to know the general organization of the construction industry and the structure and capability of its major firms or organizations. The size, capital assets, organization, amount of equipment, skill of personnel, experience, and degree of specialization will influence the capability of any construction firm.

5006. Analysis of Political, Economic, and Sociological Factors

The current and historical setting of a country is an important and integral part of intelligence analysis. Most of the analysis effort is expended on armed forces and geographic intelligence, but the factors that can make a difference in many operations, especially operations other than war, involve political, economic, and sociological aspects of the target area.

a. Political Intelligence. Political intelligence begins with an assessment of the internal political dynamics of a country by assessing its leadership, its internal political stability, economic position, labor supply, physical resources, and relative military power. The first consideration is the distribution of political power -- is it a democracy, an oligarchy, a dictatorship, or has political power devolved to multiple interest groups such as tribes, clans or gangs? Consideration must be given to the sources of political power: authority based on a legitimate constitution and the will of the people, political magnetism, skill and competence of the leaders, or brute force. It is particularly important for

western trained analysts to understand non-western political institutions. In other countries, institutions that on the surface are western in nature may in fact operate quite differently. For example, civil and military bureaucracies may not be neutral agents of policy, but may operate almost entirely in their own self interest. Armies may function as political parties or administrators rather than as guardians of the national security. Parliaments may have a developmental or honorary role, rather than a legislative role. The analyst must evaluate the political system as it really operates, not the way it is supposed to operate.

(1) Basic Principles of Government. The starting point of political intelligence is the formal political structure and procedure of a foreign nation. It includes the constitutional and legal system, the legal position of the legislative, judicial and executive branches, and the civil and religious rights of the people. Next comes an assessment of the depth and breadth of national devotion to constitutional and legal procedures.

(2) Governmental Operations. Governments are evaluated to determine their efficiency, integrity, and stability. Marked inefficiency and corruption, especially if this pattern differs substantially from the past, may be an indication of an impending change in government. Continued inefficiency and corruption may indicate popular apathy or a populace unable to effect change. Increased restrictions on the electoral process and on the basic social and political rights of the people may mean the government is growing less sure of its position and ability to survive. Information about how the government actually operates, as opposed to formal structures, and changes in the method of operation give the intelligence user clues about the probable future of a political system.

(3) Foreign Policy. Analysis of a target country's foreign policy addresses the country's public and private stance toward the U.S., foreign policy goals and objectives, regional role, and alliances. Foreign political intelligence is gathered from a variety of sources. Most important is on-the-scene collection by diplomatic and military personnel. Other sources include data from technical collection systems, official statements by foreign governments, the press, public opinion polls, international businessman, and the works of academics.

(4) Political Parties. The aims, programs, degree of popular support, financial backing and the personalities of each political party must be evaluated. Special interest parties, representing labor, religious or ethnic groups, industry, and the like, need to be studied in conjunction with the interest group they represent.

(5) Pressure Groups. With few exceptions, most states have some type of formal or informal pressure groups. Examples include political parties, associations, religious or ethnic organizations, labor unions, even officially illegal organizations (e.g., a banned political party). The analyst must identify these pressure groups and their aims, methods, relative power, sources of support, and leadership. Pressure groups may have international connections, and in some cases may be almost entirely controlled from outside the country.

(6) Electoral Procedures. Elections range from "stage shows" of limited intelligence significance to a means of peaceful, organized, and scheduled revolution. In addition to the parties,

personalities and policies, the intelligence analyst must consider the circumstances surrounding the actual balloting process and, very importantly, changes from the historical norm.

(7) Subversion. In many countries there are clandestine organizations or guerrilla groups whose intention is to overthrow or destroy the existing government. Because of these problems, analysis tends to be biographic and reportorial. Whenever possible, intelligence on subversive movements should include data on the size, character of membership, power base within the society, doctrine or beliefs system, affiliated organizations, key figures, funding, and methods of operation.

(8) Narcotics, Criminal Organizations, and Terrorism. In some countries, criminal organizations are so powerful as to influence, if not dominate, national governments. Analysts need to examine their degree and methods of influence. In some cases they simply influence, but in others they exert their control by forceful means. Most terrorist organizations are small, ephemeral, and not attached to any government. Sometimes, however, they are assisted in some way by external actors or even the government itself.

b. Economic Intelligence. The study of economics involves the production, distribution, and use of wealth -- the material means of satisfying human needs and desires. It analyzes the factors of production and how those factors are used to produce the things that people need and want. Economics focuses not only on production within nations, but also on relations between nations, especially on the competition for the world's scarce resources. That competition has been, and continues to be, a major cause of international conflict. Economic intelligence focuses on the use of natural and human resources, and especially on the functioning of national economies and economic relations between countries. The position of the U.S. as the major world economic power makes it inevitable that nearly all economic developments impinge in some way on our position in international affairs. Conversely, the inability of a nation’s economy to provide basic needs for its population is the catalyst for crisis and internal conflict. Thus the study of foreign economies is an important task of intelligence, for economic potential is one of the best measures of a nation's capabilities or liabilities. Frequently, U.S. or coalition military actions coincide with economic actions such as boycotts and embargoes.

(1) Purposes of Economic Intelligence. First and foremost, economic intelligence is vital to estimating the magnitude of military or other threats to ourselves and our allies. A nation can undertake and carry out only those operations, military or economic, that its economy is able to mount or sustain. In the short run, national strength consists of manpower that can be mobilized and weapons and supplies that have been manufactured or purchased. The extraordinary expense of modern warfare means that anything beyond the briefest of campaigns will require the total economic resources of a nation.

Despite the simplicity of the concept, this task is elusive and difficult. A large nation's economic resources offer a wide range of possible actions. For example, efforts to increase military preparedness do not necessarily foretell military aggression. While it is possible to develop probability estimates

based on key indicators, it would be unwise to think that the analysis of economic information alone will yield completely dependable results.

Economic intelligence is also critical to providing indications and warning of potential crisis or conflict. Economic failure, or its potential, often generates social unrest or disputes with neighboring nations. Many times the resulting instability will require U.S. or other national forces to intervene. Indications of economic instability thus become crucial to effective pre-crisis planning and preparation.

(2) Factors of Economic Potential. The relationship between economic and military power is close. However, we must know more than the size of an economy, we must know what it can produce, what it can purchase, and where it is vulnerable. To this end, analysts must study not only the basic statistical data on the functioning of a nation's economy, but also the mines that produce the minerals and the factories that convert the raw materials into finished products. Especially important are the so-called strategic minerals and advanced technologies that are crucial to the production of high performance military weaponry. Raw materials that lie within a country's borders are always available, and in peacetime raw materials are easily imported. In war, access to raw materials may be blocked by hostile forces. The degree to which a nation's productive capacity can be converted to wartime production is relative to its peacetime economic policies. A free-market economy focused primarily on consumer goods production may be ill adapted to rapid and inexpensive conversion to military production. In the world of high technology however, the relationship between civilian and military production has grown closer. This is not to say that the products demanded by each sector are the same, but rather that the technologies used are similar, and quick conversion to military production is possible.

(3) Sources of Economic Intelligence. In today's global economy, the most comprehensive and reliable sources of economic intelligence will be both print and electronic trade and business publications. These open sources can and should be supplemented with human reporting, foreign broadcasts, defectors, commercial contacts and clandestine sources wherever possible. Because nations and businesses often hide information to limit competition or to prevent the discovery of sensitive military related technologies, the most reliable information may have to be obtained from more traditional intelligence methods such as informed reporting by attaches and officers on the scene.

(4) Narcotics and Terrorism. Tracking profits from narcotics trafficking has been one of the most useful forms of intelligence activity against these organizations. Drugs enter the U.S. via a huge number of routes, but the profits exit by a more limited, and potentially traceable, number of routes. In some cases, narcotics are a country's prime resource and export. Terrorist organizations can also be tracked and studied using information on fund transfers, although the amounts tend to be smaller than those of narcotics traffickers.

c. Sociological Intelligence. The analyst must study the way people organize their day-to-day living, including the study of groups within society, their composition, organization, purposes and habits, and the role of the individual in relation to the wider society and its institutions. It differs from psychology in that it focuses on group behavior while psychology concentrates on individual

behavior. Foreign countries should be viewed as distinctive societies with their own unique social and cultural features, including history, language, values, and perceptions. Group behavior is studied through careful examination of social institutions, social stratification and mobility, religions, folkways (including social codes and taboos), national traditions, and the pace of, and reaction to, change. Of particular importance are the factors that affect social stability, such as the way a society deals with information, influence, and authority. For intelligence purposes, sociological factors are studied under six main headings:

Population--including location, growth rates, age and sex structure, labor force, military manpower, and migration.

Social characteristics--including ethnicity, social stratification, formal and informal organizations, and social mobility.

Public opinion--including perceptions of the government and the international picture.

Education--including educational attainment, expenditures on education, and the relationship between education and other social and political characteristics.

Religion--including the role of religious groups in the national decisionmaking process and conflict between religious groups.

Public welfare and health--including governmental and informal welfare systems, health care delivery, and the general health of the population.

(1) Population, Manpower and Labor. Demographic intelligence, using data derived from censuses and sample surveys, describe the size, distribution, and characteristics of the population, including rate of change. Fortunately, most countries now conduct censuses and publish detailed data. As a result, collection of data presents few problems, though interpretation is still difficult. Numerous unclassified publications examine demographic trends, so the intelligence community does little work in that area. Instead, effort is concentrated on the linkages between population factors and economic, political, military, and social characteristics. The U.S. Census Bureau and the United Nations are prime sources for detailed data on foreign populations.

(2) Characteristics of the People. Most important are those characteristics that contribute to national cohesion or national disintegration. The number and distribution of languages and the prejudices associated with them, the degree of social stratification (closely associated with income distribution studies done by economists), and trends in the composition and size of social groups are examined.

(3) Public Opinion. Key indicators may be found in the expression of attitudes by significant segments of the population on questions of national interest. Expressions of opinion may vary from near unanimity to a nearly uniform scattering of opinion over a wide spectrum. Care should be

taken to sample minority opinion, especially of groups capable of pressuring the government by virtue of a high degree of organization, political or economic power, parliamentary resources, personal contacts, or articulateness.

(4) Education. Concentrate on the general character of education and on the quality of all schools from elementary through graduate and professional schools. Data is collected on education levels among the various components of society, the number of students studying abroad, the extent to which foreign languages are taught, and the subjects taught. Countries with large populations of young, well-educated, but unemployed, people are often the sources of instability, ranging from mass migrations to internal conflict.

(5) Religion. Data is gathered on the size and rate of growth or decline of the various religions in a country, the attitude of religious organizations toward the government, each other and the way the government deals with religious organizations. The relationship between religions, the people they represent, and the government--whether cooperative or confrontational--is an important element in continued stability. In some cases, religious beliefs may be a potentially dangerous friction factor for deployed U.S. personnel, such as has been experienced in the Middle East with fundamentalist Islamic sects. Understanding those friction factors is essential to mission accomplishment and the protection of friendly forces.

(6) Public Welfare. This concerns the health of the population, the health delivery system, the provision of social services, living conditions, social insurance, and social problems that have a bearing on national strength and stability. Specific problems include the extent and significance of divorce, broken homes, slums, drugs, crime, and the way society copes with these problems.

(7) Narcotics and Terrorism. A population's level of tolerance for narcotics and terrorist activities depends on the relations between these organizations and the population as a whole. Narcotics traffickers may be tolerated because of the huge sums of money they pump into the economy. Or, the population may have no choice but to acquiesce because of the traffickers use of force. Terrorists may be accepted and even supported by the local populace if they are perceived to be working for the good of the local people. The intelligence analyst must evaluate these organizations in light of the local context in which they operate.

Chapter 6

THREAT ANALYSIS

6001. Overview

Threat analysis is where intelligence analysts make the greatest impact on plans and operations. Paragraphs 3 through 5 of the **Intelligence Estimate** are the product of a thorough and complete threat analysis utilizing IPB. During step 3 of the IPB process, the threat is evaluated and the information is utilized to derive paragraph 3, **Enemy Military Situation** of the Intelligence Estimate. The threat courses of action, developed and analyzed during Step 4 of the IPB process, focus on determining the threat courses of action which can be utilized to draft paragraph 4, **Capabilities and Analysis** of the Intelligence Estimate. Paragraph 5, **Conclusions and Vulnerabilities** is derived from evaluations made during the entire IPB process. It is here the G2/S2 summarizes the effects of the battlespace environment on friendly and enemy COAs, lists the set of probable threat COAs (in order of probability of adoption) based on enemy capabilities in paragraph 4 of the Intelligence Estimate, and lists the threat's exploitable vulnerabilities. The following chapter will provide a more detailed look at the knowledge essential in conducting threat analysis.

6002. Threat Order of Battle

OOB analysis is an integral part of intelligence analysis at all levels. The analyst must consider OOB intelligence and integrate it with other intelligence pertaining to weather, terrain, planned friendly operations, and other METT-T factors to determine threat capabilities, vulnerabilities, intentions, and courses of action. OOB is the identification, strength, command structure, and disposition of units, personnel, and equipment of any foreign military force. In operations involving irregular force units, auxiliary and insurgent elements are included in OOB databases. Data and intelligence are acquired from many fields outside the scope of OOB, but all intelligence is ultimately related to it. For example, technical intelligence produces intelligence on the capabilities and vulnerabilities of weapons systems. OOB intelligence determines the effect of a weapon's capabilities and characteristics, and how it is employed (tactics) within the threat organization.

a. Order of Battle (OOB) Factors. OOB analysis involves evaluating information on various factors relating to military forces. OOB is normally divided into ten factors as follows: composition, disposition, strength, tactics, training, logistics, combat effectiveness, electronic technical data, command and control warfare data, and miscellaneous data.

(1) Composition. Composition is the identification and organization of units. It applies to specific units or commands as opposed to types of units. Unit identification is the key to OOB intelligence because it leads to the answers to many questions concerning the threat. Unit identification consists of the complete designation of a specific unit by name, number, type, relative size or strength,

and subordination. Through identification, the analyst is able to develop a history of the composition, tactics, training, and combat effectiveness of a threat unit. The identification of a specific unit within an organization alerts the analyst to the possible presence of other units of the same organization. Organization is the physical structure of a unit and the relationship of the various elements within that structure. Knowledge of the organization of a unit or military force aids in developing accurate intelligence on current strength and combat efficiency. Threat capabilities are difficult to assess accurately without knowledge of the current organization.

When considering composition, look at self-sufficiency. Does the unit have everything needed to be a self-contained combat force? Units subordinate to self-sufficient tactical units, although capable of limited independent action, cannot sustain themselves over relatively long periods of time. Subordinate units are seldom employed independently or separately from the basic self-sufficient tactical unit. For example, a new threat battalion is reported to be operating in the AO. Knowing that the threat normally organizes and operates in brigades composed of three to five battalions, and that those battalions are normally not employed independently, it is probable that the remaining elements of the threat brigade are in or near the AO.

(2) Disposition. Disposition consists of the location of threat units and the manner in which these units are tactically or administratively deployed. In addition, disposition includes the recent, current, and projected (or probable) movements of threat units. Location refers to a geographical area or position occupied by a unit or units. Knowledge of the strength and location of a threat force assists in determining the capabilities of the enemy force and its effect upon the accomplishment of the friendly mission.

Tactical deployment is the relative position of units with respect to one another or to the terrain. Tactical formations are designed for executing the various tactical maneuvers and usually are based on doctrine. If this deployment can be predetermined, it may lead to an accurate appraisal of probable threat COAs. The knowledge of how units are arranged in echelon may indicate which units will be employed in supporting and reserve roles. Tactical deployment with respect to terrain is also important.

A study of disposition, with an analysis of the terrain, leads to conclusions concerning threat capabilities, vulnerabilities, and probable COAs (using doctrinal and situational templating). Movement of threat units is part of disposition, as all military forces assume movement formations. Movement is the physical relocation of a unit from one point to another. Patrol activity may be an indication of planned movement but, in itself, is not movement. Movement is significant because it automatically changes the tactical deployment of the threat force. When a threat has moved, is moving, or is planning to move, he may become capable of a number of actions which affect the conduct of the battle and the friendly mission. Such a unit may be moving into an attack position or formation, reinforcing, replacing, or withdrawing. In view of these possibilities, movement of a threat unit becomes important. The analyst must continually monitor threat movements in order to provide correct and detailed intelligence on threat dispositions.

(3) Strength. Strength describes a unit of force in terms of personnel, weapons, and equipment. Information concerning enemy strength provides the commander with an indication of threat capabilities and helps determine the probable COA or options open to threat commanders. A lack of strength or a preponderance of strength has the effect of lowering or raising the estimate of the capabilities of a threat force. Likewise, a marked concentration or buildup of units in an area gives the commander certain indications of threat objectives and probable COA. During peacetime, changes in strength of potential threat forces are important factors which may indicate the threat's intention to wage conflict.

(4) Tactics. Tactics in OOB intelligence include tactical doctrine as well as tactics employed by specific units. Tactical doctrine refers to the threat's accepted principles of organization and employment of forces for the conduct of operations. Tactics on the other hand, describe the manner in which the threat conducts an operation. From a knowledge of tactical doctrine, the analyst knows how the threat may employ his forces under various conditions and in certain type situations or special operations. Conventional threat forces normally can be expected to perform according to certain patterns within the framework of tactical doctrine. There are generally established principles and patterns for the employment of infantry, mechanized, armor, and artillery units in the offense and defense. One again, this factor is an integral part of developing IPB and other intelligence products (such as doctrinal templates).

(5) Training. Individual and unit training can significantly contribute to the combat effectiveness of any military organization. The thoroughness, degree, and quality of individual training received by the recruit, specialist, noncommissioned officer, and officer are major factors in determining the overall efficiency of an armed force. Unit training, normally conducted in seasonal cycles from small unit exercises to large scale maneuvers, is an essential part of the training necessary for a unit to operate at its full potential. Each type or phase of training accomplished by a unit adds to its capabilities and effectiveness. Crew training for weapon systems such as tanks, artillery and aircraft is also an important item; if the crew is not well trained, the effectiveness of that weapon system may be greatly diminished. A key factor in the 1991 Gulf War victory over Iraq was the superior level of individual, crew, and unit training among the coalition forces.

(6) Logistics. Logistics is also closely related to combat effectiveness. The adoption of a COA depends on the ability of the logistical system to support that action. With knowledge of the threat's logistics capabilities, a more accurate evaluation of the threat's capabilities, strength, and combat effectiveness can be made. The location of elements of a unit’s logistical support structure aid in determining the disposition of maneuver formations. Types of logistic information critical for effective intelligence analysis include:

All classes and types of supply

Lines of communication (LOC)

Logistical requirements

Procurement methods

Distribution priorities and procedures

Transportation networks and modes

Installations and terminals

Evacuation and salvage procedures

Maintenance

(7) Combat Effectiveness. Combat effectiveness describes the abilities and fighting qualities of a unit. It is affected by numerous tangible and intangible factors. Combat effectiveness affects the capabilities of all units and may be synthesized by analyzing:

Personnel strength, including estimated losses

Weapons and equipment conditions and amounts

Status of training

Quality of leadership

Length of time a unit has been committed to combat

Efficiency and training of the officer and NCO corps

Past performance and traditions

Commander's personality traits

Morale, esprit, health, discipline, and political reliability (or belief in the cause for which they fight)

Status of technical and logistical support of the unit

Adequacy of military schooling at all levels

Socioethnic characteristics of the people

Geographic area in which committed

For each unit of interest, define the factors to be evaluated, and then evaluate each applicable factor and assign a value. **This assessment is highly subjective; its validity will be determined by the experience and knowledge of the analyst and the scope of all available intelligence.** For example, when evaluating the length of time a unit has been exposed to combat, the following values might be used:

Green: Sporadic to intermittent limited combat (small arms fire, firefights)

Amber: Constant limited combat to sporadic intense combat (artillery barrage, heavy weapons)

Red: Sustained intense combat (deliberate attack/defense)

Where a factor has constituent elements, assign a value to each element and then synthesize an overall value for that factor. After assigning a value to each factor, assign an overall combat effectiveness rating to the unit. Again, this process is highly subjective, and allowances can be made for prioritizing or weighting the individual factors.

Combat effectiveness can be expressed as a color corresponding to the following example definitions. The associated percentages are **not** indicators of T/O&E strength, but are shown to indicate a relative range for each definition.

Green: *Combat Effective (80-100%)*. The unit possesses the required resources to undertake all of the wartime mission for which it is organized or designed. Few, if any, negative factors exist. The unit does not require any compensation for deficiencies.

Amber: *Marginally Combat Effective (60-79%)*. The unit possesses the required resources to undertake most of the wartime missions for which it is organized or designed. Some negative factors are present. The unit would require little, if any, compensation for deficiencies.

Red: *Limited Combat Effectiveness (40-59%)*. The unit possesses the required resources to undertake some, but not all, of the wartime mission for which it is organized or designed. Significant negative factors are present. The unit would require significant compensation for deficiencies.

Black: *Combat Ineffective (<40%)*. The unit is not prepared to undertake its wartime mission. Numerous debilitating negative factors are present.

The values assigned to factors and the definitions of the effectiveness rating may be adjusted as the situation dictates. Those values and definitions should be well understood by personnel using the

information, and should be well marked on summaries or reports disseminated outside the command.

(8) Electronic Order of Battle and Technical Data. EOB and other electronic technical data is required to plan and execute SIGINT, EW, CIS, C2W, and other operations against the threat. This data includes threat communications and non communications (such as radar) equipment parameters, such as emitter type and nomenclature (including encoding equipment), modulation, multiplex capability, pulse duration, pulse repetition, frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. The data also include critical threat C2 nodes such as CPs, air defense operations centers, and communications relay sites. Given sufficient data, it is possible to template threat emitters, which in turn can be used to locate and develop the disposition of forces based on their electronic emission assets. With electronic technical data, a more accurate evaluation of the threat's vulnerabilities to friendly electronic attack (EA) and deception can be determined. Additionally, signals intercept and direction finding (DF) for the production of SIGINT is made easier, as is enhanced support to electronic protection (EP).

(9) Command and Control Warfare (C2W) Data. C2W data includes threat assets and capabilities to conduct electronic warfare, deception operations, psychological operations, and information warfare. Building on the enemy composition, disposition, tactics, strengths, limitations, and electronic technical data and intelligence gathered, analysis of this factor reaches across training, doctrine, and technical expertise to provide the commander with an assessment of the threat’s ability to interfere with the command and control of friendly forces. Of increasing importance is the ability of any enemy to penetrate and disrupt friendly C2 and information systems, or to deceive or jam friendly position locating devices (e.g., the global positioning system). This requires knowledge of a threat's deception capabilities, what physical protection measures can be employed to defeat friendly electronic attack and electronic attack systems, and any capability to monitor battle damage to friendly information warfare systems and capabilities.

(10) Miscellaneous Data. Miscellaneous data includes supporting information needed by an analyst to develop other OOB elements and comprehensive intelligence estimates. Miscellaneous data includes basic intelligence described as "know your enemy". Information under the miscellaneous heading normally includes personalities and biographic data, unit history, uniforms and insignia, vehicle numbers, or other elements deemed important to accomplishment of the mission. For example, personality and biographic data contains information of certain characteristics and attributes which describe individual members of a threat force. A knowledge of personalities is important in identifying units and, in some cases, predicting the COA the unit will take. Personality data, therefore, is valuable because the tactics and combat efficiency of particular units are closely tied to the commander's character, schooling, and personality traits. In MOOTW, this element may include such intangibles as tribal, clan, or ethnic group traits and their effects on the combat capabilities or limitations of the threat force.

b. OOB Analytical Considerations

(1) The OOB factors are not independent of each other -- they are closely related and must be analyzed as a whole. For example, changes in training status, command personality, strength, or any other OOB factors may affect the tactics of a unit at a given time.

(2) The OOB factors form a framework for evaluation of any force, not just conventional military units. For example, when considering composition during a counternarcotics operation, extended family ties of suspected traffickers might be included. In evaluating an insurgent force, the insurgent political structure and its relationship to the military elements would be included. Composition analysis of an indigenous terrorist organization would identify the support infrastructure among the local population. Adapt the framework to the mission at hand, discarding what is not applicable.

(3) Tailor evaluation of the OOB factors to your units needs. For example, an aviation unit's evaluation of composition would focus more heavily on those units that contained air defense assets. Its evaluation of equipment would focus on the vulnerabilities of likely threat targets as well as the technical characteristics of the threat's air defense systems.

(4) A key element in effective OOB analysis is the OOB files. These files, when properly maintained, provide the details which allow the analyst to reach conclusions about the threat's operations, capabilities, and weaknesses. See Chapter 2 for a detailed discussion of OOB files.

6003. Developing a Threat Model

a. Definition. The threat model is a portrayal of how the threat prefers to conduct operations under ideal conditions. Threat models constitute the key output from Step 3, **Evaluate the Threat**, of the IPB process. They are based on the threat's normal or doctrinal organization, equipment, doctrine and tactics which have been identified during OOB analysis. Threat models allow the analyst to piece together information, identify information gaps, speculate and predict, and do problem solving. It is an method to synthesize information into a coherent evaluation of threat intentions and capabilities, and predict courses of action. Threat models consist of three parts:

Doctrinal templates.

Description of preferred tactics and options.

Identification of type HVTs.

b. Doctrinal Templates. Doctrinal templates illustrate the deployment pattern and disposition preferred by the threat's normal tactics when not constrained by the effects of the battlespace. They are usually scaled graphic depiction's of threat dispositions for a particular type of standard operation, such as a battalion movement to contact or an insurgent ambush. Construct doctrinal templates through an analysis of the intelligence data base and an evaluation of the threat's past operations. Determine how the threat normally organizes for combat and how he deploys and employs his maneuver units and

various supporting assets. Look for patterns in task organization of forces, timing, distances, relative locations, groupings, or use of terrain and weather. Generally, forces fight as they train; to radically change tactics and procedures at the commencement of hostilities risks chaos and confusion and has the potential to greatly reduce the combat effectiveness of a fighting force.

(1) Even unconventional operations lend themselves to graphic depiction. For example, an evaluation of intelligence reporting indicates that a particular ethnic or political group organizes protests against a peacekeeping force the same way every time. The mob usually forms at a religious site and is whipped up and spurred on by a member of the armed resistance faction. The crowd then moves toward its objective with large numbers of women and children in the forefront, backed by agitated young men and organizers from the resistance. Stationed on rooftops along the route of march are armed members of the resistance, waiting for an opportune moment to initiate an armed incident that can be favorably exploited in the media. This type of intelligence can be converted into a graphic representation, although not necessarily to a standard map scale.

(2) Doctrinal templates can also portray the threat's normal organization for combat, typical supporting elements available from higher commands, frontages, depths, boundaries, engagement areas, objective depths, and other control measures. Of course, the amount of this detail available will vary from situation to situation, and in some cases may not exist at all. In the latter case, the analyst will need to rely on basic principles of war and tactics to develop an initial doctrinal template.

(3) Doctrinal templates are tailored to the needs of the unit creating them. For example, a division G2 creates templates that differ in scope and detail from that constructed by a battalion S2 or the MEF G2. The ACE will construct doctrinal templates that address threat aviation doctrine such as timing and flight patterns of CAP, IAD employment and tactics, strike package composition, spacing and timing, and so forth. Although doctrinal templates usually address a threat unit or force as a whole, at times there may be utility in focusing on a particular combat asset such as artillery or air defense.

c. Description of Tactics and Options. The threat model should include a description of the threat's preferred tactics. It addresses the operations of the major units or elements portrayed on the template and the activities of the different battlespace functions. It also contains a listing or description of the options available to the threat should the operation fail (branches), or subsequent operations if it succeeds (sequels) .

(1) Even though the threat's preferred tactics can and should be depicted graphically, the threat model also should include a text description or matrix. This allows the template to become more than a snapshot in time of the operation being depicted. It aids in mentally wargaming the operation over its duration during the development of threat courses of action and situation templates (see figure 6-1).

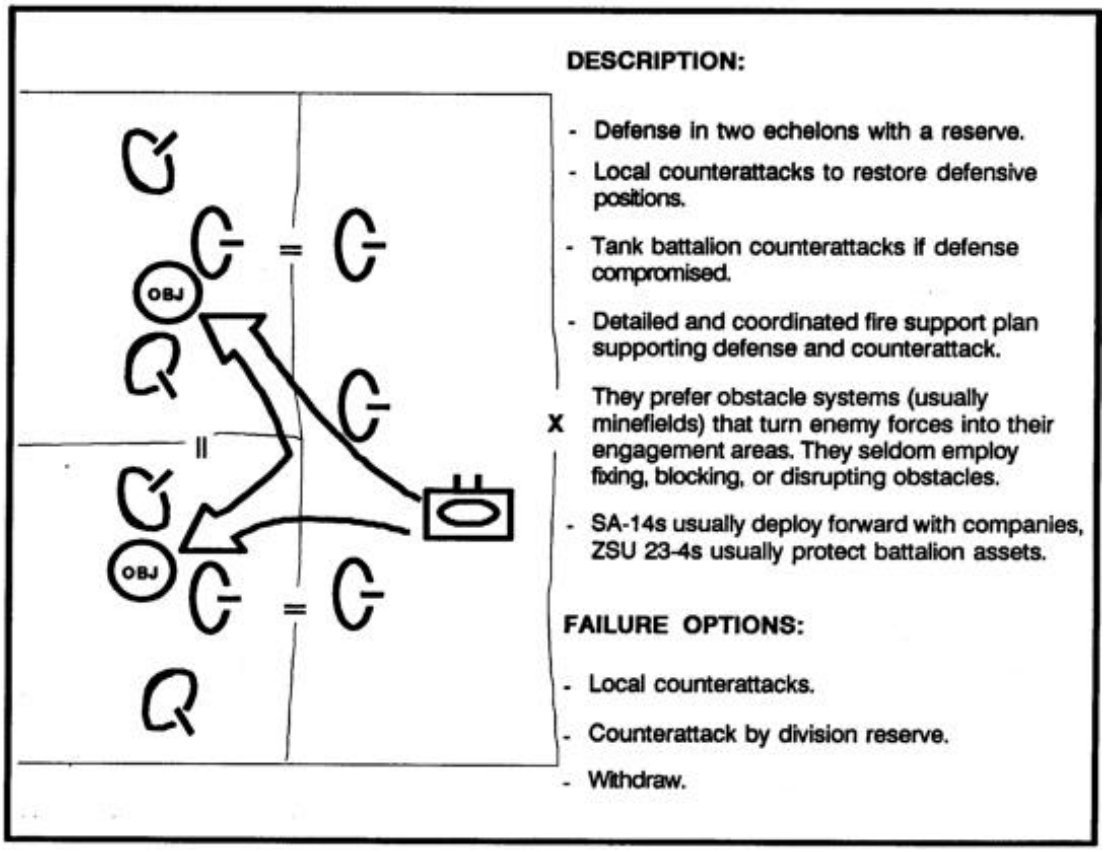

Figure 6-1. Example Using Text or a Matrix to Describe the Conduct of the COA

(2) The description should address typical timelines and phases of the operation (maneuver and support), points where units transition from one formation to another, and how each battlespace function contributes to the operation's success. Describe the actions of supporting battlespace functions in sufficient detail to allow later identification of HVTs and HPTs. Since the target's value usually varies with its role in each phase of the operation, ensure that each phase is examined separately.

(3) Like the template itself, the description of the threat's tactics and options is developed from an evaluation of his doctrine, and previous and current operations. Include a description of the branches and sequels normally available to or preferred by the threat should the depicted operation succeed or fail. For example, The threat might prefer to follow successful attacks with pursuit. Should an attack begin to fail, his preferred branches might include committing reserves, reinforcement, or shifting the main effort. Should the attack fail, his preferred sequel might be a hasty defense.

(4) If the data base reveals any decision criteria that cause the threat to prefer one option over another, include that in the description. This intelligence will aid in wargaming threat and friendly COAs, targeting, and deception planning.

(5) Techniques

(a) Start with the scheme of maneuver, then examine how each battlespace function provides support.

(b) Use time-event charts to describe how the threat normally conducts operations. These are particularly useful for describing large-scale air operations, which are difficult to depict graphically. With a time-event chart the time relationship between various echelons and their normal composition can be described easily.

(c) Marginal notations on the graphic template are an effective technique, combining words with pictures to enhance understanding. Marginal notes are particularly effective when tagged to key events or positions on the template.

(d) For threat's with well developed tactics and complex combined-arms organizations, a battlespace or warfighting function synchronization matrix can be used to dissect threat operations and relate particular actions to time (see figure 6-2).

TIME	H-10	H-1	H	H+4	H+7	H+8.5	H+10
Friendly action	Begin move to attack position	Prep fires	Cross LD	Engage 1st Echelon	Defeat 1st Echelon		
Enemy DP					☆1		
Enemy maneuver				Local CATK	CAS and Atk Helos to CATK OBJ	Reserves begin move	Reserves pass NAI 9
Enemy FS		Counter-battery	Engage HPTs	Defensive fires	Countermobility fires	Support reserve in EA 7, 8, 9	
Enemy Intelligence	Locate main effort	Locate arty, ID main effort	Locate reserve, HPTs				
Enemy C^2					Commit reserve to CATK option 1 or block options 2 and 3		
Enemy Engineers	Continue counter-mobility in MBA				Countermobility support to reserve		

Figure 6-2. Threat Synchronization Matrix

d. Identification of Type High Value Targets (HVTs). Assets that the threat commander requires for the successful completion of the mission depicted and described on the template are HVTs. At this stage, HVTs are *types* or *categories* of targets (air defense, engineer), vice specific targets (SA-13, assault bridging).

(1) Identify HVTs from an evaluation of the data base, the doctrinal template, its supporting narrative, and the use of tactical judgment. HVTs usually (but not always) fall within the non-maneuver battlespace functions. Develop the list of HVTs by mentally wargaming and thinking through the operation under consideration and how the threat will use the assets of each battlespace function to support it. Identify any that are critical to the operations success.

(2) For example, when wargaming a threat force conducting river crossing operations, certain assets such as air defense and engineers/bridging are critical. Likewise, an enemy air attack against friendly targets will require substantial defense suppression assets as part of the strike force. In both cases, the assets identified become HVTs.

(3) Identify assets which are key to executing the primary operation. Also identify any assets which are key to satisfying decision criteria or initial adoption of the branches and sequels listed in the description and option statements.

(4) Determine how the threat might react to the loss of each identified HVT. Consider his ability to substitute other assets as well as the likelihood of adopting branches to the operation.

(5) After identifying the set of HVTs, rank order them with regard to their relative worth to the threat's operation and record them as part of the threat model. An HVT's value usually varies of the course of an operation. Identify any changes in value by phase of the operation and make the necessary annotations.

(6) As key assets are identified, group them into one of the 13 categories used to develop target sets (C2; intelligence, surveillance & reconnaissance; fire support; etc.).

(7) If possible, the identified HVTs for each doctrinal template should be annotated in the margins. One technique is to use a target relative value matrix. Target value matrices give a measure of the relative worth (to the threat commander) of target types, and the resulting effects on the depicted operation (see figure 6-3).

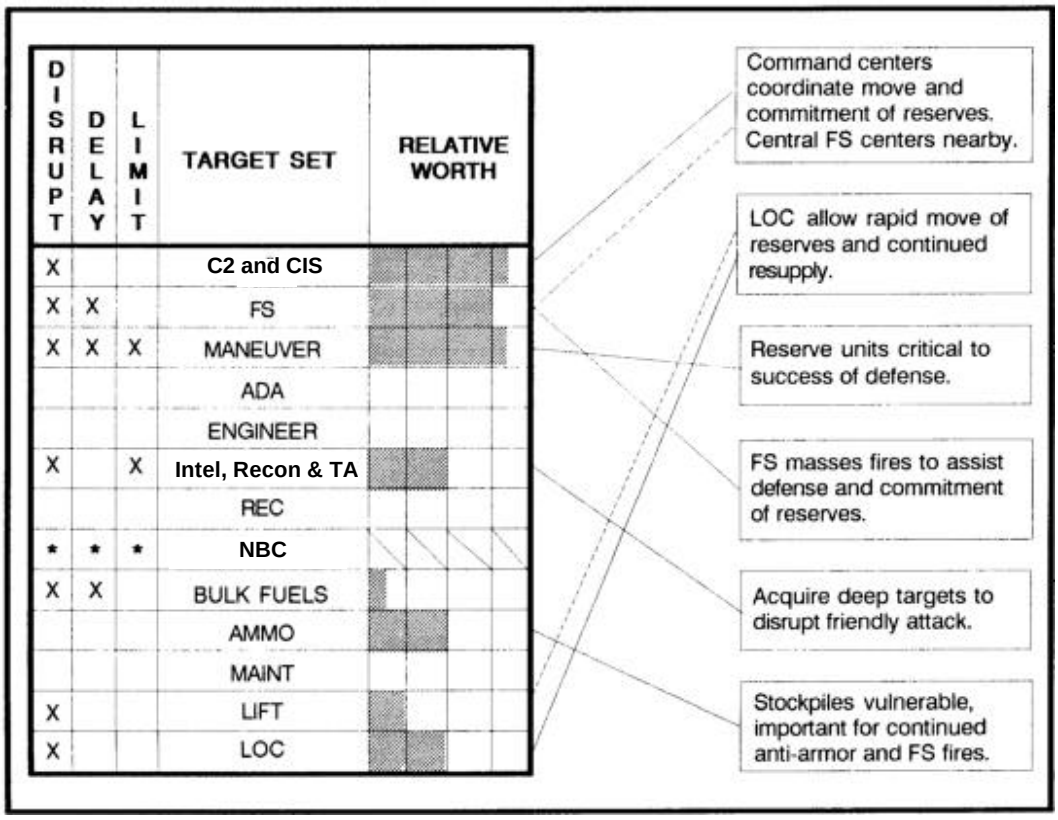

Figure 6-3. Target Value Matrix

6004. Determining Threat Courses of Action

A key responsibility of the intelligence analyst is the identification and development of likely threat COAs that will influence the accomplishment of the friendly mission. This section will deal with identification of threat objectives and how to identify COAs available.

a. Identify Threat Objectives. The analyst should start with the threat command at least one level above your own and identify likely objectives and the desired end state. As likely objectives are identified at each command level, repeat the process for the next subordinate level, working down to at least two levels below your command. Ensure that each level's objective will accomplish the likely objectives and desired end state of its parent commands. Only in rare cases will you have the intelligence needed to state the threat's objectives and intended end state as facts. They will normally be stated as assumptions. All assumptions should be discussed with the commander and remainder of the staff and officially be identified as such. During operations other than war it is important to consider more than the conventional objectives of terrain or friendly forces. This is also true at higher levels of command where the threat's political and economic objectives have a direct influence on his COAs. It is also possible that the threat's intent and objectives may not interfere with the accomplishment of the friendly mission.

b. Identify COAs Available. COAs should be evaluated and analyzed in terms of the threat force's capability to accomplish a mission in relation to time, location, strength, and concept of operations. To ensure that the full set of COAs available to the enemy are considered, the analyst should at least consider:

The COAs the threat's doctrine believes appropriate to the current situation and the likely objectives you have identified. This requires an understanding of the threat's decision making process as well as an appreciation for how he perceives the current situation.

The threat COAs which could significantly influence your command's mission, even if the threat's doctrine considers them infeasible or "sub-optimum" under current conditions. Consider any indirect or "wild card" COAs that the threat is capable of executing.

The threat COAs indicated by recent activities and events. To avoid surprise from an unanticipated COA, consider all possible explanations for the threat's activity in terms of possible COAs.

The analyst should consider each subset of COAs independently to avoid forming biases that restrict the analysis and evaluation. Once each subset has been evaluated separately, combine them to eliminate redundancy and minor variations. Compare the consolidated list to threat capabilities identified in step 3 of the IPB process, **Evaluate the Threat**, and eliminate any COAs which the threat is incapable of executing.

Based on the evaluation of the threat's capabilities (step 3 of the IPB process), select threat models that will accomplish the threat's likely objectives. Examine how the effects of the battlespace (from step 2 of the IPB process, **Describe the Battlespace's Effects**) influence their application as COAs. You will normally find that terrain, weather, and other characteristics of the battlespace environment offer a limited set of COAs, encouraging some while discouraging others.

Start with the general COAs open to the threat, such as deliberate attack, defend, and delay. Further define each general COA as a set of specific COAs by integrating the threat models from step 3 of the IPB process with the description of the battlespace's effects from step 2. Factors to consider include:

The threat's intent or desired end state.

Likely attack or counterattack objectives.

Effects of the battlespace environment on operations and broad COAs.

Threat vulnerabilities or shortages in equipment or personnel.

Current dispositions.

Location of main and supporting efforts.

Threat perception of friendly forces.

Threat efforts to present an ambiguous situation or achieve surprise.

Refine each broad COA statement into a set of specific COAs. For example, a general COA such as a "deliberate attack" might be further defined as a set of specific COAs such as "with main effort in the east... in the west...against the adjacent unit."

c. Criteria for Enemy COAs. Each enemy COA must be tested using the five criteria: suitability, feasibility, acceptability, uniqueness, and consistency with doctrine.

(1) Suitability. A threat COA must have the potential for accomplishing the threat's likely objective or desired end state. If the COA is successfully executed, will it accomplish the threat's objectives?

(2) Feasibility. Consider the time and space required to execute the COA. Are these available? Consider the resources required to execute the COA. Does the threat have the physical means required to make it a success? Occasionally, force ratios or other factors might indicate that the threat lacks the means to accomplish his likely objectives. Before discounting the threat completely, consider all actions he might take to create the conditions needed for success. For example, he might conduct economy of force operations in some sectors in order to generate sufficient combat power for offensive operations in others. His lack of resources might force him to violate his own doctrine in order to accomplish his objective. What seemingly radical measures can he take to create the conditions for success? Avoid surprise.

(3) Acceptability. Consider the amount of risk involved. Will threat forces accept the amount of risk entailed in adopting the COA? Can they afford the expenditure of resources for an uncertain chance at success? This is obviously a subjective judgment based on knowledge of the threat and his doctrine. In some instances, the threat might undertake otherwise unfavorable COAs, particularly if they are the only means to accomplishing his objective.

(4) Uniqueness. Each threat COA must be significantly different from the others. Otherwise, consider it as a variation rather than a distinct COA. Factors to consider in determining if a COA is significantly different are:

Its effect on the friendly mission.

Use of reserves or second echelon.

Location of main effort.

Scheme of maneuver.

Task organization.

This is a subjective judgment based on your experience and training.

(5) Consistency with Doctrine and Recent Activities. Each threat COA must be consistent with the threat's doctrine and recently observed activities, practices and patterns. Base the evaluation of consistency on the threat's written doctrine and observations of his past application of doctrine, as revealed in the intelligence database. Do not, however, overlook threat efforts to achieve surprise by deviating from known doctrine or using "wild card" COAs.

d. Considerations

(1) Account for the effect of friendly dispositions, or the threat's perception of friendly dispositions, when determining the COAs the threat believes are available. A technique for accomplishing this is to conduct "reverse IPB," or replicating the process the threat is employing to discern friendly COAs. This process is very difficult and requires the utmost care given the fact that the analyst is generally far more aware of friendly dispositions and intentions than the threat is or realistically could be. To accomplish this process, the analyst must consider the intelligence and reconnaissance assets available to the threat, their ability to collect information and produce intelligence, and the picture that intelligence will give threat commanders. Reverse IPB is a useful tool for a red cell to employ when preparing for wargaming.

(2) Focus on those COAs that will affect accomplishment of your command's mission. If there are indications that the threat might adopt a COA that favors accomplishment of your command's mission, include it as well. This prepares the commander to take advantage of opportunities that might arise. For example, if the friendly mission is to attack to destroy the threat, threat COAs that would interfere are **defend** (including counterattacks), **reinforce**, and **withdraw**. If the friendly mission is to seize a terrain objective, threat COAs that could interfere are **defend** (including counterattacks), and **reinforce**. Threat withdrawal would favor the accomplishment of this friendly mission and should also be included in the set of COAs *if* there are indications the threat might actually withdraw.

(3) It is possible for the threat to have objectives and choose COAs which will not interfere with success of your command's mission.

(4) Identify the *full* set of COAs available to the threat. History repeatedly demonstrates that those who predict or estimate only one COA are often surprised. Do not overlook the less likely but still viable COAs. Do not risk surprise by failing to take the time to consider all

feasible COAs. Bold and daring threat commanders may attempt actions which possess a high degree of risk, but also could result in decisive success. Identify alternative methods by which the threat can achieve his objective or desired end state. Culture and personality can have a high degree of impact. Also, be cautious to the influence of personal biases or attempting to assess enemy COAs based upon U.S. practices and perspectives. Consider the following that might lead to wild card COAs:

Superior understanding of the political, cultural, or information characteristics of the battlespace.

Ignorance of the military arts and sciences.

Immature decision making.

Uncertainty as to friendly dispositions or intent.

Unexpected objectives or desired end states.

Cultural definitions of defeat and victory.

Willingness to sustain defeat at the tactical or operational level in order to achieve victory at the strategic or political level.

Desperation.

Bureaucratic inefficiency.

Audacity.

In the effort to ensure all COAs are considered, however, care must be exercised that time is not wasted on bogus options.

6005. Evaluate, Prioritize, and Develop the COAs

a. Evaluate and Prioritize each Course of Action. The resulting set of COAs developed should depict the full set of options available to the threat. At this point the analyst should remember that the threat COAs identified are *assumptions* about the threat, *not facts*. Because of this, the analyst cannot predict with complete accuracy which of the COAs the threat will employ. However, the commander and his staff still need to develop a plan that is optimized to one of the COAs, while still allowing for contingency options if the threat chooses another COA. Therefore, the analyst must evaluate, analyze and form an estimate for each COA and prioritize it according to how likely it is that the threat will adopt that option. Establish an initial priority list to allow the staff to plan for friendly COAs. Once the commander selects a friendly COA, the analyst may need to reorder the list of threat COAs. Consider especially any changes in the threat's perception of friendly forces. To prioritize each COA:

Analyze each COA to identify its strengths and weaknesses, centers of gravity, and decisive points.

Evaluate how well each COA meets the criteria of suitability, feasibility, acceptability, and consistency with doctrine.

Evaluate how each COA takes advantage of the battlespace environment. How does the battlespace encourage or discourage selection of each COA?

Compare each COA to the others and determine if the threat is more likely to prefer one over the others. Most forces will choose the COA that offers the greatest advantage while minimizing risk.

Consider the possibility that the threat may choose the second or third best COA while attempting a deception operation portraying acceptance of the best COA.

Analyze the threat's recent activity to determine if there are indications that one COA is already being adopted. Does his current disposition favor one COA over others?

Use judgment to rank the threat's COAs in their likely order of adoption. Modify the list as needed to account for changes in the current situation. For example, the initial priority order of threat COAs does not account for the friendly COA, since one has not yet been selected. Friendly dispositions may change as the command moves to adopt its own COA. How will that change the likelihood of each threat COA? Given time, the analyst could adopt several different versions of the prioritized list of threat COAs in a different order for each potential friendly COA. Alternatively, after the commander has selected the friendly COA, reprioritize the initial list of threat COAs to reflect changed friendly dispositions and activities.

b. Develop Each Course of Action. Once the complete set of threat COAs has been identified, develop each COA into as much detail as the situation requires and time allows. Base the order in which each COA is developed on its probability of adoption and the commander's guidance. To ensure completeness, each COA must answer five questions:

WHAT - the type of operation, such as attack, defend, reinforce or conduct retrograde.

WHEN - the time the action will begin. Usually stated in terms of the earliest time that the threat can adopt the COA under consideration.

WHERE - the sectors, zones, axis of attack, avenues of approach, and objectives that make up the COA.

HOW - the method by which the threat will employ his assets, such as dispositions, location of main effort, the scheme of maneuver, and how it will be supported.

WHY - the objective or end state the threat intends to accomplish.

Consider threat forces available to at least one level of command above your own when developing each COA. This helps to ensure accountability for possible reinforcing forces and the higher command's own objectives and intent. Each developed threat COA should contain three parts: a situation template, a description of the COA and options, and a listing of HVTs.

(1) Situation Template. Situation templates are graphic depictions of expected threat dispositions should he adopt a particular COA. They represent the known/estimated threat doctrine and tactics applied against the realities of the battlespace, threat intentions, and friendly dispositions, capabilities and plans. They usually depict the most critical point in the operation as agreed upon by intelligence and operations. An analyst may prepare several templates to represent different "snapshots in time" starting with the initial array of forces. These are useful in depicting points where the threat may modify their main COA, places where the threat is most vulnerable, or other key points of battle. Situation templates are used to support staff wargaming and develop event templates.

(a) To construct a situation template, begin with the threat model representing the operation under consideration. Overlay the doctrinal template on the products that depict the battlespace environment's effect on operations. This is normally a modified combined obstacle overlay (MCOO), but may vary according to the situation and the unit’s intelligence needs. The analyst should use his judgment and knowledge of the threat's preferred tactics and doctrine as depicted in the threat model and adjust the dispositions portrayed on the doctrinal template to account for the battlespace environment's effects. Many options will be available, but attempt to view the situation from the threat commanders point of view. All the threat's major assets should be accounted for on the situation template. Include as much detail on the situation template as the time and situation allow. Ensure locations and activities of the HVTs listed in the threat model are depicted (see figure 6-4).

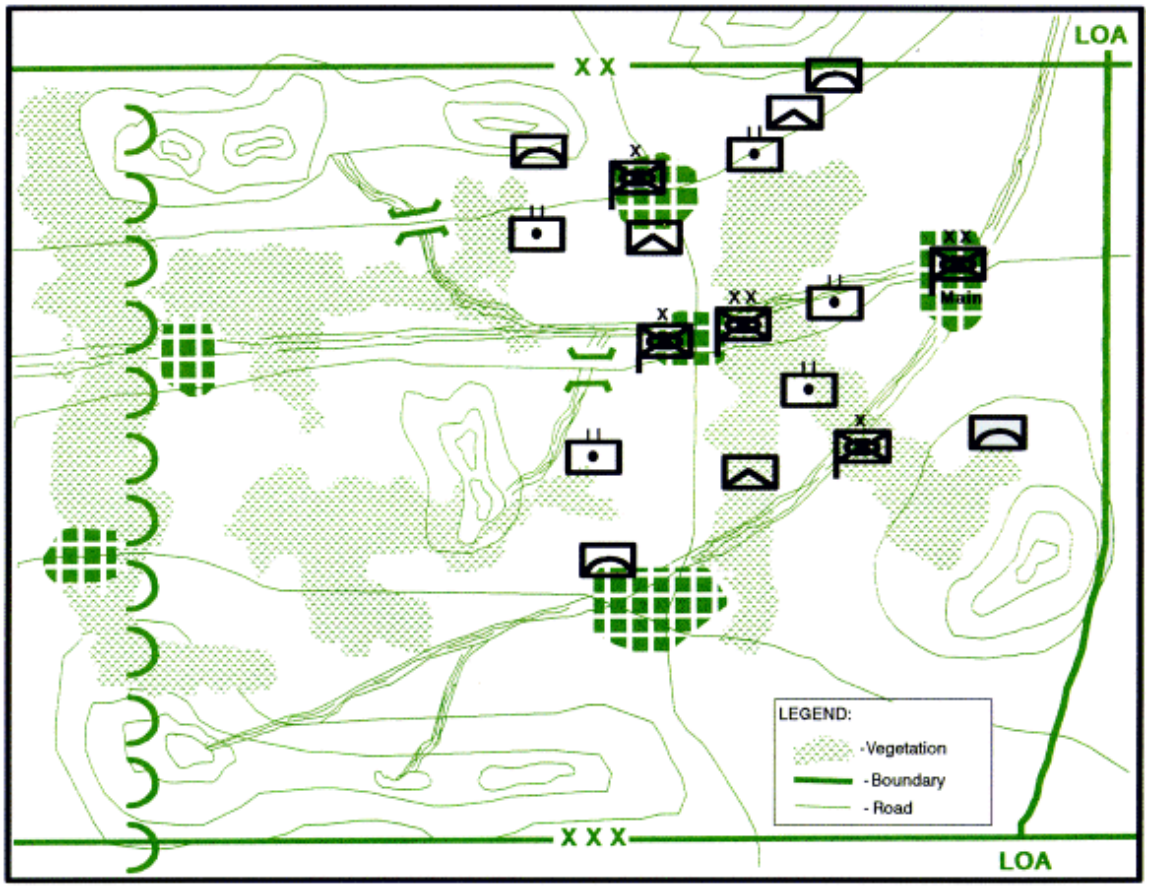

Figure 6-4. Situation Template Emphasizing HVTs

(b) Using the description of the preferred tactics that accompanies the doctrinal template as a guide, think through the COA's scheme of maneuver. Attempt to visualize how the threat will transition from his current positions to those depicted on the template. Mentally wargame the scheme of maneuver from the positions depicted on the template through the COA's success or failure. Identify points where forces will transition from one formation to another, potential assembly areas, decision points, and so forth. After working through the scheme of maneuver, identify how each battlespace function will support it, paying particular attention to HVTs. At higher command levels, a single COA may require a series of snapshots to cover the full COA from start to finish.

(c) Introduce and assess the element of time by developing time phase lines (TPLs). Draw TPLs on the template to depict the expected progress of attacking forces, the movement of reserves or counterattacking forces, and the movement of forces in the deep and rear battle areas. Base TPLs on the threat's doctrinal rates of movement modified by the effects of the battlespace and actual movement rates observed in past operations. When placing TPLs, consider only the time it will take to adopt movement formations, time to conduct movement to the selected location, and time for the unit to close after arrival. In the absence of doctrinal or data base intelligence regarding movement rates, the laws of physics and the friction of war still pertain. If contact with friendly forces is expected,

mentally wargame the effects this will have on the threat's speed as well. At this stage TPLs are only estimates, which can be refined and updated during staff wargaming (see figure 6-5).

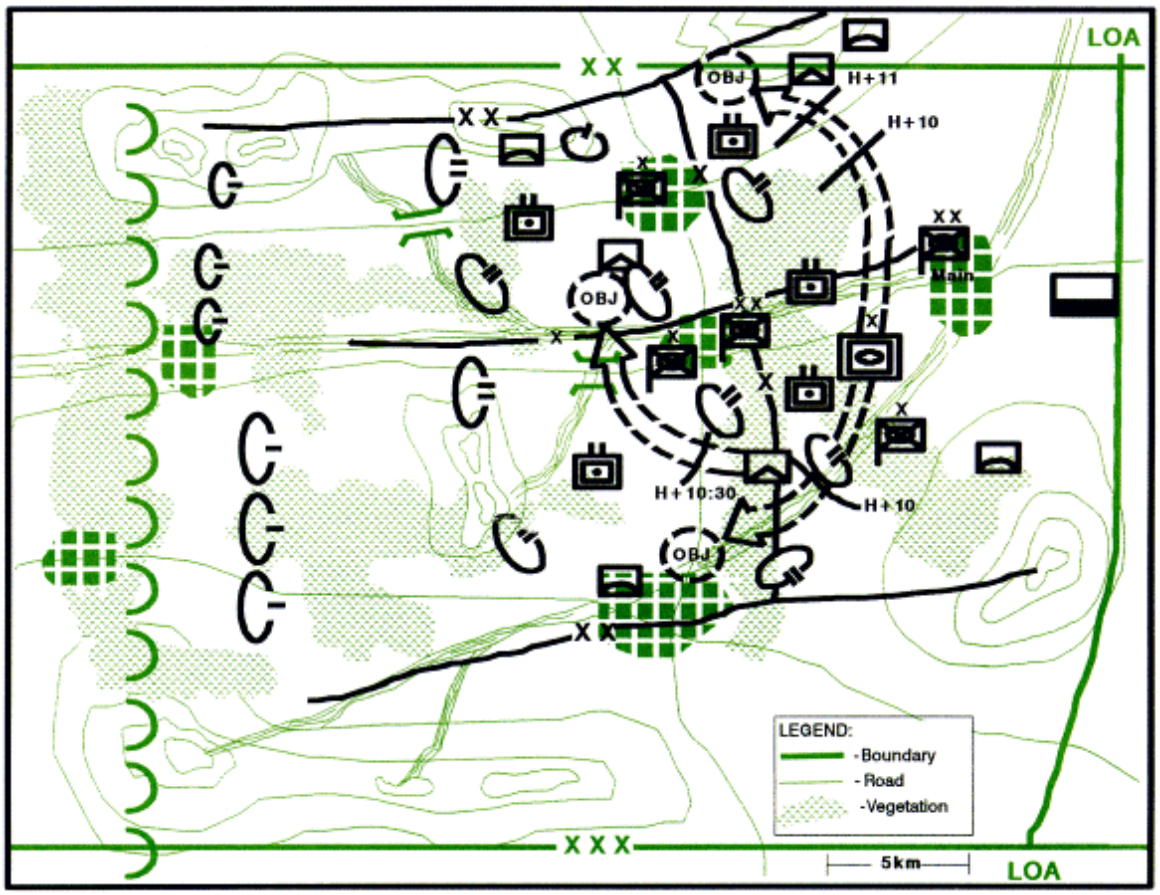

Figure 6-5. Situation Template with HVTs and TPLs

(2) Description of the COA and Options. This is a description of the activities of the forces depicted on the situation template. It can range from a narrative description to a detailed synchronization matrix depicting the activities of each unit or battlespace function in detail. It should address the earliest time the COA can be executed, COG(s) for that COA, timelines, and phases associated with the COA, and decisions the threat commander will make during execution of the COA and after. The analyst uses COA description to support staff wargaming and to develop the event template and supporting indicators.

(a) Start with the description of preferred tactics that accompanies the doctrinal template. As you mentally wargame the situation template, note when the threat is expected to take certain actions or make certain decisions, such as transition to pre-battle formation, deploy reconnaissance, etc. Record each event into the description of the COA. Where possible, tie each event or activity to TPLs or other specific geographic areas on the situation template.

(b) As the threat force approaches decision or option points, record each decision and its timeline into the COA description. The description you develop forms the basis for the development of threat branches or sequels, should they be necessary to support friendly planning. Record any decision criteria associated with each decision point.

(c) Develop the description of the COA in as much detail as time allows and the situation requires. Use whatever tools or techniques best satisfy the needs of the commander and staff. Regardless of the form initially chosen, the COA statement will be refined to greater detail during the staff wargaming or potential friendly COAs.

(3) High Value Targets. As the analyst prepares and wargames the situation template, note how enemy systems provide critical support to the COA. This leads to identification of HVTs. HVTs may themselves be COGs, or they may be assets which if destroyed or neutralized may allow us to engage or defeat a COG. Use the list of HVTs in the threat model as a guide, but do not be limited by it. Determine the effect on the COA of losing each HVT and identify likely responses. The relative worth of each HVT will vary with the specific situation under consideration and over the course of the COA's conduct. Identify the times or phases in the COA when the target is most valuable to the threat commander and make the appropriate notations on the list of HVTs. Transfer the refined and updated list of HVTs to the situation template. The list will support wargaming and the targeting process. Note on the situation template any areas where HVTs must appear or be employed to make the operation succeed. Focus on their locations at the time they are most valuable, or just before. These are potential TAIs and engagement areas. Note each potential TAI in the description of the COA that accompanies the template. During wargaming and the targeting process, those HVT, which if acquired and successfully attacked would significantly contribute to the success of the friendly commander’s mission and objectives, are designated at high-payoff targets or HPTs.

(4) Considerations

(a) When considering an attacking threat, less detail is required. For example, depending on the situation, a friendly battalion might need only to work to a level of detail of threat companies. Considering the possible variations in the threat’s COA based on the details of employment of individual platoons adds a tremendous amount of effort to the process, perhaps for little gain.

(b) When considering a defending threat, a greater level of detail generally is required. For example, an attacking friendly battalion might concern itself with individual crew-served weapons positions given their relative contribution to the threat’s defense.

(c) Operations other than war will generally require a greater level of detail. The situation template may address such things as locations and movements of potential evacuees, displaced persons, or protesters as well as threats such as individual air defense systems and irregular forces. Once again, focus on what is essential to accomplishing the friendly mission.

6006. Key Elements of the COA. The key elements of each COA are indicators, NAIs, and HVTs. These key elements will drive the collection and production efforts in order to determine which COA the threat will actually adopt. The art of identifying initial ICRs and IPRs revolves around predicting specific areas and activities, which, when observed, will reveal which COA the threat has chosen; and then determining the type intelligence products, formats, and who needs the them. The area where the analyst expects key events to occur are designated NAIs. The activities occurring in those NAIs will indicate which COA the threat has adopted.

a. Named Areas of Interest. As a threat force is visualized executing a course of action during situation templating, places where activity must occur if that COA is adopted become apparent. NAI's are points or areas along a mobility corridor where enemy activity, or lack of activity, will confirm or deny a particular enemy course of action. NAIs facilitate intelligence collection, reconnaissance and surveillance, and analysis because:

Attention is focused on areas where the enemy force must appear if the enemy has selected a particular mobility corridor or avenue of approach.

Military significant events can be framed by time and location within the NAI.

Events in one NAI can be compared to events occurring in the NAI of other mobility corridors as the basis for determining enemy intentions.

Events within NAIs can be analyzed for indicators and HVTs against which intelligence and target acquisition resources can be directed.

An NAI can be a specific point, a route, or an area. They can match obvious natural terrain features or arbitrary features, such as TPLs or engagement areas. Make them large enough to encompass activity which serves as the indicator of the threat's COA.

b. Event Template. The differences between NAIs, indicators, and TPLs associated with each COA form the basis of the event template. The event template is a guide for collection planning. It depicts where to collect the information that will indicate which COA the threat has adopted. Compare and contrast the NAIs and indicators associated with each COA against the others and identify their differences. Concentrate on the differences that will provide the most reliable indications of adoption of each unique COA. Mark the selected NAIs on the event template. The initial event template focuses only on identifying which of the predicted COAs the threat has adopted. It can be updated and refined later to support friendly decisions identified during staff wargaming (see figure 6-6)

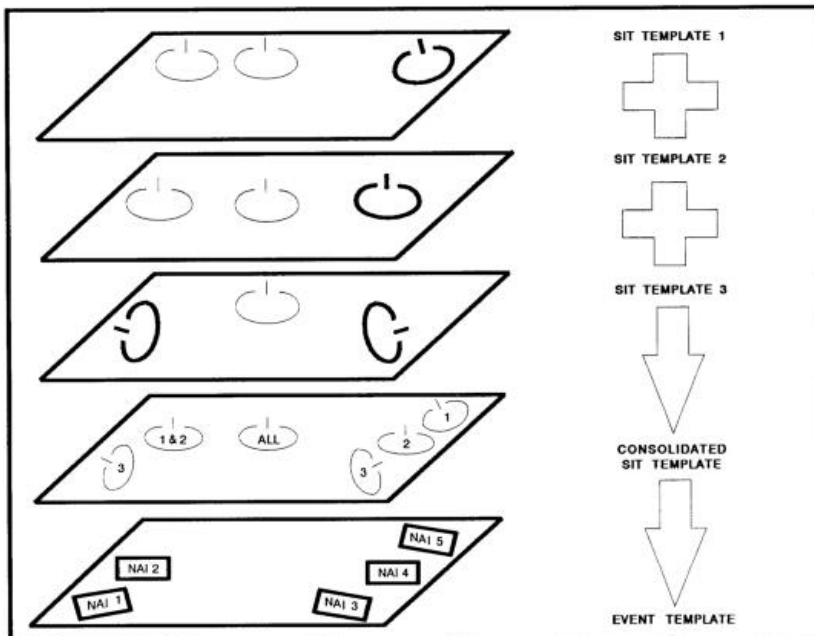

Figure 6-6. Synthesizing the Event Template

c. Event Matrix. The event matrix supports the event template by providing details on the type of activity expected in each NAI, the times the NAI is expected to be active, and its relationship to other events in the battlespace. Its primary purpose is in planning intelligence collection; however, it serves as an aid to situation development as well (see figure 6-7).

NAI No.	NO EARLIER THAN (HOURS)	NO LATER THAN	INDICATOR
NAI 1	H-7	H-2	Engineer preparation of artillery positions
NAI 1	H-2	H-30min	Artillery occupies firing positions
NAI 1	H-1	H-15min	Artillery commences preparatory fires
NAI 2	H-2	H-1.5	Combat recon patrol conducts route recon
NAI 2	H-1.5	H-30min	Rifle company (+) in march formation

Figure 6-7. Event Matrix

Examine the events associated with each NAI on the event template and restate them in the form of indicators. Enter the indicators into the event matrix along with the times they are likely to occur. Use the TPLs from the situation template or the description of the COA to establish the expected times and

the event matrix. If there is a latest-time-information-of-value (LTIOV) timeline based on the estimated flow of events, record it into the event matrix as a guide for intelligence collection, production, current operations and future operations personnel.

Like the event template, the event matrix will be refined during staff wargaming and the targeting process. Additional NAIs may be identified that support timely decisions by the commander, or assist in the tracking of HPTs. While HVTs assess the value of an asset to the enemy commander, HPTs are those targets whose loss to the enemy will significantly contribute to the success of the friendly mission. HPTs will vary from one friendly COA to another and therefore are normally identified during staff wargaming, the targeting process, or by commander's guidance.

6007. Other Analytical Techniques

While IPB provides the overall framework and techniques for analyzing the threat, situations may dictate the use of more specialized techniques to enhance the overall product. Discussed below are a few of the more common techniques used by intelligence analysts.

a. Subsystem Threat Analysis. Subsystem analysis plays a major role in determining the overall posture of a threat force. Most of the products prepared during the IPB process will only partially satisfy the requirements of other staff sections and subordinate units. The targeting process may require focus on a particular aspect of the threat force. The intelligence analyst must be aware of the important threat analysis factors that specialized staff sections and units utilize in their IPB responsibilities. Intelligence analyst will be the focal point for supplying significant information and data on a specific subsystem to other staff sections and units. Intelligence personnel assigned to specialized units will need to tailor their IPB efforts to the needs of their unit.

(1) Air Defense. When air defense units and staffs evaluate the threat, they focus on threats posed by unmanned aerial vehicles (UAVs), missiles (cruise and ballistic), fixed and rotary wing aircraft, and airborne and air assault forces. In addition to the broad range of OOB factors and threat capabilities, air defense staffs and units must evaluate the following:

Flight operations tactics.

Ordnance types and availability.

Ordnance delivery techniques such as standoff ranges, release speeds and altitudes, and guidance systems.

Technical capabilities of aircraft such as all-weather or night capability as well as maximum and minimum speeds, ceilings, range, payloads, and aerial refueling capability.

Target selection priorities for air strikes or attack by air assaults.

Air strike allocation procedures.

C2 and supporting CIS procedures and techniques.

Navigation capabilities.

Threats to friendly ADA assets, including threat ground forces and EW assets.

The threat's air activities will be a part of his overall operation. Therefore, begin determining air COAs by acquiring the supported command's basic IPB products, including situation templates. Evaluate the general COAs they portray and determine how the threat might support them with air power. Do not attempt to determine air COAs in isolation from the maneuver forces they support. The employment flexibility of modern aircraft makes the determination of specific COAs extremely difficult. However, the analyst should consider:

Likely locations of FAARPs.

Likely timing of air strikes or air assault operations.

Likely targets and objectives that the threat would like to destroy or neutralize.

Likely air corridors and air avenues of approach.

Strike package composition, flight profiles, and spacing in time and space, including altitudes.

Where friendly air defense assets fit into the threat COA.

Threat ground COAs that might require movement of friendly ADA assets.

(2) Artillery. When evaluating the threat, the artillery unit or staff should consider the following:

Refine standard threat models to focus on HVTs.

Evaluate the threat's ability to fight the counter-fire battle:

-- Identify target acquisition assets; describe their normal deployment patterns and tactics.

-- Describe the capability of each target acquisition system in terms of accuracy and timeliness.

-- Identify the communications and information systems that moves target acquisition information to decisionmakers or weapons systems and describe in terms of efficiency and timeliness.

Describe the threat's ability to locate and destroy your target acquisition assets.

Utilize techniques associated with the rear battle to evaluate rear area threat to artillery units.

When determining threat courses of action, refine the threat COA models to reflect HVTs, dispositions and activity of threat fire support, dispositions of threat target acquisition assets, and rear area threats to your units. The analyst should focus on COAs that primarily deal with counter-fire against your assets, other aspects of force protection, and threat activities that will require your units to displace.

(3) Aviation. When evaluating the threat, identify the following:

Units supported by ADA assets.

Types of ADA systems and their capabilities such as ranges, altitudes, engagement times, fusing systems, radars, countermeasures, range capabilities, altitude restrictions, etc.

Other threats such as lasers or artillery fire zones.

Artificial illumination effects on target acquisition and night vision devices.

Target characteristics, such as, normal deployment patterns, capability to detect attacking aircraft, typical reactions, and HVTs within each formation.

Refine the higher command's threat COA model.

Include AD system range fans.

Determine where radars and weapons systems are masked by terrain.

Identify areas with least amount of AD coverage.

Identify likely threat air approaches to your engagement areas and battle positions.

Develop situation templates for threat actions within the engagement area and include reactions to aviation attack.

Identify threat units along flight paths considering their reactions and developing appropriate situation templates.

Consider threat reactions to downed pilots.

(4) Counterintelligence. When describing the threat:

Describe the threat decision making process and include descriptions of the threat counterparts to the following:

-- The IPB process.

-- The command estimate or decision making process, particularly wargaming.

-- Techniques for selecting intelligence requirements.

-- Collection planning and collection management.

-- Asset reporting system.

-- Intelligence processing architecture.

-- Dissemination procedures.

Estimate the standard lengths of the threat decision cycle for both anticipated and unanticipated decisions. For example:

-- How long does it take the threat staff to plan and execute an entirely new mission?

-- How long does it take the threat staff to plan and execute changes to the current mission?

-- What is the length of time between acquisition of key indicators by collection assets until execution of that decision?

Identify the collection systems available to each threat unit. Develop doctrinal templates and descriptions for the standard employment of these systems. Rank each collection system in relative order of importance to standard threat operations.

When determining threat COAs, the analyst should:

Use the basic maneuver COA model as a start point to determine threat intelligence requirements. What does he need to know to make the operations successful? Where are the decision points? When does he need to know?

Estimate the threat's intelligence requirements and attempt to recreate his version of the event template and matrix (NAI's and indicators), and his collection plan. (Which threat collection

asset will collect against what NAI or indicator?)

Develop products that show the employment of each collection system and the ensuing coverage.

-- Depict range fans for each system.

-- Describe the type of activity that can be collected against within each range fan.

-- Highlight the strengths and weaknesses of the overall threat collection plan.

Develop a friendly event template to support counterintelligence and counter-reconnaissance. Identify locations (NAIs) and activities (indicators) that will confirm or deny key elements of the assumptions you have made about the threat collection effort.

(5) Command and Control Warfare. Threat analysis in support of C2W can be divided into two areas: threat capabilities to conduct C2W, and threat vulnerabilities to C2W.

(a) When evaluating threat C2W capabilities, the analyst should consider the following:

Ability to locate and intercept our C2 centers and agencies and supporting CIS.

Targeting speed and accuracies of threat intelligence collection systems and capabilities of its production elements.

EA effectiveness (equipment and techniques), to include capabilities against space-based systems and computer networks.

Ability to link collection systems to indirect fire systems.

Range capabilities of supporting indirect fire systems.

Ability to conduct deep strikes or SOF operations.

Threat deception doctrine, tactics, techniques, procedures, and effectiveness.

Threat psychological operations capabilities and effectiveness.

Threat models which include: deployment patterns and tactics of SIGINT collection systems and EA assets; deployment patterns, tactics, and range capabilities of long range indirect fire systems; and techniques of intrusion or electronic deception.

(b) When evaluating threat vulnerabilities to C2W, consider the following:

Threat C2 structure and CIS, with emphasis on locating key C2 nodes.

Threat decisionmaking process and speed.

Command personalities.

Threat intelligence, reconnaissance, and target acquisition assets and their vulnerability to jamming or deception.

Threat COMSEC procedures and ability to work through or around electronic attack.

Threat counterintelligence effectiveness.

Threat OPSEC procedures and effectiveness.

Effectiveness of threat electronic protect measures and computer network protection

Susceptibility of threat forces or population to psychological operations and the threat's ability to conduct counter-psychological operations.

(c) When developing threat COAs, consider threat C2W capabilities and how they will be used to support specific operations. The threat C3 posture and associated vulnerabilities are considered during the identification of COGs and HVTs, and contribute to development of HPTs and targeting strategies.

(6) Engineer. Threat analysis in support of engineer planning should evaluate the following:

Organization, equipment, and standard operations of threat engineer units and their capability to conduct types of operations such as, mobility, countermobility, survivability, obstacle placement, and breaching.

Capabilities of engineer units measured in the time required to lay each type of obstacle system, breach obstacles, entrench a type unit, and bridge different size rivers and streams.

Tactics that threat engineers employ while conducting each of the above operations.

Ability of the threat's logistical system to sustain engineer operations.

Capabilities of threat weapons to penetrate friendly survivability measures and systems.

Information on survivability techniques. For example, threat use of chain link fence to defeat antitank rounds and missiles.

Engineer capabilities of threat infantry, armor, and other non-engineer units.

Engineering considerations should be a factor in all threat models and in every type of template when determining threat COAs. In order to develop situation templates for engineers, utilize the maneuver situation template of the supported unit and develop multiple engineer COAs that include:

An estimate of the engineer status of each threat COA for the defense measured in the percentage of combat vehicles with entrenched primary, alternate, supplementary, and deception positions; and likely extent of obstacle system.

Likely locations and extent of obstacle systems required to support each defensive system categorized by effect (disrupt, turn, fix, or block).

An estimate of the mobility support for each threat COA for the offense. This should be measured in the breaching and fording capabilities for both the maneuver and the supporting engineer detachments.

(7) Combat Service Support. Threat analysis and models in support of CSS staffs and units should include the following:

Regular threat formations, particularly reserves or second echelon units that might penetrate main defenses or conduct counterattacks through CSS areas.

Details on air assault, airborne, UW, and light infantry forces and their means of infiltration - air, ground, and sea.

Insurgent and partisan forces.

Terrorist organizations.

Criminal organizations.

Threat models include:

-- Air assault, airborne, and light infantry techniques for deep attack.

-- UW techniques for deep operations.

-- Standard procedures for insurgent raids and ambushes.

-- Typical procedures for terrorist attacks.

-- Targets and methods of operations for criminal organizations.

When looking at the threat COAs, the analyst should consider each maneuver COA available to the threat and develop multiple CSS COAs that include the following:

Likely areas of penetration for ground forces.

Likely objectives in the rear area that will facilitate the threat main attack or defense.

The HVTs and HPTs that the threat will identify to support their concepts of operations (key terrain or specified CSS activities).

Situation templates for air assault and airborne operations (air avenues to LZs/DZs, infiltration lanes, exfiltration lanes).

Insurgent or partisan COAs (assembly and hide areas, infiltration routes, actions on the objective and exfiltration).

Terrorist and sabotage COAs.

b. Pattern Analysis. When faced by an opponent whose doctrine is unknown or undeveloped the intelligence analyst must create or update threat models and doctrinal templates. This is particularly true in operations other than war, such as counterinsurgency, peacekeeping or even humanitarian assistance operations, where the threat is often ill-defined and unconventional. Pattern analysis is the process of deducing the doctrinal principals and techniques, tactics, and procedures that threat forces or groups prefer to employ by careful observation and evaluation of their activities. The following tools have application for all types of operations where it is necessary to determine threat operational patterns and develop threat models.

(1) Coordinates Register. A coordinates register, sometimes referred to as an incident map, illustrates cumulative events that have occurred within the AO. Coordinates registers focus on the "where" of an event and can contain additional information as the situation dictates. Much like a situation map, the date and time of the incident is recorded next to the location. As reports of individual events or sightings are recorded, the analyst attempts to identify linkages between those events in location and time. Thus, what may appear to be random events will often develop into coordinated actions. Over time, patterns will develop, which when timelined and illustrated will provide the basis for developing threat models and doctrinal templates. Although the time of the event is normally recorded on the coordinates register, it should always be used in conjunction with the pattern

analysis plot sheet and, if already developed, doctrinal templates depicting how the threat conducts operations. Figure 6-8 provides one example of a coordinates register.

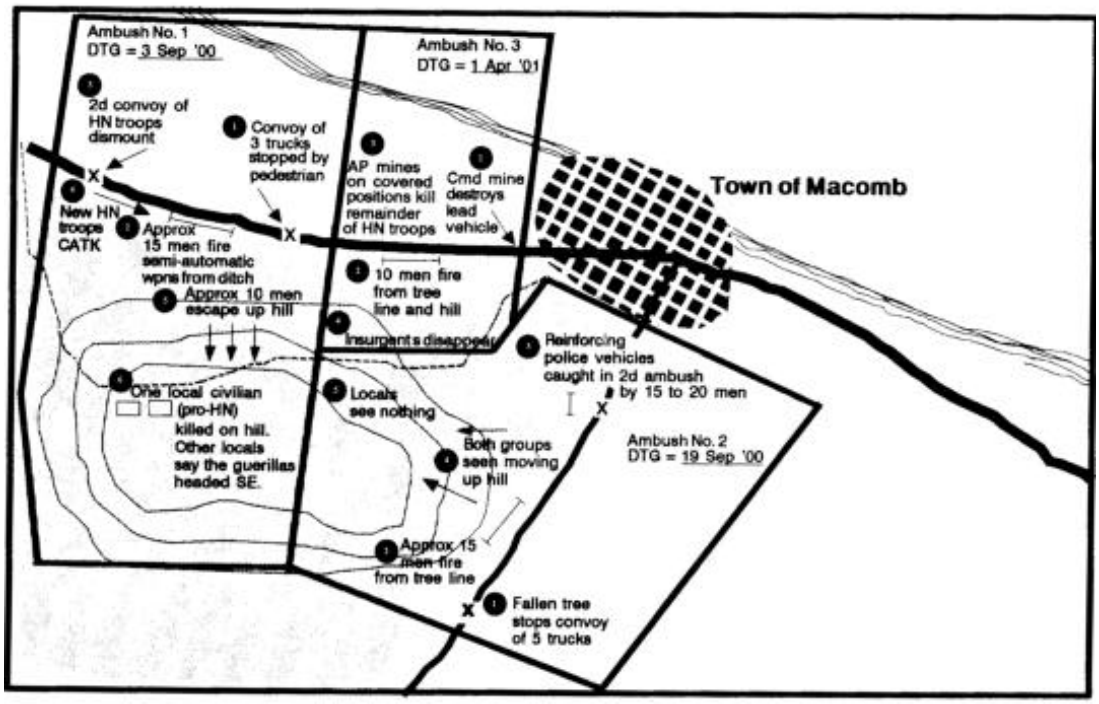

Figure 6-8. Coordinates Register

(2) Pattern Analysis Plot Sheet. The pattern analysis plot sheet is used to focus on the "time" and "date" of each incident that takes place in the AO (see figure 6-9). In the example, the rings depict the days of the month and the radial segments depict the hours of the day. Events are recorded using the same alphanumeric designator as was used on the coordinates register to allow easy cross-referencing. Along the right side of the plot sheet is another way of organizing the data. Here, the events are recorded by the day and date they occurred. By organizing the events in this manner, it is possible to identify if there are particular times of the day, and days of the week or month where threat activities occur. Used in conjunction with the coordinates register, it then becomes possible to identify where, when and how past actions have occurred. This in turn allows the analyst to develop threat models, doctrinal templates and predictions of potential threat activity in both location and time.

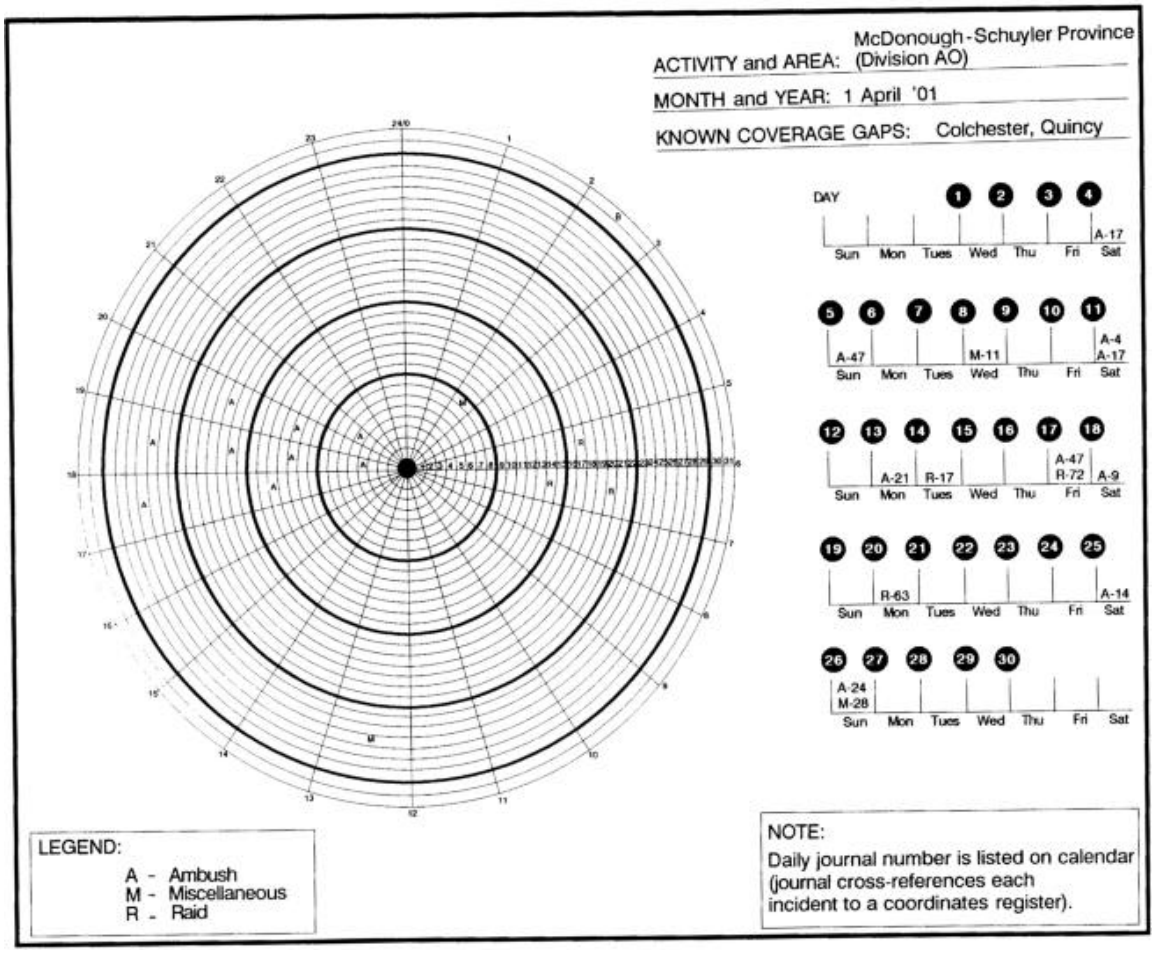

Figure 6-9. Pattern Analysis Plot Sheet

c. Matrix Analysis. Constructing a matrix is a simple, graphical way to show relationships between any number of entities. The entities can be anything important to an analyst--people, incidents, organizations, weapons, locations, or even functions and actions. Matrices are particularly useful when trying to organize a large volume of complex data, particularly in cases where the tracking of individuals and organizations is the emphasis. The two most common uses of matrices by intelligence analysts are activities matrices (people-to-events or organizations) and association matrices (people-to-people).

(1) Activities Matrix. An activities matrix can quickly display which notable personnel within the AO are related to a particular organization or type of activity. It can also be used to link certain activities or incidents within the AO with organizations or units (see figure 6-10).

LEGEND:
● - Confirmed ◍ - Probable
○ - Possible

	Remarks	Christian Reform Party (good guys)	Society for the preservation of order (right wingers)	Farmer's alliance (unk peasant group)	People's Democratic Society (peaceful moderate)	Insurgent Company	New Liberation Movement (political front for N.M.E.)	N.M.E.	Name of Individual	
Warrant outstanding	Leader in the insurgent co. Possible plt cdr or co cdr.					●	●	●	Johnston, S.D. alias "The Red"	Bardolph
	Possibly linked to death squad activities.	●	◍						Garra, N.A.	
	Mayor, ineffective due to war-torn town.	●							Mulvihill, P.	
	Possible plt leader.	○		●	◍	○	○		Daniels, P.	
	Regional governor.	◍	○	◍	●				Jenkins, T.L.	
Warrant outstanding	Tactical genius, principal trainer of insurgent co.					●	●	◍	Cormier, J.	Macomb
				○		◍	◍	◍	Webb, C.	
					◍	○	○		Seipel, B.	
	Leader in the insurgent co. Plt leader or XO.			○		◍	◍	◍	Trollinger, L.	Beardstown
	Possible head of intelligence.					○	●	●	Ahearn, E.	
	Probable plt leader.					◍	○		Timoney, J.	
Warrant						●	●		Thompson, J.	
Warrant	Probable hvy wpn plt leader.					●	○	●	Bridgeford, R.	
	Possible liaison between insurgent co and the N.M.E.			◍	○	○		○	Halbleib, M.	Bushnell
	"Doctor of Death" leads the SPO.	●	●	○	○				Mueller, H.	
Warrant						●	◍	◍	Martinez, E.	

Figure 6-10. Activities Matrix

In the example, individuals are listed down one side, with organizations listed across the top. As relationships are revealed by reporting or analysis, they are noted where that individual's row intersects the appropriate organization's column. Since reporting is sometimes scarce or ambiguous, the example demonstrates the use of color-coded dots to signify the certainty of the relationship (confirmed, possible, probable). The absence of a dot can indicate no relationship or simply a lack of information. Whatever system is used, it should as always be explained in a legend. To complete this particular example, the analyst has created a remarks column to record significant information regarding each individual. Matrices should be constructed to allow easy assimilation of the data and to answer key questions.

(2) Association Matrix. Similar to the activities matrix, the association matrix is used to show relationships between individuals (see figure 6-11).

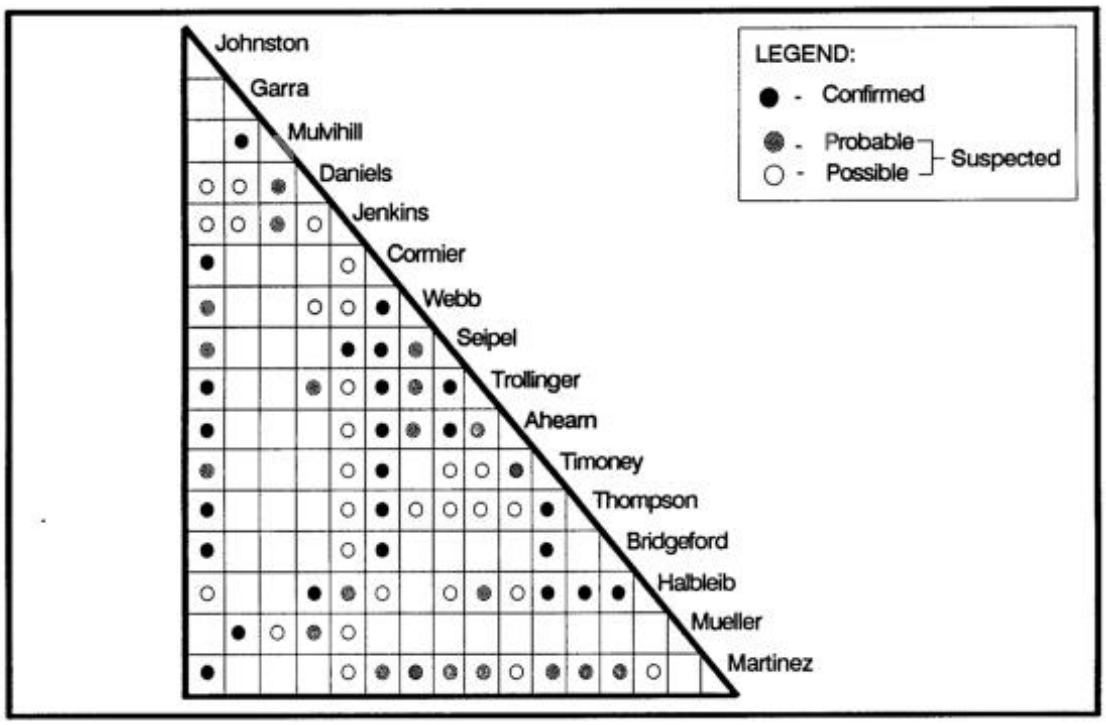

Figure 6-11. Association Matrix

In the example, the individual names constitute both a column and a row. A dot indicates that some sort of relationship exists, with the certainty of the information regarding that relationship indicated by the color. The association matrix often flows from the activities matrix. For instance, if two individuals are members of the same organization, although there may be no outward reporting or indication of a relationship, it is possible that the two individuals do know and interact with each other. Both the activities and association matrices are particularly useful in analyzing insurgent, terrorist, criminal or drug trafficking activity.

d. Link Analysis. Link analysis is an important method for displaying information and conducting analysis of relationships and activities that have been organized into matrices. In link analysis, pictures or symbols are used to display intelligence data and have the primary goal of depicting relationships between people or entities in graphic form. It is vital for the analyst to understand that a completed link diagram is *not* the end result of an analytical assignment but, rather, a stepping stone somewhere in the middle of the analytical process. The greatest value of this method is as a tool--in the process of constructing a link network and diagramming, the analyst is prompted to assess reliability and validity, gauge the nature of a relationship between individuals or entities, and like assembling the pieces of a jigsaw puzzle, will have a greater insight into the overall construction of a network from working with the pieces.

The difference between matrix analysis and link analysis is like that between a mileage chart and a road map. The mileage chart (matrix) shows the distance between two cities numerically. The map uses symbols that represent cities, locations, and roads to show how two or more cities are linked to each other. Different symbols on the map have different meanings, and it is easy to display or discover the best route between two places as well as identify obstacles that separate locations. In link analysis different symbols are used to identify different entities. Confirmed connection, and suspected connection, can be displayed easily and clearly. In many cases, the pictures are easier to follow and work with than are the matrices. Information is presented in a way that maximizes clarity and understanding. Matrices and link diagrams should always be used to support one another rather than as alternatives (see figure 6-12).

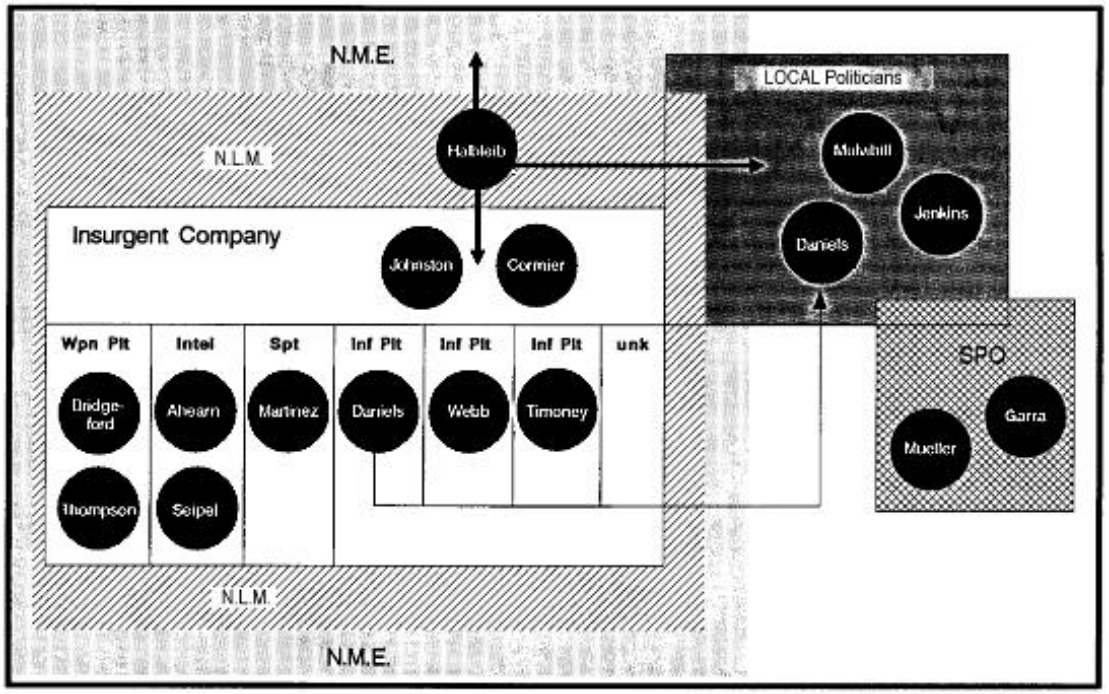

Figure 6-12. Link Diagram

As in the example, link analysis uses circles to represent people, squares to represent organizations, and lines to represent connections. Solid lines represent confirmed or strong relationships, while dashed lines indicate suspected or weak ones. In cases where references are made to two people that the analyst suspects are actually the same person, the circles are overlapped. Circles and lines should be arranged so that no lines cross. In complex cases, such as large groups, where line intersections are unavoidable, the circles should be arranged to keep the number of intersections to a minimum.

The relationship of an individual to an organization can be shown a number of ways. In cases where the individual is confirmed to belong to an organization, their circle is placed within that organization's rectangle. An individual who belongs to two organizations can be shown by overlapping the organizational rectangles around the circle representing the individual.

By overlapping organizations, the analyst is not only showing that an individual belongs to more than one organization, but also that there is a connection between the two organizations that the individual belongs to. In cases where individuals are connected to an organization, but not a member, two rules apply. First, if the individual has contacts with a cell, but the contact point is unknown, a line is drawn from the individual outside the organization to the rectangle representing the organization. If a confirmed contact in the cell has been identified, then the line would be drawn between the circles representing the individuals.

e. Indicators. As previously discussed, indicators are essential to discerning threat intentions. During IPB they are developed for each NAI to focus collection and analysis on what is important in the mass of data that is received. They are constructed to satisfy the PIR and IRs of the commander and staff. The analyst uses indicators to cross reference specific events and activities with probable threat COAs and intentions. When used with other analytical tools such as threat models, event templates, pattern analysis, matrices and link diagrams, indicators are the key to estimative intelligence.

A process that can be used to help the intelligence analyst determine a list of indicators, is the use of METT-T. METT-T serves to focus questions regarding what the threat must do and defines ambiguous and unambiguous activities. Together, "the must do and the threat's activities" become indications and warning. Figure 6-13 depicts a commander's PIR and how METT-T can focus an analyst's questions to form an indicator list.

Example:

PIR: Will the threat defend OBJ C using a reverse-slope defense between 230600 to 270800 hours?

Mission: What does the threat commander accomplish by forming a reverse-slope defense?
Enemy: What type of units are available to conduct the defense. What units are necessary to construct and aid in the defense?
Troops: Are threat troops experienced in reverse-slope techniques? What is their SOP for reverse-slope defense?
Terrain/Weather: Is OBJ C suitable terrain for a reverse-slope defense? If so, where specifically is the terrain most suited?
Time: How long will it take to develop a prepared defense versus a hasty defense? Will threat forces have long enough time to prepare or assume a defense in the specified time

Figure 6-13. Analyzing a PIR using METT-T

To further develop the indicator list, analysts can refine the questions developed using METT-T by further breaking them down by battlespace functions. Information based on IPB, OOB factors, and experience aids intelligence analysts in deriving lists of activities which, in turn, answer the commander's PIR. Indications lists are formed by asking questions. These questions serve to narrow and focus on certain activities, equipment, troops, and training which an adversary must possess or do to accomplish their mission. For a representative listing of common tactical level indicators, see appendix E.

Chapter 7

TARGET DEVELOPMENT AND BDA

7001. Overview

Targeting is the process to detect, select, and prioritize targets, match the appropriate action, and assess the resulting effects based on the commander's objectives, guidance and intent. An efficient, organized targeting effort is critical to the success of MAGTF operations. Attacking high pay-off targets (HPTs) that the threat can least afford to lose strips the enemy of the initiative, degrades his ability to prosecute combat operations, and forces him to conform to friendly battle plans.

Targeting is a complex effort which requires coordinated interaction among different elements of the MAGTF, JFC, service components, and supporting agencies. Large numbers of intelligence, reconnaissance and other sensors under the control of different MAGTF, service component and JTF agencies must be closely coordinated to rapidly and efficiently report fast moving or dangerous targets. The wide variety of attack means and munitions must be compared to the particular vulnerabilities and defenses of many different types of targets. Targeting is a multi-disciplinary effort, requiring interaction between intelligence, maneuver, fires, , and planning elements.

The object of targeting is to effect those enemy capabilities which could interfere with achievement of the friendly mission and objectives. Targeting is based on the friendly scheme of maneuver and tactical plans. It includes an assessment of the weather, terrain, and enemy to identify those enemy formations, equipment, facilities, and terrain which when attacked or controlled will ensure success. Targeting is an integral part of the planning process which begins with receipt of the mission and continues through the development of the approved plan. The targeting process includes the development of a prioritized list specifying what targets are to be attacked, and what effect is required.

This chapter will introduce the targeting cycle, the overall role of intelligence support to targeting, and the role of the intelligence analyst in target development and combat assessment. Targeting is often defined as **deliberate** or **reactive**. The process of deliberate targeting is most often associated with fixed or semi-fixed targets, while reactive targeting is most often associated with mobile targets. The term "reactive," however, does not imply that prior planning did not occur. Whether deliberate or reactive, an integrated intelligence, maneuver, fires and C2 process must occur that assists the commander in deciding which targets to engage, when, where, and to what effect. The targeting cycle is that process. As with most processes, the higher the command level performing the process, the more structured and formal in nature it becomes, and the more the process focuses on events well into the future. At lower tactical levels the same process may occur, but compressed into a much shorter time span, involving far less formality, and focused on events of an immediate nature.

7002. The Targeting Cycle

The targeting cycle describes the process by which fires planners and targeteers derive nomination lists of forces, installations or locations which, if attacked, will have the greatest likelihood of meeting the commander's warfighting objectives. Targeting is a continuous process, which ,at the MEF and JFC command echelons, involves six phases: commander's objectives, guidance and intent; target development; capabilities analysis and tasking; mission planning; execution; and effects assessment. At lower tactical levels the cycle can be simplified to decide, detect, deliver, and assess (D3A). Figure 7-1 depicts the joint targeting cycle and its relationship to D3A. Although intelligence is an integral part of all phases within the cycle, intelligence analysis and production most directly affects target development (decide) and effects assessment (assess).

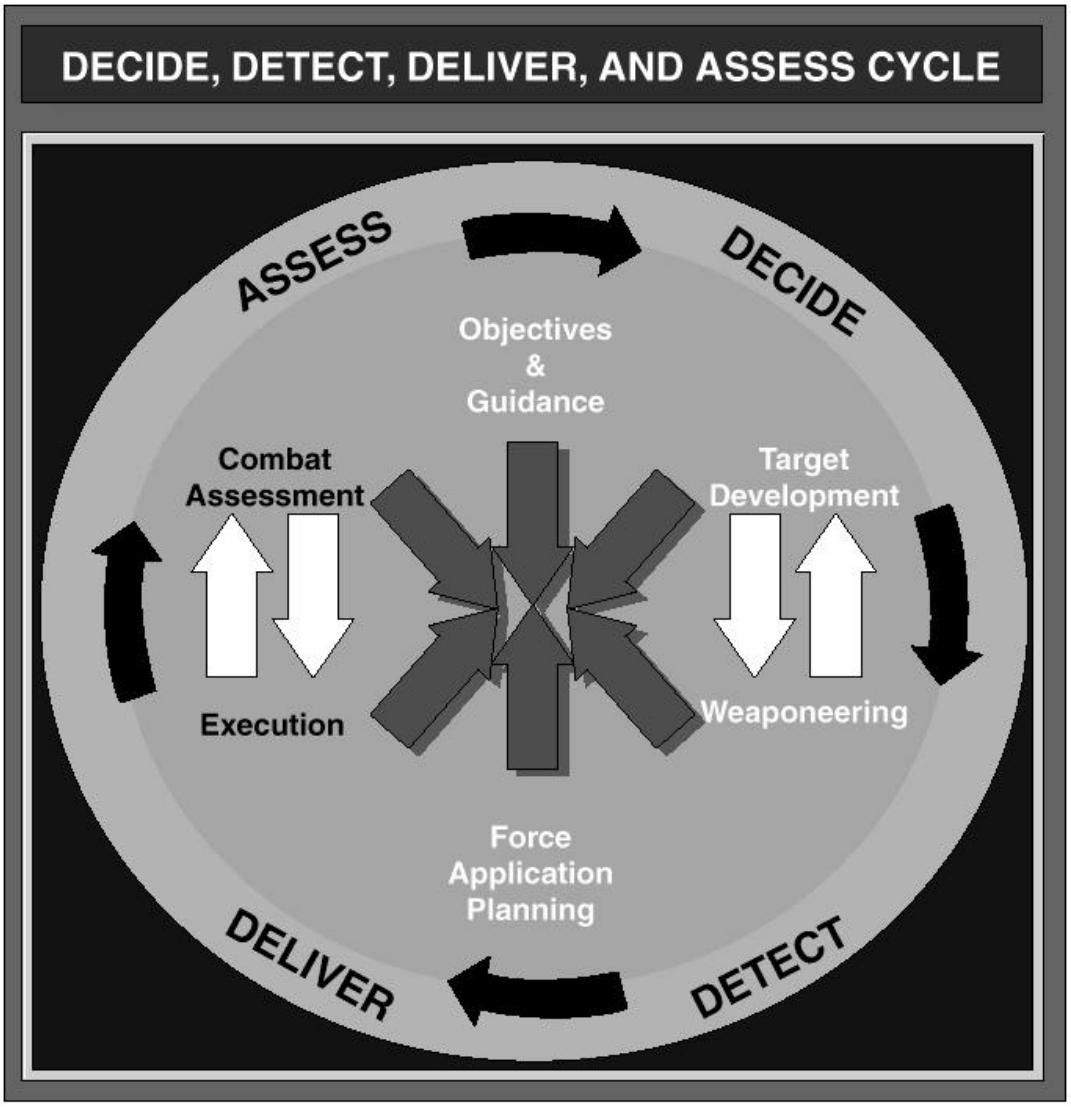

Figure 7-1. Joint Targeting Cycle and D3A

Target development is the analysis of potential enemy military, political, or economic systems, their components, and elements in order to determine their significance and relevance based on the commander's objectives, guidance, and intent. It evaluates the components and interrelationships to establish their criticality to the operation, and their vulnerability to attack. This systematic analysis is accomplished to select candidate components which should be attacked, and the type and extent of damage to be inflicted, to accomplish, or aid in accomplishing, the defined objective. The analysis proceeds from broad systems to specific components, and finally to individual elements or aimpoints. Both objective definition and target development must be performed in compliance with stated guidance, law of armed conflict, and rules of engagement.

Effects assessment is the final step of the targeting cycle and entails the determination of the overall effectiveness of force or weapon system employment during military operations. There are three components of effects assessment: battle damage assessment (BDA), mission effectiveness assessment (MEA), and reattack recommendations (RR). Intelligence analysis has a major role in determination of BDA, which concerns the physical damage, functional damage, and target assessment. Reattack recommendations are made based on conclusions drawn from analysis of BDA and MEA.

7003. Target Development

As previously discussed, target development involves the analysis of targets in order to determine their significance and relevance. From that analysis, targeting strategies are developed in order to determine the best way to achieve the commander's objectives. Each target is examined for systemic and physical vulnerabilities based on the lethal and non-lethal capabilities available, with the goal of optimizing the use of effects. The end result is a prioritized list of targets, and the intelligence requirements to support both target acquisition and combat assessment. Within the joint process, target development is a key component of Phase II. Within D3A, target development is the centerpiece of the *Decide* phase. In both cases, there are common processes and procedures which facilitate target development. As always, the scope, level of detail, and time involved will be dependent on the situation and the level of command conducting targeting. At lower tactical echelons, the targeting process may be highly reactive, compressed, and informal. At the MAGTF or joint force level, the process will be more deliberate, structured, and will encompass greater resources.

a. IPB and Target Development. IPB's impact on target development is through the information and intelligence it provides. IPB is a continuous, systematic approach to analyzing a threat's geographic region, weather, terrain, and doctrine. This approach evaluates a threat's capabilities and vulnerabilities, and facilitates information synthesis. Once synthesized, analysts have the capability to accurately determine the courses of action available to the threat commander.

During Step 3 (*Evaluate the Threat*) of IPB, a threat force is evaluated for capabilities, doctrinal principles, and TTP that are preferred. It is from their doctrine, training practices, and observed

patterns and activities that accurate doctrinal templates are constructed. These templates then aid in the initial identification of the threat's COGs , CVs, and HVTs.

During Step 4 (*Determine Threat COAs*), the construction of situation templates assists in the refinement of HVTs for a specific battlespace and COA. Concurrent with development of the situation template is an examination of the threat commander's decision cycle and points associated with each potential COA. As the analyst mentally wargames the COA and the decisions the threat commander must make, key assets become apparent. Those key assets are the HVTs associated with that particular COA or phase of a COA. Situation, event, and decision support templates help to identify NAIs. Once identified, NAIs can then confirm or deny a threats activities or adoption of a particular COA. Additionally, decision points or decision phase lines, TAIs, and HPTs are identified. Target development takes IPB a step further by analyzing the target systems, complexes and components, and developing their relevance and importance.

b. Target Value Analysis. Target value analysis is a methodology which identifies potential HVT sets within a given COA. The successful attack of the HVT can provide a tactical opportunity. The target value methodology provides a relative ranking, or worth, of target sets. The analyst must put himself into the threat commander's position. The target analyst, in coordination with the G-3/S-3, G-2/S-2, fire support coordinator (FSC), and other staff members, wargame the COAs. The purpose is to finalize individual staff estimates, develop a fire support plan, a scheme of maneuver, and both friendly and threat decision support templates. One result of wargaming is the determination of critical assets required by the threat commander to accomplish his mission.

c. High Value and High Payoff Targets. An HVT is an asset that the **threat commander** requires for the successful completion of his mission. Its loss to the threat can be expected to contribute to substantial degradation of an important battlespace function. HPTs are HVTs which, if successfully attacked, contribute substantially to the success of the **friendly commander's** mission. The G-2/S-2 section, together with the FSC and other staff, identify key threat assets that must be dealt with, and nominate HVTs to be HPTs. The key to HPTs is that they are based on the friendly commander's scheme of maneuver. The development of HPTs from HVTs is done during the wargaming process. As the different options are fought by the staff, the G-2/S-2 identifies specific HVTs. The HPTs for a specific phase of the battle are recorded on the decision support template and synchronization matrix, as are the means identified to deliver the attack. Those locations where HPTs are expected to appear become TAIs. Additional NAI may be directed to ensure timely identification of the target to allow engagement.

The process of designating HVTs as HPTs requires careful staff coordination. The G-2/S-2 and/or collection manager evaluate HVTs at different points in the battle to determine if collection assets are capable of detecting them and providing the necessary target resolution. This evaluation becomes the basis for the collection plan for intelligence support to targeting. Because of their importance, HPTs will have priority in the allocation of detection systems. The G-2/S-2 and the commander must weigh the impact the priority will have on maintaining situational awareness, since in many cases the same collection assets are used for both targeting and battlespace awareness.

The FSC, air officer, EWO, C2W and other representatives as appropriate use their knowledge of friendly lethal and non-lethal means to determine if a capability exists to attack the HVT, and the expected effects. The G-2/S-2 then assesses the threat response. This action-assess sequence helps determine if attacking the HVT is necessary to ensure the success of the friendly force. If the HVT is acquirable, attackable, and capable of ensuring friendly success, it becomes an HPT.

d. High Payoff Target List (HPTL) - The HPTL identifies the HPTs for a specific point in the battle in the order of their priority. While target value is usually the greatest factor contributing to target payoff, other things to be considered include:

- The sequence or order of occurrence.
- The ability to locate and identify the target.
- The degree of accuracy and identification available from target acquisition systems.
- The ability to engage the target.
- The ability to defeat the target.
- The resources required to do all of the above.

The HPTL, when approved by the commander, becomes a tool in determining attack guidance and developing the intelligence collection, production, and dissemination plans. Collection efforts focus on those NAI and TAI that the IPB process identifies during the decide phase. Knowledge of target type and its associated signatures (electronic, visual, thermal) enables friendly forces to direct the most capable collection asset to be tasked against the target. The asset is positioned in the best location based on friendly estimates of when and where the threat target is located. The production effort focuses on developing timely, tailored intelligence products to meet maneuver and fires needs. Finally, the dissemination effort focuses on ensuring CIS readiness to support both routine and time-sensitive intelligence reporting to support targeting needs throughout the MAGTF.

The decision to destroy, degrade, disrupt, or delay a given HPT results in a requirement to detect that target. Intelligence needs to support the detection of the target are expressed as PIR sand IRs. The PIRs and IRs that support detection of a target are incorporated into the collection plan. The collection manager translates the PIR and IR into ICRs and supporting specific intelligence requirements (SIR). The collection manager considers the availability and capability of all MAGTF and external collection assets.

7004. Target Systems Analysis

At the strategic and operational levels of war, targeting is more deliberate and often focused on fixed installations or large arrays of targets. Even at the MAGTF level, the capabilities of the

ACE's aircraft generally provide the MAGTF commander the means to strike deep targets that support threat maneuver forces or at formations of ground forces. These targets are often complex groupings of installations, units, and defenses which may require a methodical approach to ensure success. The methodology used is referred to as target system analysis.

a. Target System Analysis. A target system includes all the installations, facilities or forces that are situated in a particular geographic area and are functionally related. A target system can comprise either fixed installations or mobile target sets. While an individual target may be important or significant based on its own individual characteristics, its worth usually derives from its relative importance within a target system.

A target system is a sum of its components. These components could also comprise targets. Examples include airfields, which are a component of air defense, but are also targets in and of themselves. Within industrial or economic systems, a system component belongs to one or more groups of industries or basic utilities required to produce individual parts of an end product. Target system components can also refer to component services. For example, an air defense system may include command and control, early warning and target acquisition radars, antiaircraft artillery (AAA) and surface-to-air missile (SAM) batteries, SAM support facilities, and other components that are neither industries nor utilities. Target system elements are smaller, more intricate parts of the target system than the component and are necessary to the operation of the component as a whole. Figure 7-2 depicts the relationship of a target system, its components, and its elements.

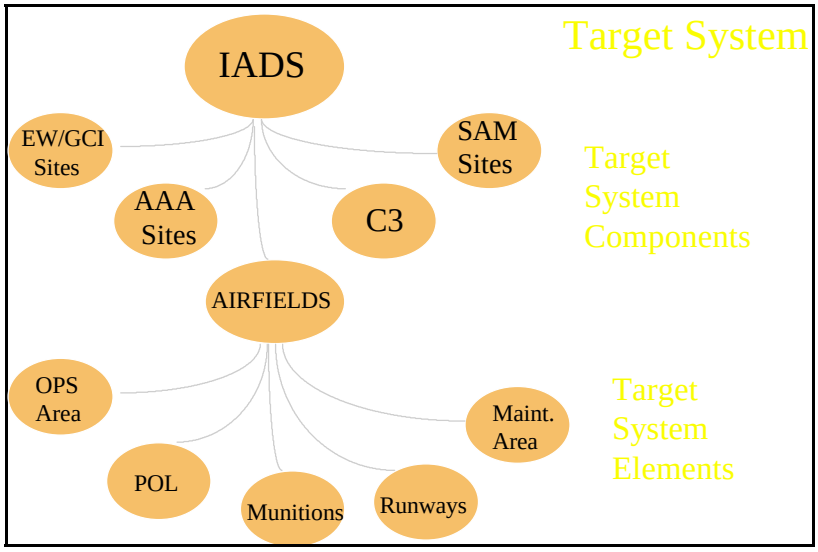

Figure 7-2. Target System, Components, and Elements

Target system activities encompass those actions or functions performed by the target system components in pursuit of system goals. By this definition, a combined-arms maneuver division could be viewed as a target system, with the components consisting of air defense units, artillery,

armor, mechanized infantry, engineers and so forth. The target development process should not focus on the systems nor its components, but rather on the activity of the system or its components. Once analysts have identified the enemy activity that must be modified or defeated, they can determine the key target systems, components, or elements that should be attacked, degraded, or exploited to produce the desired effects. For example, enemy air attacks against friendly ports and lines of communication may seriously threaten resupply of friendly forces. To modify or defeat this enemy activity, targeteers analyze the enemy's air force “system” and identify threat system components and elements. Specifically, they target the home bases of enemy aircraft and may identify runways, POL storage, and maintenance facilities as the potential target elements against which friendly forces should be employed to modify or defeat the enemy's air attack activities. A comprehensive analysis of the target system, its components, and their elements is essential to understanding the activities of the total system.

An understanding of the linkage among target system components and their interdependence is imperative for accurate analysis. Linkage is the connection between installations performing identical, similar, related, or complementary activities or functions. Critical nodes are those points where target system components and elements are linked and dependent upon each other. These key nodes also exist where target systems interact with other target systems. For example, an enemy's air defense system consists of a number of components, such as SAM sites, early warning (EW) and ground control intercept (GCI) sites, AAA sites, and airfields. To function effectively, the elements usually are linked together at a sector headquarters, which exercises responsibility for a specific geographic area. These sector headquarters constitute critical nodes within the air defense system. Severing such critical nodes is the objective of effective application of military force. Target development focuses on identifying the critical nodes within the target systems that will satisfy objectives and conform to guidance. Matrix and link analysis are highly effective tools for determining linkages and critical nodes (see chapter 6, *Threat Analysis*)

b. Target Complex Analysis. A target complex is a set of geographically related targets; examples being an airfield and nearby port facility. A complex is a group of physical elements in close proximity containing more than one target that are integrated to contribute to some function of military or civilian value. For example, a system of military airfields distributed throughout the country is made up of individual airfields (target complexes), containing multiple elements (individual aircraft, runways, hangars, etc.) in close proximity. After target system analysis identifies a critical target complex, target complex analysis identifies the target environment and defenses associated with the complex. Target complex analysis is used to determine specific targets within the complex as well as supporting actions (defense suppression, deception, tactics) that may be necessary to attack the target.

c. Target Element Analysis. A target element is the smallest identifiable activity of a target component, such as an aircraft in a revetments, the control tower, or a defensive radar site. Based on the stated targeting objectives, target elements will be translated into targets for attack. Detailed analysis must be conducted on the individual target element. Target element analysis is the responsibility of the target intelligence officer and consists of six elements:

- **Location** - exact geographic location of potential target; may be expressed in geographic or universal transverse mercator (UTM) coordinates.

- **Elevation** - altitude above sea level in feet or meters of that point of ground on which target is located.

- **Identification** - requires the accurate determination of five sub elements:

  -- **Type**: brief description which portrays the target's military functions.

  -- **Size**: accurate determination of each applicable dimension of length, width, and height.

  -- **Shape**: related to type and size and further aids in clearly defining the physical properties of target.

  -- **Attitude**: azimuth of target's long axis and, depending upon local procedures, may be expression of degrees (090-270) or descriptive words (east-west).

  -- **Dispersion**: pattern of individual elements within target area in the form of short descriptive term which conveys a word picture.

- **Vulnerability** - assessment of potential target's susceptibility to fire.

- **Recuperability** - accurate assessment of time required for enemy to return target to active status or reconstitute it in another location.

- **Importance** - assessment of target's value within enemy's overall operation, and degree to which destruction of potential target would reduce that capability.

Other considerations for analysis may be the criticality of the target, accessibility of target, recognizability of target, and the effect on the populace. Target analysis helps to determine the military importance, priority of attack, scale of effort, and weapons required to obtain a desired level of damage or casualties. Target analysis helps to determine which targets to hit, but operations planning determines how to do it.

d. Target Analysis and Production Process. The logical steps that a target analysts should complete when conducting target analysis and preparing products include the following:

- Collect target information and intelligence.

- Collate all data.

- Evaluate potential list of targets and more suitable targets using six elements.

- Construct flow of threat target component, complex, and system.

- Determine most suitable targets.

- List all targets and priorities.

- Present recommendation.

- Refine data and develop required intelligence products.

7005. Target Analysis Products

The intelligence role in target development results in at least five significant products or outputs: a list of targets, target file, no-strike target list, restricted target list, and collection requirements.

a. List of Targets. Target intelligence analysts conducts a thorough analysis of targets and, in conjunction with the other members of the A&P cell and the G-3/S-3 maneuver/fires targeting team, and provides required intelligence to support the list of targets for consideration by the commander. The list of targets is prioritized and maintained by the FSC in the order of importance relative to the commander's objectives and is directly derived from the HPTL developed during IPB and COAs wargaming. The operations section and ultimately the commander is responsible for validation of targets and formulation of the commanders target list.

b. No-Strike Target List. During the target validation process which occurs during target development, some potential targets are placed on a "no-strike list". A no-strike target is one designated by the appropriate commander upon which attacks are prohibited to avoid interference with military operations, damage to relations with indigenous personnel or governments, or violation of international law, conventions or agreements. No-strike lists are nominated by elements of the joint force and approved by the JFC. This list also includes no-strike targets directed by higher authorities. Examples of no-strike targets would be hospitals, schools, places of worship, and cultural shrines.

c. Restricted Target List. This list is composed of targets against which specific restrictions are imposed and against which actions that exceed those restrictions will not be delivered without coordination with the establishing headquarters. Restricted targets are nominated by elements of the joint force and approved by the JFC. Again, this list also includes restricted targets directed by higher authorities. An example of a restricted target would be an area where a friendly reconnaissance team is operating. To avoid fratricide, fires may be placed into the area, but only upon coordination with the establishing headquarters. Another example would be a bridge which a commander has identified as critical to his future operations. This target may be restricted as to the type of ordnance that can be used against it, or the level of damage which may be inflicted on it, to ensure it is available to friendly forces in the near future. The decision whether to restrict a target centers around the importance of the target to the threat and the plans and intentions of the friendly commander.

d. Target File. A target file contains all the pertinent information on a target system, complex, or component that has been collected during the target development process. This information may be a database, selected imagery, graphics, etc. Information in the target file will be utilized to build target studies once HPTs have been approved or validated. Generally, target files deal with fixed or semi-fixed targets.

e. Collection requirements. ICRs must be stated early and clearly in the form of PIRs, IRs, and SIRs. Analysts and planners have to think beyond the traditional "picture" (i.e., imagery) and use all possibile intelligence sources such as SIGINT (is the target talking and to whom?), HUMINT (defectors, refugees, prisoners of war, travelers, aircrew debriefs, and special forces), and other sensor data that can provide indications of a target's status. Gaining a familiarity with collection system capabilities is critical. Requesters should recognize the various intelligence sources strengths and limitations and understand how to best exploit them.

7006. Target/Objective Studies

a. Purpose. IPB affects the target development process through the evaluation of terrain, weather, and the association of threat forces at specific times and locations within the battlespace. NAIs and TAIs are identified. Additionally, HVTs and HPTs are derived and a list of targets is submitted for consideration. Once the commander has approved a target, intelligence sections develop target/objective studies to support mission planning. Target/objective studies are focused, detailed intelligence products which aid in the application of fires or the maneuver of forces against a specific target set or area. These studies can also be used by smaller MAGTFs and units, such as MEU(SOC)s for mission preparation and execution.

b. Content. Target/objective studies are graphically oriented and may use many of the graphics derived during the IPB process. One such product is a target folder, which may contain the following information depending on the specific mission:

- Orientation graphic.
- Time-distance graphic.
- Weather forecast.
- Hydrographic forecast and astronomical data.
- Intelligence briefing notes for mission.
- Graphic INTSUM.

- Objective area graphic enhancements.

  -- Orientation graphic (10-20 KM around objective)

  -- Mission planning graphic (5 KM around objective)

  -- Objective area graphics

- Objective area imagery.

- Imagery and graphics of insertion points.

- SERE plan.

- Challenge and reply passwords.

- Mission specific data as Required.

7007. Battle Damage Assessment

a. Definition. BDA is the timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against an objective or target. BDA is munitions-independent (air, ground, naval, and special forces weapon systems) and is target-independent (fixed strategic and mobile or moveable tactical targets). Producing BDA is primarily an intelligence responsibility, but requires extensive coordination with operational elements to be effective.

b. Effects Assessment (EA) and BDA. EA is the determination of overall effectiveness of force employment during military operations. The objective of EA is to identify recommendations for the course of future military operations, to include reattack recommendations (and munitions choices) against individual targets, target systems, or threat combat forces in support of operational objectives. EA represents the final step of the targeting process and is composed of three interrelated components; BDA, MEA, and RRs. EA is a G-3/S-3 responsibility, but is performed as a coordinated effort by the operations, intelligence, and fires staffs. BDA input is a key component of the combat assessment process.

MEA is conducted by operations concurrently and interactively with BDA. MEA is the assessment of the military force applied in terms of the weapon system, munitions, and weapon delivery parameters to increase force effectiveness. Operations develops the MEA by determining the effectiveness of munitions, weapons systems, and tactics. While MEA is primarily the responsibility of operations, it requires input from and coordination with the intelligence.

The operations/intelligence team considers the current level to which operational objectives have been achieved with current tactics, weapon systems and munitions, target and aimpoint selection, and attack timing using the results of the BDA and MEA analysis. Based on these considerations,

they make reattack and other recommendations as a function of the target nomination and development process. Their recommendations should address operational objectives relative to the target, target critical elements, and enemy combat forces.

c. BDA Components. BDA has three subcomponents. They are physical damage assessment, functional damage assessment, and target system assessment.

(1) Physical Damage Assessment (PDA). PDA estimates the quantitative extent of the physical damage occurring through munitions blast, fragmentation, and or fire damage effects to a planned target resulting from the application of military force. This assessment is based upon observed or interpreted damage. For example, visual observation of an enemy artillery battery (the target) verifies four self-propelled howitzers with tubes, recoil mechanisms and turrets shattered and dislodged. Track damage to one howitzer is noted. One howitzer has no visible damage. The PDA of the battery is 65 percent destroyed. PDA for larger, more complex targets is keyed to specific aimpoints and critical elements. Destruction of an entire building may not be necessary if the stated objective is to destroy a function (critical element) conducted in a section of the building. PDA is also referred to as Phase I BDA. For ground combat, PDA is often referred to as combat strength assessment. The unit controlling the weapon system, as well as the intelligence collection resources that can observe the damage, develop Phase I BDA reports. Figure 7-3 illustrates the flow of Phase I BDA.

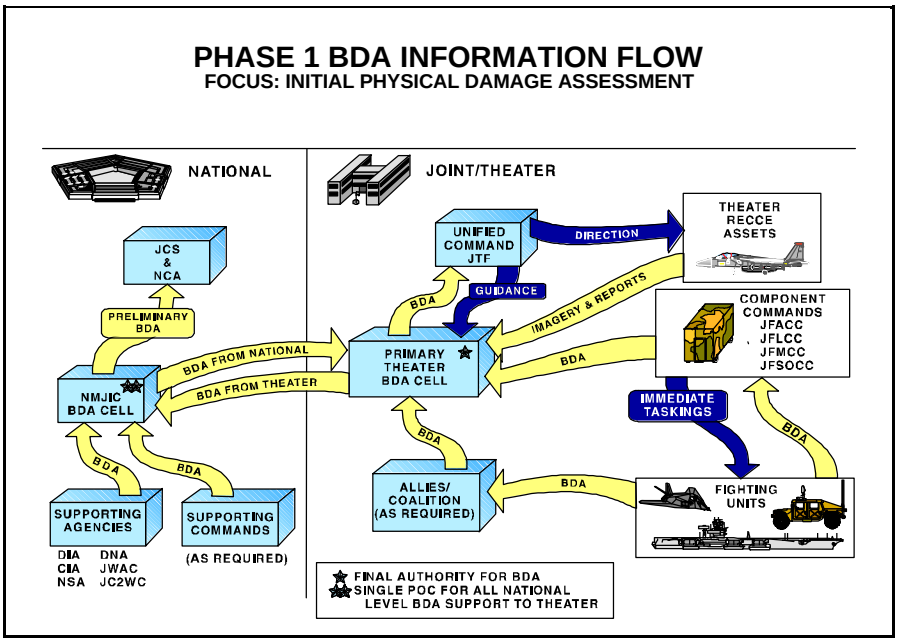

Figure 7-3. Phase I BDA/FDA Information Flow

(2) Functional Damage Assessment (FDA). FDA is an estimate of the effect of military force on degrading or destroying the functional or operational capability of the target to perform its intended mission; and, the level of success of the force applied relative to the operational objective established against the target. This assessment is inferred based upon

all-source intelligence and includes an estimate of the time required for reconstitution or replacement of the target function. For example, the physical damage to the four howitzers destroys the battery's ability to perform its intended function of providing a high rate of indirect fire from as many tubes as possible in support of the maneuver commander. Two howitzers may be able to provide limited support. Only one howitzer appears capable of providing normal fire support. The threat force is capable of reconstituting the battery (all six systems operational) within 24 hours. FDA is also referred to as Phase II BDA, and is illustrated in figure 7-4.

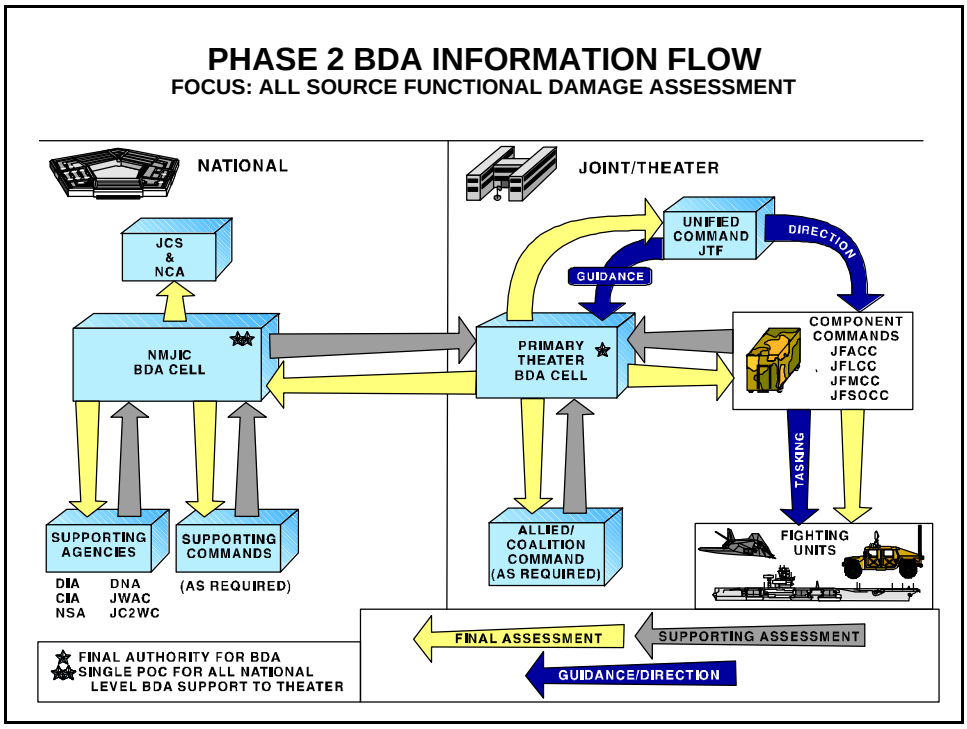

Figure 7-4. Phase II BDA/FDA Information Flow

(3) Target System Assessment (TSA). TSA is a broad assessment of the overall impact and effectiveness of the full spectrum of military operations against an entire target system's capability. It may also be applied against an adversaries combat effectiveness. A TSA may also address significant subdivisions of the system relative to the commander's stated operational objectives. TSAs are produced from a compilation of the FDAs of individual targets within a system, and applied to the current system analysis or order of battle. For example, the threat's fire support system is known to have 21 artillery battalions. Partial destruction of one battery has minor impact on the effectiveness and capability of the threat's overall fire support system. TSA is a very complex and resource intensive process. For that reason, it is generally performed at the theater BDA cell. TSA is also referred to as Phase III BDA. Figure 7-5 illustrates the flow of Phase III TSA.

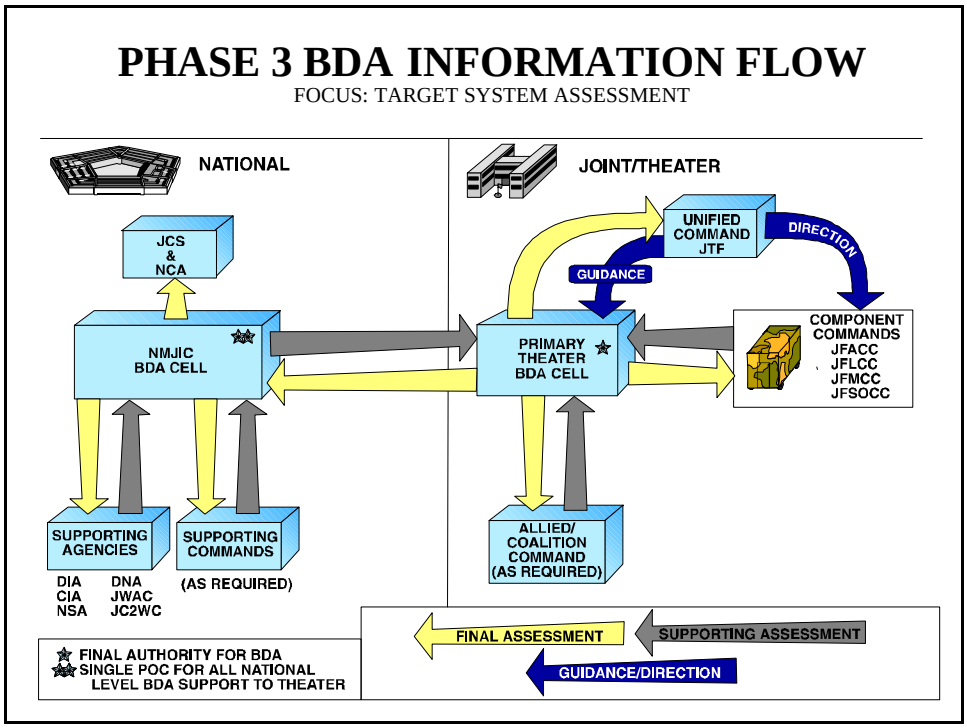

Figure 7-5. Phase III BDA/TSA Information Flow

(4) Combat Strength Assessment. When dealing with threat ground combat units, the more common term for Phase I BDA/PDA is Combat Strength Assessment. Combat Strength is defined as the actual strength on hand of a ground unit in terms of operational tanks, armored vehicles, and artillery; expressed as either a count of equipment, or as a percentage of T/O&E. Threat combat strength is a critical factor to a commander when preparing for combat. Once combat operations have begun, the commander must rely on BDA to account for enemy losses and assess remaining enemy strength. Combat strength assessment relies on a “baseline” combat strength established prior to operations. These starting numbers should remain constant for the duration of combat and serve as a benchmark against which losses (or gains) are measured. This number should only be revised if significant changes are confirmed. Losses are shown as follows:

105th Mechanized Infantry Division

	Tanks	**APCs**	**Arty**
T/O&E	**102**	**135**	**45**
Beginning Strength	**98**	**135**	**42**
Combat Losses	**17**	**22**	**4**
Replacements	**6**	**3**	**0**
Combat Strength	**87**	**116**	**38**
Percent of T/O&E	**85%**	**89%**	**84%**

Current Combat Strength = 85%

Note that while the baseline combat strength represents the maximum amount of equipment possible for a unit, combat losses represent only losses which are verifiable. Current combat strength can be viewed as a "worst case" estimate since it only takes into account *confirmed* losses. Replacements are included when known. Equipment categories are limited to generic types.

Often, multiple variants of a given platform will exist within a unit (e.g. a BTR-60 may have C2, ambulance, or NBC variants), but distinguishing between those variants can be extremely difficult for both intelligence collectors and engaged units. Therefore, combat strength should reflect basic equipment types only.

Personnel are not normally included in determining combat strength. Acquiring accurate casualty figures and accounting for replacements is extremely difficult, and past experience has shown that "body counts" are often misleading. A more appropriate and meaningful assessment of the impact of personnel losses can be made as part of Combat Effectiveness Assessment. In MOOTW, however, where personnel may be the threat principal strength, personnel losses may have to be tracked and combat strength assessed accordingly.

(5) Combat Effectiveness Assessment. Within the construct of BDA, combat effectiveness assessment represents both a FDA and TSA. The underlying premise of assessing combat effectiveness is that as combat operations progress, analysts cannot know with certainty the strength of a threat force suffering attrition or receiving replacements. Furthermore, it is reasonable to assume that regardless of the materiel strength a force may possess, the ability to execute their mission will be degraded or enhanced by other factors. Chapter 6, **Threat Analysis**, provides the factors and methodology for assessing combat effectiveness. Assessing combat effectiveness is more art than science and is a highly subjective process, but nonetheless it is essential to supporting the commander's ability to make decisions.

d. Intelligence Responsibility. The intelligence officer (and ISC at the MEF level) integrates intelligence and operational data such as weapon system and munitions effectiveness provided by the G-3/S-3 to determine the effects of an executed COA on threat strength and

combat effectiveness. In coordination with the G-3/S-3, the intelligence officer or ISC conducts the following:

- Recommends HVTs.
- Develops and recommends IRs to include those for targeting and BDA. Some of the intelligence requirements become PIR.
- Coordinates with the G-3/S-3, air officer, and FSC to develop fully coordinated targeting, intelligence, BDA, MEA and RR plans.
- Develops integrated collections, production, and dissemination plans to answer the commander's IRs and tracks and maintains BDA charts and files.
- Tasks or requests collection and/or production support from the appropriate unit or agency to collect the information and produce the intelligence required to satisfy the commander's targeting objectives and BDA in context with the overall intelligence and operational requirements.
- Establishes procedures to ensure reports from forward observers, reconnaissance, pilots, etc., are made quickly available to BDA analysts.
- Matches BDA against the commanders objectives to determine targeting success and refines intelligence estimates of the threat's situation and capabilities, recommends target reattack, develops and maintains historical BDA databases, and disseminates hard and soft copy intelligence and BDA products.
- Uses the results of BDA and combat assessment in determining the need to develop further adversary courses of action.

e. Methodology. After the commander identifies his PIRs, IRs and targeting priorities, the intelligence officer or ISC (at MEF level) tasks intelligence collection assets to locate, identify, and track the designated targets, and production assets to plan and prepare needed intelligence products. The ISC, FSC, and air officer coordinate to identify the appropriate physical destruction, EA or other attack system to capture, destroy, degrade, suppress, or neutralize the target.

Based on targets the commander wants to attack, and if the commander sets conditions he wants met, the ISC refines the commander's BDA related requirements and then integrates them into the intelligence operations plan. These BDA requirements are answered in the same manner as the commander's other PIRs and IRs through execution of the intelligence cycle.

As targets are attacked, the ISC coordinates A&P company's BDA through execution of the intelligence cycle. The commander uses BDA to decide if he needs to reattack the target or if his objectives have been met. Once a BDA related PIR has been satisfied, the commander decides if

he needs to establish a new BDA related PIR or if he will use his limited intelligence assets to support another aspect of his overall mission. Although the commander can have more than one PIR at a time dedicated to BDA, BDA related PIRs should only address the commander's most critical requirements.

At the tactical level, BDA provides a series of timely and accurate "snapshots" of the effect operations are having on the adversary. This helps commanders determine when or if their targeting effort is accomplishing their goals and objectives and provides commanders the information they need to quickly allocate or redirect forces in order to make the best use of available resources and combat power.

f. BDA Principles. BDA is only one of many tools the commander and his staff have to measure progress towards mission accomplishment. The G2 must work closely with the commander and his staff to make sure they know the characteristics and limitations of BDA. There must be a realistic level of expectation regarding the ability to measure things that are important to the commander.

- **Objectivity** - BDA must be objective and supported by the most reliable data available. Generally, data collected through objective means (imagery) are more reliable than data collected through subjective means (pilot reports). The intelligence officer and ISC should strive to verify conclusions and resolve discrepancies in BDA reporting. It is particularly important to maintain BDA objectivity when BDA becomes the deciding factor for determining and executing a specific COA or decision. Likewise, when disseminating intelligence to commanders and others, the ISC must ensure it is clear as to what is fact and what are estimates.

- **Reliability** - The quantity and quality of available collection and production assets significantly impact upon the reliability of BDA. Highly reliable reports are concrete, quantifiable, and precise. The degree of reliability and credibility of the assessment relies to a great extent upon the resources employed for BDA collection. Collection and production assets must be properly balanced, managed, and supervised.

- **Accuracy** - accurate BDA information can be obtained in many instances if the area of operations is frequently and adequately covered by a combination of national, theater, and tactical collection and production assets. Frequent coverage is necessary to accurately determine pre- and post-strike damage. Sporadic collection coverage (limited and infrequent) and product preparation may produce a distorted picture of the battlespace and mislead BDA analysts and the commanders who use the BDA.

g. BDA Reporting. The intelligence officer or ISC ensures BDA reports conform to the operational plan, report the nature of damage inflicted or unit/systems destroyed, and assess the degree of mission success as it relates to the initial objective. When possible, BDA reporting includes the physical damage assessment and an analysis of the consequence of the damage on the threat unit. The intelligence officer or ISC must attempt to obtain visual verification of the target damage and destruction.

MAGTFs and their subordinate elements are primarily concerned with conducting Phase I BDA/PDA. Sources of information for Phase I/BDA include:

- Mission reports (MISREPs) and in-flight reports (INFLTREP)
- Aircraft cockpit video (ACV) or weapons system video (WSV)
- Imagery and imagery intelligence (IMINT) including national, theater, and tactical imaging systems and unmanned aerial vehicles (UAVs)
- Signals intelligence (SIGINT)
- Human resource intelligence (HUMINT)
- Open source intelligence (OSINT), including television and radio broadcasts, newspapers, etc.
- Visual reports from combat units, air controllers, or forward observers.

At each echelon, the intelligence officer compiles, refines, and validates the various sources of BDA and develops consolidated physical damage assessments and/or combat strength assessments. The MSCs/MSEs will forward consolidated BDA reporting of their subordinates and forward a summary BDA report to the MEF, usually covering set time periods. See appendix F for an example of a summary BDA report format.

At the MEF level, the P&A Co, intel bn, is responsible for compiling the overall Phase I/PDAs for the MEF, and for adjusting the master OOB databases to reflect threat combat losses. The BDA cell will also prepare and disseminate formal Phase I BDA reports in accordance with theater and national policies and procedures. The DIA Defense Intelligence Reference Document *Battle Damage Assessment (BDA) Reference Handbook* (U), DI-2820-1-97, provides detailed joint procedures and formats regarding BDA analysis, reporting formats, standard terminology, and resources. This document is available on-line via INTELINK-S and INTELINK.

Chapter 8

INTELLIGENCE PRODUCTION

8001. Overview

Intelligence production is the conversion of information into intelligence through the integration, analysis, evaluation, interpretation, and synthesis of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production involves translating the results of analysis into usable intelligence products that are timely and tailored to the unit's, subordinate units and other supported commands' missions and IRs. The analyst must strive to provide knowledge and understanding that the decisionmaker can visualize and absorb. To the greatest extent possible, that knowledge and understanding should be presented in the form of coherent, meaningful images that are easily assimilated by commanders rather than in the form of accumulated lists, texts or data fields. During the production phase of the intelligence cycle, information is:

- Evaluated to determine pertinence, reliability, and accuracy.
- Analyzed to isolate significant elements.
- Integrated with other relevant information and previously developed intelligence.
- Interpreted to form logical conclusions that bear on the situation and support the commander's decisionmaking process.
- Applied to estimate possible outcomes.
- Placed into the product format that will be most useful to its eventual user.

Intelligence production can be extremely simple or incredibly complex. At the MAGTF CE level -- particularly during deliberate planning -- production normally entails the development of detailed, all-source intelligence estimates and studies through the combined efforts of several intelligence and reconnaissance operations elements. During tactical execution, time constraints and the demands of the ongoing battle require rapid processing and production, with an emphasis on development of simple, mission-focused intelligence products such as an annotated image, a target description, or an overlay depicting current and future threat dispositions. An enlisted intelligence specialist on duty in an infantry battalion COC may develop dozens of intelligence "products" in the form of answers to questions concerning the enemy situation, targets, or terrain to be traversed. The value of intelligence production is not measured solely in terms of time or resources expended; instead it is measured by how well it places information into context, converts it into knowledge and understanding through analysis and synthesis, answers the PIRs and IRs and is the applied to the decisionmaking process.

There is an inherent friction between the desire to provide as complete and accurate an intelligence product as possible and the continuous requirement to support the time-sensitive urgency of tactical decisionmaking. In practice, these conflicting demands must be balanced by using both stated direction, such as the commander's intent and PIRs, and knowledge of the operational situation to determine when to finish and disseminate a product.

To provide a framework to make these determinations, intelligence production can be viewed as occurring on two levels: **deliberate** and **immediate**. **Deliberate** production is employed when there is sufficient time to thoroughly evaluate, analyze, and synthesize all available information and intelligence and then produce formal, comprehensive and detailed intelligence products such as a written intelligence estimate, summary report, or detailed target/objective area study. **Immediate** production is conducted to identify, process, and place in context elements of data, information, and intelligence that have a direct effect on current or near-term operations. These elements are subjected to a compressed version of the production cycle, and the resulting product is rapidly disseminated to those who are affected. Immediate production is normally conducted during execution and results in simple, mission-specific intelligence products: situational assessments or answers to specific, individual intelligence requirements. There is no absolute distinction between the two levels; the nature of the situation and pertinent intelligence requirements will dictate the amount of time available to complete each production effort. Often, immediate production is facilitated by, and builds on, a deliberate production effort that has been previously completed.

8002. Principles

Production, whether deliberate or immediate, no matter what level it occurs at, should be guided by the following principles:

- **Focus on the Purpose and Use of Intelligence.** To better understand the exact needs of the consumer and the best way of answering the IRs, the producer needs to know the level of command that will utilize the intelligence, their mission, IRs, time sensitivity, responsibilities, and purpose of the intelligence products.

- **Objectivity.** Producers must be objective and unbiased and avoid any tendency toward preconceived ideas. When conflicting information exists, efforts should be made to resolve the difference. If time and resources are inadequate to provide unambiguous intelligence, the commander must be made aware of the ambiguity or uncertainty. Commanders need all available pertinent intelligence, including conflicting or contradictory information and opinion.

- **Provide Integrated and Tailored Products.** Intelligence analysts should use information available from multiple sources, integrate it, tailor it to the commander's and other users' needs to provide decisionmakers with a clear picture of the battlespace.

- **Coordinate Production Among Echelons.** Intelligence production should be coordinated from national to tactical levels. These production activities should be directed and coordinated by the JTF J-2 so they are mutually supporting and nonduplicative. Intelligence production for joint or combined operations is accomplished by forces at every echelon. This includes Service-unique products at the component commands and operating forces. Intelligence produced at higher echelons is derived from both collection assets and production capabilities organic to that echelon or higher and a refinement and compilation of intelligence received from subordinate units and external organizations. Subordinate units, in turn, use the intelligence products sent to them by the senior command to determine or adjust their mission and operations.

- **Production Responsibilities.** Higher echelons are responsible for ensuring subordinates are provided any required intelligence exceeding the subordinate's organic capabilities. Higher echelon commanders and intelligence officers should identify organizations able to contribute to resolution of subordinate commanders' IRs, and take necessary actions to provide subordinate commands with required intelligence products and services.

- **Production Management.** Production management is a critical element in ensuring effective and efficient intelligence production in support of operations. At all levels, production requirements must be received, reviewed, validated, prioritized, and coordinated to determine the task, producer, forms, and production schedule.

8003. Production Cycle

At its heart, the goal of the intelligence cycle is to produce timely, useable intelligence. The production cycle, therefore, is in essence the intelligence cycle, with its constituent parts of directing, collecting, processing and exploiting, analyzing, and finally producing, disseminating and using the intelligence. The production cycle can be extremely simple or very complex, and can span months or minutes depending on the level of command conducting it and the nature of the requirement to be satisfied. The following is a breakdown of the production cycle; note however, intelligence sections should never be hostage to the *process*. Instead they must always stay focused on delivering the *product* in a timely, tailored, complete and useable manner.

a. Defining the Intelligence Requirements. IRs drive the production of intelligence. Properly articulated, mission-oriented requirements focus the intelligence effort in general, and specifically define IPRs. The commander, the entire staff, and all subordinate commanders play a role in developing the command's IRs. The intelligence officer formulates most of the initial requirements during Step 1 (**Define the Battlespace Environment**) of IPB by identifying gaps in current intelligence holdings and also defining the scope and detail of production required in support of IPB. As IPB and staff planning progresses, additional IRs are identified. These requirements are generally linked to proposed COAs, potential decisions, and targeting. As analysts work to satisfy the IRs of the command and all supported units, they too will generate new IRs. All of these requirements must be validated, refined and prioritized by the intelligence officer based on the commander's intent and the current phase of the PDE&A cycle, and then converted into integrated ICRs, IPRs and IDRs. This is not a one-time effort, but instead a

dynamic process of new, existing, and satisfied or no longer relevant requirements. The relative importance of each requirement changes as the PDE&A cycle progresses, and as phases of the operation are executed. The intelligence officer must periodically confirm the assignment of priorities with the commander to ensure the intelligence effort is focused in accordance with the commander's desires.

b. Define and Prioritize IPRs and other Production Tasks. Once the IRs have been clearly stated and properly defined, the analyst must define and prioritize the IPRs and other production tasks to be accomplished. There are many considerations. The analyst must determine their research needs. What do I need and where can I obtain the information? The tactical intelligence analyst is likely to have access to a wide range of information and intelligence sources and documents. The product required may have already been produced by another source or agency. Conversely, the requirement may generate intelligence collection requirements to provide the necessary information. When is the product required (priority) and in what form? Time requirements and elements of the final product will have a lot to do with deciding who can produce the intelligence product. What does the product have to look like upon completion and who will it be disseminated to? Will it be a document, report, supporting study, briefing, etc.? A small intelligence section does not have the assets to complete a large, detailed, hardcopy study in a short period of time. Classification and releasability also must be considered when dealing with intelligence products. Is this a product that can or must be shared with our multinational allies? The analyst must also determine if there is any supporting work required, such as requests for imagery exploitation, topographic analysis, etc.

c. Develop Intelligence Production Plan and Schedule. When dealing with large or complex IRs and IPRs, developing a production plan and supporting schedule will aid in effectively applying resources to accomplish the task. Production plans and schedules are particularly important at higher echelon commands and intelligence centers where numerous long-term projects must be managed and coordinated. At lower echelons, production plans and schedules may consist simply of the intelligence officer conducting a quick mental assessment of the task and developing a timeline for its completion.

When developing a production plan and schedule, the first consideration is always the priority. The requester's needs will drive the due date or time. Once the priority and time available are established, factors to be considered include: research required; time to collect new information and data; need for coordination, review and quality control; the commander's and other users' desired formats; graphic preparation; reproduction or conversion; and dissemination time. For large, long-term products, the production schedule can be time-lined, with various milestones, due dates, and completion projections annotated. In large organizations with distinct elements which conduct collection, exploitation, editing, graphics and dissemination, this timeline serves to synchronize those assets to ensure efficient and timely completion of the project.

d. Allocation of Resources. Determine organic and external resources required to produce the intelligence product and their availability. Resources include available personnel, time, analysis, preprocessed information sources, collection assets, AIS, and communications.

e. Assign Tasks. Specific tasks are assigned to the various collection and production resources that can assist in the production process. The relative priority of those tasks is defined based on the priority of the IR, time available and the production schedule.

f. Prepare the Product(s). During this step, research of existing information, data, and intelligence is conducted and integrated with new information derived from collection operations and other all-source intelligence reporting. The resulting information set is analyzed and synthesized to develop conclusions and estimates. A draft of the final intelligence product(s) is produced based on the analysis performed.

g. Review and Quality Control. Procedures must be established for proper review and quality control of the intelligence product before final approval and dissemination. A balance must be achieved between timely delivery and the review process.

h. Approval and Distribution. Responsibility for final approval of the intelligence product normally rests with the producing unit G-2/S-2; at the MEF level, this responsibility will generally be delegated to the ISC. However, time and the situation may dictate delegating authority to lower levels. Proper distribution is important as the intelligence product will be of no value unless it arrives to the requester on time and is properly utilized.

I. Use. The final and most critical step in the production cycle is to follow-up with the commanders and other users who receive the intelligence product(s) to:

- Ensure that it is understood.
- Determine whether their PIRs and IRs have been fully satisfied.
- Determine in a timely manner if any new PIRs or IRs have been generated in response to the new intelligence.

8004. Production Management

a. Definition. Production management is a critical element in ensuring effective and efficient military intelligence production in support of MAGTF and joint operations. As is implied, it involves managing the production cycle. It encompasses determining the scope, content, and format of each product; developing a plan and schedule for the development of each product; assigning priorities among the various intelligence production requirements; allocating processing, exploitation and production resources; and integrating production efforts with collection and dissemination. At intelligence production centers and agencies, a separate production manager performs these functions. At the MEF CE level, the intel bn CO in his staff role as the ISC is responsible for this function under the staff cognizance of the MEF AC/S G-2. At the MSC level, the G-2 intelligence operations officer/air combat intelligence officer performs these functions. At lower tactical echelons, the S-2 performs production management as an inherent part of his overall responsibilities. In the event that an intelligence DST is supporting a lower unit, it's OIC may be tasked with this responsibility.

b. Purpose. The purpose of production management is to satisfy established PIRs and IRs in a complete, timely and efficient manner. Production management helps prioritize competing requirements to ensure timely response. Proper management also helps to ensure the most effective use of limited intelligence resources.

c. Relationship to Collection and Dissemination Management. Production management starts in the planning and direction phase of the intelligence cycle where intelligence requirements are determined. PIRs and IRs are either answered by intelligence products that are readily available or they become a collection or production requirement. Ultimately, all products must be disseminated in some form to individuals and organizations that need them. Although collection, production and dissemination all involve their own unique internal procedures and cycles, all three must be synchronized in order to provide a timely, pertinent, and usable intelligence product.

d. Elements of Production Management. The following elements are essential for the conduct of production management and are keyed to the production cycle:

(1) Production Requirements Development. IRs must be validated through the chain of command. Each requirement must be examined to determine scope, form, and content of the request. Together these constitute the IPR. A well developed IPR has the following items:

- A point of contact and best way to communicate.
- The priority of the requirement.
- The date required and latest time the intelligence is of value (LTIOV).
- Classification, releasability, and format desired.
- Mission background.
- A brief paragraph describing what is desired.
- Justification for the requirement.
- Sources and documents previously consulted.
- Dissemination instructions (primary and alternate communications means/channels for both routine and time-sensitive situations, designated recipients, quantities required, etc.).

(2) Prioritization of Requirements. All requirements compete for utilization of limited intelligence resources, and prioritization will drive the use of those resources.

(3) Asset Allocation. The intelligence officer and intel bn production manager will consider all internal (organic) and external resources (JTF, theater and national level) for intelligence production tasking. Consideration should first be given to answering the requirement internally, however, care must be exercised to not overburden organic resources with large, complex products that are more appropriately produced at higher command levels. For example, IPB is an inherent function of staffs at every level, however, the production of detailed terrain analysis products may be more appropriately performed by the MEF Intelligence Battalion or other supporting agencies.

(4) Scheduling. All the elements of the task must be scheduled and synchronized within the time allotted to successfully complete intelligence production.

(5) Integration with Collection and Dissemination. Intelligence production must be synchronized with collection to obtain needed information and data, and with dissemination to ensure delivery to the requester when required.

8005. Intelligence Products

Intelligence products can vary in form, from graphic to written to oral. Products may be as simple as an answer to a question or as complex as a contingency intelligence study. They may be used to produce warnings or identify opportunities, but ultimately all intelligence products are intended to facilitate the planning and decisionmaking.

Because decisionmaking is a mental process and human beings think and understand primarily in the form of images, the goal of intelligence products is to convey an accurate image of the battlespace or threat to the decisionmaker in a form that facilitates rapid understanding of that image. For this reason graphics are the preferred product form. Although oral briefings and written reports were the primary product forms used in the past, the use of automated information systems today is increasing the capability to develop graphic products. Digital imagery, terrain analysis, threat overlays, diagrams, 3D perspectives, video, and virtual orientation products-- enhanced with appropriate textual data and annotations and disseminated and displayed over web-based automated information systems-- are becoming the standard for intelligence products. Graphics developed MEF ASC may be “pulled” via the MAGTF TDN from the MEF SIPRNET website or shared via IAS and used by the MSCs or their subordinates to support their commanders and staffs, thus reducing or eliminating the requirement for those organizations to produce their own. In time-sensitive situations, however, the verbal report or short text message may still be the most expeditious and useful intelligence product form.

Whether oral, text, or graphic, intelligence products should use standard formats whenever possible. Standard formats facilitate ease of preparation and dissemination, as well as usability of the intelligence product. The basic intelligence products used in MAGTFs (e.g., IPB templates and matrices, intelligence estimates, summaries, reports, and briefings) have baseline formats. Individual units may modify formats to suit local needs, but modifications may have an impact on interoperability -- and thus must be thoroughly coordinated with all. The bottom line is that intelligence must be presented such that the commander truly understands its significance in terms

of affects on the battlespace and on military operations. The following intelligence products are the principal intelligence products developed and used in the MAGTF.

a. MAGTF Contingency Intelligence Study. A baseline intelligence study prepared in advance for standing OPLANs and likely contingencies. In written form, it is based on the Intelligence Estimate format and can be converted to an intelligence estimate when a contingency becomes a reality. Many of the products produced in Steps 1 through 4 of the IPB process (MCOO, weather effects charts, threat models, doctrinal templates, etc.) can be prepared either as supporting graphics or as stand-alone products. The format can be modified to suit the user, especially for military operations other than war.

b. Intelligence Estimate and Supporting Studies. The intelligence estimate is a product for providing basic and current intelligence and results of the IPB effort focused on a specific mission. Estimates are normally prepared by all echelons of battalion/squadron size and larger during the planning phase and are frequently disseminated to other units to keep them current on intelligence. Supporting studies may cover particular aspects of the enemy situation or the area of operations. See appendix C for the intelligence estimate format and chapter 4 for a discussion of the relationship between IPB and the intelligence estimate.

c. Target/Objective Area Study. An intelligence product used to provide basic, detailed, tailored, mission-specific intelligence in support of small unit execution. There is one basic form, but many variations can be utilized. This study is not just for attack aviation. It can be used to support MEU (SOC) and regular combat operations, e.g. a rifle company attacking or defending a hill. (See Chapters 4 and 7 for the basic target/objective area study format.)

d. Intelligence Summary (INTSUM). The INTSUM provides a summary of the intelligence situation covering a specified period normally prescribed by the unit SOP for intelligence or the intelligence annex to the operation order. It is used to report threat activities, changes to threat capabilities, and the results of further analysis and production. It is designed to update the original and subsequent intelligence estimates. At lower tactical echelons, INTSUMs will be prepared in accordance with unit SOP or annex B to the OPORD. At higher commands, particularly JTFs and combatant commands, a DISUM (or daily intelligence summary) will usually be published every 24 hours. Using the basic format, units can tailor the INTSUM to fit the situation. With new automated information systems, INTSUMs and DISUMs are increasingly produced in graphic form and posted on networks for wide dissemination, with links to detailed supporting intelligence products, reports and databases. (See appendix G for the INTSUM format.)

e. Intelligence Report (INTREP). The INTREP is a standardized report which, based on its importance to the current situation, is disseminated without regard to a specific time schedule. That is, an INTREP is not prepared on a periodic basis, but as information is acquired and assessed. It is the primary means for transmitting new and significant information and intelligence when facts influencing threat capabilities have been observed, or when a change in threat capabilities has taken place. It is prepared at all echelons by the first intelligence element acquiring the information and is disseminated as rapidly as possible to all units which may have

need of the reported information. It may be prepared on any item of intelligence, regardless of source. Generally each report will concern only a single item. When time permits, the INTREP should include the originator's interpretation of the information or intelligence being reported. (See appendix H for the INTREP format.)

f. Briefings. Intelligence personnel at all command levels will frequently brief the commander, his staff or subordinate units. The ability to prepare and orally convey relevant intelligence in a clear, concise manner is an essential skill for intelligence personnel. The most common form of briefing is the **information brief**, with the primary purpose of enhancing situational awareness and understanding. Common examples are the commander's morning update or "boardwalk" brief. A second common form is the **decision brief**, with the intended purpose of eliciting a decision from the commander. An example would be briefings conducted to convey the results of wargaming and gain a decision from the commander regarding his preferred course of action. A third type of briefing is a **confirmation brief**, which is conducted as a final review of a planned action to ensure those participating are certain of the objectives and synchronized with each other.

Briefings at lower tactical levels will generally be very informal and often short notice. At higher levels the briefings may be more structured and scheduled on a recurring basis. Most often, the intelligence brief will be part of an overall staff briefing coordinated by the chief of staff/executive officer or the G-3/S-3. Regardless of the level of command, intelligence briefings should always convey mission-essential intelligence and other pertinent information and be tailored to the mission or other intended purpose, the audience, and their current IRs. Briefings should be supported with graphics to the maximum extent possible to enhance understanding in the least amount of time. Graphics may be as simple as a sketch or acetate overlay, or as complex as a multimedia presentation delivered via video teleconferencing. Ensure graphics are clear, legible, simple, visible to the audience and focused on key relevant information. (See appendix I for a sample format for an information briefing.)

8006. Intelligence Production in the MAGTF

a. Categories of Production. As previously discussed, there are two primary categories of intelligence production in the MAGTF:

(1) Deliberate Production - Deliberate production is a detailed, comprehensive, all-source intelligence product that usually supports planning. It is intended to extract the full meaning from all the information, data, and intelligence available and is usually not time sensitive. Deliberate production draws heavily on external production sources (national, theater, and service level) and is tailored to the mission and needs of the MAGTF. Intelligence products that fit into this category include contingency intelligence studies, detailed fully-developed IPB studies, intelligence estimates, and target/objective area studies.

(2) Immediate Production - Immediate production is a limited time, highly focused effort to satisfy an immediate tactical requirement. It involves the rapid processing, analysis, production, and dissemination of intelligence to influence tactical decisionmaking. This

is the primary effort of small unit intelligence sections and intelligence watches at the regiment/MAG and battalion/squadron levels and their supporting intelligence DSTs (when assigned). Intelligence products that fit into this category include intelligence reports that provide alarm or warning information, reconnaissance and surveillance data tied to decision points for branches or sequels, reactive targeting intelligence or hastily prepared intelligence briefings for initiation of small unit action.

b. Unit Intelligence Section Production

(1) Deliberate Production. MAGTF and major subordinate command intelligence sections primarily conduct deliberate production to satisfy planning requirements. They produce the contingency intelligence studies which lower level commands can tailor and utilize to fit their needs as appropriate. All units conduct IPB and prepare estimates and target/objective area studies that are tailored and focused on their mission and level of command. IRs that are beyond their capability to produce are normally referred to the MEF G-2/intel bn via the chain of command.

(2) Immediate Production. Small unit intelligence sections (regiment/battalion and MAG/Squadron) primarily conduct immediate production to satisfy tactical decisionmaking and operations (e.g., engagement of mobile targets). At higher echelons, immediate production focuses on alarms or triggers associated with the commander's decision points or reactive targeting against identified HPTs. As units and sensors collect data related to NAIs, TAIs, DPs, and HPTs, this information is rapidly assessed, placed in context, and disseminated as intelligence to the commander and appropriate agencies for immediate action. Often the product will be a verbal report or short INTREP sent via electronic means. A well-prepared IPB is the basis for rapid and effective immediate intelligence production.

c. Intelligence Direct Support Teams. Two DSTs are organic to the A&P Co, intel bn, and to each of the MSC G-2 sections. They are designed to allow the MEF or MSC commander and their G-2s to focus intelligence support to designated subordinate units, much as fire support or logistics are focused to support the main effort. The teams are made up of six enlisted personnel who have a mix of intelligence specialty skills (MOS' 0231, 0241 and 0261). DSTs are used to provide an enhanced IR management, analytical, production, and dissemination capability to the supported unit's intelligence section and to link the broader external intelligence support structure (e.g., linkage to the intel bn's AFC) to the unit. DSTs will augment the supported unit's intelligence section to carry out the following functions:

- Provide an extension of the intel bn's A&P cell or MSC G-2 intelligence operations element for the receipt, collaborative analysis, production, and dissemination of intelligence to the supported unit.

- Tailor higher and external intelligence products to the needs of the supported unit.

- Assist the supported unit's intelligence officer in the formulation and management of external IRs.

- Assist the supported unit in the production of IPB and other intelligence products to support detailed mission planning and execution.

- Augment and enhance the intelligence dissemination efforts of the supported unit's intelligence section.

d. Analysis and Production Company (A&P Co), Intelligence Battalion, Production. The A&P Co's mission is to produce and disseminate all-source fused tactical intelligence, IMINT, and GEOINT products in support of the MAGTF, MSCs, and other commands as directed. The A&P Co is the focus of the deliberate production effort to satisfy IPRs for the entire MAGTF. The A&P Co orients itself on the MEF's stated contingency planning priorities, preparing contingency intelligence studies, estimates and other products in support of MEF OPLANs and CONPLANs. The A&P Co has the personnel and equipment resources and CIS connectivity to external organizations' intelligence products and production resources at the national, theater, and Services levels to augment organic capabilities (see chapter 9, *All-Source Fusion Cell*, for further information.)

8007. External Production Support

Marine Corps intelligence assets are optimized for the production of tactical intelligence in support of MAGTF operations. While organic assets are generally sufficient to meet MAGTF requirements, national, theater, and service intelligence agencies and centers provide unique capabilities that are not duplicated in the MAGTF intelligence support structure. The MAGTF has the ability to exploit external intelligence assets to enhance its organic capabilities, bringing the full range of these capabilities to bear on MAGTF requirements. The following are key external capabilities employed to support MAGTF operations:

- National, theater, and service-level intelligence analysis and production.

- Geospatial information and services.

- Analysis and production of target intelligence and target materials.

- National imagery collection, exploitation, and production.

- SIGINT collection and production support from the U.S. SIGINT System.

- National and theater-level CI and HUMINT collection and production.

- Liaison elements from national and theater intelligence agencies.

The following capabilities are required to fully exploit the resources of external intelligence support assets:

- Personnel trained and experienced in the capabilities, limitations, employment and tasking procedures, and type products of external intelligence assets.

- Sufficient, reliable, CIS connectivity and interoperability with national, theater, and other-Service intelligence architectures.

- The ability to receive, process, and disseminate information gathered by national and theater collection assets.

- Integration of Marine intelligence specialists into national, theater, and Service intelligence organizations to articulate Marine Corps capabilities and requirements, influence decisions, and optimize intelligence support to expeditionary forces.

- Establishment of liaison between the MAGTF and supporting intelligence agencies through the establishment of dedicated communications and the exchange of liaison officers.

a. Department of Defense Intelligence Production Program (DODIPP)

(1) Overview. The DODIPP provides the analytical and production resources to support the full range of DoD's intelligence customers in the fundamental objective of supporting operational forces. It is the production program within the Department of Defense Intelligence Production Community (DODIPC). The DODIPC is defined as the Defense Intelligence Agency, the Service production centers (e.g., MCIA), the Unified Commands' JICs or joint analysis centers (JAC), components, reserves, and allied production activities when participating in the shared production program (SPP) or during crisis surge situations. The National Security Agency (NSA) and National Imagery and Mapping Agency (NIMA) also are DOD assets. NSA produces SIGINT, while NIMA produces geospatial information and GEOINT and is one of several producers of IMINT. Both agencies also contribute to and support DODIPP production and respond to the intelligence requirements of many of the same warfighter, policy, and acquisition customers, but are not formally governed by DODIPP guidelines. The DODIPP incorporates basic principles that minimize duplication of effort and make the unique and specialized expertise of its analytical personnel available to support all DOD customers.

(2) National Production Support. The Defense Intelligence Agency (DIA) and its supporting agencies (Armed Forces Medical Intelligence Center (AFMIC) and Missile and Space Intelligence Center (MSIC)) are responsible for the following areas:

- Analysis and production on foreign national military policy, doctrine, strategy, and planning on production covering national military leadership; mobilization process and potential; strategic/large scale military operations; and integrated, combined, or joint

forces on military net assessments and assessments/estimates focusing on military issued at the national, regional, and global levels.

- Analysis and production of current/I&W intelligence and strategic targeting and planning by the joint staff..

- Analysis and production of integrated force trends and projection assessments.

- Analysis and production of nuclear weapon programs and doctrine.

- Analysis and production/management of intelligence on proliferation and technology transfer.

- Analysis and production on technological capabilities of antitank guided missiles, surface to air missiles, short range ballistic missiles, and antiballistic and antitactical ballistic missiles.

- Analysis and production on medical and biological warfare intelligence.

- Analysis and production on global topics, such as military geography, industrial resources, transportation systems, demographics, military industrial and resources bases, and military economics.

- Analysis and production/management of intelligence production programs on counterterrorism, counterdrug intelligence support to law enforcement agencies, foreign intelligence and security forces, and deception analysis.

- Analysis and production/management of intelligence programs fulfilling DoD-wide responsibilities of common concern, such as targeting and foreign materiel.

- Analysis and production of orders of battle and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.

(3) Unified Command Joint Intelligence Centers (JIC). A Unified Command's intelligence production is performed by a production center, or JIC, which is assigned directly to the Unified Command in support of theater or specialized forces. JICs are the cornerstones of fulfilling the intelligence requirements of the Commanders in Chief of the Unified Commands and their subordinate commanders. The JICs provide tailored, finished intelligence products in support of theater mission planning and execution. The DODIPP recognizes that defense production challenges for regional and functional Unified Commands are different and that resources and other factors vary among them. The Unified Command JICs include:

- USACOM’s Atlantic Intelligence Command (AIC).

- USCENTCOM's JIC.
- USEUCOM's Joint Analysis Center, Molesworth, UK (JAC Molesworth).
- USPACOM's Joint Intelligence Center Pacific (JICPAC).
- USSOCOM's JIC.
- USSOUTHCOM's JICSOUTH.
- USSPACECOM's Combined Intelligence Center.
- USSTRATCOM's JIC.
- USTRANSCOM's JICTRANS.

The JICs are responsible for the following:

- Analysis and production of operational intelligence, current intelligence, and I&W for forces deployed within the command's area of responsibility.
- Analysis and production of orders of battle and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.
- Analysis and production of foreign military forces unit-level training and/or operational readiness.
- Analysis and production on the physical environment of forces/deployed/committed, including terrain analysis and intelligence preparation of the battlespace.
- Analysis and production on targeting support, including target materials, bomb damage assessments, tactical battle damage assessments, and special operations forces targeting support.
- Analysis and production to support command-sponsored joint planning and exercises.
- Analysis and production of tailored and focused intelligence produced elsewhere to meet the specific requirements of command customers.
- Analysis and production of background and tactical intelligence to customers within the theater, including operational forces and allied forces.

(4) Service Production Centers. The Service production centers, subordinate to the Services, are responsible for Service-specific Title X responsibilities for planning, training,

equipping, and other functions relative to U.S. forces and for production assigned for the Shared Production Program. The Service production centers include:

- **Army** -- National Ground Intelligence Center (NGIC).
- **Navy** -- National Maritime Intelligence Center (NMIC).
- **Marine Corps** -- Marine Corps Intelligence Activity (MCIA).
- **Air Force** -- National Air Intelligence Center (NAIC).

The Service production centers are responsible for the following areas:

- Analysis and production of weapon system technical data, characteristics, performance, system vulnerabilities, and capabilities to support Service and defense acquisition activities and force developers and for use in acquisition and reference documents to support Service operational training and preparation for contingencies/conflicts.
- Analysis and production of basic ground, naval, and aerospace intelligence to include tactics, and foreign intentions and capabilities.
- Analysis and production of Service-unique doctrine, force structure, force modernization, training and education, and acquisition.
- Analysis and production in support to Service schools and commands relative to training, exercises, predeployment, or crisis responsibilities/activities.
- Analysis and production of OOB and associated facilities and installations assigned under the Shared Production Program, to include assessing the general military capabilities of those forces.
- For the NGIC, production of ground-related systems and development, to include armor, infantry, field artillery, air defense guns, landmines, chemical warfare, helicopters, munitions, engineering and transport/logistic equipment, and associated technologies.
- For the Office of Naval Intelligence in the NMIC, production of naval-related systems and development, to include surface and subsurface combatants; antisubmarine/surface and auxiliary and support naval ships and programs; weapons, merchant shipping, and ocean science information; and associated technologies.
- For the NAIC, production of aerospace-related systems and development, to include ICBMs, IRBMs, MRBMs, bombers, fighters, special mission aircraft, munitions, space launch systems and satellites, and associated technologies.

- For the MCIA, production of amphibious and expeditionary warfare topics, to include very shallow water mines, coastal artillery, foreign marine and naval infantry forces, antilanding capabilities, and expeditionary studies.

(5) Non-DOD Intelligence Production Support. In addition to the DOD production agencies discussed above, production in support of military forces is also available from a number of non-DOD agencies (such as the Central Intelligence Agency). Generally, DIA serves as the focal point for tasking these agencies. Theater and JTF intelligence staffs, however, can access support through their resident national agencies liaison offices or a National Intelligence Support Team (NIST) when assigned. A NIST is a nationally sourced task-organized team composed of intelligence and communications experts from either DIA, CIA, NSA, NIMA, or any combination of these. They are intended to provide the supported command increased IR management, production and dissemination capabilities, to include being a direct conduit to national agencies . The size and composition of the NIST will vary according to the size and nature of the crisis and the mission and intelligence needs of the supported command.

b. Requesting Production Support

(1) Requests for Intelligence (RFIs) and Production Requirements (PRs). At the most basic level, a production requirement begins as an intelligence requirement levied on the unit intelligence section. The requesting unit intelligence officer must determine if:

- The IR or RFI is most appropriately answered by intelligence resources.
- The information or intelligence is already available in unit intelligence files, databases or information resources.
- The intelligence can be obtained by organic collection assets and developed into intelligence by its production assets.
- The intelligence can be answered from other units or components intelligence elements.

Once the intelligence officer at the requesting unit determines that the requirement cannot be met with local resources, the requirement must then be forwarded up the chain of command for satisfaction. Requirements can either be RFIs, ICRs, or intelligence production requirements (IPR or PR[1]); the decision of which avenue to pursue is the responsibility of the intelligence officer.

Generally, an RFI will be submitted if the requirement is a fairly straightforward question. In a NEO, an RFI may be *"How many personnel require evacuation?"* In this case, no extensive collection or production is required. Instead, the intelligence is generally available, but outside the requesting unit. When the IR is more complex or substantial, a RFI or PR may be more

[1] The term/acronym *intelligence production requirement* (IPR) is currently unique to the Marine Corps. The term/acronym *production requirement* (PR) is established in joint doctrine and is chiefly applicable to intelligence operations at the MEF CE level and above.

appropriate. For example, the requirement "What is the capability of country X to defend its coastline against an amphibious assault?" may result in an IPR for the MEF CE or a PR or RFI to the JTF headquarters. In this case, the answer will be fairly complex and require the collection and analysis of a large amount of information ranging from hydrographic conditions to available threat weapon systems. Such analysis may be beyond the capabilities of a small unit intelligence section and more appropriately performed at the theater or service level where the access to information and ability to task collection resources are much greater. A PR may be more appropriate to satisfy a requirement that may be recurring in nature or in a denied area, such as *"How many aircraft are maintained on alert status at airfield Y?"* In this case, the airfield will need to be monitored for a period of time to gauge the answer. In addition, the requesting unit probably does not have the collection resources to monitor the airfield, thus a request for theater or national assets is required.

As an RFI travels up the chain of command, it is either satisfied (from available information or intelligence or by collecting new data), converted into a PR, or forwarded to the next higher level for satisfaction. In the case of a PR to be handled by the unit, the RFI may be grouped with other related RFIs and expanded into a PR more appropriately answered by a single product. In rare cases, an RFI can be denied, either after determining the requesting unit already has the information or intelligence, or for lack of specificity or relevance. PRs flow in much the same manner; each unit in the chain of command validates the PR and either satisfies it from within, or passes the requirement to the next higher authority for action. Figure 8-1 illustrates the generic flow of PRs.

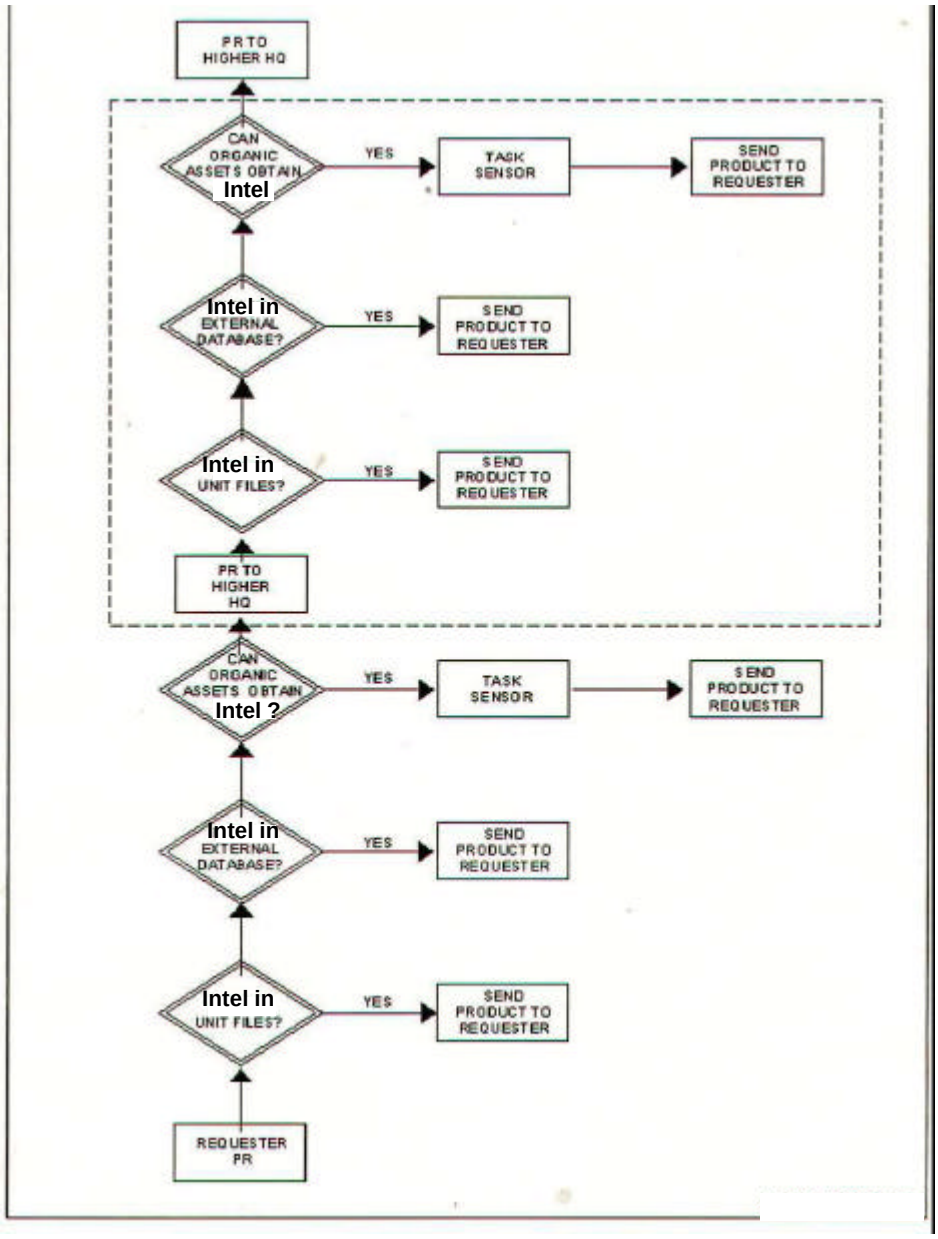

Figure 8-1. Intelligence Production Requirements Flow

(2) Request Procedures. As the principal deliberate production entity within the MAGTF, most IPRs will be levied on the intel bn, specifically the A&P Co's A&P cell. Based upon the commander's guidance, the G-2/S-2's direction, the intel bn commander/ISC will plan, manage and conduct all MAGTF IPR management (to include overall staff cognizance of radio battalion, VMU, and other MEF organic collection and production elements external to intel bn) to include determining which products will be produced locally and which will be forwarded to the appropriate theater, service, or national validation office (VO). Each of the 14 DODIPP production centers has an associated VO, which is the final office reviewing the PR before it is assigned to a production center. The tasked VO will continue the process by either accepting and

satisfying the requirement, forwarding it to another production center or, in rare cases, invalidating the requirement. Figure 8-2 illustrates this process.

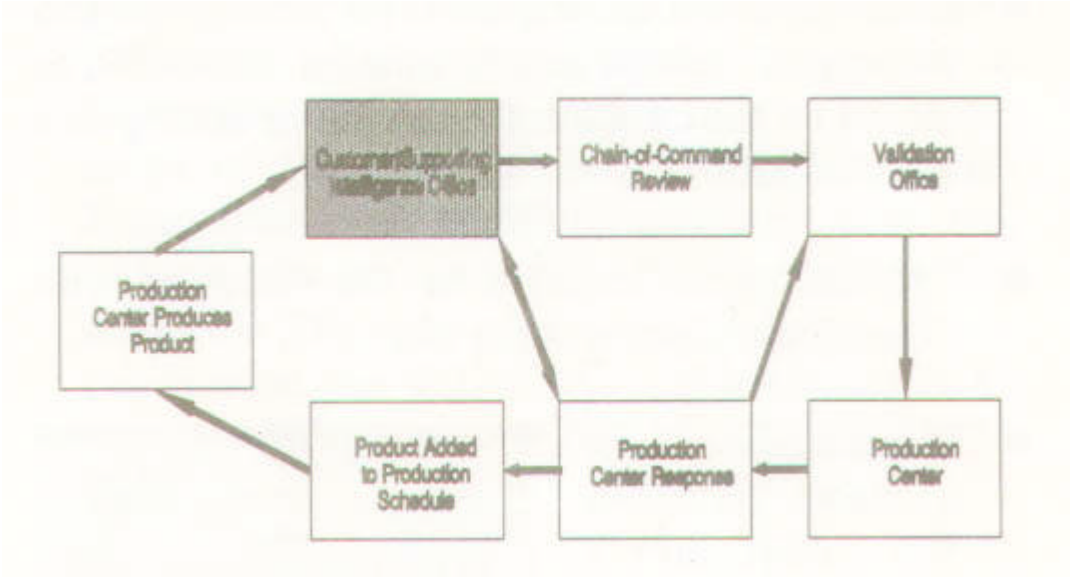

Figure 8-2. DOD Production Requirements Process

The actual procedures for production requirements and RFIs may vary from theater to theater and will be as directed by the combatant commander, the JFC or the MAGTF commander. For example, for MAGTFs located in CONUS conducting planning or preparing to deploy, MCIA may function as the VO for production requirements submitted through the normal Service chain of command. However, a MEU(SOC) or other MAGTF operationally assigned to a combatant commander would submit their requirements through the established operational chain of command to the VO supporting that theater. Likewise, a theater J-2 may delegate VO authority to a JTF J-2 during a crisis, providing the JTF J-2 a streamlined path for JIC production support and priority over all other non-crisis production requirements. For most crises and contingencies annex B to the joint force commander's OPLAN/OPORD will specify policies and procedures for requesting intelligence production support.

(3) Request Format. At the most basic level, a production request requires the following:

- **Who** - Organization(s) and specific office(s) or individual(s) requesting the product.
- **What** - Statement describing the information and intelligence required.
- **When** - Latest time information of value (LTIOV).
- **How** - Forms that the product should be in (hardcopy text, soft-copy on CD-ROM, etc.) and total quantity of each.

In practice, the same basic format is generally used for RFIs and PRs. This facilitates conversion of an RFI into a PR at a later time if necessary. The key to RFI/PR generation is specificity; the more specific the statement describing the intelligence required the greater likelihood that the requirement will be fulfilled to the requesters satisfaction. This statement should also address sources already consulted by the requester and the specific shortcoming of those sources relative to the question being asked. If a PR is submitted with multiple information requirements or elements, they should be prioritized.

The basic format provided above is sufficient at lower tactical levels, however, at higher levels the format becomes more structured. This is particularly true at the MEF level and higher where it is necessary to effectively and efficiently track and satisfy literally hundreds of IRs, RFIs and PRs. The *Department of Defense Intelligence Production Program: Production Procedures (U),* DoD-0000-151C-95 manual stipulates the format for PRs which ultimately will be forwarded to a DoDIPP VO and production center (see appendix J for format.). Each combatant command will further define formats and procedures in their applicable intelligence TTP documents. Finally, MEF CE and MSC headquarters SOPs will further define formats for their HQs subordinate elements.

(4) Community On-Line Intelligence System for End Users and Managers (COLISEUM). COLISEUM provides an automated capability for the preparation, submission, validation, and assignment of production requirements within the DOD Intelligence Production Community. It allows the requester to research existing requirements and any responses to reduce the submission of duplicate requirements. All commands and production centers with access to COLISEUM have immediate visibility of both existing and new requirements, their status within the validation/production chain, and notification of product completion. COLISEUM is designed (but not limited) to function as an application under the joint deployable intelligence support system (JDISS) program. It is currently available on JDISS 1.01 and JDISS 2.0 under *corporate services*. The IAS will also provide access and capability through incorporated JDISS functionalities. COLISEUM is also available on INTELINK (SCI) under the Defense Intelligence Agency, Directorate of Intelligence Production. At this time, the principal inject sites for Marine Corps FMF production requirements are the MEF and MARFOR G2s. Future plans for extending IAS to MSCs will increase access. Policies and procedures for submitting production requirements via COLISEUM will be governed by MEF, MARFOR, CINC, and DoD policy documents.

(5) Considerations. Deliberate production, whether performed by the A&P Company or DODIPP production centers, is generally a labor and time intensive process. With sufficient lead-time and management, most or all requirements can be fulfilled in a timely and efficient manner. Although crisis production can and does occur, it carries a significant impact on collection, processing and analytical resources; resources which are also heavily tasked with maintaining I&W, situational awareness, and target surveillance for the NCA and numerous command levels involved in the crisis at hand. Although the requirement may be of priority to the requesting unit, it may be of lower priority relative to the CINC's requirements or those of other forces involved. To ensure critical intelligence is available when needed, unit planning staffs and

intelligence officers at all levels should attempt to identify production requirements related to potential contingencies as far in advance as possible.

Chapter 9

ANALYSIS AND PRODUCTION CELL

9001. General

The analysis and production company (A&P Co), intel bn, is the focal point for deliberate intelligence production within the MEF. The A&P company is organized as shown in Figure 9-1. Although all elements of the company contribute to the deliberate production process, the focal point for all-source analysis, OOB, target intelligence, BDA assessments, and deliberate production is the all-source fusion platoon, which during operations forms the core of the analysis and production cell.

Staff Cognizance
(Source: MCWP 6-2, "MAGTF Command & Control)

The broad responsibility and authority over designated staff functions assigned to a general or executive staff officer (or their subordinate staff officers) in his area of primary interest. These responsibilities & authorities can range from coordination within the staff to the assignment or delegation to the staff officer by the commander to exercise his authority for a specified warfighting function or sub-function. Staff cognizance includes the responsibility for effective use of available resources and may include the authority for planning the employment of, organizing, assigning tasks, coordinating, and controlling forces for the accomplishment of assigned missions. Marine Corps orders and doctrine provide the notional staff cognizance for general or executive staff officers, which may be modified by the commander to meet his requirements.

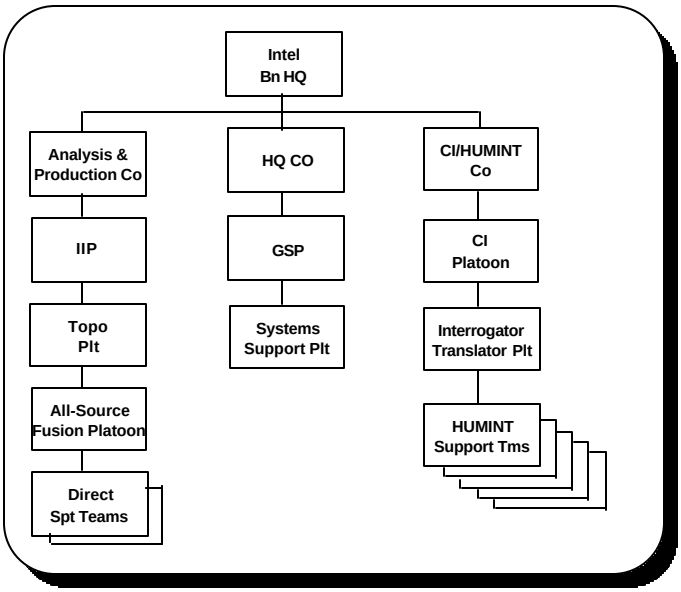

Figure 9-1. Intelligence Battalion Organization

9002. Mission

The mission of the A&P cell is to plan, coordinate, and produce fused all-source tactical intelligence in support of the MEF, its MSCs, and other MAGTFs and commands as directed. The A&P cell, as a consolidated, multi-discipline, closely knit group of intelligence officers and specialists, will provide the intelligence necessary to support contingency planning and current intelligence threat requirements of the MEF, its subordinate MAGTFs, and other commanders as directed. During operations and exercises, the A&P cell will provide the intelligence necessary to support current and future operations, future plans, targeting, and development of enemy situation and capabilities. It will process information and intelligence from both organic MEF collection and reporting as well as that from external commands and intelligence organizations.

9003. Capabilities

The AFP, in conjunction with other elements of the intel bn (particularly the IIP, topo plt, the DSTs, and CI/HUMINT Co) and production elements of radio battalion, force reconnaissance company, VMAQ and VMU squadrons, provides the capability for all-source intelligence analysis and production support to the full range of operations conducted by the MEF and other MAGTFs. A&P cell tasks include the following:

From all available sources, receives, processes and exploits, integrates, analyzes, evaluates, interprets, and synthesizes intelligence and other information into comprehensive, accurate, complete and tailored intelligence products required for the planning and execution of MAGTF

operations.

Provide intelligence support across the conflict spectrum, and in support of deliberate and crisis planning, MAGTF deployments, and other operations as directed.

Provide a dynamic, detailed OOB picture of threats within the MAGTF AO and AI.

Provide detailed intelligence analysis and production support to targeting.

Maintain a MAGTF-wide summation of damages caused to hostile targets and augment BDA efforts of MAGTF elements as required.

Provide MAGTF-level BDA assessments for forwarding to the component, JTF, and/or theater CINC as applicable.

Provide IPB support to the MAGTF G-3/S-3 and G-5 for battle management and planning efforts and provide IPB-related support to MAGTF elements beyond those units' organic capabilities.

Disseminate intelligence products and information to the MAGTF staff and MSCs in a timely, relevant manner.

Establish and maintain intelligence databases to support intelligence analysis and production.

In concert with the collections officer, provide the SARC with collection requirements for MAGTF and external collection units.

In concert with the dissemination manager, coordinate dissemination of intelligence products throughout the MEF and to external organizations.

In coordination with the MEF G-2 and intel bn commander/ISC, ensure the understanding of disseminated intelligence and products, determine whether these have fully answered the PIRs of the commanders and IRs of other users, identify new IPRs that may result from these, and assess the overall effectiveness of intelligence production operations.

9004. Organization

The all-source fusion platoon, as part of the A&P Co, is organized to provide intelligence support to all elements of the MEF command element and the MSCs. It is functionally organized into teams to match the "cellular" organization of the MAGTF staff (see table 9-1).

INTEL BN A&P CO TEAM OR UNIT	MEF CE SUPPORTED CELL
ANALYSIS & PRODUCTION CELL	
ANALYSIS TEAM	G-3 CURRENT/FUTURE OPS, G-5 PLANS & MEF STAFF ELEMENTS
ORDER OF BATTLE TEAM	G-3 CURRENT/FUTURE OPS, G-5 PLANS & MEF STAFF ELEMENTS
TARGET ANALYSIS/BDA TEAM	G-3 TARGETING CELL & ALL MEF STAFF ELEMENTS
INTELLIGENCE PREPARATION OF THE BATTLESPACE TEAM	G-3 CURRENT/FUTURE OPS, G-5 PLANS & ALL MEF STAFF ELEMENTS
OTHER MAJOR A&P COMPANY ELEMENTS	
TOPOGRAPHIC PLATOON	MEF-WIDE
IMAGERY INTELIGENCE PLATOON	MEF-WIDE
DIRECT SUPPORT TEAMS	A&P CELL, G-3 CURRENT/FUTURE OPS, G-5 PLANS, OR DESIGNATED MSC G-2

Table 9-1. Analysis & Production Company Tactical Organization and Support

This organization provides for the analysis and production functions required to support current and future operations, future planning, targeting, and BDA. The internal organization and subordinate teams and units of the A&P cell are:

Analysis and Production Cell Staff: Provides leadership and support functions such as maintenance of the intelligence library. Additionally -- in conjunction with the intel bn's collections management and dissemination officer in the support cell -- is responsible for production & IPR management as well as coordination of IPRs with intel bn's overall IR collection and dissemination .

Analysis Teams (2): Composed of all-source analysts, and specialists from other disciplines such as medical, weather, CI/HUMINT, imagery, terrain, and SIGINT. With support from other elements of the A&P Co, the rest of intel bn, radio battalion, force reconnaissance, VMU, VMAQ, and MSC G-2 intelligence analysts, this team produces integrated all-source

intelligence products such as contingency studies, intelligence estimates, intelligence summaries, briefings, and other intelligence studies of a more focused nature but requiring a multi-discipline intelligence approach.

Order of Battle Teams (2): These teams analyze and maintain a detailed, comprehensive, evolving picture of ground, air, naval, electronic, WMD and other threats within the MAGTF AO and AI. The OOB teams perform the specific analysis of threat organization, disposition, training, leadership, etc., which are the components of OOB analysis. Primary products include graphic or electronic situation overlays, OOB databases and files, and threat models for various threat elements.

Target Analysis and BDA Teams (2): These teams focus on detailed analysis of targets identified by the MAGTF commander, his staff, and MSCs which are not destined for the air tasking order (ATO). Target and BDA analysis and intelligence support for ATO-nominated targets are generally managed by the MAW G-2 section. These teams provide the full range of target development and analysis to support the deliberate and reactive targeting efforts of the MAGTF. The BDA elements also maintain the comprehensive picture of battle damages caused to targets and prepares the BDA reports and assessments which support the MEF combat assessment effort.

IPB Teams (2): These teams focus on IPB production support to the MEF G-3 and G-5 in the areas of current battle management and future planning. They also assist subordinate units intelligence personnel with IPB-related production when requirements are beyond the organic capabilities of that unit.

Direct Support Teams (2): Allows enhanced IR management, intelligence analysis and production, and dissemination capabilities to be focused down to one or more MSCs.

The A&P cell is essentially organized in garrison as it would be organized for operations. Each team has the flexibility to add intelligence and non-intelligence (e.g., Red Cell members) specialists from other intelligence and reconnaissance organizations as required based on the specific mission and intelligence needs of the MAGTF. For sustained MEF-level operations, global sourcing from other Marine Corps organizations may be required to augment the current A&P Co team structure and provide sufficient personnel depth for 24-hour operations. To support this, all three active AFCs are organized in a virtually identical manner and share common intelligence operational and organizational concept of operations and employment in order to facilitate the attachment and immediate integration of additional platoons or teams from a uncommitted MEF's intel bn.

9005. Supporting Organizations

Several organic MAGTF intelligence organizations support the A&P cell analysis and production effort by contributing specialized MAGTF intelligence expertise and resources. The intel bn commander, in his staff capacity as the ISC, is directly responsible to the MEF AC/S G-2 for overall MEF IR

management, developing the MEF intelligence concept of operations, determining collection, production and dissemination priorities, taskings and supporting plans, and exercising C2 staff cognizance (see definition in figure 9-2 below) of supporting intelligence and reconnaissance organizations to ensure unity of effort and production of all-source intelligence (see paragraph 9006, *Concept of Employment*, below). These supporting organizations do not normally produce their own products beyond certain intelligence discipline unique products, but instead contribute to fused, all-source MAGTF intelligence products. The following supporting intelligence and reconnaissance organizations provide significant specialized support to the A&P cell analysis and production effort.

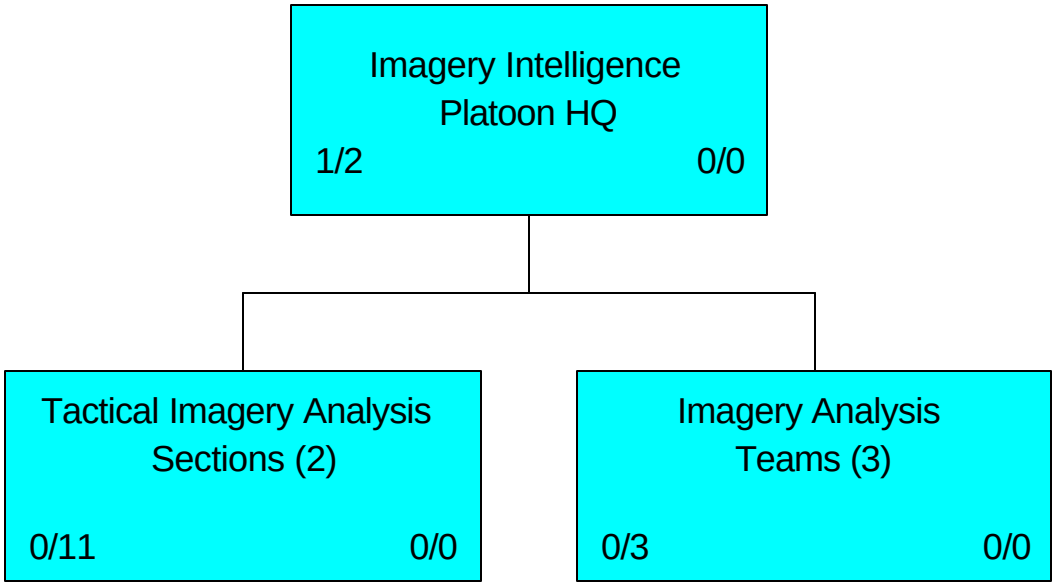

Figure 9-2. Definition of *Staff Cognizance*

a. Imagery Intelligence Platoon, A&P Co. The IIP provides imagery interpretation support for all MEF requirements and maintains the imagery database and imagery library for the MAGTF. The IIP is capable of providing IMINT derived from all available sources of imagery in support of MEF A&P cell products. This includes annotated imagery in support of MEF A&P cell production or in response to separate IRs. A key imagery exploitation resource organic to the IIP is the tactical exploitation group (TEG; it is an element of the broader joint service imagery processing system). The IIP will normally concentrate on the exploitation of imagery and production of IMINT from MEF, JTF and other tactical resources such as UAVs or the F/A-18D (RC) advanced tactical aerial reconnaissance system (ATARS). Figure 9-3 shows the organization of the IIP.

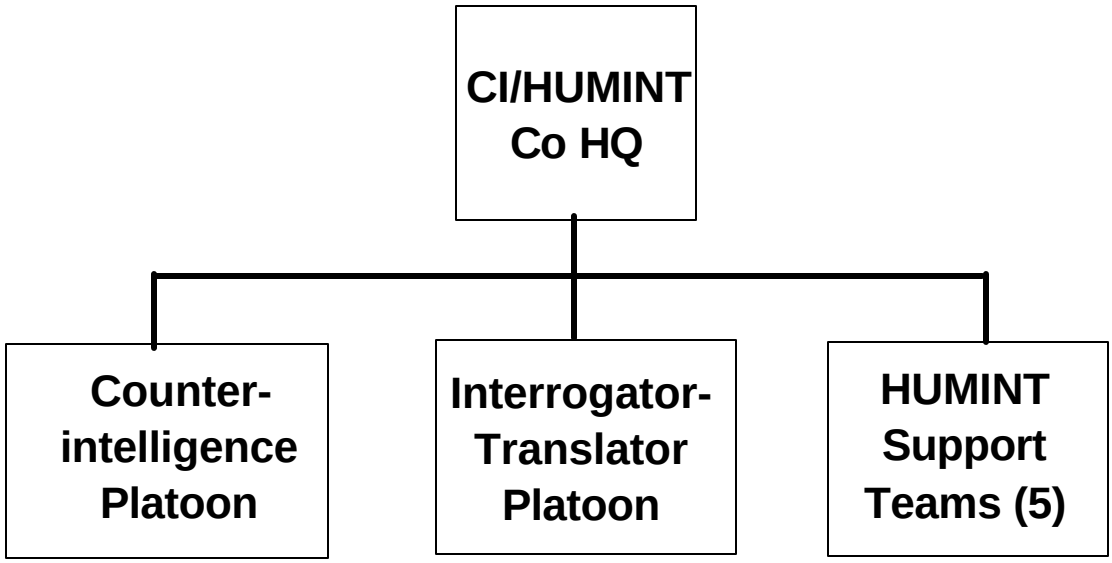

Figure 9-3. Imagery Intelligence Platoon Organization

b. Marine Corps Imagery Support Unit (MCISU). This unique organization is currently assigned to the 1st Intelligence Battalion and OPCON to the CG, I MEF. More specifically, it operates daily in general support of all Marine Corps operating forces and may be tasked with providing direct support to designated MAGTFs. The MCISU is responsible for production of imagery and imagery-derived products based on the exploitation of national imagery. In conjunction with the support MEF's IIP (or a MEU(SOC)'s imagery analysis detachment), and as directed by the MAGTF G-2/S-2 and the intel bn commander/detachment OIC, the MCISU will complement and support the full range of imagery exploitation and production requirements of the A&P cell and supported MAGTFs. Products may be posted to an imagery server for electronic retrieval, or disseminated directly via electronic means. The key resource utilized by the MCISU is the joint service imagery processing system, national input segment (JSIPS/NIS). Figure 9-4 shows the organization of the MCISU.

Combat Intelligence Center (CIC)—overarching intelligence operations center established within the MEF main command post. Encompasses the primary functions of the MEF intelligence section and Intelligence Battalion. It includes the sub-elements listed below.

Intelligence Operations Center (IOC)—principal MEF intelligence operations and C2 center that is established by Intelligence Battalion. Performs intelligence requirements management, planning and direction of MAGTF intelligence operations and their integration with those of external organizations, staff cognizance of ongoing organic and supporting collection operations, intelligence analysis and production, and intelligence dissemination.

*** Support Cell**— primary element for conducting MEF-wide intelligence requirements management; weather support; collections and dissemination planning and direction; and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.

*** Analysis and Production Cell**—primary analysis and production element of the MAGTF. Processes and produces all-source intelligence products in response to requirements of the MAGTF. Additionally, principal IMINT and GEOINT production element of the MEF.

*** Surveillance and Reconnaissance Cell (SARC)**—primary element for the supervision of MAGTF collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.

*** CI/HUMINT Company Command Post**—primary element for conducting CI/HUMINT planning and direction, command and control, and coordination of MAGTF CI/HUMINT operations with external CI/HUMINT organizations.

G-2 Operations—main element of the G-2 section for coordinating and providing intelligence support to the MEF CE CG, battle staff and current operations center elements; target intelligence support to the force fires and future operations; G-2 section intelligence requirements management activities; Red Cell support; and MEF intelligence liaison with external commands and organizations.

G-2 Plans—main element of the G-2 section for coordinating and providing intelligence support to the MEF CE future plans team; and leadership and direction of the G-2 section's imagery and mapping, SIGINT, and weather sections.

OCAC—main node for the C2 of radio battalion SIGINT operations and the overall coordination of MAGTF SIGINT operations. Processes, analyzes, produces, and disseminates SIGINT-derived information and directs the ground-based electronic warfare activities of the radio battalion.

Figure 9-4. MCISU Organization

c. Topographic Platoon, A&P Co. The topo plt provides geospatial information (GI) and geographic intelligence (GEOINT) support for all MAGTF requirements. The platoon is capable of integrating, deconflicting, analyzing, and disseminating theater, service, and national geospatial databases for the MAGTF. The topo plt is capable of providing GEOINT and specialized mapping, graphics and other GI&S services and GEOINT products in support of A&P cell all-source intelligence products. They are key participants in the IPB process. They may produce independent GEOINT studies in response to separate requirements. The topo plt and IIP work closely as both use many of the same baseline intelligence data and sources for production (see paragraph 9006, Concept of Employment). Figure 9-5 shows the organization of the topo plt.

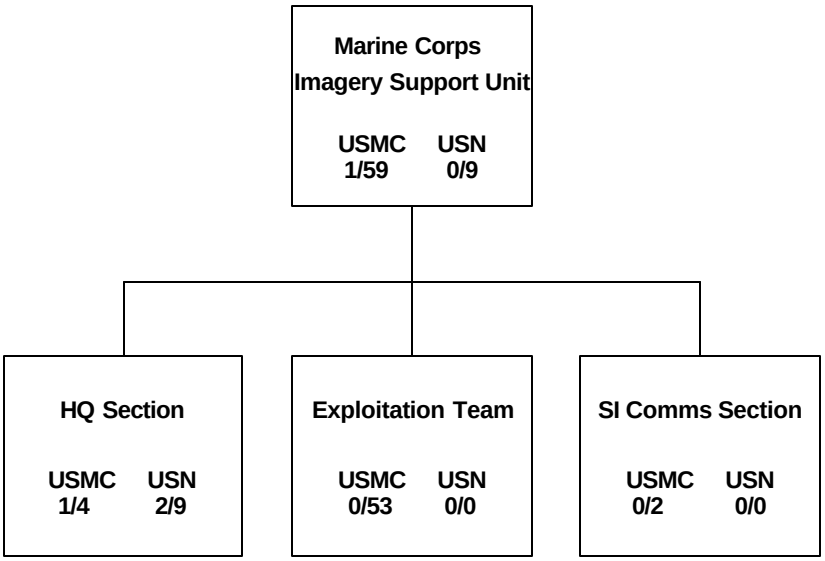

Figure 9-5. Topographic Platoon Organization

d. Counterintelligence and Human Intelligence (CI/HUMINT) Company, Intelligence Battalion. The CI/HUMINT Company is responsible for the development and maintenance of the MEF CI estimate and the reporting information and production of intelligence derived from human source exploitation, to include interrogations of enemy prisoners of war (EPW), refugees, and displaced persons, counterintelligence operations, and human source operations. Information may also be derived from exploitation of captured documents or materiel. Specialized CI or force protection assessments may also be produced in support of A&P cell production or in response to specific IPRs.

Figure 9-6 shows the organization of CI/HUMINT company.

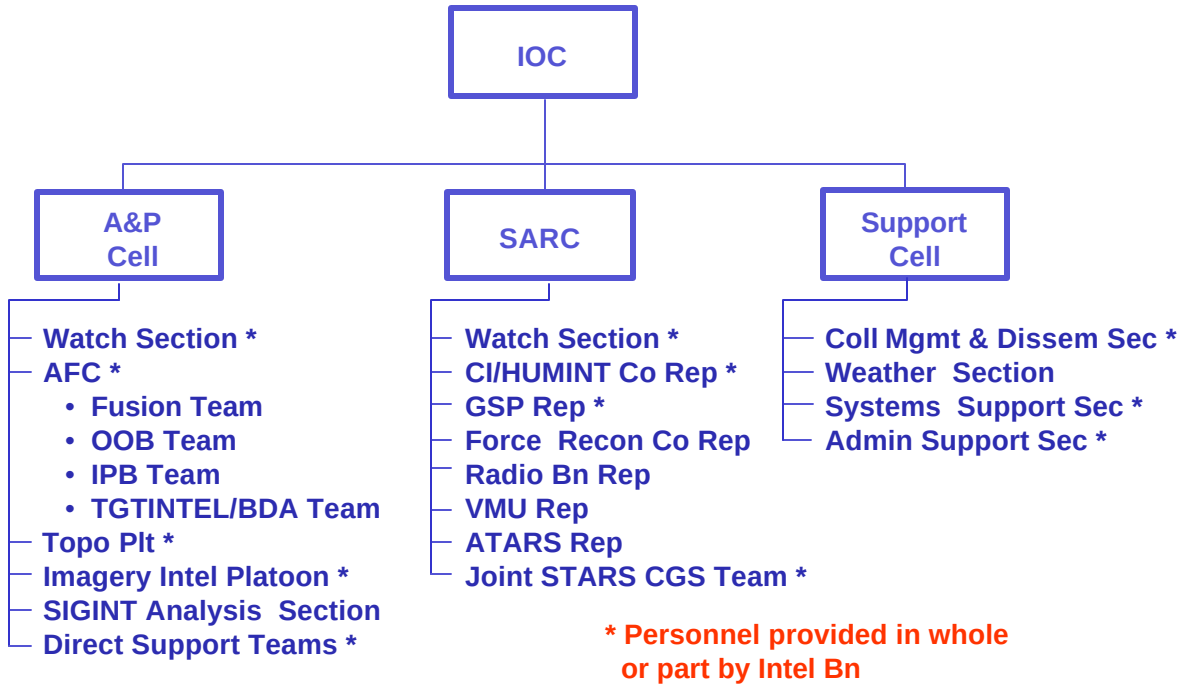

Figure 9-6. CI/HUMINT Company Organization

e. Radio Battalion Operational Control and Analysis Center (OCAC). The radio battalion OCAC provides the principal MEF SIGINT analytical and production support to all MEF IRs. Rad Bn, under the staff cognizance of the ISC, generally will be tasked with responsibility to maintain the MAGTF EOB and SIGINT databases and provide SIGINT analytical and production support to A&P cell production. Time-sensitive SIGINT and product reporting will be provided to various units in the MAGTF in accordance with intelligence reporting criteria and the MAGTF intelligence dissemination plan developed by the ISC.

f. Marine Tactical Electronic Warfare Squadron (VMAQ). In conjunction with the MAW G-2, VMAQ is responsible for the processing, analysis, and production of routine and time-sensitive ELINT reports resulting from EA-6B operations. The resulting information and intelligence is used to help update and maintain the threat EOB which is used in the planning and execution of aviation and other MAGTF operations. A threat's EOB and the location of electronic emitters in the battlespace are important indicators of threat dispositions, capabilities and intentions.

g. Force Reconnaissance Company. The mission of the force reconnaissance company is to conduct amphibious reconnaissance, surveillance, and limited-scale raids in support of the MEF, other MAGTFs, or JTFs as directed. Regarding intelligence production and under the staff cognizance of the ISC, force reconnaissance company conducts specialized terrain reconnaissance and prepares products to support hydrographic, beach, roads, bridges, routes, urban areas, HLZs, DZs, landing craft air cushion (LCAC) LZs, and aircraft forward operating sites intelligence studies.

9006. Concept of Employment

a. MEF CE Combat Intelligence Center (CIC). The A&P cell as, part of the Intelligence Battalion, will function when deployed (and possibly in garrison) as part of the MEF CE's CIC. The key CIC elements (see figure 9-7 below) are designed to provide tailored, yet flexible, intelligence C2 and functional capabilities to meet the MEF and all subordinate commander's IRs and supporting intelligence and reconnaissance operations.

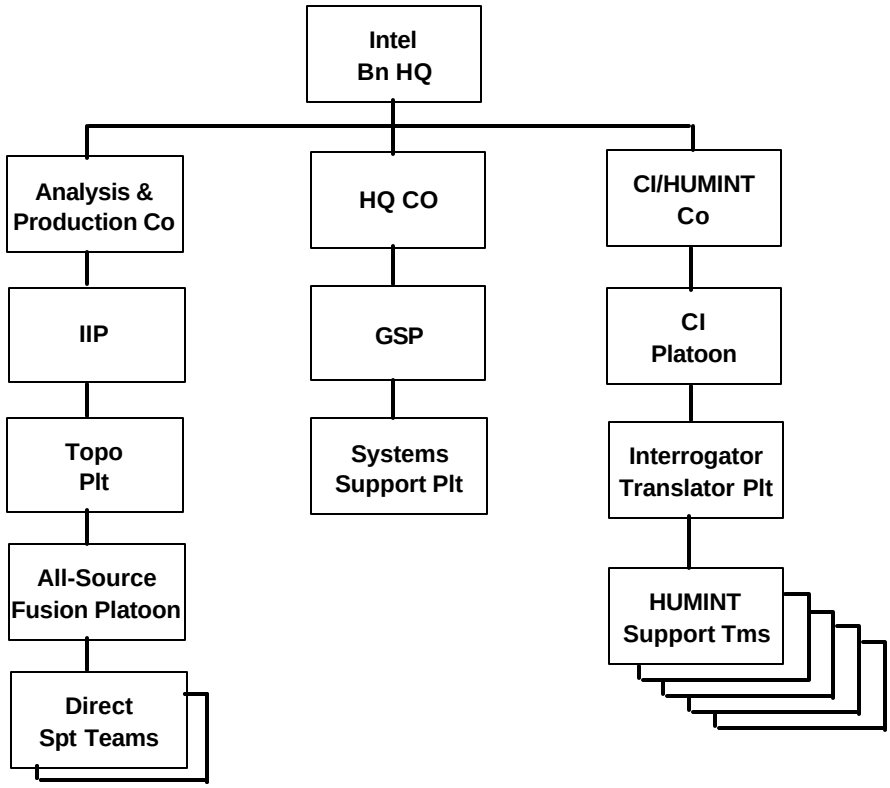

Figure 9-7. MEF CE's Combat Intelligence Center and Intelligence Battalion's Intelligence Operations Center Key Elements

The MEF AC/S G-2 focuses on overall C2 and direction of MEF intelligence and reconnaissance operations. He exercises staff cognizance C2 of intel bn, radio bn, force reconnaissance company, and other MEF intelligence and reconnaissance assets. Within this C2 authority, the intel bn commander, in his role as the G-2's Intelligence Support Coordinator performs MEF wide IR management, develops, integrates and manages all supporting intelligence plans, and then supervises their execution These plans encompass the MEF-wide organic efforts for the collection, processing, production, and dissemination activities of intelligence and reconnaissance operations. As described above and shown in figure 9-8 below, the intel bn commander/ISC is responsible for the establishment and operations of the IOC.

ISC	G-2 Ops O	G-2 Plans O	Intel & Recon Units COs
-- Planning & execution of intel ops to support all MEF IRs	-- Intel support to MEF CE battlestaff & current ops center agencies	-- Intel support to the future planning team for future planning IRs	-- Command of unit consistent with ISC staff cog & taskings
-- Est & direct the IOC (A&P Cell, SARC, & Support Cell)	-- Coord & support to higher & adjacent HQs & agencies	-- Recommends validation, prioritization & tasking to AC/S G-2	-- Est & direct: OCAC; ROC; others as approp
-- IR mgmt (coll, prod & dissem) validation, pri's & tasking (includes staff cog of designated G-2 elements)	-- Recommends validation, prioritization & tasking to AC/S G-2	-- Est & direct future planning intel element	-- Coord & spt G-2; Intel Bn; higher, adjacent & subordinate HQs
-- Intel ops command of Intel Bn and Staff Cog over RadBn, Force Recon, UAV Sqd & others as appropriate	-- Est & direct COC intel element, Tgt Intel Sec, FOC, Red Cell, intel LnOs	-- G-2 section's imagery & GI , CI/HUMINT, SIGINT, & Wx Sections (less that under staff cog of the ISC)	-- Coll, some Prod, Dissem, & C2

Figure 9-8. Intelligence Battalion's Intelligence Operations Center Organization and Functions

b. Request Procedures and Intelligence Production Support Flow

Requests for intelligence production support from the A&P cell, or any other MEF intelligence or reconnaissance element, must be validated and forwarded via the chain of command to the MEF G-2 for validation, prioritization and tasking. The intelligence battalion commander, in his role as ISC, generally will perform this function for the G-2.

The intelligence battalion commander will, upon approval by the AC/S G-2, use these prioritized ICRs, IPRs and IDRs for planning and direction, follow-on taskings to MEF organic and supporting intelligence and reconnaissance units, C2 and execution. The ISC's overall intelligence production staff cognizance relationships and resulting A&P cell intelligence production support flow are as indicated in figure 9-9.

Figure 9-9. Senior Intelligence Staff Officers Relationships and Intelligence Production Support Flow

Figure 9-10 highlights the key responsibilities, roles and tasks of key MEF senior intelligence staff officers and intelligence and reconnaissance units commanders.

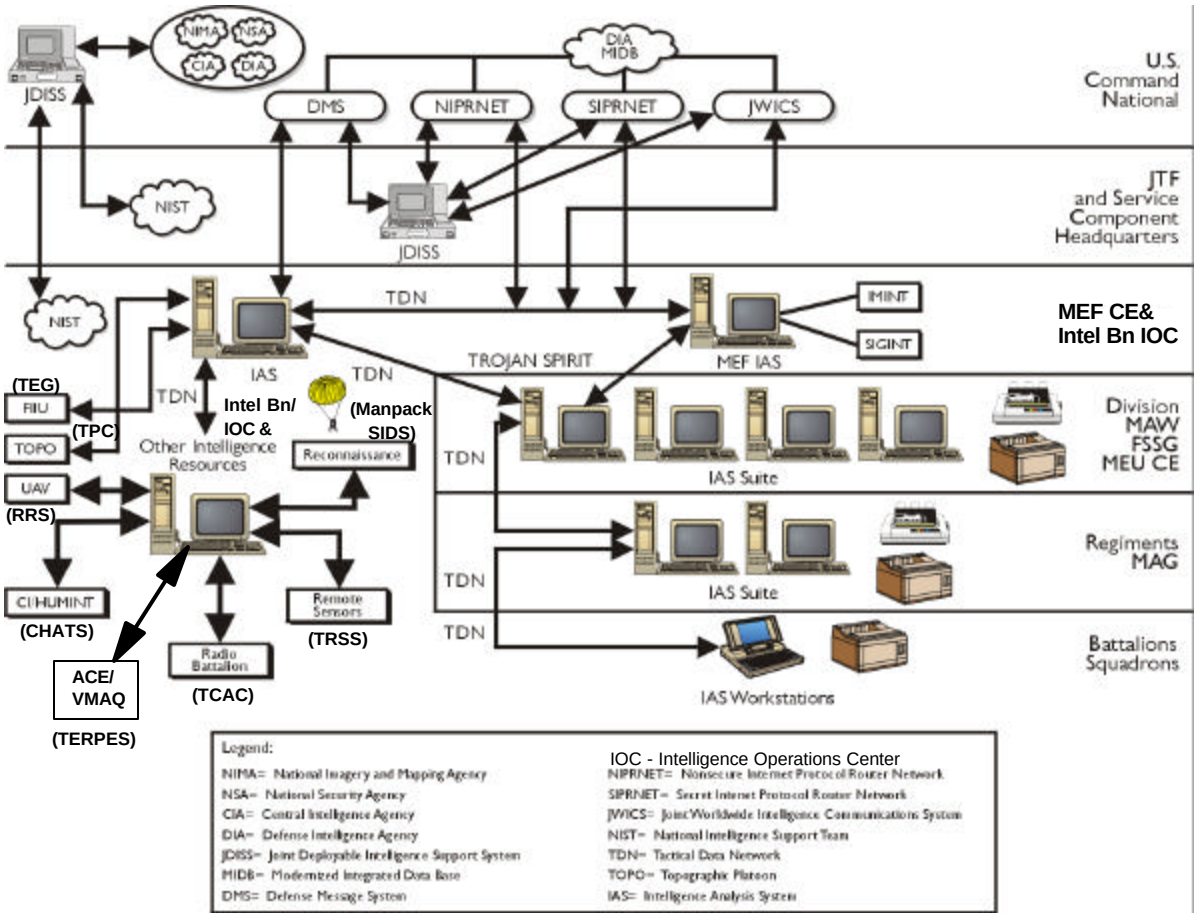

Figure 9-10. Senior MEF Intelligence Staff Officers and Intelligence and Reconnaissance Unit Commanders Responsibilities, Roles and Tasks

See chapter 8 for a detailed discussion of intelligence production and production management.

c. Garrison or Pre-Hostilities Operations. The intel bn and its A&P cell tailor their day-to-day garrison operations to support the IRs of the commander, his staff, and the MEF subordinate units. With minor adjustments, the organization and garrison functioning of the A&P cell will facilitate the transition from pre-hostilities to crisis or combat operations. In practice, the A&P cell supporting each MEF will be organized based on the prospective missions of that MEF and the corresponding potential areas of operation.

d. Contingency or Combat Operations. During contingency or combat operations, the A&P cell will continue to function as part of the MEF CE's CIC and the intel bn's IOC. The A&P cell may also be tasked to provided limited personnel support to an intelligence node or cell with the MEF lead (also called MEF(fwd)) or tactical echelons. In such cases the intelligence component of these command echelons will contain a limited analysis and production capability focused on providing the commander with situational awareness, with the A&P cell providing the majority of intelligence analysis and production support for each. Both the lead and the tactical echelons' intelligence nodes are heavily reliant on electronic CIS connectivity to allow reach back to the more robust and capable analytical and production resources of the MEF and intel bn.

e. Detachments. The A&P cell may be tasked to provide personnel to support intel bn detachments provided to subordinate commands, MEU(SOC) and other MAGTFs, or separate units. Each A&P cell contains within its T/O two DSTs which can be used to augment the IR management, analysis, production, and dissemination capabilities of the supported unit. DSTs can be employed by the MEF AC/S G-2 or ISC to focus intelligence planning, direction, analysis, production and dissemination support to the main effort or other specified MEF priority. When not so assigned, the DSTs will be integrated within other A&P cell or intel bn operations.

When a MAGTF of less than full MEF size is deployed, the A&P cell may contribute personnel to a task-organized intel bn detachment that will normally be attached to the MAGTF or SPMAGTF command element. A common example would be the detachments currently provided to MEU(SOC) CEs, although those detachment historically have do not included elements from the A&P cell.

9007. Communications and Information Systems

a. Basic IMINT CIS Requirements. The following identifies the standard intelligence production CIS requirements for any MAGTF operation:

(1) The Capability to Command and Control Subordinate Units. Intelligence officers and intelligence production element commanders/OICs must be capable of positive C2 of subordinate units and integration of their operations with broader MAGTF and external intelligence and operations C2. Traditionally single-channel radio (SCR) and record message traffic have been used to support C2 of MAGTF intelligence units, particularly at echelons below the MSCs level. At the MSC/MSE, MAGTF CE and higher command echelons, high capacity communications networks now are the principal means supporting intelligence production C2, operations, and product dissemination. In semi-static situations, secure e-mail or telephone will also provide significant communications capabilities, while in highly fluid or mobile scenarios, cellular, SATCOM, and VHF and HF radio may be used.

(2) The Ability to Receive Collected Data, Information and Intelligence from the Full Range of Organic and External Intelligence Organizations and Production Elements. The CIS architecture must provide connectivity between organic and supporting intelligence units and production elements. This requirements includes: the capability to transmit imagery, GEOINT and other

intelligence products with large data files; the capability to disseminate IMINT reports digitally via fiber-optics, wire, or radio formats; and the capability to disseminate products in voice formats. Which means will be the principal and alternates are METT-T dependent; regardless, these means will be influenced significantly based upon the desired formats of all supported commanders and other intelligence users.

(3) The Ability to Provide Intelligence to Supported Commanders. Intelligence production CIS requirements will be influenced by supported commanders' intents, concepts of operations and intelligence, command relationships, and standing PIRs and IRs. The CIS architecture must be capable of integrating all production elements' C2 and supporting CIS operations (to include both GENSER and SCI communications) with the primary CIS channels used by all supported commanders. In addition to the above requirements for the capability to transmit imagery, GEOINT and other intelligence products with large data files, this CIS requirement includes: the capability to disseminate SCI and GENSER all-source and intelligence discipline unique reports digitally via fiber-optics, wire, or radio formats; and the capability to disseminate products in voice formats. Which means will be the principal and alternates are METT-T dependent; regardless, these means will be influenced significantly based upon the desired formats of all supported commanders and other intelligence users.

(4) The Ability to Share Intelligence Products and Reports with All-Source JTF, Other Components, Theater, National, and Multinational Intelligence Organizations, Agencies and Centers. The traditional means for providing this capability are MAGTF GENSER secure record and voice communications. While these techniques continue to be used, for MAGTF intelligence production they are now secondary in importance to the use of JWICS, SIPRNET, and other CIS capabilities which allow participants to access each others' intelligence products and databases and to immediately pull required data, intelligence and other products. Finally, this CIS requirement includes the capability to disseminate intelligence with designated non governmental organizations, private voluntary organizations, and other U.S. and multinational governmental agencies -- particularly during MOOTWs.

b. Communications. The intel bn, A&P cell, their subordinate elements, and other key intelligence producers such as radio battalion have sufficient communications resources to support internal command and control, operations, and intelligence requirements support. Communications capabilities generally consist of short- and medium-range voice communications equipment. Intel bn and its subordinate units, however, have no dedicated communications personnel. Intel bn communications requirements beyond those discussed above must be provided by the communications battalion or, in the case of intel bn detachments, by the supported unit's communications element.

c. Information Systems. Information systems such as IAS and their associated networks are the lifeblood and lifelines of the A&P cell and the MAGTF intelligence analysis, production, and dissemination operations. Intel bn has sufficient information systems resources to satisfy internal C2, operations and intelligence needs. The vast majority of these will require access to the SECRET internet protocol router network (SIPRNET) for GENSER requirements, and to the joint worldwide intelligence communications system (JWICS) for SCI requirements, in order to provide intelligence and databases access to all MAGTF elements, JTF and other components elements, and theater and

national intelligence reporting and databases. The non-secure internet protocol router network (NIPRNET) is also a key resource for intelligence analyst research and access to public domain information, as well as a means to exchange unclassified information. The necessary network connectivity will need to be provided by the supporting MEF communications battalions (for GENSER information networks and all communications pathways) and radio bn (for SCI networks). Figure 9-11 illustrates the MEF's intelligence processing, analysis, production, and dissemination communications and key intelligence all-source (e.g., IAS) and intelligence discipline unique (e.g., radio bn's TCAC, FIIU's TEG, SCAMP's TRSS, CI/HUMINT Co's CHATS, VMAQ's TERPES) information systems architecture and resources.

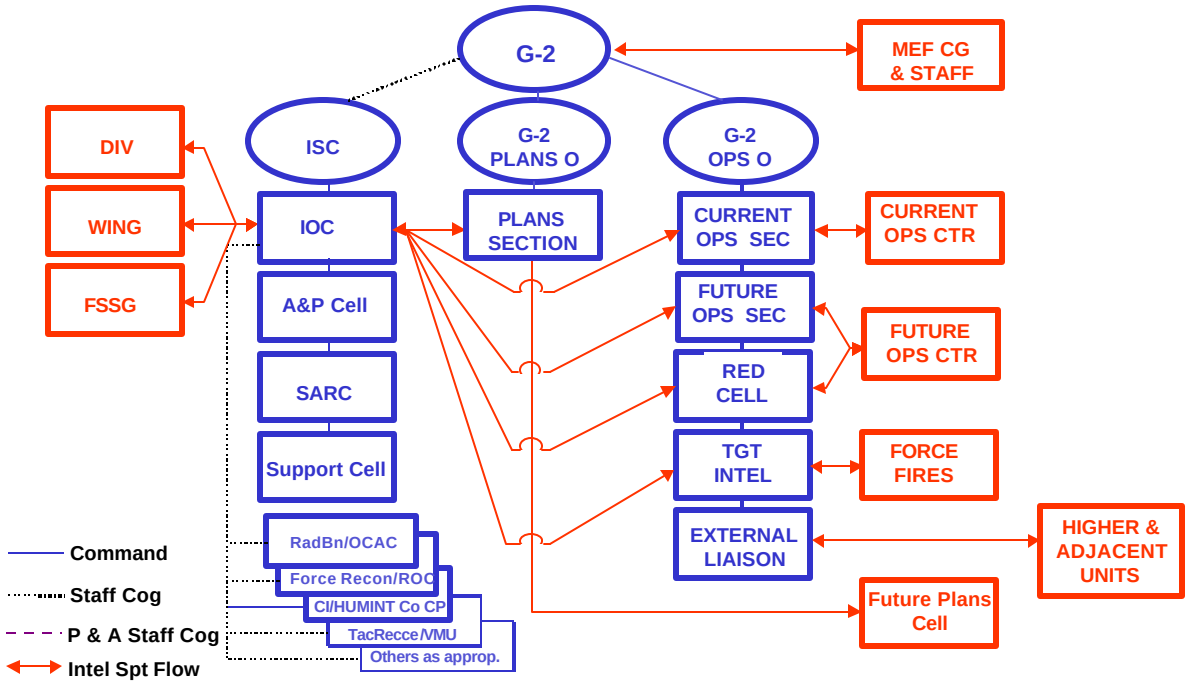

Figure 9-11. MEF Intelligence Processing, Analysis, Production, and Dissemination Communications and Information Systems Architecture

Chapter 10

ANALYSIS AND PRODUCTION IN MAGTF OPERATIONS

10001. Overview

Intelligence enables the planning and execution of successful operations. MAGTF operations are characterized by unity of effort, high tempo, timely decisionmaking, rapid execution, and the relentless exploitation of decisive opportunities. MAGTF intelligence analysis and production must have the flexibility, agility, and sustainability to support these types of operations. MAGTF operations are expeditionary in nature and are conducted in accordance with the Marine Corps's maneuver warfare and emerging operational concepts of::

- **Operational Maneuver From The Sea (OMFTS).** The maneuver of naval forces at the operational level that projects seabased power ashore to deal a decisive blow at a place and time of our choosing. OMFTS is focused on operational objectives and embodies the application of the principles of maneuver warfare to a maritime campaign.

- **Sustained Operations Ashore (SOA).** Those campaigns in which MAGTFs fight as seabased operational maneuver elements (OME). Embracing the tenets of OMFTS, SOA envisions a series of operational-level missions designed to enhance the joint force campaign and exploit weaknesses exposed in the opposing force. Normally, SOA will involve a MEF assigned to a much larger joint/combined force.

- **Military Operations Other Than War (MOOTW).** The conduct of Marine and naval expeditionary operations across the range of military operations short of war. MOOTW encompasses a wide variety of activities intended to deter war, resolve conflict, promote peace, and support civil authorities.

Each category of operation presents unique challenges and considerations for intelligence support. In addition, all MAGTF operations are likely to be conducted in the context of a joint operation and many will be executed in conjunction with our allies; intelligence activities in joint and combined operations require special planning and coordination.

10002. Intelligence Analysis and Production in OMFTS

Success in OMFTS depends on the ability to seize fleeting opportunities and quickly take advantage of enemy vulnerabilities. Emphasis is placed on deception, surprise, speed, and battlespace preparation to create delay, uncertainty, and ineffectiveness in enemy actions. Intelligence provides the knowledge and understanding which enables the effective conduct of OMFTS. OMFTS is characterized by:

- Widely dispersed forces utilizing the sea as maneuver space.

- Ship-to-objective maneuver.

- Independence from established beachheads or shore bases.

- Seabased C2 and sustainment.

OMFTS relies on intelligence to drive planning, COA development, wargaming and selection, and execution. Intelligence discovers the enemy's center(s) of gravity, strengths, and weaknesses, exposing critical vulnerabilities to be exploited by naval forces operating from the sea. Intelligence also assesses the potential for maneuver offered by the battlespace, to include identifying entry points where the force can establish itself ashore.[1] Intelligence also provides the foundation for effective force protection and command and control warfare (C2W) efforts; these efforts facilitate the preservation of surprise and the employment of deception to disrupt and disorient the enemy during the execution of OMFTS.

a. Requirements. OMFTS requires the following intelligence analysis and production support:

- IPB and situation development covering a broad air, sea, and land maneuver space.

- Threat analysis focused on determining centers of gravity and critical vulnerabilities.

- Detailed terrain and hydrographic analysis to identify suitable entry points and to support maneuver of widely dispersed combat and CSS elements.

- Responsive processing, analysis, and production capabilities which can rapidly develop the critical intelligence required to shape operational and tactical decisionmaking and provide the intelligence segment of the common operation/tactical picture.

- In-depth intelligence support of force protection and C2W activities.

- Detailed information regarding local resources (POL, water, etc.) that may be exploited by the MAGTF in order to reduce ashore sustainment requirements.

Although these requirements appear similar to the traditional requirements for support to amphibious operations, there are differences. First and foremost is the large potential area of operations; at this time envisioned as up to 200NM from the seabase. Points of entry may be widely dispersed instead of being grouped into a single force beachhead. The seaspace becomes a maneuver area for LCACs and AAAVs transiting to the shore from well over the horizon, requiring extensive and detailed hydrographic analysis over a larger area. OMFTS forces rely on rapid maneuver for maximum effectiveness and survival, thus detailed and accurate analysis of

---

[1] The term entry point encompasses beaches, boat landing sites, craft landing sites, HLZs, DZs, ports and airfields that can be used to introduce elements of the force ashore.

terrain becomes important at every level. OMFTS envisions dynamic, precision fires at maximum engagement ranges, which in turn will require precise targeting data and BDA. All of this must occur in real or near-real time and be available to virtually every unit and element of the MAGTF simultaneously. OMFTS products will increasingly consist of data of all forms which can be rapidly updated and displayed in graphic form on automated information systems used by units, staffs and decisionmakers.

b. Analysis and Production Support During OMFTS Planning. Initial production efforts are directed at providing an extensive description of the battlespace and threat required to focus the planning effort. Under the direction of the senior Navy and Marine intelligence officers, the MAGTF, MSC, Naval Expeditionary Force (NEF), amphibious staff, and ship's intelligence sections engage in a collaborative effort to plan and execute intelligence and reconnaissance operations necessary to support development of intelligence products that support the entire force. Individual intelligence sections will normally concentrate on their particular areas of expertise, satisfying their units' requirements while contributing a broad-scope product to the general production effort. For example, the MAGTF G-2 CIC/AFC may focus on describing the battlespace and the enemy's C2, logistics, and reserves while the GCE studies the enemy ground forces, the NEF and ACE look at the air and air defense threats, and the Navy intelligence staffs concentrate on the naval, sea mine, and coastal defense threat. National, theater, and adjacent component resources are tapped via reach back to augment those organic to the OMFTS force. From this effort, the amphibious task force intelligence center (ATFIC) provides a comprehensive IPB analysis, intelligence estimate, HVT list, and supporting intelligence studies. As the planning phase continues, production efforts concentrate on identifying enemy vulnerabilities to be exploited, providing IPB products, HPTs and intelligence estimates to support specific courses of action under consideration. In the final stages of the planning process, the production effort shifts to development of mission-specific intelligence products focused on the selected COA(s). These products include IPB graphics, point of entry studies, and target/objective studies. In addition, an extensive all-source intelligence effort is conducted to support deception, OPSEC, psychological operations (PSYOP), and EW planning in accordance with the commander's information operations or C2W strategy. During this stage, the production effort becomes increasingly decentralized as MSC and subordinate element intelligence sections focus on the specific requirements of their units. The MAGTF intelligence section continues to provide products to support the entire force, with efforts concentrated on elements designated as the main effort.

c. Analysis and Production Support During Execution. During the execution phase, emphasis is placed on rapid processing and production of intelligence that supports timely decisionmaking, enhanced situational awareness, and engagement of HPTs. OMFTS depends upon decisive action and the generation of operational tempo to break the enemy's cohesion and ability to resist; intelligence sections must demonstrate the flexibility, agility, and responsiveness to recognize threat vulnerabilities and identify opportunities as they develop during the battle. To do this, intelligence sections at all levels must be aware of ongoing operational and tactical activities and potential threat actions/reactions. They must be able to rapidly integrate all-source intelligence information with sensor data and combat reporting to develop a coherent, timely and tailored picture of enemy dispositions and an assessment of his intentions and capabilities. Once developed, they must be able to rapidly convey this picture and assessment (preferably in graphic

form) to commanders in time to exploit identified opportunities. In addition to supporting the ongoing battle, intelligence sections must also be fully engaged in planning for future operations -- continuing IPB analysis, delivering BDA results, satisfying new intelligence requirements, and participating in the decisionmaking process.

10003. Intelligence Analysis and Production in SOA

SOA require broad-based intelligence support which bridges the operational and tactical levels. Tactical plans are based upon the results of operational level intelligence assessments, which identify the enemy's center(s) of gravity and critical vulnerabilities across the entire theater. In SOA, MAGTF intelligence operations contribute to the operational level assessments while translating the conclusions from those assessments into relevant tactical intelligence. Considerations for the development of intelligence in support of SOA are similar to those for OMFTS. Intelligence support during the execution of SOA requires the same agility and responsiveness as in OMFTS, with the focus on providing critical intelligence to support tactical decisionmaking. However, SOA are normally conducted over a greater area and with a larger size force than in OMFTS, creating the requirement for a larger and more widely distributed intelligence operations support structure. The potential for integration with theater, allied, and other service intelligence assets is also greater.

a. Requirements. SOA requires the following analysis and production support:

- IPB and situation development in support of both operational and tactical level planning.
- Processing, analysis, and production capabilities which can provide the extensive products required to support a MEF potentially composed of multiple USMC, other service, and allied ground, air, and service support elements, both during planning and execution.
- Area specialists and linguists with skills pertinent to the area of operations.
- Support to extensive force sustainment operations through the provision of detailed intelligence regarding infrastructure.
- Support to force protection efforts conducted throughout an extensive operating area, with emphasis on the security of critical rear area C2 and logistics facilities.

While OMFTS is focused on operations from a seabase, SOA entails large-scale, potentially long-term, land operations supported from the sea. While analysis and production in OMFTS is heavily tasked with identifying points of entry, SOA has a greater focus on infrastructure related to sustaining a large force. Analysis of threat centers of gravity and vulnerabilities, detailed terrain studies, precise targeting data and BDA all remain requirements under SOA.

b. Analysis and Production in Support of SOA. Analysis and production efforts in support of SOA parallel those for OMFTS. Initial production is broad in scope, with the focus narrowing as particular COAs are selected and a concept of operations developed. In SOA,

geographic intelligence production takes on added importance; opportunities for ground and air maneuver as well as line-of-sight profiles for observation, weapons employment, and the operation of communications-electronic equipment are major considerations. Mapping enhancements, lines-of-communication studies, and IPB graphics such as cross-country mobility, weather effects, and combined obstacle overlays are key products. Threat analysis must be comprehensive, and generally deals with large ground and air formations; this analysis covers reserves as well as committed forces and must take into account all factors which impact the enemy's ability to fight at the operational and tactical levels such as leadership, doctrine, training, readiness, and sustainability. In addition, an extensive production effort is devoted to supporting logistics operations; the main components of this effort are studies on the local climate, infrastructure, and resources as well as the threat to the rear area. Products from national, theater, and joint force intelligence agencies contribute to the production effort, but many of these products will have to be tailored by the intel bn's P&A Co, other intelligence producers, and the MSCs' intelligence sections to satisfy particular MAGTF requirements. During execution, emphasis is placed on rapid processing and production of tactical intelligence to support operational decisionmaking in the current battle, while at the same time providing detailed intelligence to shape plans for future operations.

10004. Intelligence Analysis and Production in MOOTW

MOOTW encompasses a broad range of missions and tasks, each with their own unique intelligence requirements. Potential MOOTW missions include:

- Humanitarian assistance and disaster relief (HA/DR)
- Noncombatant evacuation operations (NEO)
- Maritime intercept operations (MIO)
- Show of force
- Strikes and raids
- Peace operations, including peace enforcement (PE) and peace keeping (PK)
- Support to counternarcotics (CN) operations
- Recovery operations

Intelligence analysis and production activities in MOOTW are generally characterized by:

- The initial lack of detailed databases on the area of operations and threat forces.

- An extensive list of non-standard intelligence requirements which must be satisfied to support planning and execution.

- Analysis of non-military related data.

- A rapidly changing situation resulting from crisis conditions in the area of operations.

- Compressed time frame for intelligence development.

- Restrictions on collection operations and the dissemination of intelligence (particularly with multinational military forces, NGOs and PVOs).

Intelligence shapes operations during MOOTW as it does during other types of MAGTF operations. However, in addition to understanding the physical environment and the threat, the commander must have intelligence on political, economic, and sociological conditions in order to develop sound military plans that will accomplish the assigned mission. To support MOOTW, MAGTF intelligence sections must focus on areas with the greatest potential for the execution of contingency operations and be able to respond with minimal warning and preparation. They must also have the flexibility to adapt to the wide variety of potential missions, possessing the expertise and specialized capabilities to provide intelligence across the entire scope of MOOTW.

b. Analysis and Production in Support of MOOTW. Intelligence analysis and production requirements in MOOTW are normally focused on non-traditional subject areas and IRs. For example, more detailed knowledge of the host nation's economic, transportation, medical, and public works infrastructure will be required to develop plans for humanitarian assistance operations, while a threat study to support a peacekeeping mission must encompass an extensive treatment of political, cultural, and sociological factors related to various insurgent or paramilitary factions in addition to the conventional military capabilities of the opposing sides. Use of area specialists and expertise from external intelligence organizations, non-DOD agencies (State Dept, Office of Foreign Disaster Assistence, US Agency for International Development, etc) and NGOs/PVOs is crucial to satisfying these requirements. In turn, the requirement to share information and intelligence with those same agencies, as well as the host-nation and allied forces, has a significant impact on analysis and production. While the goal is to provide necessary information and intelligence to all participants in the operation, there will typically be some that must remain releasable only to U.S. forces or allies with long-standing intelligence exchange agreements.

Production formats generally must be adapted to the requirements of a particular situation; e.g., normal IPB products must be modified to highlight factors critical to the specific MOOTW mission. In addition, analysis and production in MOOTW must be responsive to the unique needs of a large number of small elements, conducting independent activities throughout the area of operations. Production in support of these elements must be tailored to specific mission requirements and provide details pertinent to the small unit level. Intelligence that increases the

situational awareness of individual Marines such as information on local customs, language, health and sanitation, etc. is an important part of this effort.

c. Intelligence Preparation of the Battlespace for MOOTW. The principles and steps of the IPB process remain constant in MOOTW regardless of the mission, unit, staff section, or echelon. The analyst must define the battlespace and its effects, evaluate the threat, and determine threat courses of action (COAs). Application of these steps, however, will vary with each specific situation. The principal difference between IPB for conventional war and MOOTW activities is the focus and the degree of detail required to support the commanders decisionmaking process. Another major difference is the enormous demand for demographic analysis, since the population often is the focus in MOOTW. Finally, force protection IRs typically take on greater priority. The four steps of the IPB process and sample aspects and considerations for various MOOTW activities, are discussed below. (See FM 34-130/MCRP 2-12A, *Intelligence Preparation of the Battlefield*, Chapter 6, for a detailed discussion of each type of operation.)

(1) Define the Battlespace Environment

(a) Expand the Area of Interest (AI). Identify potential sources of assistance to friendly force operations from outside the country or operations area. Identify all military, paramilitary, governmental, non governmental, and private volunteer organizations that may interact with the friendly force. Identify and locate all external influences on the operation. Consider media, political arrangements, and third nation support or interference. Identify the geographic boundaries of the operation, any applicable legal mandates or terms of reference, and any other limitations or constraints that may impact on the operation.

(b) Assemble Data on Terrain and Infrastructure. Identify all existing infrastructure that have the potential for use by either threat or friendly forces in the operational area. Include sources of basic sustenance and energy, as well as transportation and communication networks. Identify facilities in adjacent or intermediate countries that could support the introduction of friendly forces or the delivery of necessary materials. Compile data on the geography and climate of the area, to include unusual or violent weather patterns or natural disturbances.

(c) Assemble Data on Host Nation. Identify the existing government and military infrastructure. Pay particular attention to their capabilities and limitations with regard to support for or interference in the operation. Begin compiling demographic data on the population. Include such things as age, education, religious beliefs, cultural distinctions, ethnic makeup, allocation of wealth, political affiliations and grievances, languages, values, and practices.

(d) Identify the Best and Worst Case Timelines of the Operation.

(2) Describe the Battlespace Effects

(a) Identify Legal Aspects. The MAGTF staff judge advocate should fully explain the impact of any legal mandates, terms of references, or other diplomatic agreements. Any legal mandates in place are of primary concern and will have a major effect on friendly courses of action, particularly Rules of Engagement (ROE) and use of force.

(b) Conduct Terrain Analysis. Conduct a standard terrain analysis using the military aspects of terrain, KOCOA. Pay particular attention to routes and areas that offer good observation for friendly security forces. Depict all potential obstacles, choke points, and ambush sites. In addition to ground avenues, ensure that all air avenues of approach are included. Since MOOTW often occur in urban areas, additional analysis of the urban terrain will be essential.

(c) Conduct Weather Analysis. Conduct a standard weather analysis for the AO. Consider the effects of weather on displaced persons/refugees, hostile groups, trafficability, air operations, seaborne operations, night operations, and communications. Weather can also have a significant impact on threat tactics and civil disturbances, such as rallies and demonstrations.

(3) Evaluate the Threat. There is no universal threat model in MOOTW. Consequently, there rarely are any doctrinal templates for the typical types of threats faced in this type of environment. The threats are many and will have to be evaluated according to the specific mission.

In missions involving humanitarian assistance and disaster relief, where the actual belligerent is nature itself, the weather and the environment are the threats. Evaluate their impact on the population and friendly operations. Could continued rains and flooding trigger mud slides isolating portions of the population and inhibiting relief operations? Climatic studies showing historical paths and frequencies of destructive weather (hurricanes/typhoons) can serve as a sort of doctrinal template. Could further earthquake after shocks collapse fragile water and sewage treatment facilities leading to an increase in waterborne diseases and environmental hazards?

In missions involving competing factions, some critical information and intelligence may exist in US, coalition, or host nation databases which could be used to begin building a threat model for the operation. Recognize differences in types of threat, strategy, modus operandi and tactics as well as weapons, equipment, material and personnel.

Determine if the environment is permissive, uncertain, or hostile to US forces entering with or without host nation approval. Determine if the population supports US forces. Is that support contingent on some type or form of material compensation from US forces, such as food, water, shelter or weapons? Determine if the population is organized to oppose US forces. If so, are they armed, and at what level (weapons, mines, vehicles)? Identify dissident groups among the population which will publicly support but clandestinely oppose US forces. Identify which terrorist groups are present, or thought to be present, or have access to the AO. Are they state

supported or directed? Personalities become a prime OOB factor. Identify leaders, trainers, key staff members, etc. and develop psychological profiles of all key personnel.

(4) Determine Threat Courses of Action. This step in the IPB process is the culmination of our analysis of the battlespace environment and our evaluation of the threat. Determine COAs using the following steps:

- Template or describe the actions of the threat that would interfere with friendly operations. In peacekeeping operations, for instance, any violations of the existing legal mandates by either belligerent could adversely effect friendly operations and security. Initiating hostilities or disregarding established terms of reference are examples of violations.

- Develop course of action models depicting the reactions of the threat to friendly operations within the AO and AI.

- Wargame each COA.

- Analyze the reactions of the local populace, multinational partners, NGOs, PVOs, and other key third/neutral parties to friendly COAs.

- Wargame terrorist and sabotage actions and other activities where the threat could reasonably avoid claiming responsibility and that could jeopardize friendly operations or security.

Given the nature of these types of potential threats to US forces, it will be difficult to obtain much of this information without an interagency approach to the IPB process. As recent history has demonstrated, the success of U.S. operations in MOOTW will increasingly depend on the combined efforts of state department officials, numerous government agencies, a unified command and its component services, SOF, and the National Security Council, all working together to accomplish the foreign policy objectives of the U.S. and our foreign allies.

d. IPB Products Useful in MOOTW. IPB products which may be useful in the MOOTW environment include (but are not limited to) the following:

(1) Population Status Overlay. Construct a population status overlay encompassing all areas included in the operation. At a minimum, attempt to depict the population by political affinity or regional majority sentiment, i.e. pro-government, anti-American, neutral, etc. If you are able to ascertain some root causes of the unrest in the region, for example, religious, ethnic, racial, or economic differences, it may be useful to display the population in terms of those demographic differences. Points where demographic differences intersect often pose the greatest potential for conflict and possible disruption of friendly operations.

(2) Logistics Sustainability Overlay. Identify available sources of food, potable water, fuel, etc. that could be utilized by the population, threat, or friendly forces.

(3) Lines of Communication (LOC) Overlay. Construct an LOC overlay for the operation. Identify all routes into and out of the operational area. Include all major streets, highways, railways, subways, waterways, etc. Analyze and depict the communication systems in place that could be used to support the operation, such as telephones, radio, TV, satellite and microwave systems, etc.

(4) Key Facilities and Target Overlay. Construct a key facilities and target overlay depicting all mission essential facilities to the operation, as well as potential targets for the threat. Whether something is a key facility or a target will be a matter of perspective. In a NEO, for example, the US embassy or the evacuation control center would be considered mission essential facilities, but also potential targets for belligerents. Include such things as embassies, military installations, television and radio facilities, government buildings, airports, port facilities, medical facilities, public utilities, etc.

10005. Intelligence Analysis and Production in Joint Operations

With few exceptions, MAGTF operations are increasingly joint operations. Marine forces participate in full partnership with other services in joint operations, either as a component or as the nucleus of a joint force. A coordinated intelligence effort makes a critical contribution to the success of joint operations. During joint operations, Marine intelligence analysis and production must be fully integrated with joint intelligence activities to ensure unity of effort, mutual support, and effective employment of limited intelligence resources. Effective intelligence support in joint operations depends on:

- Agreement on policies and procedures.
- Mutual intelligence support.
- Sharing of intelligence capabilities and assets.
- Full interoperability and connectivity among participants.
- Robust liaison.

a. Joint Intelligence Operations. The Joint Force Commander (JFC) is responsible for all aspects of intelligence support within his command. JFCs have the responsibility and authority to determine, direct, and coordinate all mission-related collection, production and dissemination activities through centralized or apportioned intelligence requirements management efforts. Component commanders remain responsible for the intelligence function within their commands and employ organic intelligence capabilities to support their assigned missions. The JFC makes the national, theater, and joint force intelligence assets available to support the efforts of his component commanders. At the same time, component capabilities must be available to assist the joint intelligence effort.

b. Marine Component Analysis and Production. When assigned as a joint force component, intelligence analysis and production techniques and procedures discussed in this publication are virtually unchanged. Each level of command performs the analysis and production required to support their planning and decisionmaking based on prioritized information requirements; requirements unable to be satisfied with organic resources are forwarded up the chain of command. Likewise, each level disseminates intelligence products to subordinate and adjacent units. The difference lies in the fact that higher, adjacent, supporting, and even subordinate units may be from a different service. For that reason, Marine intelligence sections and units participating in joint operations, particularly as the Marine component HQs and MAGTF CE, must:

- Operate in accordance with joint intelligence doctrine, theater TTP, and individual joint force procedures.
- Participate in joint intelligence mechanisms for the coordination of IR management (collection, production, and dissemination requirements).
- Provide analysis and production support to the joint force headquarters and other component commanders, as required.
- Employ joint or component analysis and production assets in support of Marine component operations.
- Ensure complete and reliable CIS connectivity within the joint intelligence architecture.
- Exchange liaison elements with the JTF J-2's joint intelligence support element (JISE), and/or other joint force component analysis and production entities as required.

c. Analysis and Production When Assigned as a Joint Force Headquarters. In certain situations, particularly in MOOTW, a MAGTF may be designated as a JTF, with the MAGTF CE forming the nucleus of the JTF headquarters. In this case the G/S2 must be prepared to function as the JTF J2, with the MEF CE's intelligence section serving as the base for the establishment of a J2 section and JISE. The JISE provides intelligence support to the JFC and the entire JTF. Key functions performed in the JISE include:

- Centralized collection, production, and dissemination management for joint force and supporting intelligence and reconnaissance assets.
- All-source intelligence analysis and production to satisfy JFC and component IRs.
- Development and maintenance of intelligence databases which support planning, operations, and targeting.

- Production of target studies and materials and intelligence support to force protection.

- Access to supporting national and theater intelligence assets.

It is essential that MAGTF intelligence sections operating as a JTF J2 do so in accordance with joint doctrine and theater TTPs. Increasingly, service doctrine is being brought into line with joint doctrine. Thus, for example, IPB for the Army (and soon the Air Force) will be conducted in essentially the same manner as Marine forces. There will, however, be unique IRs and products required by components of the JTF. The MAGTF G/S2 must ensure that the analysis and production portion of the JISE is appropriately augmented (or supported) by specialists from National agencies, the theater JIC, and other services who possess the necessary skills to satisfy the requirements of the force.

Intelligence product formats, standards, and dissemination means must be defined early to ensure all elements of the JTF can exchange and utilize intelligence products. Where possible these definitions and standards should be planned for in advance and published in an SOP or TTP that is available to other-service units that may be assigned as part of a Marine-led JTF. The TTP or SOP should be exercised whenever possible to refine procedures and ensure unity of effort.

The JFC, through his J2, exercises complete control over the analysis and production efforts of the joint force. Often, the J2 is delegated direct IR validation, prioritization, and tasking authority for intelligence production by the supporting theater JIC. Incumbent with that authority is the responsibility to manage the intelligence requirements and associated production requirements of the entire force.

10006. Intelligence Analysis and Production in Combined Operations

Marine forces may participate in a wide variety of combined operations, ranging from routine bilateral exercises to coalition warfare in major regional contingencies. Instances of unilateral US military operations are becoming less frequent, particularly in MOOTW. There is no single intelligence doctrine for combined or multinational operations; however, joint doctrine serves as the point of departure. Each coalition or alliance must develop its own TTP for each operation; the coalition commander determines standardized procedures for coalition forces.[2]

[2] NATO standardization agreements (STANAGs) and quadripartite standing agreements between U.S., British, Canadian, and Australian forces provide standards and guidance for the conduct of military operations by forces in these alliances. STANAG 2936 governs intelligence operations.

a. Principles. Combined intelligence operations are based on the following principles:

- **Adjust National Differences Among Nations.** Effective combined operations require minimizing the differences in national concepts and TTP for intelligence support. Commanders and their intelligence officers must be prepared to make adjustments to U.S. TTP to facilitate the sharing of intelligence and the integration and interoperability of intelligence and reconnaissance operations.

- **Unity of Effort Against Common Threat.** Intelligence operations must be directed at the common threat. A threat to one alliance member must be considered a threat to all.

- **Determining and Planning Intelligence.** Combined forces intelligence requirements and procedures should be identified, planned for, coordinated, and exercised prior to execution of operations.

- **Special Arrangements.** Special arrangements should be considered for developing, communicating, and using intelligence where there are differences in nations' language, culture, doctrine, terminology, organization, and intelligence and CIS equipment.

- **Full Exchange of Intelligence.** Each member of the coalition should share intelligence which supports planning and execution of coalition operations. Authorization for foreign disclosure must be obtained and procedures for disclosure and release outlined as part of the planning process. During execution, the exchange must be monitored and adapted to ensure it is meeting the needs of all coalition partners.

- **Complementary Intelligence Operations.** Each nation's intelligence assets should be employed to capitalize on their strengths and offset their weaknesses, providing the coalition with the most effective blend of intelligence and reconnaissance capabilities.

- **Combined Intelligence Centers.** A combined command should be supported by a combined intelligence center. The center develops coalition IRs, validates and establishes priorities, develops integrated intelligence plans, C2 of intelligence operations, fuses intelligence received from alliance members, and disseminates this intelligence to the combined force. The center should be manned by personnel from each nation and include appropriate linguist and translator support.

- **Liaison Exchange.** Exchange of intelligence liaison personnel between alliance partners bridges national differences and facilitates the exchange of intelligence and intelligence support.

b. Foreign Disclosure and Releasability. A key consideration for intelligence analysis and production in combined operations is the ability to release or disclose intelligence to non-U.S. members of the combined force. **Releasability** involves the conveyance of information in documentary form to a foreign national. The “document” may be a publication, map overlay, imagery, a computer disk or any such media which is physically provided to the foreign national

for their retention, even if only for a limited time period. **Disclosure** is the conveyance of classified information to a foreign national through either oral or visual means. Disclosure covers cases where classified information is discussed, briefed or viewed by a foreign national, but remains under the control of a U.S. person. Often, regardless of whether information and intelligence is released or disclosed, the source(s) of that information and intelligence must not be revealed. Although theoretically the members of a coalition are united toward a common goal, it must still be assumed that members' intelligence services will attempt to gather information on U.S. capabilities.

Foreign disclosure and releasability are governed by DCI, DOD, Service and theater policies and procedures. The theater CINC is ultimately responsible for establishing policy regarding disclosure and releasability. He may choose, however, to delegate authority to subordinate U.S. joint, combined or component commanders during crises or contingencies. When so delegated, each recipient of that authority is responsible for publishing releasability and disclosure guidance and procedures for their subordinate elements. During combined operations, Marine MAGTFs may find themselves acting as either a component or as a CTF headquarters; in either case foreign disclosure oversight and guidance must be performed. Even when operating simply as an element of a combined force, every unit and individual Marine must be aware of foreign releasability and disclosure guidance.

Based on the established guidance and procedures, intelligence analysts must pay particular attention to the sources of information and the releasability of the information and intelligence derived from each of those sources. Often two versions of an intelligence product will need to be produced -- one for U.S. forces (and some standing alliance or quadripartite partners) only and one releasable to the multinational force as a whole. A balance must be struck between safeguarding classified information and intelligence and ensuring our coalition partners are adequately informed and protected. The commander has the ultimate authority to authorize foreign disclosure of information and intelligence directly related to a threat to any coalition partner.

c. Formats. The form in which intelligence is conveyed is always important, however, in combined operations it is critical. Many potential coalition partners lack the technological and functional sophistication we increasingly rely on to collect, produce and disseminate intelligence and exercise C2 over intelligence operations. Access to networks using SIPRNET or JWICS is generally not possible due to the inability to restrict the user from roaming to intelligence they are not cleared for. Procedures such as IPB often will not apply. Even less sophisticated forms such as text documents or briefings may be impacted by language barriers. To compound the problem, the ability to exchange and use intelligence may vary from partner to partner. Like foreign disclosure, solutions for these challenges are difficult, but they must be addressed early in planning. Generally, production requirements will increase due to the need to tailor intelligence for multiple recipients. Those increased IRs should be matched with increased analysis, production, and dissemination resources, including translators if necessary, to ensure the timely provision of intelligence throughout the force. Where possible, coalition intelligence personnel should assist in the production of intelligence tailored to support their forces.

d. Information Sources. The intelligence analyst in a combined operation has the increased burden of assessing the reliability and credibility of non-U.S. information and intelligence sources. While foreign militaries may lack the sophisticated technical means available to the U.S., they often enjoy superior capabilities in HUMINT. This is particularly so if they are ethnically or linguistically related to the population of the AO. It may take some time, however, for an analyst to establish the reliability of the source or the accuracy of the information. The analyst also must be aware that foreign forces may withhold, filter or "spin" the information provided to the U.S. After all, foreign nations must safeguard their intelligence sources and methods in the same manner as we do. The analyst should still apply the techniques and procedures for assessing reliability and accuracy and be conscious of biases that may develop due to preconceived notions regarding the source. (See Chapter 3, **Analytical Thinking**).

10007. Pre-Crisis (Peacetime) Analysis and Production

a. Data Base Management. The key to effective intelligence analysis and production is the identification and maintenance of intelligence sources and databases (both hard copy and electronic formats). The time to work on developing databases is not when a crisis occurs. To the greatest extent possible every attempt should be made to develop and maintain relevant databases during day to day operations in garrison. Given the potential worldwide employment of Marine forces, these databases can be voluminous and their development and maintenance can be time consuming. Nonetheless, without the necessary pre-crisis work, the ability to provide needed support in a crisis will be diminished.

(1) Intelligence Reference Library. Although intelligence is produced and disseminated increasingly in electronic form, for the near future every intelligence section has a requirement for a basic intelligence library to support command and intelligence functioning. Included in the library should be publications necessary to support day-to-day intelligence planning, operations and contingency operations tailored to the unit's mission and echelon. This should include maps, charts, imagery, graphics, pertinent finished intelligence, and key supporting publications. Publications contained in libraries can be divided into two categories: required and nonrequired.

(a) Required Publications. Required publications are those that the command has been directed by higher HQs to maintain as minimum holdings. These holdings represent the minimum required material needed to support intelligence and command functioning. Listings of required holdings are contained in part B of the Naval Intelligence Publications Register (NIPR), table of authorized material (TAM), and as directed by higher headquarters. It is the intelligence officer's responsibility to review and validate the command's, and subordinate command's required holdings to ensure that they meet the minimum requirements to support intelligence operations. If it is determined that changes are needed, either to delete or add publications, a request will be submitted via the chain of command in accordance with the guidance contained in the NIPR and current directives.

(b) Nonrequired Publications. These are publications that are used by the intelligence section to supplement minimum required holdings, to conduct planning and

training, or to be used as reference material. It is the intelligence officer's responsibility to ensure that nonrequired publications are available to support the command intelligence requirements. Intelligence publications which provide intelligence and guidance for intelligence functioning are produced by national, service, and unified commands. Procurement procedures are contained in the NIPR, current directives, and local SOPs. Procurement of doctrinal and tactical publications (Joint Pubs, MCDPs, MCWPs, MCRPs, FMs, etc.) is a G-1/S-1 responsibility, however, the intelligence officer is responsible for identifying requirements for these publications.

(2) Statement of Intelligence Interest (SII). Each command must establish a SII with the Defense Intelligence Agency (DIA) in order to be receive automatic distribution of intelligence publications in support of command requirements. It is the responsibility of the intelligence officer to ensure that the command's SII is up to date. The SII is the vehicle by which commands register requirements for intelligence information reports, all-source nonrecurring finished intelligence, and initial issue of all-source finished intelligence. In the recent past, SIIs where compiled manually and submitted up the chain of command for approval. DIA has now instituted an on-line SII registration system (Joint Dissemination System or JDS) via INTELINK under the Director for Information Systems and Services (DS), Dissemination Services (SVD-2). The JDS login screen can be found at: (**http://136.197.177.66:1776/jds/plsql/jds.login)**. Accounts can be applied for on-line and are forwarded to the appropriate Dissemination Manager (DM). The DM for all Marine Corps units is MCIA. Once approved and registered, an account is established. The account may be modified at any time on-line. Specific policies governing echelons that may apply for JDS accounts are determined by the appropriate MARFOR and MEF. DIA is developing an on-line system similar to the old Registry of Intelligence Publications (RIP) which will identify DoD and "selected other" intelligence publications available. The Defense Intelligence Production Schedules (DIPS) lists all DoD planned general intelligence production. Most intelligence producers maintain some type of production forecast on their INTELINK and INTELINK-S websites.

(3) Intelligence Databases. The establishment of intelligence databases allows the intelligence section to manage and use the large volume of information and intelligence available. Many intelligence agencies have established various databases suited to their needs, resulting in many different systems available to support intelligence operations at various levels. It is the responsibility of the intelligence officer to be aware of those that are relevant and plan their use to support operations. The intelligence officer should maintain access to appropriate national, theater, and service data bases. Many data bases are available to Marine Corps commands equipped with the JDISS and the IAS, either as applications or through access to INTELINK and INTELINK-S. As modern information systems technologies mature, the structure and titles of the data bases change frequently. The Marine Corps Intelligence Activity publishes the MAGTF contingency reference guide, which is a compendium of agencies, products, databases, and INTELINK sites of potential interest. The publication is available in hardcopy, CD-ROM, and on-line via both INTELINK and INTELINK-S. In addition, virtually all national, theater, and service producers have created electronics links from their INTELINK web-sites to other pertinent sites.

The intelligence section should create their own local data bases to support their contingency planning and the development of contingency intelligence support products. Most all current intelligence files can be maintained on automated database systems. Finished intelligence products, imagery, maps, and graphics are all available on-line to provide interface for data search, access, and retrieval. As systems such as IAS become more mature and available, the only limiting factor will be the imagination of the intelligence officer. When assembled, a pre-crisis data base should consist of :

- Intelligence reference publications (e.g., intelligence TTP for all combatant commands the unit may support, as well as the intelligence TTPs/SOPs for other Services with which the unit may operate)
- Standard intelligence database (MID) segments
- Mapping, charting, geodetic, and other geospatial holdings
- Imagery library and related holdings
- Current intelligence files
- Open source publications

b. Pre-Crisis Production

(1) Contingency Intelligence Production. The main analysis and production effort of the MAGTF and MSC intelligence section is contingency intelligence production in support of the potential missions in their assigned regional areas. The intelligence section must review their standing contingency plans and tasking in conjunction with the operations and plans sections of the staff. Proper coordination with operations and plans personnel will help define the mission, scope, and tasks involved. The following methodology applies:

(a) Define the intelligence requirements. The IRs should be well defined after proper coordination with commanders and their staffs. Properly focused IRs will save time and not waste valuable intelligence assets.

(b) Research databases. All available intelligence databases should be reviewed before submitting RFIs, ICRs/IPRs/IDRs, or PRs requests.

(c) Analyze and synthesize data. Consider data, information, and intelligence from all available sources for analysis and synthesis.

(d) Prepare the products. The products are the end result (outputs) of the intelligence processing, analysis and fusion process. These must be delivered to all needing these in the time required and in forms most usable to the requester.

(2) Pre-Crisis Intelligence Preparation of the Battlespace. Pre-crisis IPB is conducted to develop descriptive (i.e., basic and current) intelligence needed to support the planning and execution of contingency operations. The extensive and detailed nature of the intelligence required to support expeditionary operations demands that a comprehensive research, analytical, and production effort be undertaken far in advance of the initiation of such operations. This demands that commanders and staff principals conduct sufficiently detailed contingency planning across all functional areas and command echelons to identify specific detailed IRs. The pre-crisis period offers the opportunity to carry out a thorough, measured study of potential areas of MAGTF employment. The pre-crisis IPB will drive contingency planning efforts and is the principal contribution of intelligence to combat readiness. The greatest challenge to performing pre-crisis IPB is the often generalized nature of a prospective mission. IPB products that can be generated in pre-crisis include:

- Analysis of the characteristics of the battlespace.
- Terrain and weather analyses and templates.
- Weather effects matrices for various seasons and conditions.
- Threat models.
- Threat capabilities assessments.
- When possible, threat COAs.

When completed, the pre-crisis IPB process will provide the following for each potential contingency area:

- A tailored intelligence database(s).
- A contingency intelligence study.
- Intelligence and counterintelligence estimates.
- Validated intelligence collection, production and dissemination requirements.
- An integrated intelligence operations plan (collection, production and dissemination).
- Tentative tasks for supporting intelligence and reconnaissance units.

In addition to the primary purpose of supporting contingency planning and execution, pre-crisis IPB serves the following secondary purposes:

- Develops an intelligence data base for selected areas.

- Educates personnel on potential missions and areas of operations.

- Identifies intelligence collection, production, and dissemination shortfalls (to include not only IRs, but also key personnel and equipment shortfalls).

- Trains intelligence personnel in the IPB process and the development of intelligence in support of actual contingency missions.

(3) Exercise Intelligence Production. Exercise intelligence production should follow the same procedures as contingency intelligence production and result in products which mirror image what will be utilized in an actual operation. The intelligence section should try to utilize real-world databases, IPB and scenarios whenever possible to enable realistic training of intelligence personnel and staff -- as well as solid area and threat familiarization training for all Marines and Sailors in the unit. When conducting field training exercises, the intelligence section must provide the same quality of GEOINT, IMINT, SIGINT, CI/HUMINT and other intelligence support as would be provided in an actual operation. Weather conditions and terrain will factor heavily into the success, and most importantly safety, of an exercise involving the actual maneuver and movement of air, land and seaborne forces.

(4) Other Intelligence Production. In garrison, the intelligence section is expected to provide indications and warning information and promote threat awareness. The intelligence section must keep the commander and staff (as well as those of subordinate units) informed on items of interest in the unit's assigned or potential contingency areas. This can be accomplished by providing periodic current intelligence briefings, providing access to intelligence publications, and/or preparing a current intelligence readboard for commanders and staff members. As access to web-based technologies increases, pertinent information can be posted on a web-site for daily review by the commander, staff and subordinate units. The intelligence section should always be prepared to field ad-hoc requirements as directed by the commander or his staff.

c. Analysis and Production Training

(1) Individual Training. The intelligence analyst receives an introduction to analysis and production topics at formal intelligence MOS training courses. However, in order to develop analysis and production proficiency, the intelligence section must have a continuing training program to enhance analysis and production skills. The Marine intelligence analyst must conduct training in the following areas:

- Intelligence preparation of the battlespace which covers analysis of contingency AOs, threat COGs, CVs, tactical practices, capabilities, and COAs.

- Intelligence research methods to include information and intelligence sources, agencies, functions, capabilities, limitations, use of AIS, and database availability and procedures.

- Methods of collecting and reporting information and their capabilities and limitations.

- Processing, recording and filing information to include preparing overlays and posting situation maps, both manually and electronically.

- How to integrate, analyze, evaluate, interpret, and synthesize information in order to rapidly produce tailored intelligence products.

- How to utilize AIS to manage data, analyze information, and produce and disseminate finished intelligence products -- both GENSER and SCI -- using all possible means of presentation (e.g., briefings, text reports, graphics, overlays.

Wargaming and command post exercises (CPXs) are the best vehicles for analytical training and must be done independently of major exercises in order to enhance analytical skills before they are needed. Normally, the majority of training will come as a result of practical application, i.e. preparation of IPB and other products in response to exercise or contingency requirements. Each product must be evaluated and critiqued with the analyst who developed it to improve their skills. Specific goals of the intelligence officer in wargaming should include:

- Provide a thorough orientation on the area and situation to all participants.

- Validate the scope and area coverage of the initial IPB.

- Determine gaps in existing intelligence.

- Identify areas for additional study.

- Develop new collection, production, and dissemination requirements.

- Develop an initial intelligence concept of operations and supporting contingency collection, production, and dissemination plans.

(2) Analysis and Production Element Training. Each intelligence section or element must have an integrated training program in order to develop the individual, team, and unit skills and capabilities necessary to execute intelligence and reconnaissance operations during any MAGTF operations. Section training should first emphasize building individual skills (specialization) within the context of the overall production effort. Once individual skills are mastered, cross-training and development of depth should be emphasized. A building block approach is utilized, starting with small group or team training (such as watch section, country

team, or production element), working up to exercises employing the entire G-2/S-2 section and those of subordinate commands. While a command staffex, CPX, or field exercise normally provides the best environment for the conduct of intelligence section training, independent G-2/S-2 section training should be conducted in advance of any major command training event in order to develop and test SOPs, cross train personnel in a variety of functions, and conduct in depth instruction in intelligence analysis and production. Additionally, each production requirement or exercise is a training opportunity and should have specific training objectives associated with it.

(3) Unit Training. Each intelligence unit conducts training in accordance with the unit's specific mission and functions. As intelligence specialty units are often employed as small, independent subelements, the majority of their training should be targeted at the team, subteam, or detachment level. Intelligence unit training should also emphasize the planning and execution of operations in response to the requirements of the supported unit. Each unit training evolution is an opportunity to enhance analysis and production training, so objectives should be developed for each exercise. Additionally, unit training must encompass specific, detailed intelligence objectives for commanders and other staff sections personnel. Unit training for analysis and production should emphasize the following:

- Train intelligence sections in meeting tactical requirements exercising both deliberate and immediate tactical production.
- Exercises the IR management process and intelligence cycle between consumers and producers.
- Test and improve standard product formats and content.
- Feedback and critique of analysis and production effort.
- Evaluate the effectiveness of integrating intelligence production operations with those of collection and dissemination.

(4) MAGTF Training. MAGTF training will combine all units and train on a larger scale. It provides an opportunity to exercise the production management function as well as integrate collections and dissemination with analysis and production. MAGTF training will provide the opportunity to test requirement priorities and procedures, test the integrated production between the MEF CE CIC, other intelligence and reconnaissance units, and the MSCs, and determine if the resulting products meet the needs of the commander and his staff.

10008. Analysis And Production During the Warning/Deployment Phase

a. Warning/Deployment Phase. The warning/deployment phase is a critical phase where the intelligence foundation is set for the entire operation. It is a high pressure phase where intelligence is expected to produce a high volume of critical support in a short period of time to support planning and decisionmaking. This phase is further complicated by the need to prepare

analysis and production elements for deployment within the MAGTF. The IPB and contingency intelligence study prepared in the pre-crisis period and the knowledge and skills gained by all (intelligence personnel as well as commanders and other staff personnel) during training exercises using actual intelligence operational procedures and products will be the key to being able to deliver products early in the warning/deployment phase.

b. Initial Analysis and Production

(1) Determine Initial Requirements. Key to the success in determining initial IRs is a clear understanding of the command's mission, assigned tasks, commander's intent and guidance, and a defined area of operations. The requirements of all command and staff elements should be integrated so that comprehensive products can be developed to meet as many needs as possible -- particularly PIRs. The goal should be to produce a certain product only once and not duplicate effort and waste time and assets. Time is the driving factor in determining the amount of detail that can be put into the analysis and production effort in this phase.

(2) Assemble and Focus Data Bases. With an understanding of the mission and area of operations, data bases and other intelligence holdings can be further refined. The intelligence section must coordinate with supporting agencies and subordinates to gather all pertinent information and data. The intelligence section should have a data base consisting of intelligence reference publications, MIDB segments, mapping and other geospatial products, imagery and other IMINT, CI/HUMINT, SIGINT, current intelligence, and open source material. All units should agree on standardization of products and data bases early on in the process. This should be a minor effort if SOPs/TTPs exist and all units have worked and coordinated together previously in IPB contingency intelligence study preparation and training. This effort is far more complicated in a joint or combined force.

(3) Develop Initial Estimate and Supporting Studies. If the contingency intelligence study is prepared and IPB is in progress, preparing the intelligence estimate will be much easier. The initial IPB will provide the baseline descriptive intelligence to initiate planning and, when paired with the contingency intelligence study, will support the preparation of an initial estimate and supporting studies. Preparation may only require a cut and paste effort to update and focus. Overall, a rapid, accurate, and detailed effort is required to generate the intelligence needed to drive all planning and decisionmaking.

(4) Develop Collection/Production/Dissemination Requirements. The preparation of the initial intelligence and CI estimates should identify shortfalls in existing intelligence. Those shortfalls and requirements become the basis for development of new collection, production, and dissemination requirements beyond organic capabilities. The new requirements must be turned into collection, production, and dissemination plans and necessary requests for support to the component, JTF, and/or theater commands for action. The MAGTF intelligence section is responsible for this effort and coordination with the planning effort is essential to ensure these requirements are focused on operations.

c. Production Management. Production management validates and prioritizes IPRs among all competing requirements to determine which ones have the most impact on the outcome of the mission. Production must be managed ruthlessly during this phase to ensure that limited assets are properly focused. The commander must be actively involved in directing the overall intelligence operations effort, setting priorities, providing guidance to the intelligence officer on where to focus the effort and what requirements are most important, and evaluating the overall effectiveness of operations. Continuous interaction with staff planners and subordinate commanders and intelligence officers is required to ensure ongoing production supports the development of friendly COAs. Requirements will typically change frequently during this phase as the COAs are identified, refined, rejected, etc. Production management must ensure flexibility and responsiveness. Time will be the critical element in production during this phase as requirements must be met on time, even at the expense of detail.

d. Establishment of Standard Products. The use of standard products simplifies production and dissemination. This can be a common estimate, studies, reports, templates, graphics, etc. All can and should be automated to the degree possible in order to provide a cut and paste or fill in the blank capability. Establishing standard products and a regular update schedule is an effective way of managing production and dissemination during this phase. If used properly, it can head off constant requests for updates by various organizations which can drain production and dissemination resources and detract from focusing on essential requirements. Ideally, a system of standard products should be developed during training and carried over with only minor modifications.

10009. Analysis and Production During Execution

a. Production Management. Production management remains critical during the execution phase as requirements tend to change even more rapidly. Analysis and production resources must be focused on the main effort in accordance with the commander's guidance and intent, the PIRs, and the unit’s operations and intelligence concepts of operation. The challenge is to balance the production effort between support to current operations, future operations planning, and future planning. As a rule of thumb, the higher the echelon, the greater the focus is on future operations and planning; the lower the echelon the greater the focus on current operations. During execution, the time element is even more critical since execution often depends on timely receipt of intelligence required for decisionmaking.

b. Support to Current Operations. Support to current operations consists primarily of immediate tactical production and is keyed to the commander’s decision points, PIRs, and the location of HPTs. Each piece of data/information/intelligence received undergoes immediate tactical processing and assessment in order to determine if it is pertinent to the ongoing operation. If deemed pertinent, it is quickly analyzed, impacts determined and intelligence estimates prepared, and the result disseminated to all needing it. This performs an indications and warning and situation development function. Maintaining situational awareness among intelligence personnel is necessary in order to anticipate and meet the needs for immediate tactical production. It is essential that intelligence personnel understand the operational situation, current PIRs and IRs, and likely enemy reactions. Support to current operations must include analysis and

production in support of deep and rear operations, resisting a natural tendency to focus on the close battle. Intelligence support to current operations must also be balanced against the need to support future operations and plans. All assets cannot be devoted to current operations at the expense of supporting planning for future operations. In addition to short, tailored, mission-focused products in response to an immediate tactical needs, production includes regular scheduled update briefs and intelligence summaries which helps maintain a common picture of the battlespace supporting situation development.

c. Support to Future Operations. Support to future operations consists of a mix of both immediate and deliberate production depending on the time frame of the operation, scope of the operation, and level of command. Future operations focuses on the "deep battle," defined either by distance or time. Intelligence products in support of future operations must also focus on that same planning window and seek to provide the future operations team a coherent projection of the battlespace and threat within that window. The future operations cell focuses on a rolling or near-continuous IPB process, generating new COAs, ICRs/IPRs/IDRs and targeting priorities, DSTs and synchronization matrixes as the battle or operation unfolds. Intelligence production supporting the future operations cell is focused on those products generated during IPB, but constantly modified by the results of friendly and threat actions. Daily situation update briefings are necessary to ensure the future operations team remains aware of current actions which may impact future operations.

The primary contributions from intelligence analysis and production are the results from BDA and the estimate of the situation focused on the appropriate planning horizon. BDA provides input into combat assessment which in turn helps determine the nature of future operations. The estimate of the situation is derived from the continuous IPB effort and provides the basis for planning. During future operations planning, IPB and estimates tend to be less formalized and extensive, drawing on and extending previous work rather than generating completely new production. The intelligence analysis and production effort requires continuous interaction with the future operations cell. As decisions are made concerning future operations, integrated collection, production, and dissemination requirements are developed and prioritized, missions assigned, and mission specific products are prepared. Management of the time element is again critical to ensure that products reach the future operations cell and mission planners/executers in a timely manner.

d. Support to Future Plans. MEF CEs, components and JTF HQs often require an additional planning cell focused on the next campaign or major phase change within the CINCs campaign plan. By definition this cell -- called the *operations planning* team, or OPT, in the MEF CE -- is looking far ahead into the future and deals more in assumption than fact. Production in support of future planning will tend to be more deliberate and more generalized, but will still encompass the basic elements of IPB. Often, the future plans cell will be located out of the immediate operations area and may even locate in close proximity to the CINC headquarters to facilitate communication and collaboration. Given the timeframe and location of potential future operations, the supporting theater intelligence center may be more suited to produce the required intelligence products, with MAGTF intelligence personnel taking these products and tailoring them to support the needs of the future plans cell.

e. Support to Targeting. Intelligence support to targeting requires a continuous effort integrating support to both current and future operations. This support consists of target development (generated through IPB), immediate tactical production of new intelligence related to particular targets, and BDA of the results of mission execution. At higher echelons of command, the targeting cycle can span days, while at lower echelons it may span hours or even minutes. In MAGTFs with organic fixed-wing aviation, the intelligence support to targeting will be driven by the ATO cycle. An important goal is the synchronization of the collection and production phases with the appropriate phases of the PDE&A and ATO cycles to ensure the provision of relevant and timely target intelligence.

APPENDIX A

GLOSSARY

Section I

Acronyms

Note**:** Acronyms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official military acronyms:

1. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.

2. MCRP 5-12C, Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms.

AA ..... avenue of approach
AAA ..... antiaircraft artillery
AAAV ..... advanced amphibious assault vehicle
A/CS ..... assistant chief of staff
ACE ..... aviation combat element
ADA ..... air defense artillery
AFMIC ..... Armed Forces Medical Intelligence Center
AFP ..... all-source fusion platoon
AGL ..... above ground level
AIC ..... Atlantic Intelligence Command
AIS ..... automated information systems
AO ..... area of operations
AOA ..... amphibious objective area
AOB ..... air order of battle
AOI ..... area of interest
AOR ..... area of responsibility
A&P cell ..... analysis and production cell
A&P Co ..... analysis and production company
ATARS ..... advanced tactical airborne reconnaissance system
ATF ..... amphibious task force
ATFIC ..... amphibious task force intelligence center
ATO ..... air tasking order

BDA ..... battle damage assessment

C2 . . . . . command and control
C2W . . . . . command and control warfare
CATF . . . . . commander, amphibious task force
CCIR . . . . . commander's critical information requirements
CE . . . . . command element
CENTCOM . . . . . United States Central Command
CI . . . . . counterintelligence
CIA . . . . . Central Intelligence Agency
CIC . . . . . combat intelligence center
CINC . . . . . commander in chief
CLF . . . . . commander landing force
CN . . . . . counter narcotics
COA . . . . . course of action
COC . . . . . combat operations center; current operations center
COG . . . . . center of gravity
COLISEUM . . . . . community on-line intelligence system for end users and managers
COMINT . . . . . communications intelligence
COMSEC . . . . . communications security
CONOPS . . . . . concepts of operations
CONPLAN . . . . . operation plan in concept format, concept plan, contingency plan
CPX . . . . . command post exercise
CSS . . . . . combat service support
CSSE . . . . . combat service support element
CV . . . . . critical vulnerability

D3A . . . . . decide, detect, deliver, assess
DCI . . . . . Director of Central Intelligence
DIA . . . . . Defense Intelligence Agency
DISUM . . . . . daily intelligence summary
DOD . . . . . Department of Defense
DODIPP . . . . . Department of Defense Intelligence Production Program
DON . . . . . Department of the Navy
DP . . . . . decision point
DR . . . . . disaster relief
DS . . . . . direct support
DST . . . . . direct support team, decision support template
DSSCS . . . . . defense special security communications system
DZ . . . . . drop zone

EA . . . . . electronic attack; engagement area
EEFI . . . . . essential elements of friendly information
ELINT . . . . . electronic intelligence
EOB . . . . . electronic order of battle
EP . . . . . electronic protection
EPW . . . . . enemy prisoner of war

ES ..... electronic warfare support
EW ..... electronic warfare, early warning
EWO ..... electronic warfare officer

FAARP ..... forward area arming and refueling point
FAO ..... foreign area officer
FDA ..... functional damage assessment
FFIR ..... friendly force information requirements
FM ..... field manual (Army)
FOC ..... future operations center
FSC ..... fire support coordinator

GCE ..... ground combat element
GCI ..... ground control intercept
GEOINT ..... geographic intelligence
GI&S ..... geospatial information and services
GIST ..... geographic intelligence support team
GIT ..... geographic intelligence team
GMI ..... general military intelligence
GOB ..... ground order of battle
GS ..... general support
GSP ..... ground sensors platoon

HA ..... humanitarian assistance
HLZ ..... helicopter landing zone
HN ..... host nation
HOC ..... HUMINT operations center
HPT ..... high-payoff target
HPTL ..... high-payoff target list
HQ ..... headquarters
HUMINT ..... human intelligence, human resources intelligence
HVT ..... high-value target

I&W ..... indications and warnings
IAS ..... intelligence analysis system
IADS ..... integrated air defense system
ICBM ..... intercontinental ballistic missile
ICR ..... intelligence collection requirement
IDR ..... intelligence dissemination requirement
IIP ..... imagery intelligence platoon
IMINT ..... imagery intelligence
intel bn ..... Intelligence Battalion
INTELINK ..... intelligence link
INTELINK-S ..... intelligence link-SECRET
INTREP ..... intelligence report

INTSUM ..... intelligence summary
IOC ..... intelligence operations center
IPB ..... intelligence preparation of the battlespace
IPR ..... intelligence production requirement
IR ..... intelligence requirement
IRBM ..... intermediate-range ballistic missile
ISC ..... intelligence support coordinator

JCS ..... Joint Chiefs of Staff
JDISS ..... joint deployable intelligence support system
JFC ..... joint force commander
JIC ..... joint intelligence center
JICPAC ..... Joint Intelligence Center, Pacific
JISE ..... joint intelligence support element
JMCIS ..... joint maritime command information system
JOG ..... joint operations graphic
JSIPS ..... joint service imagery processing system
JTF ..... joint task force
JWICS ..... joint worldwide intelligence communications system

KOCOA ..... key terrain, observation and fields of fire, cover and concealment, obstacles, and
..... avenues of approach and mobility corridors

LCAC ..... landing craft air cushion
LOC ..... line of communication
LOS ..... line of sight
LOTS ..... logistics over-the-shore
LTIOV .....
latest time information of value
LZ ..... landing zone

MAGTF ..... Marine Air-Ground Task Force
MARFOR ..... Marine Corps forces
MASINT ..... measurement and signature intelligence
MC&G ..... mapping, charting, and geodesy
MCDP ..... Marine Corps doctrinal publication
MCIA ..... Marine Corps Intelligence Activity
MCISU ..... Marine Corps Imagery Support Unit
MCOO ..... modified combined obstacle overlay
MCPP ..... Marine Corps planning process
MCRP ..... Marine Corps reference publication
MCWP ..... Marine Corps warfighting publication
MEA ..... mission effectiveness assessment
MEF ..... Marine expeditionary force

MEU ..... Marine expeditionary unit
METT-T ..... mission, enemy, terrain and weather, troops and support available, time available
MEU(SOC) ..... Marine expeditionary unit (special operations capable)
MIDB ..... modernized integrated database
MIO ..... maritime intercept operations
MOOTW ..... military operations other than war
MRBM ..... medium-range ballistic missile
MRC ..... major regional contingency
MSC ..... major subordinate command
MSI ..... multi-spectral imagery
MSIC ..... Missile and Space Intelligence Center
MTI ..... moving target indicator

NAI ..... named area of interest
NAIC ..... National Air Intelligence Center
NAVOCEANO ..... Naval Oceanographic Office
NBC ..... nuclear, biological, and chemical
NCO ..... noncommissioned officer
NEO ..... noncombatant evacuation operation
NGIC ..... National Ground Intelligence Center
NGO ..... non governmental organization
NIMA ..... National Imagery and Mapping Agency
NIPRNET ..... non-secure internet protocol routing network
NIS ..... national input segment
NIST ..... national intelligence support team
NMIC ..... National Maritime Intelligence Center
NOB ..... naval order of battle
NOE ..... nap of the earth
NSA ..... National Security Agency

OCAC ..... operations control and analysis center
OMFTS ..... operational maneuver from the sea
ONI ..... Office of Naval Intelligence
OOB ..... order of battle
OPCON ..... operational control
OPLAN ..... operation plan
OPORD ..... operation order
OPSEC ..... operations security
OPT ..... operations planning team
OSINT ..... open-source intelligence

PACOM ..... United States Pacific Command
PDA ..... physical damage assessment
PDE&A ..... planning, decision, execution, and assessment
PIR ..... priority intelligence requirement

POL . . . . . petroleum, oils, and lubricants
PR . . . . . production requirement
PSYOP . . . . . psychological operations
PTTDB . . . . . planning terrain tactical data base
PVO . . . . . private voluntary organization

rad bn . . . . . Radio Battalion
RAO . . . . . regional area officer
RFI . . . . . request for intelligence; request for information
ROE . . . . . rules of engagement
ROC . . . . . reconnaissance operations center

S&T . . . . . scientific and technical intelligence
SAM . . . . . surface-to-air missile
SARC . . . . . surveillance and reconnaissance cell
SCI . . . . . sensitive compartmented information
SCIF . . . . . sensitive compartmented information facility
SECDEF . . . . . Secretary of Defense
SIGINT . . . . . signals intelligence
SIPRNET . . . . . SECRET internet protocol router network
SIR . . . . . specific information requirement
SOA . . . . . sustained operations ashore
SOP . . . . . standing operating procedure
SPMAGTF . . . . . special-purpose Marine air-ground task force
STANAG . . . . . standardization agreement (NATO)
SWO . . . . . staff weather officer

TAI . . . . . target area of interest
TCAC . . . . . technical control and analysis center
TCO . . . . . tactical combat operations
TDA . . . . . tactical decision aid
TEG . . . . . tactical exploitation group
TERPES . . . . . tactical electronic reconnaissance processing and evaluation system
TPFDD . . . . . time-phased force deployment data
T/O . . . . . table of organization
T/O&E . . . . . table of organization and equipment
topo . . . . . topographic
topo plt . . . . . topographic platoon
TPL . . . . . time phase lines
TRSS . . . . . tactical remote sensor system
TRANSCOM . . . . . United States Transportation Command
TSA . . . . . target system assessment
TTP . . . . . tactics, techniques, and procedures

UAV . . . . . unmanned aerial vehicle
UTM . . . . . universal transverse mercator

VMAQ . . . . . Marine tactical electronic warfare squadron
VO . . . . . validation office

WMD . . . . . weapons of mass destruction

Section II

Definitions

Note: Definitions of military terms change over time in response to new operational concepts, capabilities, doctrinal changes and other similar developments. The following publications are the sole authoritative sources for official definitions of military terms:

1. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms.

2. MCRP 5-12C, Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms.

A

all-source intelligence -- Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the finished intelligence. (Joint Pub 1-02)

amphibious objective area - A geographical area, delineated in the initiating directive, for purposes of command and control within which is located the objective(s) to be secured by the amphibious task force. This area must be of sufficient size to ensure accomplishment of the amphibious task force's mission and must provide sufficient area for conducting necessary sea, air, and land operations. Also called AOA. (Joint Pub 1-02)

area of interest - That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (Joint Pub 1-02)

area of operations - An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their mission and protect their force. Also called AO. (Joint Pub 1-02)

B

basic intelligence - Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (Joint Pub 1-02)

battle damage assessment - 1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (Joint Pub 1-02) 2. The timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCWP 5-12C)

battlespace - All aspects of air, surface, subsurface, land, space, and electromagnetic spectrum which encompass the area of influence and area of interest. (MCRP 5-12C)

battlespace dominance - The degree of control over the dimensions of the battlespace which enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical mission. It includes all actions conducted against enemy capabilities to influence future operations. (MCRP 5-12C)

branch(es) - A contingency plan or course of action (an option built into the basic plan or course of action) for changing the mission, disposition, orientation, or direction of movement of the force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions. See also sequels. (MCRP 5-12C)

C

centers of gravity - 1. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. Also called COG. (Joint Pub 1-02) 2. A key source of strength without which an enemy cannot function. (MCDP 1-2)

centralized control - In military operations, a mode of battlespace management in which one echelon of command exercises total authority and direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (MCRP 5-12C)

collate - 1. The grouping together of related items to provide a record of events and facilitate further processing. 2. To compare critically two or more items or documents concerning the same general subject; normally accomplished in the processing phase of the intelligence cycle. (Joint Pub 1-02)

collection - The gathering of intelligence data and information to satisfy the identified requirements. (MCWP 5-12C)

collection agency - Any individual, organization, or that has access to sources of information and the capability of collecting information from them. (Joint Pub 1-02)

collection asset - A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (Joint Pub 1-02)

collection management - 1. The process of converting intelligence requirements into collection requirements, establishing priorities, and tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (Joint Pub 1-02)

collection manager - An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. Also called CM. (Joint Pub 1-02)

collection plan - A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (Joint Pub 1-02)

combat data - Data derived from reporting by operational units. (MCWP 5-12C)

c**ombatant command -** A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (Joint Pub 1-02)

combined operation - An operation conducted by forces of two or more allied nations acting together for the accomplishment of a single mission. (Joint Pub 1-02)

command and control - 1. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (Joint Pub 1-02) 2. The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

command and control warfare - The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Also called C2W. (Joint Pub 2-0)

commander's critical information requirements - Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining

situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirement; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent - A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

commander's planning guidance - Directions and/or instructions which focus the staff's course of action development during the planning process. Also called CPG. (MCRP 5-12C)

communications intelligence - Technical and intelligence information derived from foreign communications by other than the intended recipients. Also called COMINT. (Joint Pub 2-0)

communications security - The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. (Joint Pub 1-02)

component command - One of the subordinate organizations that constitute a joint force. Normally a joint force is organized with a combination of Service and functional components. The Service component command consists of its Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under the command, including the support forces that have been assigned to a combatant command, or further assigned to a subordinate unified command or joint task force. (Joint Pub 1-02)

coordination - The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence - 1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on the behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (Joint Pub 1-02) 2. Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called CI. (MCRP 5-12C)

crisis action planning - The time-sensitive planning for the deployment, employment, and sustainment of assigned and allocated forces and resources that occurs in response to a situation that may result in actual military operations. Crisis action planners base their plan on the circumstances that exist at the time planning occurs. (Joint Pub 1-02)

critical information - Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (Joint Pub 1-02)

critical intelligence - Intelligence which is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential/ actual enemy. It includes but is not limited to the following:

- Strong indications of the imminent outbreak of hostilities of any type (warning of attack)

- Aggression of any nature against a friendly country

- Indications or use of nuclear-biological-chemical weapons (target)

- Significant events within potential enemy countries that may lead to modification of nuclear strike plans. (Joint Pub 1-02)

critical node - An element, position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations. (Joint Pub 1-02)

critical vulnerability - An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called CV. (MCRP 5-12C)

D

daily intelligence summary - A report prepared in message format at the joint force headquarters that provides higher, lateral, and subordinate headquarters with a summary of all significant intelligence produced during the previous 24-hour period. The “as of” time for the information, content, and submission time for the report will be specified by the joint force commander. Also called DISUM. (Joint Pub 1-02)

data - Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning or insight is or might be assigned. (Joint Pub 1-02)

database - Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (Joint Pub 1-02)

database replication - Process by which like databases reflect commonality in information and timeliness of that information. (MCRP 5-12C)

debriefing - Interviewing of an individual who has completed an intelligence or reconnaissance assignment or who has had knowledge, whether through observation, participation, or otherwise, of operational intelligence significance. (MCRP5-12C)

decentralized control - In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

deception operation - A military operation conducted to mislead the enemy. A unit conducting a deception may or may not make contact with the enemy. Deception operations include demonstrations, diversions, displays, feints, ruses, actions, events, means, and objectives. (MCRP 5-12C)

decision point - An event, area, or point in the battlespace where and when the friendly commander will make a critical decision. Also called DP. (MCRP 5-12C)

deliberate planning - A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed. (Joint Pub 1-02)

deliberate targeting - The methodical identification, compilation, and analysis of potential fixed and semifixed targets followed by the decision of which potential targets will be attacked, when, and/or by what weapon and ordnance. It is practiced primarily during the planning phase of an operation, when planning for an attack, or when the tempo of combat is slow. (MCRP 5-12C)

descriptive intelligence - Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: *basic intelligence*, which is general background knowledge about established and relatively constant conditions; and *current intelligence*, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment - 1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. (Joint Pub 1-02)

direction finding - A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receive or ancillary equipment. (Joint Pub 1-02)

direct support - A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance. (Joint Pub 1-02)

dissemination - Conveyance of intelligence to users in a suitable form. (Joint Pub 1-02)

dissemination management - Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

E

electromagnetic spectrum - The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (Joint Pub 1-02)

electronic attack - That division of electronic warfare involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. (Joint Pub 1-02)

electronic intelligence - Technical and geolocational intelligence derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (Joint Pub 1-02)

electronic protection - That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment or electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. (Joint Pub 1-02)

electronic reconnaissance - The detection, identification, evaluation, and location or foreign electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (Joint Pub 1-02)

electronic warfare - Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. Also called EW. (Joint Pub 1-02)

electronic warfare support - That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence (SIGINT), communications intelligence (COMINT), and electronic intelligence (ELINT). Also called ES. (Joint Pub 1-02)

essential elements of friendly information - 1. Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Also called EEFI. (Joint Pub 1-02) 2. Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence - Class of intelligence which attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. See also **descriptive intelligence**. (MCRP 5-12C)

F

fires - The effects of lethal or non lethal weapons.

force protection - Security programs designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, and supported by intelligence, counterintelligence, and other security programs. (Joint Pub 1-02)

force reconnaissance company - A unit whose mission is to conduct preassault and deep postassault reconnaissance operations in support of a landing force and its subordinate elements. (MCRP 5-12C)

friendly force information requirements - Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

fusion - In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (Joint Pub 1-02)

fusion center - In intelligence usage, a physical location to accomplish fusion. It normally has sufficient intelligence automated data processing capability to assist in the process. (Joint Pub 1-02)

future operations section - 1. In MAGTF operations, a section normally under the staff cognizance of the G-3 which focuses on planning/producing new fragmentary orders or the next change of major subordinate command mission; this section forms and leads the integrated planning effort with a planning horizon of 72-120 hours out. It develops branch plans and sequels. 2. In Marine aviation, that portion of the tactical air command center and aviation combat element commander's battlestaff responsible for the detailed planning and coordination of all future air operations conducted by the aviation combat element in support of the Marine air-ground task force. The future operations section plans for and publishes the next air tasking order(s) (normally a 48/72-hour period). (MCRP 5-12C)

G

general military intelligence - Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or allied military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries,; military and civilian C4 systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) Also called GMI. (Joint Pub 1-02)

general support - That support which is given to the supported force as a whole and not to any particular subdivision thereof. (Joint Pub 1-02)

geographic coordinates - The quantities of latitude and longitude which define the position of a point on the surface of the earth with respect to the reference spheroid. (Joint Pub 1-02)

geographic intelligence - The process of collecting, organizing, analyzing, synthesizing, disseminating and utilizing geospatial information and services (GI&S) with regards to the military aspects of the terrain. Also called GEOINT. GEOINT is the integration and analysis of all-source geospatial information in support of specific Marine Corps operations. The analysis is focused on a specific mission and includes intensification of information detail and resolution to meet tactical requirements. GEOINT analysis is focused on the intelligence preparation of the battlespace (IPB) process and addresses key terrain, observation & fields of fire, cover & concealment, obstacles, avenues of approach & mobility corridors. This analysis is commonly referred to as KOCOA for easy reference.

geospatial information and services - The concept for collection, information extraction, product generation, storage, dissemination, and utilization of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data. These data are used for military planning, training, and operations including aeronautical, nautical and land navigation, as well as mission planning, mission rehearsal, modeling and simulation and precise targeting. It also includes the evaluation and analysis of topographic, hydrophobic, littoral, or aeronautical features for their effect on military planning, operations and intelligence. This analysis could also include the development of a commander's visualization and preparation of the battlespace. It may be presented in the form of printed maps, charts and publications; in digital simulation and modeling databases; in photographic form; or in digital form. Also called GI&S. (Nominated for inclusion in Joint Pub 1-02)

global sourcing - A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

H

helicopter landing zone - A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. Also called HLZ. (Joint Pub 1-02)

high-payoff target - A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through wargaming, which must be acquired and successfully attacked for the success of the friendly commander's mission. Also called HPT. (Joint Pub 1-02)

high-value target - A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. Also called HVT. (Joint Pub 1-02)

human intelligence - 1. A category of intelligence derived from information collected and provided by human sources. (Joint Pub 1-02) 2. In Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called HUMINT. (Joint Pub 1-02)

humanitarian assistance - Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have primary responsibility for providing humanitarian assistance. Also called HA. (Joint Pub 1-02)

hydrography - The science which deals with the measurement and description of the physical features of the oceans, seas, lakes, rivers, and their adjoining coastal areas, with particular reference to their use for navigational purposes. (Joint Pub 1-02)

I

imagery exploitation - The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (Joint Pub 1-02)

imagery intelligence - Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (Joint Pub 1-02)

imagery interpretation - The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. (Joint Pub 1-02)

indications and warning - Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events. Also called I&W. (Joint Pub 1-02)

information - 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

information report - Report used to forward raw information collected to fulfill intelligence requirements. (Joint Pub 1-02)

information requirements - Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (Joint Pub 1-02)

information exchange requirement - The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom as well as why the information is necessary and how that information will be used. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included in the information exchange requirement. Also called IER. (MCRP 5-12C)

integration - A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. (Joint Pub 1-02)

intelligence - 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation,

analysis, or understanding. (Joint Pub 1-02) 3. Knowledge about the enemy or the surrounding environment needed to support decisionmaking. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence annex - A supporting document of an operation plan or order that provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures. (Joint Pub 1-02)

intelligence cycle - The process by which information is converted into intelligence and made available to users. (Joint Pub 2-01)

intelligence data - Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline - A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open source intelligence. (Joint Pub 1-02)

intelligence estimate - The appraisal, expressed in written, oral, or graphic form, of available intelligence relating to a specific situation or condition with a view to determine the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (Joint Pub 1-02)

intelligence journal - A chronological log of intelligence activities covering a stated period, usually 24 hours. It is an index of reports and messages that have been received and transmitted, and of important events that have occurred**,** and actions taken. The journal is a permanent and official record. (Joint Pub 1-02)

intelligence operations - The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (Joint Pub 1-02)

intelligence preparation of the battlespace - 1. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (Joint Pub 1-02) 2. In Marine Corps usage, the systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence report - A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (Joint Pub 1-02)

intelligence requirement - 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (Joint Pub 1-02) 2. In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called IR. (MCRP 5-12C)

intuitive decisionmaking - The act of reaching a conclusion which emphasizes pattern recognition based on knowledge, judgment, experience, education, intelligence, boldness, perception, and character. This approach focuses on assessment of the situation vice comparison of multiple options. (Joint Pub 1-02)

J

joint deployable intelligence support system - A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (Joint Pub 1-02)

joint force - A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (Joint Pub 1-02)

joint intelligence center - The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (Joint Pub 1-02)

joint intelligence support element - A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (Joint Pub 1-02)

joint operations - A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (Joint Pub 1-02)

joint task force - A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a sub unified commander, or an existing joint task force commander. Also called JTF. (Joint Pub 1-02)

joint worldwide intelligence communications system - The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced

networking technologies that permit point-to-point or multi-point information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (Joint Pub 1-02)

L

large-scale map - A map having a scale of 1:75,000 or larger. (Joint Pub 1-02)

line of communication - A route, either land, water, and/or air, which connects an operating military force with a base of operations and along which supplies and military forces move. (Joint Pub 1-02)

M

main effort - The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maneuver warfare - A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope.
(MCRP 5-12C)

mapping, charting, and geodesy - Maps, charts and other data used for military planning, operations, and training. These products and data support air, land, and sea navigation; weapon system guidance; target positioning; and other military activities. These data are presented in the forms of topographic, planimetric, imaged, or thematic maps and graphics; nautical and aeronautical charts and publications; and, in digital and textual formats, gazetteers, which contain geophysical and geodetic data and coordinate lists. Also called MC&G. (Joint Pub 1-02)

Marine Corps planning process - A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. NOTE: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

measurement and signature intelligence - 1. Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT.

medium-scale map - A map having a scale larger than 1:600,000 and smaller than 1:75,000. Joint Pub 1-02)

meteorological data - Meteorological facts pertaining to the atmosphere, such as wind, temperature, air density, and other phenomena, which affect military operations. (Joint Pub 1-02)

military operations other than war - Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other elements of national power and occur before, during, and after war. Also called MOOTW. (Joint Pub 1-02)

modified combined obstacle overlay - A product used to depict the battlespace's effects on military operations. It is normally based on a product depicting all obstacles to mobility, modified to also depict the following, which are not prescriptive nor inclusive: cross-country mobility classifications (such as RESTRICTED); objectives; avenues of approach and mobility corridors; likely locations of counter mobility obstacle systems; likely engagement areas; and key terrain. Also called MCOO. (MCRP 5-12C)

multinational operations - A collective term to describe military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance. (Joint Pub 1-02)

multi-spectral imagery - The image of an object obtained simultaneously in a number of discrete spectral bands. (Joint Pub 1-02)

N

named area of interest - A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of interest will help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

national intelligence support team - A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called NIST. (Joint Pub 2-01)

near real time - Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (Joint Pub 1-02)

noncombatant evacuation operations - Operations directed by the Department of State, the Department of Defense, or other appropriate authority whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens or the United States. Also called NEO. (Joint Pub 1-02)

no-strike target list - A list designated by a commander containing targets not to be destroyed. Destruction of targets on the list would interfere with or unduly hamper projected friendly military operations, or friendly relations with indigenous personnel or governments. (Joint Pub 1-02)

O

open-source intelligence - Information of potential intelligence value that is available to the general public. Also called OSINT. (Joint Pub 1-02)

operational architecture - A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanged requirements. Also called OA. (MCRP 5-12C)

operational control - Transferable command authority which may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations; normally this authority is exercised through the service component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. (Joint Pub 1-02)

operations control and analysis center - Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of MAGTF signals intelligence operations. Processes, analyzes, produces, and disseminates signals intelligence-derived information and directs the ground-based electronic warfare activities of the radio battalion. Also called OCAC. (MCRP 5-12C)

operational level of war - The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives. (Joint Pub 1-02)

order of battle - The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OOB. (Joint Pub 1-02)

P

paramilitary forces - Forces or groups which are distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (Joint Pub 1-02)

priority intelligence requirements - 1. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (Joint Pub 1-02) 2. An intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

production - The conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production is a process of synthesis -- the most important action in developing usable intelligence for the commander. (MCWP 2-1)

production management - Encompasses determining the scope, content, and format of each product, developing a plan and schedule for the development of each product, assigning priorities among the various production requirements, allocating processing, exploitation, and production resources, and integrating production efforts with collection and dissemination. (MCRP 5-12C)

R

reach back - The ability to exploit resources, capabilities, expertise, etc. not physically located in the theater or a joint area of operations, when established. (MCRP 5-12C)

reactive targeting - The method used for targeting target of opportunity. It is used when time and situation do not allow for deliberate targeting,; i.e., during an attack, when defending against an attack, or upon discovery of the location of a target such as a radio jammer, tank, or antiaircraft weapon. (MCRP 5-12C)

request for information - Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater commander's procedures. (Joint Pub 1-02)

S

scientific and technical intelligence - The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b.

scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. Also called S&T. (Joint Pub 1-02)

SECRET internet protocol router network - Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (Joint Pub 1-02)

sensitive compartmented information - All information and materials bearing special intelligence community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. Also called SCI. (Joint Pub 1-02)

sensitive compartmented information facility - A restricted access facility providing SCI communications, processing, and storage. Also called SCIF. (Joint Pub 1-02)

sensor data - Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

sequel(s) - Major operations that follow the current major operations. Plans for these are based on the possible outcomes (success, stalemate, or defeat) associated with the current operation. (MCRP 5-12C)

signals intelligence - A category of intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumental signals intelligence, however transmitted. Also called SIGINT. (Joint Pub 1-02)

situational awareness - Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

surveillance and reconnaissance center - Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (MCRP 5-12C)

sustained operations ashore - The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called SOA. (MCRP 5-12C)

T

tactical intelligence -- 1. Intelligence that is required for planning and conducting tactical operations. (Joint Pub 1-02) 2. Tactical intelligence concerns itself primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

target - A geographical area, complex, or installation planned for capture or destruction by military forces. (Joint Pub 1-02)

target analysis - An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. (Joint Pub 1-02)

target area of interest - The geographical area or point along a mobility corridor where successful interdiction will cause the enemy to either abandon a particular course of action or require him to use specialized engineer support to continue, where he can be acquired and engaged by friendly forces. Not all target areas of interest will form part of the friendly course of action; only target areas of interest associated with high-payoff targets are of interest to the staff. These are identified during staff planning and wargaming. Target areas of interest differ from engagement areas in degree. Engagement areas plan for the use of all available weapons. Target areas of interest might be engaged by a single weapon. Also called TAI. (MCRP 5-12C)

target complex - A geographically integrated series of target concentrations. (Joint Pub 1-02)

target component - A major element of a target complex or target. It is any machinery, structure, personnel, or other productive asset that contributes to the operation or output of the target complex or target. (Joint Pub 1-02)

target folder - A folder containing target intelligence and related materials prepared for planning and execution action against a specific target. (Joint Pub 1-02)

target intelligence - Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (Joint Pub 1-02)

target system - 1. All the targets situated in a particular geographic area and functionally related. (DOD) 2. A group of targets which are so related that their destruction will produce some particular effect desired by the attacker. (Joint Pub 1-02)

tempo - The relative speed and rhythm of military operations over time. (MCRP 5-12C)

terrain analysis - The collection, analysis, evaluation, and interpretation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (Joint Pub 1-02)

terrain study - An analysis and interpretation of natural manmade features of an area, their effects on military operations, and the effect of weather and climate on those features. (Joint Pub 1-02)

W

warfighting functions - The six mutually supporting military activities integrated in the conduct of all military operations are:

1. **Command and control** -- the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.

2. **Maneuver** -- the movement of forces for the purpose of gaining an advantage over the enemy.

3. **Fires** -- those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight.

4. **Intelligence** -- knowledge about the enemy or the surrounding environment needed to support decisionmaking.

5. **Logistics** -- all activities required to move and sustain military forces.

6. **Force protection** -- actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. (MCRP 5-12C)

APPENDIX B

REFERENCES

Defense Intelligence Management Document (DIMD)

0000-151-94	Department of Defense Intelligence Production Program
0000-151C-95	Department of Defense Intelligence Production Program: Production Procedures

Joint Publications (Joint Pubs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Doctrine for Intelligence Support to Joint Operations
2-01	Joint Intelligence Support to Military Operations
2-01.1	Tactics, Techniques, and Procedures for Intelligence Support to Targeting (Draft)
2-01.3	Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (Draft)
2-02	National Intelligence Support to Joint Operations
2-03	Joint Tactics, Techniques and Procedures for Geospatial Information and Services Support to Joint Operations
3-02	Joint Doctrine for Amphibious Operations
3-02.1	Joint Doctrine for Landing Force Operations
3-07	Joint Doctrine for Military Operations Other Than War
3-09	Joint Doctrine for Fire Support
3-13	Joint Doctrine for Information Operations
3-13.1	Joint Doctrine for Command and Control Warfare
3-50.3	Joint Doctrine for Evasion and Recovery
3-55	Doctrine for Reconnaissance, Surveillance, and Target Acquisition
3-60	Doctrine for Joint Targeting (Draft)
5-00.2	Joint Task Force Planning Guidance and Procedures

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-2	Campaigning
2	Intelligence
3	Expeditionary Operations
5	Planning
6	Command and Control

Marine Corps Warfighting Publications (MCWPs)

0-1.1	Componency
2-1	Intelligence Operations
2-11	MAGTF Intelligence Collections (draft)
2-12.1	Geographic Intelligence (draft)
2-13	MAGTF Intelligence Dissemination (working outline)
2-14	Counterintelligence (draft)
2-15.2	Signals Intelligence
2-15.3	Ground Reconnaissance (draft)
2-15.4	Imagery Intelligence (draft)
3-1	Ground Combat Operations (draft)
3-16	Tactics, Techniques and Procedures for Fire Support Coordination (draft)
3-2	Aviation Operations (draft)
3-35.3	Military Operations on Urbanized Terrain
3-35.7	MAGTF Meteorological and Oceanographic Support
4-1	Logistics Operations
5-1	Marine Corps Planning Process (draft)
6-2	MAGTF Command and Control (draft)
6-22	Communications and Information Systems
6-23	Information Management (draft)

Marine Corps Reference Publications (MCRPs)

5-12C	Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms
5-12D	Organization of Marine Corps Forces

Army Field Manuals (FMs)

34-8-2	Intelligence Officer’s Handbook
34-81	Weather Support for Army Tactical Operations
34-81-1	Battlefield Weather Effects
34-130/MCRP 2-12A	Intelligence Preparation of the Battlefield

APPENDIX C

INTELLIGENCE ESTIMATE FORMAT

The following pages provide detailed formats and suggested contents for written intelligence estimates. An intelligence estimate can be prepared at any level, from the battalion/squadron through the MEF command element and MARFOR headquarters levels. The scope and detail of the estimate will be governed by the level of command preparing it, the nature of the operation it is intended to support, already available intelligence, prior contingency planning, and the time and resources available. The intelligence estimate should be succinct, yet provide the commander and staff the necessary information for decisionmaking.

Whenever possible, the intelligence estimate should clearly present the analysis and conclusions developed during IPB. The finished estimate may be written, graphic or verbal in form, but should always follow the general five paragraph structure presented in the following pages. Subparagraphs and tabs may be added and omitted as necessary, based on their relevance to the stated mission. For topics that require a large amount of data, information and intelligence (i.e. beaches, weapons capabilities and technical characteristics, etc.), the salient facts and conclusions should be summarized in the body of the estimate and the detailed data included as a tab.

For a discussion of the relationship between IPB and the intelligence estimate, see Chapter 4, *Intelligence Preparation of the Battlespace*. Chapter 5, *Analysis of the Battlespace*, provides a discussion of the various factors that constitute paragraph 2 (Characteristics of the Area of Operations) of the estimate. Chapter 6, *Threat Analysis*, provides a discussion of the factors that constitute paragraph 3 (Enemy Military Situation).

The first example is for an intelligence estimate in support of conventional combat operations. The second example provides an example of an intelligence estimate in support of MOOTW.

Copy no.__of__copies
Issuing headquarters
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (Number)

Ref : (a) Maps and Charts
(b) Other pertinent intelligence documents and online databases

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. MISSION. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. CHARACTERISTICS OF THE AREA OR OPERATIONS. (State conditions which exist and indicate the effect of these conditions on enemy capabilities and the assigned mission. Assess the estimated effects of these conditions on both enemy and friendly capabilities and operations.)

a. Military Geography

(1) Topography

(2) Drainage

(3) Vegetation

(4) Surface materials

(5) Military aspects of terrain

(6) Effects of terrain on enemy and friendly capabilities and operations

b. Hydrography

(1) Coastline description

(2) Hydrographic conditions

(a) Surf

(b) Tides

(c) Currents

(3) Beaches

(4) Effects of hydrography on enemy and friendly capabilities and operations

c. Climate and Weather

(1) Type and characteristics

(2) Temperature

(3) Precipitation

(4) Visibility

(5) Winds

(6) Light Data

(7) Flight conditions

(8) Effects of weather on enemy and friendly capabilities and operations

d. Transportation

(1) Airfields

(2) Helicopter landing zones

(3) Port facilities

(4) Roads

(5) Railroads

(6) Inland waterways

(7) Effects of transportation on enemy and friendly capabilities and operations

e. Civilian Telecommunications and Media

(1) International

(2) Domestic

(3) Mass communications -- types, capabilities, key facilities

(a) Radio

(b) Television

(c) Print media

(4) Effects of telecommunications and media on enemy and friendly capabilities and operations

f. Economics and Infrastructure

(1) General economic activity and conditions (industry, public works and utilities, finance, banking, agriculture, trades and professions, labor force, etc.)

(2) Monetary system

(3) Power and utilities

(4) POL facilities

(5) Effects of economics and infrastructure on enemy and friendly capabilities and operations

g. Politics

(1) Political system and climate

(2) Local political conditions

(3) Local political leaders

(4) Policy and attitudes towards the U.S. and the U.S. military

(5) Effects of political situation on enemy and friendly capabilities and operations

h. Sociology

(1) Cities and towns

(2) Population and distribution of area and of key cities and towns

(3) Ethnic composition

(4) Languages

(5) Religions

(6) Customs and norms

(7) Social institutions and attitudes

(8) Effects of sociological situation on enemy and friendly capabilities and operations

i. Health and Medical

(1) Food supply

(2) Water supply

(3) Diseases and other medical problems

(4) Plant and animal hazards

(5) Sanitation

(6) Medical facilities

(7) Effects of health and medical situation on enemy and friendly capabilities and operations

3. ENEMY MILITARY SITUATION

a. Ground Forces

(1) Composition, organization and strengths. (Describe the structure of enemy forces [i.e., order of battle] and describe unusual organizational features, identity, etc. State the number and size of enemy units in and others available for use in the area of operations. Provide estimated combat effectiveness of enemy forces.)

(2) Disposition, locations, movements and activities. (Describe the geographic location and latest known activities of enemy forces, including command and control facilities, fire support elements, and other key combat support forces.)

(a) Committed forces. (For ground forces, include all units currently in contact or with which contact is imminent within the unit's AO, regardless of the specific friendly course of action. For amphibious or forcible entry operations, committed forces would be those which could immediately engage friendly units at their point of insertion. All fire support assets within range are normally considered committed, regardless of subordination. Conventional military forces are referred to by numbers of unit types (armor, infantry, etc.) two echelons below the friendly unit. Guerrilla or insurgent forces are expressed in terms of total numbers of personnel and fire support weapons.

(b) Reinforcements. (Describe the enemy's reinforcement capabilities in terms of possible forces and weapons that can react in time to affect the accomplishment of the mission. Factors to be considered include time available to react, terrain, weather, road and rail nets, transportation, replacements, and possible aid from sympathetic or participating neighbors.)

(3) Weapons and equipment. (Describe the operational capabilities and technical characteristics of major items of equipment in the enemy's inventory.)

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics. (Describe levels of supply, resupply ability, and capacity of beaches, ports, roads, railways, airfields, and other facilities to support supply and resupply. Consider transportation, hospitalization and evacuation, military construction, labor resources, and maintenance of combat equipment, etc.).

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

b. <u>Naval Forces</u>

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

c. Air Forces

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

d. Air Defense Forces

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

e. Paramilitary and Security Forces

(1) Composition, organization and strengths

(2) Disposition, locations, movements and activities

(3) Weapons and equipment

(4) Command and control

(a) Organization

(b) Key C2 nodes

(c) Communications and information systems

(5) Logistics

(6) Training, tactics, operating patterns

(7) Capabilities and effectiveness

f. Command and Control Warfare Capability

(1) Intelligence, counterintelligence, and reconnaissance capabilities

(2) Electronic warfare capabilities

(3) Psychological warfare capabilities

(4) Deception capabilities

(5) Operational security capabilities

g. Nuclear, Biological and Chemical Capabilities

h. Night Combat Capabilities

i. Unconventional Warfare Capabilities (guerrilla, subversion, sabotage, terrorism)

4. CAPABILITIES AND ANALYSIS. (List separately each enemy capability which can affect the accomplishment of the assigned mission. Each enemy capability should contain information on what the enemy can do, where they can do it, when they can start it and get it done, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering all applicable factors from paragraphs 2 and 3, and attempt to determine and give reasons for the estimated probability of adoption by the enemy. Examine the enemy's capabilities by discussing the factors that favor or militate against its adoption by the enemy. The analysis of each capability should also include a discussion of enemy strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indications that point to possible adoption of the capability. Finally, state the estimated effect the enemy's adoption of each capability will have on the accomplishment of the friendly mission. The term "capabilities" includes not only the general courses of action open to the enemy (i.e. attack, defend, withdraw, etc.), but also the particular courses of action possible under each general course of action. These COAs should correspond exactly to the enemy COA models developed during step 4 of IPB.)

5. CONCLUSIONS AND VULNERABILITIES. (Conclusions resulting from discussion in paragraph 4. Include: enemy centers of gravity, critical and other vulnerabilities and estimated exploitability of these by friendly forces, enemy courses of action beginning with the most probable and continuing down the list in the estimated order of probability, and the estimated effects adoption of each capability would have on the friendly mission.)

/s/ _____

_____

TABS (omit or add other tabs as required)

A. Tactical Study of Terrain

B. Beach Studies

C. Climatology Study

D. Airfield Studies

E. HLZ and DZ Studies

F. Port Studies

G. Lines of Communications Study

H. Order of Battle Study

MOOTW ESTIMATE FORMAT

Copy no.__of__copies
Issuing headquarters
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (Number)

Ref : (a) Maps and Charts
(b) Other pertinent intelligence documents and online databases

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. MISSION. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. CHARACTERISTICS OF THE AREA OR OPERATIONS. (Discuss characteristics of the host nation (HN), the area, and their probable effects upon the threat(s), the mission force, and the host government.)

a. Geography

(1) Strategic location.

(a) Neighboring countries and boundaries.

(b) Natural defenses including frontiers.

(c) Points of entry and strategic routes.

(2) Size and dimensions.

(3) Relief.

(4) Beach Data.

(5) Hydrography.

(a) Coastal.

(b) Lakes.

(c) Rivers.

(6) Land use.

(7) Geological basics.

(8) Vegetation

(9) Water sources.

(10) Natural foods.

(11) Population centers.

(12) Wildlife.

b. Climate and Weather

(1) Type and characteristics.

(2) Temperature.

(3) Precipitation.

(4) Visibility.

(5) Winds.

(6) Light Data.

(7) Flight conditions.

(8) Seasonal effects of weather on terrain and visibility.

c. Demographics

(1) History.

(2) Ethnic composition.

(3) Languages.

(4) Social system.

(5) Education.

(6) Living conditions.

(7) Cultural customs.

(8) Religions.

(9) Taboos.

(10) Grievances.

(11) Psychology (Behavior patterns and motivating factors.)

d. Transportation

(1) Airfields

(2) Helicopter landing zones

(3) Port facilities

(4) Roads

(5) Railroads

(6) Inland waterways

e. Civilian Telecommunications and Media

(1) International

(2) Domestic

(3) Mass communications -- types, capabilities, key facilities

(a) Radio

(b) Television

(c) Print media

f. Politics (Address existing situation, effects on threat(s), HN, and mission force.)

(1) National government.

(a) Structure.

(b) Regional and/or international role.

(c) Degree of popular support.

(2) Political parties (Both sanctioned and unsanctioned.)

(3) Foreign dependence or alliances.

(4) Controls and restrictions.

(5) Legal system (both civil and religious.)

(6) Grievances.

g. Economics (Address existing situation, effects on threat(s), HN, and mission force.)

(1) Current value of currency and wage scales.

(2) Financial structure to include national and international.

(3) Foreign dependence.

(a) Assistance programs.

(b) Foreign-owned businesses and enterprises in country.

(c) Trade agreements.

(4) Agriculture and domestic food supply.

(5) Natural resources and degree of self-sufficiency.

(6) Industry.

(a) Types.

(b) Production levels.

(c) Consumer demands.

(d) Unions.

(7) Black market and illicit trades (drugs, weapons, etc.)

(8) Technology.

(a) Capabilities.

(b) Expertise.

h. Health and Medical

(1) Food supply

(2) Water supply

(3) Diseases and other medical problems

(4) Plant and animal hazards

(5) Sanitation

(6) Medical facilities

3. THREATS (Note: For each category of threat (except medical/environmental and natural disasters) discuss organization and leadership (to include composition); strength and dispositions; recent and present significant activities, strengths and weaknesses; and relationships with other threat categories.)

a. Conventional.

b. Insurgent.

c. Clans, Tribes, or Factions.

d. Terrorist.

e. Drug producers or traffickers

f. Criminal organizations.

g. Third-party nation and external.

h. Civil unrest

i. Medical and environmental.

j. Natural disasters.

4. CAPABILITIES AND ANALYSIS (List current threat capabilities and discuss in regard to probability of adoption)

a. Enumeration. (Includes what, where, when, and how, for each category of threat.)

(1) Basic capabilities.

(a) Conventional.

(b) Insurgent.

(c) Clans, Tribes, or Factions.

(d) Terrorist.

(e) Drug producers or traffickers

(f) Criminal organizations.

(g) Third-party nation and external.

(h) Civil unrest

(i) Medical and environmental.

(j) Natural disasters.

(2) Supporting capabilities. (Includes intelligence, security, recruitment, organization, training, finance, and logistics.)

(a) Conventional.

(b) Insurgent.

(c) Clans, Tribes, or Factions.

(d) Terrorist.

(e) Drug producers or traffickers

(f) Criminal organizations.

(g) Third-party nation and external.

(h) Civil unrest

(i) Medical and environmental.

(j) Natural disasters.

b. Analysis and Discussion. (Includes all evidence supporting or rejecting the adoption of each capability.)

5. HN SECURITY

a. Situation. (For each sub-paragraph describe organization and leadership; strength and disposition; recent and present significant activities; and strengths and weaknesses.)

(1) Public order/internal security forces.

(2) Armed forces.

(3) External support forces an dependency. (Regional peacekeeping, foreign forces, mercenaries, etc.)

b. Capabilities. (What, where, when, how for both basic capabilities and supporting capabilities.)

(1) Public order/internal security forces.

(2) Armed forces.

(3) External support forces an dependency.

c. Analysis and discussion.

6. FRIENDLY AND NEUTRAL THIRD-PARTY

a. Situation. (For each sub-paragraph, as defined in 5.a.)

(1) Embassies and consulates.

(2) Military.

(3) Business interests.

(4) NGO/PVO.

b. Capabilities. (As defined in 5.b.)

(1) Embassies and consulates.

(2) Military.

(3) Business interests.

(4) NGO/PVO.

c. Analysis and discussion.

7. CONCLUSIONS and VULNERABILITIES

a. Effects of the operational environment. (State total effect of the AO upon COAs.)

b. Probable threat COAs. (Listed in order of relative probability of adoption.)

c. Threat vulnerabilities. (List exploitable threat vulnerabilities.)

TABS (as necessary)

APPENDIX D

WEATHER CRITICAL VALUES

Establishing weather critical values is essential to the analysis of weather effects on threat and friendly operations. Critical values provide the parameters for assessing exactly what impact particular weather conditions will have. Critical values can be established for personnel, specific types of equipment, and types of military operations. The functions or categories selected will be dictated by the echelon of command, the composition of the force, and the likely operations the force will be expected to conduct. For example, a MEF may be concerned with general categories such as amphibious operations, fixed-wing aviation operations, visual reconnaissance operations, and so forth. A battalion may be more concerned with foot mobility, LOS restrictions, and effects on indirect fire support, while a UAV unit might be more concerned with visibility, cloud cover, precipitation, and temperatures aloft. Each level of command should focus on the mission-essential functions of their unit and its specific equipment.

For each category or function, only those weather elements that have a potential impact are listed, adjusted for the terrain and season in which operations will occur. For example, troops operating in a desert environment will generally not be affected by snowfall. Similarly, wind chill is not a critical factor when assessing fixed-wing aviation operations (although it may affect ground crews).

For each weather element selected, critical values are established that define levels of impact. In the example below, those levels of impact are defined as “favorable, marginal, and unfavorable.” An alternative would be; “no impact, moderate impact, and severe impact.” An effective technique is to assign a color-code (such as green, yellow, red) to each level, which can then be transferred easily to a graphic weather effects matrix.

Although usually compiled by the intelligence section (at the MEF CE level, assisted by the G-2 section’s staff weather officer, the intelligence support coordinator, and the intelligence battalion), the selected functions, weather elements, and critical values must be defined by the commander, his operations staff, and functional elements of the friendly force. Within a MAGTF, for example, the air officer and ACE should establish what elements have potential impact on aviation operations/platforms and define the values that constitute the levels of impact. Within an infantry battalion, the artillery liaison officer is the best source for affects on supporting fires and artillery delivered munitions.

Regardless of who compiles the list, the commander has the final say regarding what constitutes a relevant weather effect. Just as a commander defines his intelligence requirements regarding the threat, he similarly must define what elements of weather intelligence he regards as important or critical to his decisionmaking. Those identified weather elements and their established critical values are tracked much more closely and serve as the basis for weather effects graphics and updates. Like other intelligence requirements, the weather elements and their critical values must be reevaluated as the mission or season changes.

Unit intelligence sections should work to develop misson, type unit, and equipment-focused critical value lists during peacetime operations, to include those equipment types and units which will normally be attached or in direct support during operations. See MCWP 3-35.7, *MAGTF Meteorological and Oceanographic Support* (especially appendices E and F), and FM 34-81-1, *Battlefield Weather Effects*, for additional doctrine and TTP guidance. Upon receipt of an alert or execute order, these critical values lists can then be refined and tailored to the forces, mission, and environment assigned.

The table below provides and example of a weather critical values chart.

Table D-1. Weather Critical Values Chart

FUNCTION	WEATHER ELEMENT	FAVORABLE (UNRESTRICTED)	MARGINAL (RESTRICTED)	UNFAVORABLE (SEVERELY RESTRICTED)
Maneuver: Mobility (Track vehicles, Day)	Visibility Rainfall Snow Depth	> 1.5 km < 0.1 in/hr < 12 in	0.8 to 1.5 km > 0.5 in/hr > 12 to 20 in	< 0.8 km > 0.5 in/hr > 20 in
Maneuver: Mobility (Track vehicles, Night)	Visibility Rainfall Snow Depth	> 0.2 km < 0.1 in/hr < 12 in	0.1 to 0.2 km 0.1 to 0.5 in/hr 12 to 20 in	<0.1 km > 0.5 in/hr > 20 in
Maneuver: Mobility (Dismounted infantry)	Visibility Rainfall Snow Depth Temperature Windchill	> 0.3 km < 0.1 in/hr < 3 in < 89.6° F/32° C > 32° F/0° C	0.1 to 0.3 km 0.1 to 0.5 in/hr 3 to 6 in > 89.6° F/32° C 32° F/0° C to -22° F/-30° C	< 0.1 km > 0.5 in/hr > 6 in ---------- < -22° F/-30° C
Fire Support (155mm)	Visibility Ceiling Surface wind Snow depth	> 5.0 km > 800 ft < 35 knots < 4.0 in	1.5 to 5.0 km 500 to 800 ft 35 to 50 knots 4.0 to 6.0 in	< 1.5 km < 500 ft > 50 knots > 6 in
Fire Support (CAS)	Visibility Ceiling	> 8.0 km > 3000 ft	5.0 to 8.0 km 500 to 3000 ft	< 5.0 km < 500 ft
Aviation (Rotary wing)	Visibility Ceiling Surface wind Precipitation	> 1.5 km > 500 ft < 20 knots None	0.4 to 1.5 km 300 to 500 ft 20 to 30 knots Light	< 0.4 km < 300 ft > 30 knots Freezing rain or hail
Aviation (Air Defense)	Visibility Ceiling Rainfall	> 5.0 km > 5000 ft < 0.5 in/hr	3.0 to 5.0 km 3000 to 5000 ft 0.5 to 1.0 in/hr	< 3.0 km < 3000 ft > 1.0 in/hr

The companion weather effects matrix would list the same functions. If any one weather element falls within the unfavorable/severely restricted range, the weather effects matrix would be color-coded “red” for that function during the period of time that unfavorable element is forecast to occur. A note would be made indicating what specific weather element(s) or phenomena resulted in any marginal or unfavorable assessments (see figure 5-2).

Weather critical values should be established for threat as well as friendly forces. Due to differing weapons and personnel characteristics, the same weather may have differing effects--either good or bad--on the threat. For example, threat tanks without thermal sights will be severely restricted during periods of reduced visibility, while friendly tanks may be only marginally effected. Comparing the varying effects of weather on friendly and threat forces helps to identify advantages and vulnerabilities that may be exploited by either side.

APPENDIX E

TACTICAL INDICATORS

Indicators are any positive or negative evidence of threat activity or any characteristic of the operations area that points toward threat capabilities, vulnerabilities, or intentions. Individual indicators cannot stand alone. Each indicator is integrated with other factors, indicators, information, and intelligence before patterns are detected and threat intentions established. Indicators are developed by intelligence analysts to assist in discerning answers to a commander's PIRs and IRs. The analyst uses indicators to correlate particular events or activities with probable threat courses of action.

Indicators are also used to determine what events or activities must occur for a threat to follow a particular course of action. During IPB, as NAIs and the event template are developed, corresponding indicators are developed which, when detected, will assist in rapidly identifying the particular course of action the threat may be adopting. While some indicators may apply to most or all of the possible threat courses of action, some indicators may be unique to a particular COA. Well developed indicator lists can also aid in detecting threat deception operations. By comparing indicators, intelligence, and operations reporting from all sources, the analyst can arrive at an accurate picture of the battlespace and intelligence estimates.

As stated above, it is important to note that indicators may be present for more than one course of action in the same threat force. For example, a division forced to withdraw (and providing indicators accordingly) may employ a subordinate unit (brigade/regiment/battalion) in a delaying action to cover the withdrawal. Thus, units in contact with the delaying force may characterize the indicators as delaying in nature, but the threat force overall is withdrawing. Again, it is important to analyze indicators from all sources in order to assess the true intentions of the threat.

The following tables provide some types of intelligence indicators, organized according to the types of operations they are commonly associated with. These lists are by no means complete, nor are they intended to apply to all situations or all potential threat forces. Instead, they are intended to provide a basis from which intelligence personnel can develop indicators specific to the threat and environment they are faced with. No one indicator can stand alone, and all indicators must be examined within the context of the doctrine, tactics, and structure of the specific threat force.

a. Offensive Indicators

ACTIVITY	EXPLANATION
Massing of maneuver elements, armor, artillery, and logistical support.	Areas of secondary importance are often weakened to mass maximum strength for the main effort.

Deployment of combat elements on a relatively narrow frontage (not forced by terrain).	Combat forces often reduce frontages to provide maximum combat power at the point of attack.
Massing of indirect fire support assets.	Large groupings of artillery or mortars generally indicate initiation of a main attack.
Extensive artillery preparation of up to 50 minutes in duration or longer.	Many military doctrines call for extensive artillery preparation preceding an attack.
Dispersal of tanks and self-propelled or towed artillery to forward units.	Can indicate formation of combined-arms assault formations with tanks accompanying the leading maneuver elements and artillery following in bounds.
SSM units located forward.	Provides depth to threat offensive operations; places friendly support and rear areas in range. May also be employed alone for harassing or special weapons delivery.
AAA and mobile SAMs located well forward with maneuver elements..	Provides increased protection to massed forces prior to attack; extends air defense umbrella forward as units advance.
Demonstrations and feints.	Frequently precede an attack; may be used to deceive regarding actual point of attack.
Establishment and strengthening of counter-reconnaissance screen.	Used to cover assembly and preparation of forces for attack
Concentration of mass toward one or both flanks within the forward area.	May indicate intent for single or double envelopment, particularly if massing units are armor-heavy.
Increased patrolling (ground reconnaissance).	May indicate efforts to gather detailed information regarding friendly dispositions prior to attack.
Command posts located well forward; mobile command posts identified.	Forward and mobile command posts enhance command and control during offensive operations.
Movement of noncombatants out of the combat zone.	Noncombatants hinder rapid forward movement of follow-on forces.
Extensive conduct of drills and rehearsals in rear areas.	Major attacks, particularly against fortified positions or strongly defended natural or man-made barriers, of require rehearsal of specialized tactics and skills.
Increased activity in supply, maintenance, and motor transport areas.	Major attacks must be sustained and additional forces moved to the front, creating a surge in rear area activities.
Increased aerial reconnaissance (including UAVs).	Threat refining intelligence picture prior to operations.

Establishment of FARPs, auxiliary airfields, or activation of inactive airfields.	Forward basing of aircraft and aviation sustainment increases sortie rate and turn-around time.
Clearing lanes through own obstacles.	Usually immediately precedes and attack. Lanes facilitate forward movement and grouping of assault units, particularly at night.
Reconnaissance, marking, and destruction of opponents obstacles.	Facilitates movement of assault echelons through opposing obstacles.
Gap-crossing equipment (swimming vehicles, bridging, ferries, boats, etc.) located in forward areas (provided there is a water or large gap obstacle).	Located with assault echelons to maintain tempo of the assault when faced with significant gap obstacles. Normally concentrated with main effort.
Staging of airborne, air assault, or special forces with modes of transportation/insertion.	Such elements are used to provide depth to the assault and target friendly COGs.
Increased signals traffic or radio silence.	Both may indicate intent to conduct offensive operations. Increased traffic may be an attempt to deceive. Radio silence intended to deny information derived from SIGINT by opponent.
SIGINT and electronic warfare assets located forward.	Provides enhanced EA and ES for assault forces.

b. Defensive Indicators

ACTIVITY	EXPLANATION
Preparation of battalion and company defensive areas consisting of company and platoon strongpoints.	Indicates intent for holding terrain with defense in depth. Normally supported by armored counterattack forces.
Extensive preparation of field fortifications, obstacles, and minefields.	Associated with strong positional defense.
Attachment of additional anti-tank assets to front-line defensive positions.	Indicates intent to contest friendly armor in forward positions; attempt to attrite and channel friendly armor into engagement areas for armor counterattack forces.
Formation of anti-tank strongpoints in depth along avenues of approach.	Intent to allow penetration of friendly armor into rear engagement areas.
Preparation of alternate artillery positions.	Increases survivability of artillery in the defense.
Concentration of armor units in rear area assembly areas.	Armor units held in reserve for possible counterattack/counteroffensive.
Presence of concentrated anti-tank reserves.	Provides quick reaction capability against armor penetrations.
Displacement of logistics and medical units towards the rear.	Logistics and medical units are displaced to facilitate maneuver defense and counterattack.

Pre-stocking of ammunition, supplies, and engineer/pioneer equipment in forward positions.	Pre-stocking reduces the burden on logistics during the battle, reduces vulnerability of interdiction of supplies, and ensures strongpoints can survive for reasonable periods if by-passed or cut off.
Increased depth from the FLOT of artillery and SSM units.	Allows continued employment of artillery during maneuver defense without significant rearward displacement.
Increased use of land line communications.	Land lines imply intent to remain in position and are less vulnerable to EW.
Presence of dummy positions, command posts, and weapons.	Complicates friendly targeting and analysis of actual threat locations and strengths.
Air defense more concentrated in rear areas.	Location of numerous HVTs (armor, logistics, artillery, command posts) dictates strong air defenses in rear areas.

c. Delaying Indicators

ACTIVITY	EXPLANATION
Withdrawal from defensive position(s) before becoming heavily engaged.	In delaying actions, units avoid decisive engagements.
Numerous local counterattacks with limited objectives; counterattacks broken off before position is restored.	Counterattacks are used to assist in disengaging units in contact, rather than restoring positions.
Units leapfrogging to new defensive positions.	Units engage then conduct local withdrawals to new positions while another force takes up the engagement. Units alternate engaging and withdrawing.
Maximum firepower located forward; firing initiated at long ranges.	Intent is to inflict casualties, slow advance, and provide sufficient combat power to avoid decisive engagement.
Extremely large unit frontages as compared to normal defense.	Delaying actions are often economy of force efforts to allow larger formations to withdraw.
Indications of chemical or biological agent weapons in forward areas.	Chemical and biological weapons employed as barriers or in minefields can cause significant delays to the advancing force.
Identification of dummy positions and minefields.	Advancing force forced to determine whether active or inert, causing delays.

d. Withdrawal Indicators. Indications of threat intent to withdraw are often the same as those for delaying actions, with the addition of the following indicators:

ACTIVITY	EXPLANATION
Systematic destruction of bridges, communications facilities, and other assets.	Intent is to deny the advancing force the use of infrastructure and installations in the areas withdrawn from.
Establishment of a covering force or rear guard.	Covers the withdrawal of the main body. Usually consists of a sub-element of the main force. Unlike delay, rear guard is usually the only element engaged.
Increased rearward movement noted at night, particularly during inclement weather.	Units will often attempt to withdraw under the concealment of darkness and weather.
Minimal presence of logistics and medical units. Destruction of dumps and depots.	Nonessential logistics and medical elements are normally withdrawn first. Depots and dumps unable to be moved are destroyed.
Establishing and marking withdrawal routes and traffic control points.	Facilitates the rapid movement of forces rearward.
Preparation of new defensive positions beyond supporting range of present positions.	If the withdrawal is deliberate, the threat will attempt to establish new positions along suitable terrain prior to the arrival of withdrawing forces.
Increased engineer activity and stockpiling of explosives in the threat rear area near bridges, tunnels, built-up areas, etc.	Facilitates maintenance of LOCs for own forces; demolition of infrastructure in front of opposing force.
Rearward movement of long-range artillery.	Long-range artillery will be moved to new positions before withdrawal takes place.
Activation of command posts well removed (beyond doctrinal norms) from the present battle area.	Withdrawing forces will create C2 nodes in the new position/assembly area to command and control arriving forces.

e. MOOTW Indicators. Given the wide range of military operations other than war, the possible indicators of various activities can be enormous. However, most MOOTW evolutions still involve the requirement to identify risks to friendly forces. By their nature, MOOTW are generally concerned with indigenous populations, regardless of the nature of the mission. The following indicators, therefore, focus on those indicators associated with possible threats emerging from an indigenous populations. Once again, these lists are by no means intended to be all-inclusive, but instead provide the analyst with a point of departure for developing case specific indicators.

1. Population

(a) General Activity

- Identification of agitators, insurgents, militias or criminal organizations, their supporters, and sympathizers who suddenly appear in, or move out of, an area.

- New faces in a rural community.

- Unusual gatherings among the population.

- Disruption of normal social patterns.

- Mass urban-rural migration or vice versa.

- Massing of combatants of competing power groups.

- Increase in the size of embassy or consulate staffs from a country or countries which support indigenous disaffected groups, particularly those hostile to the United States and/or the current intervention.

- Increase in neighboring countries of staff and activities at embassies or consulates of countries associated with supporting indigenous disaffected groups.

- Increased travel by suspected subversives or leaders of competing power bases to countries hostile to the United States or opposed to the current intervention.

- Influx of opposition leaders, both resident and expatriate, into the operations area.

- Reports of opposition or disaffected indigenous population receiving military training in foreign countries.

- Increase of visitors (tourists, technicians, businessmen, religious leaders, officials) from groups or countries hostile to the United States or opposed to the current intervention.

- Close connections between diplomatic personnel of hostile countries and local opposition groups.

- Communications between opposition groups and external supporters.

- Increase of disaffected youth gatherings.

- Establishment of organizations (no matter how small) of unexplained origin and with unclear or nebulous aims.

- Establishment of a new organization to replace an existing organizational structure with identical aims.

- Appearance of many new members in existing organizations such as labor unions.

- Infiltration of student organizations by known agitators.

- Appearance of new organizations stressing grievances or interests of repressed or minority groups.

- Reports of large donations to new or revamped organizations.

- Reports of payment to locals for engaging in subversive of hostile activities.

- Reports of the formation of opposition paramilitary or militia organizations.

- Reports of lists of targets for planned opposition attacks.

- Appearance of “professional” agitators in gatherings or demonstrations that result in violence.

- Evidence of the participation of paid and armed demonstrators in riots.

- Significant increase in thefts, armed robberies, and violent crime in rural areas; increase in bank robberies in urban areas.

(b) Opposition-Directed Activity

- Refusal of population to pay rent, taxes, or loan payments or unusual difficulty in collecting the same.

- Trends of demonstrated hostility on the part of the population toward government forces and/or mission force.

- Unexplained disappearance of the population from or avoidance by the people of certain areas.

- Unexplained disappearance or dislocation of young people.

- Reported incidents of attempted recruitment to join new movements or underground organizations.

- Criminals and disaffected youth who appear to be acting with and for the opposition.

- Reports of extortion and other coercion by opposition elements to obtain financial support from the population.

- Use of fear tactics to coerce, control, or influence the local population.

- Reports of surveillance of HN government and/or mission force facilities and personnel.

(c) Activity Directed Against the Government

- Failure of police and informer nets to report accurate information. May indicate sources are actively supporting opposition elements, or have been intimidated into silence.

- Decreasing success of government law enforcement/military infiltration of opposition or disaffected organizations.

- Assassination or disappearance of government sources.

- Reports of attempts to bribe or blackmail government officials, law enforcement employees or mission personnel.

- Reports of attempts to obtain classified information from government officials, government offices, or mission personnel.

- Classified information leaked to the media.

- Sudden affluence of certain government and law enforcement personnel.

- Recurring failure of government or mission force raids on suspected opposition organizations or illegal activities apparently due to forewarning.

- Increased hostile or illegal activity against the government, its law enforcement and military organizations, foreigners, minority groups, and/or competing political, ethnic, linguistic, or religious groups.

- Demonstrations against government forces, minority groups, or foreigners, designed to instigate violent confrontations with government or mission forces.

- Increased anti-government or mission force rhetoric in local media.

- Occurrence of strikes in critical areas intended to cast doubt on the government's ability to maintain order and provide for the people.

- Unexplained loss, destruction, or forgery of government identification cards and passports.

- Recurring unexplained disruption of public utilities.

- Reports of terrorist acts or extortion attempts against local government leaders and businessmen.

- Murder of kidnapping of government, military, and law enforcement officials or mission force personnel.

- Closing of schools.

2. Propaganda

(a) General Propaganda Indicators

- Dissident propaganda from unidentified sources.

- Increases in the number of entertainers with a political message.

- Increase of political themes in religious services.

- Increased appeals directed at intensifying general ethnic or religious unrest in countries where ethnic or religious competition exists.

- Increased agitation on issues for which there is no identified movement or organization.

- Renewed activity by dissident or opposition organizations thought to be defunct or dormant.

- Circulation of petitions advocating opposition or dissident demands.

- Appearance of opposition slogans and pronouncements by word-of-mouth, graffiti, posters, leaflets, etc.

- Propaganda linking local ethnic groups with those in neighboring countries/regions.

- Clandestine radio broadcasts intended to appeal to those with special grievances or to underprivileged ethnic groups.

- Use of bullhorns, truck-mounted loudspeakers, and other public address equipment in “spontaneous” demonstrations.

- Presence of non-media associated photographers among demonstrators.

- Rallies to honor "martyred" opposition personnel. Mass demonstrations honoring local dissident heroes or dates significant to the opposition.

- Nationwide strikes called to demonstrate the strength of the opposition movement(s).

(b) Directed Against the Established Government

- Attempts to discredit or ridicule national or public officials.

- Attempts to discredit the judicial and law enforcement system.

- Characterization of government leaders as puppets and tools of foreign intervention forces.

- Agitation against government projects and plans.

- Radio propaganda from foreign countries, aimed at all or part of the target country's population, accusing its government of failure to meet the needs of its people.

(c) Directed Against the Mission Force and Host Nation (HN) Military and Law Enforcement

- Spreading accusations that the HN military and police are corrupt and out of touch with the people.

- Spreading accusations that mission force personnel will introduce customs or attitudes that are in opposition to local cultural or religious beliefs.

- Character assassinations of mission, military, and law enforcement officials.

- Demands to remove strong anti-opposition or anti-crime military and law enforcement leaders from office.

- Calls for the population to cease cooperating with the mission force and/or HN military and law enforcement.

- Deliberate incidents to provoke mission, military, or police reprisals during demonstrations or strikes.

- Widespread hostile media coverage of even minor criminal violations or incidents involving mission force personnel.

- Accusations of brutality or ineffectiveness or claims that mission/government forces initiated violence following confrontations.

- Publication of photographs portraying repressive and violent acts by mission force or government forces.

- Refusal of businessmen and shop-owners to conduct business with mission force personnel.

(d) Directed Against the Education System

- Appearance of questionable doctrine and teachings in the educational system.

- Creation of ethnic, tribal, religious, or other interest-group schools outside the government educational system, which propagate opposition themes and teachings.

- Charges that the educational system is only training youth to do the governments bidding.

- Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

3. Commodities

(a) Food

- Diversion of crops or meat from markets.

- Unexplained shortages of food supplies when there are no reports of natural causes.

- Increased reports of pilfering foodstuffs.

- Sudden increase in food prices possibly indicating a tax being levied by opposition elements.

- Unwillingness of farmers to transport food to population centers, indicating a fear of traveling highways.

- Spot shortages of foodstuffs in regions or neighborhoods associated with a minority group or weaker competing interest group, while food supplies are generally plentiful in other areas. Conversely, sudden local shortages of foodstuffs in rural areas may indicate the existence of an armed opposition group operating in that region.

- A sudden increase of meat in markets, possibly indicating they are being slaughtered due to lack of fodder to sustain them.

- Appearance of emergency relief supplies for sale in black markets, possibly indicating diversion from starving population.

- Appearance of relief supplies for sale in normal markets, in a country or region recently suffering from large-scale hunger, may indicate the severity of the food crisis is diminishing.

(b) Arms and Ammunition

- Increased loss or theft of weapons from military and police forces.

- Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.

- Attacks on patrols resulting in the loss of weapons and ammunition.

- Increased purchase of surplus military goods.

- Sudden increase in prices for arms and ammunition on the open market.

- Reports of large arms shipments destined for neighboring countries, but not intended for that government.

- Reports of known arms traffickers establishing contacts with opposition elements.

- Increase in armed robberies.

- Reports of thefts or sudden shortages of chemicals which could be used in the clandestine manufacture of explosives.

- Reports of large open-market purchases of explosives-related chemicals without an identifiable industrial user.

- Appearance of arms either manufactured or smuggled from non-contiguous foreign countries.

(c) Clothing

- Unusual systematic purchase or theft of clothing materials which could be used for the manufacture of uniforms or footwear.

- Unusual scarcity of clothing or material used in the manufacture of clothing or footwear.

- Distribution of clothing to underprivileged or minority classes by organizations or recent or suspect origin.

- Discovery of caches of uniform clothing and footwear or the materials which could be used to manufacture the same.

- Increase of males in the streets wearing military style clothing or distinctive markings.

(d) Medicines

- Large-scale purchasing or theft of drugs and medicines or the herbs used to manufacture local remedies.

- Scarcity of drugs and medical supplies on the open or black markets.

- Diversion of medical aid donations.

- Discovery of caches of medical supplies.

(e) Communications

- Increases in the purchase and use of radios.

- Discovery of caches of communications equipment.

- Unusual increase in amateur radio or cellular telephone communications traffic.

4. Environment

(a) Rural

- Evidence of increased foot traffic in the area.

- Increased travel within and into remote or isolated areas.

- Unexplained trails and cold campsites.

- Establishment of new, unexplained agricultural areas, or recently cleared fields.

- Unusual smoke, possibly indicating the presence of a campsite or a form of communication.

- Concentration of dead foliage in an area, possibly indicating use of camouflage.

- Presence of foot traps, spikes, booby-traps, or improvised mines along routes and trails.

(b) Urban

- Apartments, houses or buildings being rented, but not lived in as homes.
- Slogans written on walls, bridges, and streets.
- Defacement of government and mission force information signs.
- Sabotage of electrical power network; pollution of urban area's water supply.
- Terrorist acts against physical targets such as bridges, dams, airfields, or buildings.
- Change of residence of suspected agitators or opposition leaders.
- Discovery of message dead-drops.
- Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.
- Appearance of abnormal amounts of counterfeit currency.
- Increase in bank robberies.
- Work stoppages or slowdowns in essential industries.
- Marked decline in product quality in essential industries.
- Marked increase in equipment failures in essential industries.
- Unexplained explosions in essential utilities and industries.
- Establishment of roadblocks or barricades around neighborhoods associated with opposition elements.
- Attempts to disrupt public transport through sabotage.
- Malicious damage to industrial products or factory machinery.

APPENDIX F

BATTLE DAMAGE ASSESSMENT REPORT FORMAT

The following is an example of a periodic summary battle damage assessment (BDA) report that may be used by MEF major subordinate commands' intelligence personnel to provide consolidated Phase I/Physical Damage Assessment BDA from their subordinates to the intelligence battalion's analysis and production cell. The report is a compilation of BDA reporting from subordinate elements, as well as any additional BDA obtained at the MSC level during the designated time period. The aviation combat element would normally be responsible for providing BDA on any ATO-related missions, while the ground combat element would focus on the results of engagements by their subordinate elements, to include the observed effects of CAS.

The target intelligence/BDA team, analysis and production company, intelligence battalion, is responsible for consolidating, deconflicting, and refining these reports, introducing any additional information and intelligence obtained from other sources, and preparing the overall Phase I BDA (or Physical Destruction Assessment) for the MEF commander. The A&P company would also be responsible for adjusting the MEF OOB databases to reflect combat losses and developing the overall combat strength assessment for each unit. The A&P company target intelligence/BDA team would also prepare Phase II/Combat Strength Assessments based on the consolidated reporting from subordinate, higher and adjacent commands. Formats for BDA reporting to the JTF, theater, and national level will be established in the theater intelligence TTP or as directed by the joint task force commander.

SAMPLE BDA REPORT FORMAT

SUBJECT: 6 HR BDA REPORT (SUBMIT TO Intelligence Battalion's TgtIntel/BDA Team, A&P Cell, AT SPECIFIED TIMES)

REPORTING UNIT:

REPORTING PERIOD (FROM/TO):

ENEMY UNIT OR FACILITY #1: (DOWN TO BDE NAME FOR MANEUVER, BN FOR FIRE SUPPORT, or as directed in unit SOP or OPORD. REPEAT THIS SECTION FOR EACH UNIT OR FACILITY).

UIC OR BE#: DHGKNxxxxx

DAMAGED/DESTROYED:

	LOC	TYPE	#DEST	#DMGD/EXTENT
1. ARMOR:				
2. FIRE SUPPORT:				
3. TRUCKS:				
4. AIR DEFENSE:				
5. C2 SYSTEMS				
6. MOB/CNTRMOB: (Engineers assets, bridges, LOC's, mines, etc.)				
7. CSS:				

	LOC	WIA	KIA
8. PERSONNEL:			

REMARKS:

IF UNIT NAME IS UNKNOWN, INCLUDE TIME OF REPORT (TOR), UNDER HEADING "ENEMY UNIT: UNKNOWN". DO NOT SUMMARIZE: LIST EACH REPORT. FOR EXAMPLE:

ENEMY UNIT: **UNKNOWN**
UIC: **UNKNOWN**

DAMAGED/DESTROYED: LIST ALL UNKNOWN UNIT BDA REPORTS BY TIME

	TOR*	LOC	TYPE	#DEST	#DMGD/EXTENT
1. ARMOR:					
2. FIRE SUPPORT:					
3. TRUCKS:					
4. AIR DEFENSE:					
5. C2 SYSTEMS					
6. MOB/CNTRMOB: (Engineers assets, bridges, LOC's, mines, etc)					
7. CSS:					

	TOR*	LOC	WIA	KIA	EPW
8. PERSONNEL:					

REMARKS: *TOR: TIME OF REPORT. (NOTE: REMARKS ARE A MEANS OF REPORTING INFORMATION THAT DOES NOT FIT INTO THE TABLES DESCRIBED ABOVE. SPELL IT OUT IN A REMARKS SECTION, FOR EACH UNIT IF NECESSARY, IF YOUR ASSESSMENT GOES BEYOND "BEAN COUNTING".)

APPENDIX G

INTELLIGENCE SUMMARY FORMAT

The INTSUM provides a summary of the reporting unit's intelligence situation covering a specified period of time. It is used to report threat activities, changes to threat capabilities, and the results of further collections, analysis and production to higher, adjacent, and subordinate forces. It is designed to update the current intelligence estimate and provide a continual intelligence assessment of threat actions and estimated capabilities and courses of action.

Guidance regarding the periodicity and deadline for submission of INTSUMs generally begins at the theater J-2 level. Theater TTPs and the specific OPLAN/OPORDER will designate INTSUM reporting requirements for subordinate JTFs or Service/functional components. Based on those requirements, the MAGTF G-2/S-2 (at the MEF CE level, the intelligence support coordinator) will establish INTSUM reporting requirements for their subordinate commands/elements, and publish those requirements as part of their OPLAN/OPORDER. The deadlines established are to allow the intelligence battalions analysis and production cell sufficient time to incorporate subordinate INTSUMs into their own. The G-2/S-2s of MAGTF subordinate elements will likewise determine INTSUM requirements for their subordinate elements. Where possible, MEF TTPs and SOPs, reflecting the TTPs of anticipated theaters of operations, should establish standard INTSUM reporting requirements.

Theoretically, all units can produce INTSUMs, however, in practice they are normally generated at the MSC level or higher. The decision to produce INTSUMs at lower echelons must be balanced between the relatively small size of intelligence sections at regiment/group and battalion/squadron and the requirement for information and intelligence at higher command levels. A more abbreviated INTSUM format may be appropriate for lower tactical echelons, focused on significant threat actions and anticipated future actions.

At higher command levels, particularly JTFs and Unified Commands, a DISUM, or daily intelligence summary, will be published every 24 hours. While INTSUMs, particularly at lower tactical echelons, provide a generally fine-grained but limited tactical perspective, the DISUM is more broad in scope, potentially encompasses more aspects of a threat country's elements of national power, and focuses on operational-level analysis and estimates. MAGTF command elements tasked as JTF headquarters will generally be required to submit DISUMs to the combatant command CINC. See the combatant command's TTP for the DISUM format. Although generally the same, formats may vary from theater to theater.

Below is provided a sample format for an written INTSUM that may be posted on a website. It is generally based on the intelligence estimate format. Like the intelligence estimate, the INTSUM should be tailored and focused to mission, the type of unit, and the information and intelligence needs of the commander. The format provided is representative of a format that would be used at the MAGTF or MSC level for conventional military operations. For MOOTW evolutions, the format generally will need to be modified.

Note: For paragraphs not applicable to the reporting unit, the notation "NA" (not applicable) may be used, or the paragraph may be skipped (paragraph numbering should remain the same). If no significant information or intelligence is available for a particular paragraph, the notation "NSTR" (nothing significant to report) may be used. The annotation ( ) reflects classification of that information line.

CLASSIFICATION/RELEASABILTY
INTSUM #: (Sequentially numbered such, as "DD-001-97")
DTG: DDHHMM(Time Zone) (Month) YY
INFO cutoff DTG
PERIOD: DDHHMM TO DDHHMM (Month) YY

I. ( ) Highlights:

A. ( ) Ground: Highlights of the current ground situation, usually divided by area or sector.

B. ( ) Air: Highlights of the current air situation.

II. ( ) Summary of Enemy Situation: (Each category should use the commander's related PIRs as the basis for the analysis and assessment.)

A. ( ) Ground: Detailed analysis of the battlefield by area or sector with comments on projected activity in the next 12 hours.

B. ( ) Air: Detailed analysis of the air and air defense situation with comments on projected activity in the next 12 hours.

C. ( ) Naval: Detailed analysis of the naval situation with comments on projected activity in the next 12 hours.

D. ( ) SSM/WMD: Detailed analysis of the SSM/WMD situation with comments on projected activity in the next 12 hours.

E. ( ) SOF Forces: Detailed analysis of the SOF, force protection, and rear area security situation with comments on projected activity in the next 12 hours.

F. ( ) Other: May be used for detailed analysis of paramilitary, insurgent, terrorist, or other significant threat categories not discussed elsewhere. For MOOTW operations, separate paragraphs for each category of threat or significant power group may be created as necessary to either supplement are replace the above categories.

III. ( ) MEF (or MSC) Assessment:

A. ( ) Most Likely Course of Action:

B. ( ) Most Dangerous Course of Action:

C. ( ) Others (as necessary):

IV. ( ) Enemy Movement During the Reporting Period: Major enemy units (to include at least two levels below that of the reporting command); include UTM coordinates of the new position.

V. ( ) PIRs: The commander's current (previous and new) PIRs are listed here, each with a current assessment regarding the level of satisfaction of the intelligence requirement (i.e.. partially satisfied, satisfied, not satisfied).

VI. ( ) Intelligence Plans, Missions and Systems Status: Key intelligence collection, production, and dissemination plans updates; information on planned intelligence and reconnaissance missions; and intelligence systems status (generally only for those systems that are less than fully operational). The period covered by this paragraph will be per unit SOP or annex B to the operations order.

GRAPHIC INTSUM

In an effort to enhance the understanding of the INTSUM, and save clogging communications lines with disseminating a written INTSUM, it is now common to graphically portray the INTSUM as a single or set of map overlays. With the proliferation of web-based automated information systems, it is increasingly common for INTSUMs to be "posted" in graphic and text formats, providing a wide range of MAGTF intelligence users the option to "pull" and use desired intelligence and products. By posting the graphics and supporting text products to a website (e.g., INTELINK or INTELINK-S), it is available to anyone with access to that site, to include operations personnel using systems such as TCO. Care must be exercised, however, to not place an over-reliance on electronically generated graphic INTSUMs. Graphics can require large bandwith and processing power to be pulled over a web-based system, with possible degradation of the overall MAGTF tactical data network. Lower-level tactical units and allied nation forces may also not possess the means to access and use the information. This generally requires INTSUMs to be disseminated over multiple paths, both electronically and via hard copy (to sometimes include couriers), in both graphic and text form.

The challenge with graphic INTSUMs, as with any graphic representation, is to convey essential intelligence and other information in a clear, concise, and easy to understand visual format. Because of the volume of detail to be presented, most graphic INTSUMs, particularly at higher commands, have evolved into multiple "slides" created with software such as Microsoft Power Point. There is no one approved format for graphic INTSUMs; they are established per unit SOP or the operations order (see annex B, *Intelligence*) tailored to the level of command, type of

operation, and most importantly, the intelligence requirements of the commander. They do, however, generally contain the same elements. Listed below are some common elements of graphic INTSUMs. These should not be taken as absolutes, but instead as examples.

- **Weather Graphic(s) -** Composite graphics, based on satellite imaging, showing weather fronts, cloud coverage, high and low pressure areas, etc. for the area. May include forecast graphics for specified future periods.

- **5-Day Forecast -** Similar to television weather forecasts, showing forecast weather conditions (cloudy, partly cloudy, rainy, etc.), high and low temperatures, winds, normal temperatures based on climatology, and any other elements that may be of interest to the commander. Should also include light data for the same period.

- **Weather Impacts Graphic(s) -** Normally presented in "gumball" chart (green, yellow, red) format. Should include those forces, types of operations, or critical items of equipment that are essential to unit mission performance, both friendly and enemy.

- **PIRs -** Include current and new PIRs. May include assessment of level of satisfaction (not answered, partially answered, answered).

- **Activities and Assessments -** Consists of a graphical situation map, denoting locations of threat forces of interest and, if possible, graphically indicating status/combat effectiveness (color coding or other symbology). Depending on the level of command and information needs, separate graphics for categories of threat forces (ground, air, air defense) may be created to reduce clutter. Each graphic should:

  -- Note significant threat activity over the reporting period, with text comment boxes tied to locations or an event numbering system with marginal text comments.

  -- Provide an assessment(s) keyed to the commander's PIRs.

  -- Use supporting graphics to examine items in more detail, such as aircraft sortie analysis or the location and status of a particular category of force or equipment (i.e.. HETs, specialized units, etc.)

- **Collection, Production, and Dissemination Plans and Status of Planned Missions and Tasks -** Graphically presents locations of organic collection assets (reconnaissance teams, RADBN assets, UAV tracks, sensor strings, etc.) and/or provides a timeline showing daily projected availability windows and mission-tracks (as applicable) of non-organic supporting assets (AWACS, RC-135, U2, etc.). Also identifies changes to previous production and dissemination plans and any new plans.

- **Outlook/Assessment-** Provides overall assessment of estimated threat COA(s) (at a minimum, the threat's most likely and most dangerous COAs). It may be broken into estimate time periods, such as 24-48 hours, 48-96 hours, or whatever periods of time are applicable to the commands requirements to plan future actions. COAs should be graphically portrayed. In pre-hostilities or MOOTW, these graphics may be used to address anticipated political or societal actions/events that may impact on the force.

APPENDIX H

INTELLIGENCE REPORT FORMAT

An intelligence report (INTREP) is a standardized report which is used to disseminate important intelligence without regard to a specific schedule. It can be prepared at any echelon by the first intelligence element acquiring the information and is disseminated as rapidly as possible to all units which may have need of the reported information. It may be prepared on any item of intelligence, regardless of source; generally, each report will concern only a single item.

An INTREP is generally required whenever an event occurs that is likely to result in a change in the friendly plan or when a change to the current or future analytical assessment is made. It is generally initiated when facts influencing threat capabilities have been observed, or when a change in threat capabilities has taken place. The commander's PIRs serve as the basis for determining what information warrants an INTREP. Whenever possible, the INTREP should include the originator's assessment of the significance of the intelligence, as well as an evaluation of the reliability and accuracy of the source. The format below provides an example of an INTREP format that would be posted on a website or forwarded via SIPRNET email.

INTREP FORMAT

```
CLASSIFICATION/RELEASABILITY
INTREP#:  DD-001-97 (Sequentially numbered by originating unit)
DTG:  DDHHMM(Time Zone) (Month) YY

I.  ( ) Significant Event(s): A summation of the significant
event(s) or developments that initiated the INTREP.  Use either
the "5Ws" (i.e., Who, What, Where, When, Why) or the SALUTE
(i.e., Situation, Activity, Location, Unit, Time, Equipment)
formats.

II.  ( ) Assessment: The effect of the current activity on threat
capabilities or courses of action.

III.  ( ) Evaluation of Source:  State the original source of the
information and an evaluation of the accuracy and reliability of
that source.

Note: ( ) Reflects classification of that information line.
```

APPENDIX I

INTELLIGENCE INFORMATION BRIEF FORMAT

Of the three most common types of military briefings --information, decision, and confirmation-- intelligence personnel will most often be required to provide intelligence information briefings. The intent of the intelligence information brief is to enhance situational awareness and impart understanding. Intelligence information briefings may be as simple as a quick verbal update to a commander in front of a situation map, or as complex as a MEF or JTF level daily update to the commanding general and his staff. Briefings at lower tactical levels, where the element of time is often scarce, will be generally less formal, but often short-notice. Higher commands generally employ regular, scheduled, daily update briefings, of which intelligence is only one part. Regardless of the degree of formality or the level of command, a standard briefing format or outline can assist intelligence personnel in rapidly and effectively organizing for the brief.

The keys to developing and delivering an effective intelligence information brief are as follows:

- Know your audience. Is it the commander, his staff, his subordinate commanders? Who is the focus of the brief? What is their level of knowledge concerning the subject? Does the commander have any personal preferences as to how he is briefed?

- Be sure of the purpose and intent of the briefing. Is the brief an update on critical events in the last couple of hours, or is it intended to describe in detail the threat and area of operations prior to the initiation of crisis action planning?

- Concentrate on essential information and intelligence, but be prepared to provide details or expanded intelligence should questions arise.

- Use clear, concise, readable graphics. If presenting to a large audience, ensure the graphics can be seen from the rear of the room or, at a minimum, by your primary target audience.

- **Know your information.** If you anticipate questions on subjects where you have little depth, either arrange to have someone there that does, or take the question for follow-up research. Admit when you don't know something; never make up an answer.

- Always distinguish between what you know (facts), what you don't know (gaps), and what you think (estimates).

The most common types of intelligence information briefing are the "boardwalk" and, at higher command echelons, the commander's morning/evening update briefs. The boardwalk is an informal, on-demand brief conducted using the COC map boards or screen displays from automated systems. The brief is generally by exception, meaning only significant changes to threat capabilities or courses of action are briefed. It is also an opportunity for the commander to ask directed questions.

APPENDIX J

PRODUCTION REQUIREMENT AND REQUEST FOR INTELLIGENCE FORMAT

At the most basic level, a intelligence production requiremnt (IPR), production requirement (PR) or request for intelligence (RFI) begins as an intelligence requirement (IR) levied on a unit's intelligence section. If the unit cannot satisfy the requirement within the resources available to them, the requirement must be forwarded up the chain of command for satisfaction. At this point the requirement becomes either an intelligence collection requirement (ICR), a RFI, or an intelligence PR (IPR). At any level, singular or multiple requests for information may be combined into one production requirement.

Regardless of the type of requirement, at the most basic level there are four required elements:

- Who - Organization and specific office or individual that submitted the original requirement.
- What - Statement describing the intelligence required.
- When - Latest time information of value.
- How - Form that the product should be delivered in (hard-copy, soft-copy, verbal report, quantities, all units to receive these, etc.)

Most theater TTP tend to combine all three forms of requirements into one basic PR/RFI format. The receiving HTF headquarters J-2 or combatant command JIC will then take that requirement and determine whether collection is necessary and whether or not an actual product needs to be developed. DIA has also established a basic PR/RFI format. This format is used in the Community On-Line Intelligence System for End Users and Managers (COLISEUM), which has become the standard medium for requirements submission throughout the DOD Intelligence Production Community. The format provided below is the COLISEUM format and can be found in the Defense Intelligence Management Document *Department of Defense Intelligence Production Program: Production Procedures (U)*, DoD-0000-151C-95. Although the theater TTP formats generally follow the same elements, in some cases they have been modified according to the specific needs of that theater. MAGTFs (particularly MEFs and their intelligence battalions) and MARFORs headquarters must pay particular attention to the procedures established in their theater(s) of operations.

Item 1. PR Number: A 12-space number having 10 characters. This number is entered by the unit intelligence section and is unique to the unit requesting the information/production. The first four characters are the customer's SII account number (or UIC in a crisis). The second two numbers are the fiscal year. The last four numbers are the customer's sequence number for PRs/RFIs submitted in the fiscal year. (e.g. C610-94-0001)

Item 2. Subject: A short descriptive title which, if possible, provides a good idea of the topic and scope and is unclassified. Clarity is more important than keeping the subject unclassified.

Item 3. Customer's Organization: This is the end customer(s) to whom the intelligence product(s) will be disseminated. This line should include a name, organization, mailing address, e-mail address (clearly identify if JWICS or SIPRNET, naval message address, and commercial and DSN phone numbers of the customer if possible.

Item 4. Date of Request: Entered by the supporting Intelligence Office in YYMMDD format.

Item 5. Date Product Required: The latest date the customer can receive the product/information and have it still be of value. Also referred to as LTIOV.

Item 6. Form and Frequency of Response: This section is key to getting the desired response to the requirement. All subitems should be narrative with an emphasis on clarity.

- **Media.** This is the form that the response should take. The request should identify the preferred form along with second and third alternatives. Examples are message, floppy disk, CD-ROM, on-line data base, data base printout, bound hardcopy report/study/handbook, etc. In addition to the media requested, the production element often will also disseminate the intelligence and other pertinent information in other media to increase access to a wider number of potential users.

- **Frequency.** A request for scheduled production (non-crisis related) can specify frequency as one-time, as required, or recurring. Requests for crisis or immediate production are normally handled as one-time requests unless otherwise specified.

- **Revision or New Product.** If a product already exists that requires update, specify the product as completely as possible. Otherwise, specify as a new PR.

- **Classification and Releasability.** Provide the desired classification and the highest classification that can be used by the customer. If the product needs to be releasable to foreign forces, specify which forces (if known) and justify.

Item 7. Statement of Requirement: The first paragraph should provide a summary of the requirement in 50 words or less. If the requirement supports an OPLAN/CONPLAN, the first sentence should identify which plan. Subsequent paragraphs should be used to provide greater detail, specific intelligence and information elements, and justification. The justification should specify what intelligence and other information sources have already been consulted and why they were not sufficient to answer the requirement. If the requirement addresses separate questions, or multiple countries/topics, they must be prioritized. If all carry the same priority, list them by time urgency.

Item 8. Comments: Available for any additional comments as necessary.

Item 9. Security Classification: The highest classification of the question and information contained in the requirement. Obviously, the lower the classification, the easier it will be to process and use. However, clarity should not be sacrificed for a lower classification. Codeword or special access program requirements will be submitted through the appropriate channels and will likely require additional time to transmit and process.