
Information Management



U.S. Marine Corps

Coordinating Draft of 1 June 2000

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20308-1775

xx Month 1999

FOREWORD

1. PURPOSE

Marine Corps Warfighting Publication (MCWP) 6-23, *Information Management*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*. MCWP 6-23 discusses the role of “*information*” as one of the three basic elements of command and control (C2): people, information, command and control support structure.

2. SCOPE

This publication discusses how information supports the C2 process and decisionmaking. It provides a variety of techniques and guidelines to effectively manage information used to support decisionmaking. More detailed tactics, techniques and procedures (TTPs) are provided by MCRP 6-23 (E), *Information Management TTP*. MCWP 6-23 supports all users and handlers of information who plan, make decisions, execute, and conduct assessments. MCWP 6-23 discusses the following key topics:

- Fundamentals of information.
- Personnel responsibilities.
- Command and control support (C2S) structure development.
- Security of information

3. SUPERSESION

None.

4. RECOMMENDATIONS AND CHANGES

Recommendations and changes for improving this publication are invited from commands as well as directly from individuals. Forward suggestions using the user suggestion format via either of the following means:

COMMANDING GENERAL
DOCTRINE DIVISION (C421)
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VIRGINIA 22134-5021

E-mail:

Banyan — FORCE[smb@doctrine div@mccdc]
Internet — smb@quantico.usmc.mil

Recommendations should include the following information:

- Location of change: publication number and title; current page number; paragraph number (if applicable); line number; figure number (if applicable).

- Nature of change: add, delete; and proposed new text (preferably double-spaced and typewritten).
- Justification and/or source of change.

5. OBTAINING ADDITIONAL COPIES

Additional printed copies of MCWP 6-23 may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. Electronic copies may be obtained from the Doctrine Division, MCCDC, worldwide web homepage which is found at the following universal reference locator (letters in lower case): **<http://138.156.107.3/docdiv>**.

6. ADDITIONAL INFORMATION

- The proponent for MCWP 6-23 is the Marine Air-Ground Task Force Staff Training Program (MSTP), Marine Corps Combat Development Command.
- Unless otherwise stated, whenever the masculine or feminine gender is used, both men and women are indicated.

7. CERTIFICATION

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

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

DISTRIBUTION: 143 000xx 00

Table of Contents

	Page
Chapter 1. Information	
1001. Introduction	1-1
1002. Principles	1-3
1003. Hierarchy	1-3
1004. Information Quality Characteristics	1-5
1005. Information Format	1-5
1006. Information Management Filtering Tools	1-5
1007. Assessment	1-6
1008. Understanding	1-7
1009. Relationship between Common Operational Picture, Common Tactical Picture, and Common Tactical Dataset	1-8
1010. Decision Support Matrix	1-9
1011. Planned Decisions	1-10
1012. Spontaneous or “Unplanned” Decisions	1-11
Chapter 2. Personnel and Duties	
2001. Key Information Management Functions	2-1
2002. Organizations that Influence Information Management	2-4
2003. Information Management Coordination Cells	2-5
2004. Security Personnel	2-6
2005. Information and Information System User Responsibilities	2-7
Chapter 3. Command and Control Support Structure Development	
3001. Advantages	3-1
3002. Information Flow	3-1
3003. Process Flow	3-2
3004. Configuration Flow	3-3
3005. Personnel Requirements	3-4
3006. Documentation	3-4
3007. Request for Information Management	3-5
3008. Information Management Plan	3-6
3009. Networks	3-7
Chapter 4. Security	
4001. Information Assurance	4-1
4002. Protection	4-1
4003. Virus Attack	4-2
4004. Virus Protection	4-2
4005. Information Security	4-3
4006. Future Initiatives	4-4

Appendices

A	Information Management Annex Format	A-1
B	Information Management Support to Planning	B-1
C	Information Management Support to Execution	C-1
D	Integrated Training	D-1
E	Information Management in an Exercise Environment	E-1
F	Glossary	F-1
G	References	G-1

Figures

1-1	Elements of Command and Control	1-2
1-2	Information Flow through the Information Hierarchy	1-4
1-3	Planning, Decision, Execution, and Assessment Cycle	1-7
1-4	Managing Information to Support Planned Decisions	1-10
1-5	Managing Information to Support to Unplanned Decisions	1-11
3-1	Process Flow for Collect Intelligence	3-3
3-2	Configuration Flow for Collect Intelligence	3-3
3-3	Personnel Requirements for Collect Intelligence	3-4
3-4	Example of a Process Flow Used to Support Request for Information Management	3-5
B-1	The Marine Corps Planning Process	B-1
B-2	Mission Analysis	B-2
B-3	Using MS Exchange to Record Commander's Battlespace Area Evaluation	B-2
B-4	Visual Display Product	B-3
B-5	Mission Analysis Products	B-3
B-6	Course of Action Development	B-4
B-7	Course of Action Development Products	B-5
B-8	Course of Action War Game	B-5
B-9	Course of Action War Game Products	B-6
B-10	Course of Action Comparison and Decision	B-6
B-11	Course of Action Comparison and Decision Products	B-7
B-12	Orders Development	B-7
B-13	Orders Development Products	B-8
B-14	Transition	B-8
B-15	Transition Products	B-9
C-1	Example of a Decision Support Matrix Used to Develop a Decision Support Template	C-1
E-1	Configuration to Support an Exercise	E-2

Tables

1-1	Information Quality Characteristics	1-5
1-2	Sample Decision Support Matrix	1-9
E-1	Real-Time to Game-Time Matrix	E-1

Chapter 1

Information

“The commander must work in a medium which his eyes cannot see, which his best deductive powers cannot always fathom, and with which, because of constant changes, he can rarely become familiar.”

—von Clausewitz

Commanders require quality information to understand situations and events and to quickly control the challenges that confront them. Quality information, that which adds value to the decisionmaking process, can determine success or failure. Management of this information is critical. Marine Corps unit headquarters are predominantly organized along warfighting functional boundaries. Information has traditionally flowed into and through the staff sections, restricted by their functional boundaries. The Marine Corps operating environment of today and the emerging concepts of tomorrow require force mobility, unit dispersion, and mission depth. As we move into the 21st Century, the ability to simultaneously share useful information with personnel at distant locations will be required to support command and control processes that satisfy decisions made throughout the decision cycle. These requirements contribute to the growing information challenge facing the Marine air-ground task force (MAGTF). Effective information management (IM) can deliver critically important information in a timely manner to those whom need it in a form they quickly understand.

Commanders make decisions based on their understanding of the location, disposition, and status of friendly and threat forces. Historically, they achieved situation awareness by personally viewing the battle. As the size and scope of competing forces increased, the ability of the commander to understand the battle became limited. Commanders have tried to improve their feel of the battle by reviewing information displayed on situation maps, text files (messages, reports, status boards, etc.), and voice reports. The situation map and text information, combined with the commander's experience (intuitive reasoning, judgment) and personal contact with frontline units, enabled the commander to attain a level of understanding he required to make decisions. Information that provided enhanced understanding of the situation or event was often available, but not provided to those that required it in a form they quickly understood. Technologies used to manage information were often slow and cumbersome. Functional capabilities used to manage information made it difficult to disseminate quality information simultaneously to multiple dispersed units at all levels of command. Rarely did each level of command reach the same level of understanding needed to make informed decisions.

Today, commanders and staff still rely on quality information to attain an understanding of the battlespace. Information requirements remain relatively the same. What has changed over time is the technological capability to produce more data. Commands now possess the ability to simultaneously disseminate quality information used to support all aspects of the planning, decision, execution, and assessment cycle for multiple dispersed units. Automated capabilities and commonly understood procedures can now be used to display battlespace information in a dynamic environment.

1001. Introduction

Our environment now threatens to overwhelm us with information. Technological advances place enormous amounts of information virtually at the commander's fingertips. More information is available than one Marine can possibly collate, assimilate, and evaluate. The temptation is to use information technology to provide vast amounts of information to everyone in the hope of reducing uncertainty. However, combat is by its very nature chaotic, disruptive and unpredictable. Information collected in such an environment can often be inaccurate or misleading. Most of the

information may not be important, relevant, or available within the time constraints of the commander's decisionmaking process. Collecting and disseminating more information will not reduce information overload. The philosophy contained in MCDP-6, *Command and Control*, emphasizes that Marines must learn to operate in an environment of uncertainty. It states that information serves two purposes—

- To help create situation awareness as the basis for decisions.
- To direct and coordinate actions in the execution of a decision.

IM offers a solution to the information requirements of decisionmaking. Effective IM procedures enables users to reap the benefits of technology—to provide quality information to commanders, facilitating decisionmaking, while avoiding information overload.

IM is defined in this publication as the sum of all activities involved in the identification, collection, filtering, fusing, processing, dissemination and usage of information. Information that promotes understanding of the battlespace enables commanders to better formulate and analyze courses of action, make decisions, execute those decisions with adjustments to the plan as necessary, and accurately understand results from previously made decisions. IM focuses on providing quality information used to support decisionmaking. IM addresses information as a commodity instead of a technology and is performed at all levels, regardless of the extent of automation. The goal of IM is to provide a timely flow of quality information, enabling the commander to anticipate and understand the consequences of changing conditions.

MCDP 6 states that the three elements of command and control (C2) are *information, people*, and *command and control support (C2S) structure*. See figure 1-1. Information addresses information requirements and information flow. People addresses command relationships and organization of the force. C2S addresses organizations, procedures, equipment, and facilities used to assist command and control processes. All three basic elements of C2 interact to produce effective and harmonious actions.

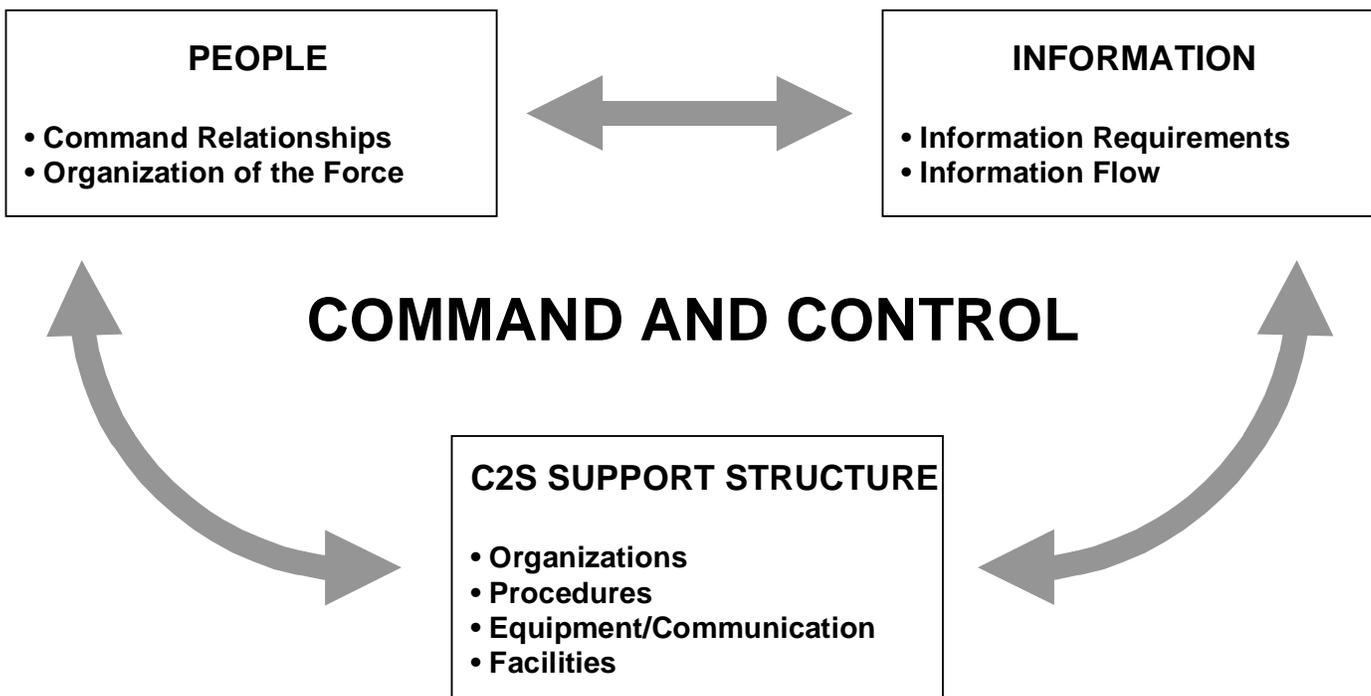


Figure 1-1. Elements of command and control.

The remainder of this publication examines the way in which these three basic elements of C2, supported by an aggressive information security program, assist the command to develop and execute effective information management procedures that support all aspects of decisionmaking. This chapter will address information, tools to filter information, and the role that information plays to support decisionmaking.

1002. Principles

The following principles are required to efficiently and effectively manage information necessary to support decisionmaking. These principles are addressed throughout the rest of this publication and should guide the information management program at every level of command. The principles of IM apply in every situation in which a decision is made.

- **Use Requirements to Define the Information Flow.** Command relationships, organization of the force, and information needs influence the flow of information. Recognition of user requirements and the resulting information flow allows commands to apply the proper mix of personnel, equipment, training, procedures and network infrastructure to produce information that they need to make decisions.
- **Tailor Information for the Commander.** Filter out unnecessary, redundant, or irrelevant information according to the defined information requirements in order to prevent information overload. Provide information in a format that the commander has specified.
- **Use Multiple Sources of Information.** Knowledge is normally gained from information derived from fused products. Use of multiple sources normally improves information accuracy and reduces error. Use of multiple sources also increases network traffic and can add to the delay between gathering information and gaining knowledge. There needs to be a balance between collecting, processing and dissemination.
- **Deliver Information on Time.** Information provided late supports command chronologies, not decisionmaking. When information requirements are defined, the requirements should be in sufficient detail to enable personnel to determine *when* the information is required.
- **Disseminate Accurate and Relevant Information.** Inaccurate or irrelevant information is worse than no information at all. However, even fragmentary information that supports critical information requirements may be of some value, if validated and provided in a timely manner in a form that is clearly understood.
- **Create Flexible and Redundant Procedures and Plans.** The IM plan must be able to overcome changes generated by battle damage, sudden increases in the volume of information, and the needs reflected by different commanders at all echelons of command. The IM plan should have redundant capabilities and incorporate back-up procedures, alternate paths, and primary and alternate personnel/organizations. It should avoid having any “single point of failure” anywhere in the network, security, information, or information assurance architectures.
- **Protect Information Through a Vigorous Security Program.** IM must assure the integrity of the information and the sources/databases from which that information was derived. Corrupted or degraded information is of little value and will adversely affect the quality of the decisionmaking process.

1003. Hierarchy

The term “information” is generically used to refer to all “facts, data, or instructions in any medium or form” (Joint Pub 0-1). Information is broken down into four different classes: *raw data*, *processed data*, *knowledge*, and *understanding*, each of which holds different value, supporting its own role in the decisionmaking process. As information moves through the information hierarchy (see figure 1-2), it becomes more valuable to the decisionmaker.

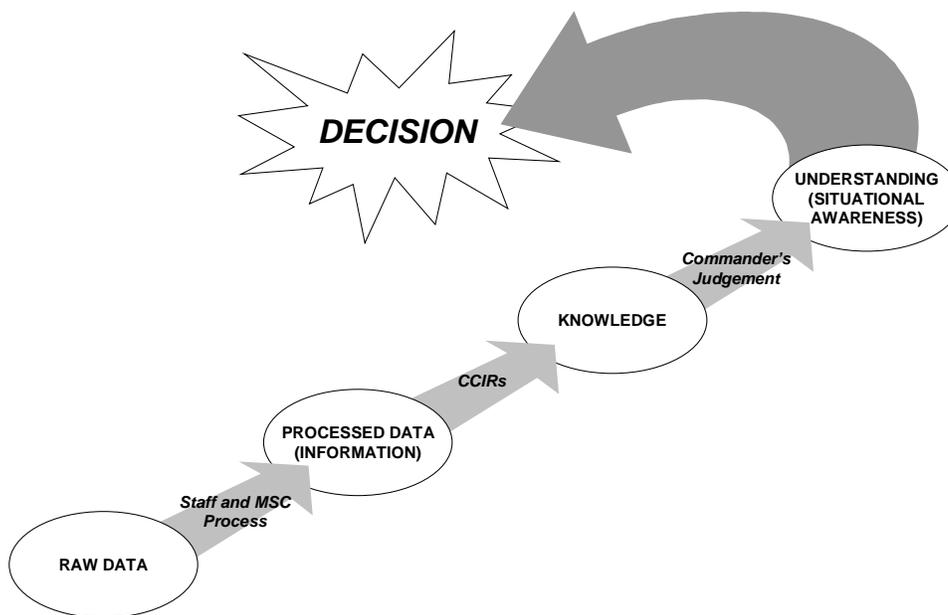


Figure 1-2. Information flow through the information hierarchy.

a. Classes of Information

- **Raw Data.** Raw data are the facts and individual pieces of information (data) that are the building blocks of processed information. This initial class of information is rarely of much use until transformed and processed in some way to give it meaning.
- **Processed Data.** Processed data comes from organizing, correlating, comparing, processing, and filtering raw data and making it readily understandable to the potential user. The act of processing gives the information a limited amount of value. Processed data may have some immediate, obvious and significant tactical value but it has not been evaluated or analyzed.
- **Knowledge.** Knowledge is the result of analyzing, integrating and interpreting processed data; it brings meaning and value to a situation or event. Simply put, knowledge is a representation of “what” is happening.
- **Understanding.** Understanding is the highest level of information and the most valuable. Understanding is an appreciation for “why” things are happening. Understandings results when personnel synthesize bodies of knowledge and then apply experience, judgment, and intuition to reduce gaps generated by uncertainty to arrive at a complete mental image of the situation. MCDP 6 states, “*Understanding means we have gained knowledge and achieved situation awareness. Understanding allows the commander to be better prepared to anticipate future events and to make sound decisions, even in the face of uncertainty*”.

The graduations between the different classes of information may not always be clear. The goal of IM is to facilitate the development of *quality* information throughout the information hierarchy, thus increasing its value and relevance, and ensure the development of understanding by the commander.

b. Situational Awareness

Situational awareness permits the commander to make decisions with incomplete information—less than perfect understanding. Situational awareness is a personal perspective or ability to determine the relevance of unfolding events. There are two elements of situational awareness.

- **Information.** The staff and major subordinate commands provide analytical information in the form of feedback to help build the commander's understanding of the situation.
- **Skill.** The commander must provide the intuitive aspect of situational awareness in order to understand the situation in the absence of complete information. It is a personal element of situational awareness that is based on the commander's experience, education, judgement, and intuition.

The combination of information and skill provides the commander with an image of the situation from which he can base future decisions. Some level of situational awareness can be achieved with raw data. Situational awareness tends to strengthen as information higher in the information hierarchy is received. Enhanced situational awareness enables the commander to be better prepared to anticipate future conditions, visualize operations, provide guidance and accurately assess situations. Developing accurate situation awareness with limited and uncertain information under severe time constraints is the fundamental challenge of IM.

1004. Information Quality Characteristics

Quality information adds value to the decisionmaking process. Information is susceptible to distortion, both by the enemy (intended) and by friendly sources (unintended). In the face of uncertainty, it is important to consider information quality characteristics (outlined in table 1-1).

ACCURACY	Information that conveys the true situation
RELEVANCE	Information that applies to the mission, task, or situation at hand
TIMELINESS	Information that is available in time to make decisions
USABILITY	Information that is in common, easily understood format and displays
COMPLETENESS	All necessary information required by the decisionmaker
BREVITY	Information that has only the level of detail required
SECURITY	Information that has been afforded adequate protection where required

Table 1-1. Information quality characteristics.

1005. Information Format

Recognizing the personality of the commander enables the staff to produce information in a format tailored to the commander's needs. Some commanders prefer visual products, yet other commanders prefer textual information, while still others may require a combination of several products to attain *understanding*. It is important for the staff to clearly learn which form of information is most *useable* to the commander. For example, sight is the most used human sense and 75% of all environmental stimuli are received through visual reception. Retention rate of graphic presentations is four times that of verbal presentations. Whether visual, textual, or verbal, the presentation format should be commonly understood and used consistently to minimize confusion and facilitate understanding.

1006. Information Management Filtering Tools

In the example provided by figure 1-2, information management tools can be used to filter large volumes of available data to permit the efficient flow of quality information through the information hierarchy. These tools provide the necessary guidance to identify information that satisfies critical information requirements linked to key decisions. The commander frames the development of information filtering tools. *Commander's intent, commander's guidance, and commander's critical information requirements (CCIR)* enable personnel to enhance the transmission of information used to support decisionmaking.

a. Commander's Intent

MCWP 5-1, *Marine Corps Planning Process*, states, "Commander's intent is the commander's personal expression of the purpose of the operation. It must be clear, concise, and easily understood. It may also include how the commander envisions achieving a decision as well as the end state or conditions, that when satisfied, accomplish the purpose." The commander's intent establishes the standards by which success will be judged. Through commander's intent the aims of the commander are articulated, his information requirements can be discerned, and the framework for effective information management is formed.

b. Planning Guidance

Commander's guidance is clear, concise guidance that forms the basis for planning. Although not prescriptive in nature, the planning guidance assists the staff to make initial judgments on the ways and means to achieve a decision. Based on his personal experience and judgment, the commander articulates clear and concise guidance that helps to focus the information management efforts of the staff and subordinate commanders.

c. Commander's Critical Information Requirements

As stated in MCWP 5-1, *Marine Corps Planning Process*, CCIR are a tool for the commander to reduce information gaps generated by uncertainties that he may have concerning his own force, the threat, and the environment. CCIR define the information required by the commander to better understand the battlespace and to make sound, timely decisions. CCIR are information requirements, identified by the commander, that once answered, enable the commander to better understand the flow of the operation, identify risks, and make timely decisions to retain the initiative. CCIR aid the commander by reducing information needs to a manageable set. More importantly, they focus the staff on the type and form of quality information required by the commander. Instead of reacting to the threat, commanders are able to maintain tempo by controlling the flow of quality information they require to attain the level of understanding they need within the battlespace. As events unfold, information requirements may change as new decisions are required. CCIR are continuously assessed for relevance to support current and future decisions/situations. The commander approves CCIR, but the staff recommends and manages CCIR to assist the commander. The commander identifies CCIR in the following three categories—

- **Friendly Activities.** Information the commander needs pertaining to his assigned forces to make timely and appropriate decisions. This category includes such information as force closure, critical supply levels, and levels of combat effectiveness.
- **Threat Activities.** Critical items of information required by a particular time that relates with other available information and intelligence, to assist in assessing and understanding the situation. This category involves indications and warnings of threat intent and/or actions by the threat. Examples include information regarding troop movements, changes in opposing force intents or policies.
- **Environment.** Critical information the commander needs to understand regarding the battlespace environment. This includes, but is not limited to meteorological conditions, supporting infrastructure, geopolitical considerations, and relevant activities of non-governmental and private organizations.

1007. Assessment

Assessment is the final step in the planning, decision, execution, and assessment cycle. The planning, decision, execution, and assessment cycle is the process the commander and his staff use to plan operations, make accurate and timely decisions, direct effective execution of operations, and assess the results of those operations. It is a framework that supports the commander's efforts to assimilate information in the chaotic environment of war to increase tempo through timely and decisive actions.

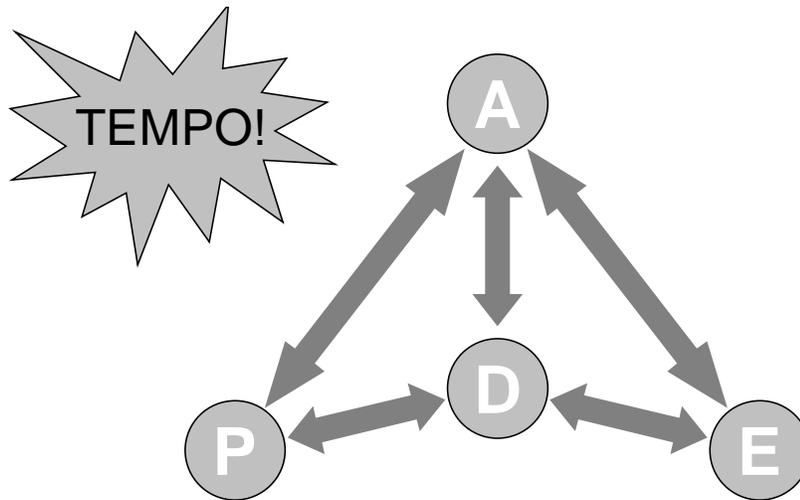


Figure 1-3. Planning, decision, execution, and assessment cycle.

Assessment answers the commander's question, "*How are we doing?*" It should help the commander identify success or failure, determine the extent to which required conditions have been met for follow-on action, and recognize when a particular end state has been reached. More specifically, assessment should enable the commander to measure the overall progress of an operation as it unfolds on the battlefield. By accurately measuring this progress, the commander can make informed decisions for future actions. "Decisionmaking requires both the situational awareness to recognize the essence of a given problem and the creative ability to devise a practical solution" (MCDP 1).

MCDP-6, *Command and Control*, establishes the doctrinal foundation and the conceptual framework for assessment.

The commander commands by deciding what needs to be done and by directing or influencing the conduct of others. Control takes the form of feedback—the continuous flow of information about the unfolding situation returning to the commander—which allows the commander to adjust and modify command action as needed. Feedback indicates the difference between the goals and the situation as it exists...Feedback is the mechanism that allows commanders to adapt to changing circumstances—to exploit fleeting opportunities, respond to developing problems, modify plans, or redirect efforts.

The assessment process is continuous throughout planning and execution. Planning is where the commander establishes his intent (purpose) for the mission as well as his envisioned end state. It is also where the staff identifies the essential tasks and associated conditions that must be accomplished in order to achieve mission success. These are amplified and supported by measures of effectiveness (MOEs), indicators, and pertinent information in the commander's order, and are expressed in clear, precise, and accurate language. They are used as the "gauges" for measuring performance in execution and become information requirements for evaluating the effectiveness of previously made decisions.

1008. Understanding

Understanding is used to support decisions and is a basis for future planning and execution. Understanding can affect decisions made and allow the commander to better visualize success or failure. Experience, personality, and intuitive reasoning by personnel making decisions often influence the type and form of information used to achieve understanding. The development of conditions, measures of effectiveness, indicators, and pertinent information can be useful tools to recognize quality information used to achieve understanding.

a. Tasks

MCDP-1 states that “there are two parts to any mission: the task to be accomplished and the reason or intent behind it...The task describes the action to be taken.” If tasks are to be assessed, planners must craft proper task statements. Tasks that are developed must have a corresponding purpose that describes effects in tangible and measurable terms. Generally, these effects can be described in terms of time, sizes of units, observable capabilities, or terrain. Once a purpose is identified and some tangible qualifiers in terms of time and terrain are provided in planning, assessing the degree to which the task has been accomplished during execution will be easier.

b. Conditions

A condition describes the status of battlespace elements that the commander would like to have in place before executing a decision. It can also be used to determine when a task, stage, or phase of an operation is complete. Conditions must be tied to tasks. Conditions are expressed in enough detail to allow personnel to realistically assess progress, yet broad enough to provide commanders the flexibility to adjust actions to meet unexpected changes. Conditions must be understandable, relevant, and measurable in order to be effective assessment tools. Conditions are expressed as a positive statement rather than a negative statement to enable personnel to realistically assess status of associated battlespace characteristics.

c. Measures of Effectiveness

MOEs are those characteristics of the battlespace that comprise specific components of a condition. MOEs support highly specific information needs. Often MOEs identify desired results to support a key decision that satisfies components of a condition. MOEs are defined in terms of indicators and pertinent information. The establishment of an MOE enables the commander to realistically assess whether or not conditions have been satisfied. This allows the commander to realistically evaluate whether or not decisions have achieved the desired results.

d. Indicators

Indicators are measurable observations that show the MOE is, or is about to be, satisfied. Indicators are supported by one or more pertinent information criteria used to evaluate the supported MOE. Traditionally each staff section identifies and monitors specific indicators. This procedure can result in the same indicator being managed by multiple staff sections. A better approach is to ensure all staff sections are aware of all indicators associated with each MOE. Sharing this information can prevent staff sections from duplicating efforts to satisfy the same indicator. More than one indicator can support an MOE, a condition, and/or a CCIR.

e. Pertinent Information

Recognition of information needed to satisfy indicators enables the determination of pertinent information. Pertinent information satisfies indicators that are established relative to each MOE used to support a desired condition or CCIR. Staff sections identify information they need to satisfy each indicator for which they are responsible. Timely identification of pertinent information enables the staff to efficiently allocate resources to routinely produce “quality” information. Even more importantly, it is the tool that enables the information management officer (IMO) to work with each staff section to create an information management plan (IMP) that identifies procedures used to facilitate the delivery of quality information to those who need it in a format they quickly understand.

1009. Relationship between Common Operational Picture, Common Tactical Picture, and Common Tactical Dataset

Joint force commanders and component commanders maintain their situational awareness through the use of a common operational picture (COP). The Marine Corps component and subordinate echelons of command maintain a

common tactical picture (CTP). The COP and CTP help commanders execute the single battle by maintaining situational awareness. The CTP displays friendly and threat forces, as well as relevant tactical control and fire support coordinating measures. This CTP information is displayed graphically using amplifying text as required. The CTP and COP are derived using a common tactical dataset (CTD) and other sources of information. The CTD consists of shared information derived from numerous sources that support the COP and CTP.

Views of the battlespace may vary at each echelon of command. There is nothing “common” about the view, unless people elect to display the same view. What is common are the datasets and other sources of information. When commanders need to share information to support specific events or situation, they can achieve situational awareness that they need using CTP and COP.

1010. Decision Support Matrix

The following section provides a sample decision support matrix (DSM). The DSM links information to key decisions and helps the commander to coordinate activities and maintain situational awareness. A DSM is normally found in Appendix 2 of Annex X. The following example (see table 1-2) demonstrates how an expanded DSM can be used to assist people with identification of quality information used to support assessment.

Decision	Task	CCIR	Condition	MOE	Indicators	Pertinent Information	NAI	Collection Plan	TAI
Attack the 3 rd Regimental Artillery Group (RAG) to prevent it from disrupting the heliborne assault on LZ Bluebird.	Neutralize the 3 rd RAG	What is the capability of the 3 rd RAG to mass fires against our heliborne assault?	The 3 rd RAG is unable to mass fires at or above the battalion level on LZ Bluebird from H-Hour to H+36	No massed fires observed from 3 rd RAG units within 30 km of LZ Bluebird for 48 hours prior to H-Hour.	Volume and accuracy of artillery fire within 30 km of LZ Bluebird decreased.	Number of artillery rounds fired from within 30 km of LZ Bluebird.	4	Unit SHELLREPs; Counter-battery radar reports.	3
				No observed reinforcement of 3 rd RAG units for 72 hours prior to H-Hour.	Vehicular traffic on 3 rd RAG lines of communication decreased	Number of vehicles travelling on 3 rd RAG lines of communication.	7		BDA from MAW missions, unmanned aerial vehicles, Arty forward observers.

Table 1-2. Sample decision support matrix.

The commander and staff develop a DSM during the planning process. The DSM identifies key decisions the commander expects to make during the next stage or phase of the operation. A decision support template (DST) is a mapping product that graphically displays the text information contained in the DSM.

The commander identifies CCIRs to reflect information he requires to gain knowledge to achieve the understanding he needs before he is willing to make each key decisions. CCIRs are associated with key decisions the commander expects to make to achieve desired results.

Conditions and MOE are identified to assist in recognizing when desired results for each decision are achieved. For certain decisions, MOE and approved conditions may be one and the same, but that determination depends upon the type of decision being made by the commander. Indicators to support each MOE are identified. Indicators may be developed to support the designated condition directly. Each staff section identifies pertinent information used to support each indicator. Indicators are managed using tools that enable all personnel to share pertinent information that satisfy indicators. Staff sections ensure the IMO is aware of pertinent information used to satisfy indicators and any changes.

1011. Planned Decisions

Planned decisions are developed during the planning phase and implemented during execution. Decision points (DPs) identify points in time or space where the commander expects to make key decisions. Friendly and threat forces and environmental factors influence those key decisions. Understanding the type of information necessary to support “planned” decisions enables the unit to implement effective and efficient information management procedures. These procedures enable the commander and staff to clearly identify what type of information is required, who needs it, when it needs to be shared, and the required format. The commander and his staff will—

- Develops DPs during planning that will influence actions and events during execution. The DSM and DST list these DPs and any associated named areas of interest (NAIs).
- Establish CCIRs that identify friendly, threat and environmental information the commander requires to gain knowledge he needs to make key decisions listed in the DSM and DST.
- Establish indicators to help determine whether the MOE has been met.
- Develop NAIs on geographic locations for intelligence collection assets to monitor that would confirm or deny enemy activity/indicators for the appropriate threat CCIR. Report requirements are determined for subordinate commands that support friendly, threat, and environmental CCIRs.
- Ensure that information that satisfies an indicator is immediately sent to the combat operations center (COC), flagged as input to a CCIR, and immediately shared with all other staff sections. If the indicator provides knowledge the commander needs to satisfy his CCIR, the staff is notified and the commander decides whether or not he has adequate understanding of the situation to make a decision.

Figure 1-4 demonstrates how personnel can identify and manage quality information to support planned decisions (identified by DP-1).

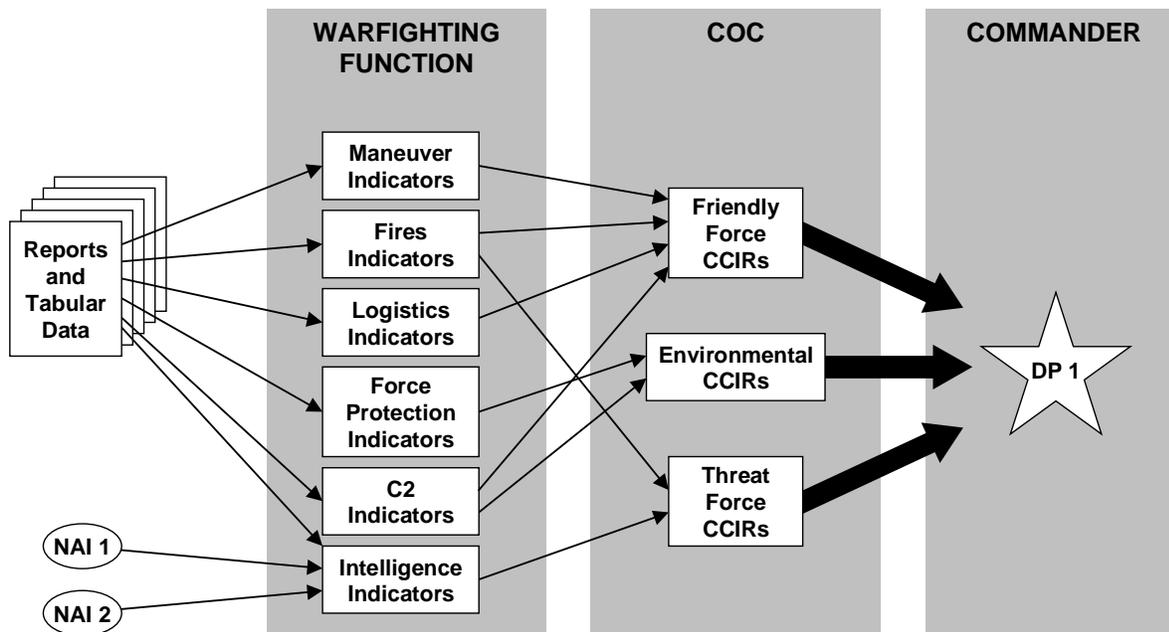


Figure 1-4 Managing information to support planned decisions.

As indicators flow in and understanding develops, the senior watch officer consults the DSM/DST to determine what preplanned solutions are still valid. These facts are then placed before the commander who applies his experience, judgment, and intuition to the information to make the decision.

1012. Spontaneous or “Unplanned” Decisions

Spontaneous or unplanned decisions are those decisions generated by unexpected or unplanned actions or activities. The purpose of course of action (COA) wargaming is to identify environmental factors and threat activities that could affect the friendly course of action, and to develop branch plans to address these possibilities. However, combat is inherently uncertain. Potentially, planners could develop multiple branch plans, be intimately aware of friendly, threat, and environmental actions, reactions and counteractions, and still be surprised. When the plan is executed, the threat could perform an unexpected action or activity that would require a completely new branch plan to be developed and executed. However, armed with the knowledge and understanding gained by developing the numerous branch plans, the commander and staff planners are now better prepared to observe, orient, and react with “unplanned” decisions. Knowledge and understanding of current and anticipated actions by the threat, friendly forces and the environment enables the commander to make sound, timely decisions that controls tempo even in the face of uncertainty. IM must be flexible enough to provide information that supports both planned and spontaneous decisions for which no prior planning could be conducted.

- Indicators are generated as an event develops. Some of these indicators are collected and reported in accordance with commander’s guidance and intent as articulated during planning.
- As this information is reported, the COC will at some point in time recognize that an event is occurring that is not on the DSM/DST and for which no planning has been done.
- Recognition of an unplanned event requires new plans and decisions to be made. This action generates new information requirements from the commander and staff. These information requirements focus on the impending event *indicators* to determine timing, location, disposition, and/or status of the event, and its probable outcome.
- Once sufficient information is collected on the indicators, an understanding of the event is developed. This understanding enables the commander to make an informed decision and control tempo despite unexpected events.

Figure 1-5 demonstrates how personnel identify and manage quality information to support unplanned decisions. It is used when events occur during executions that were not accounted for during planning.

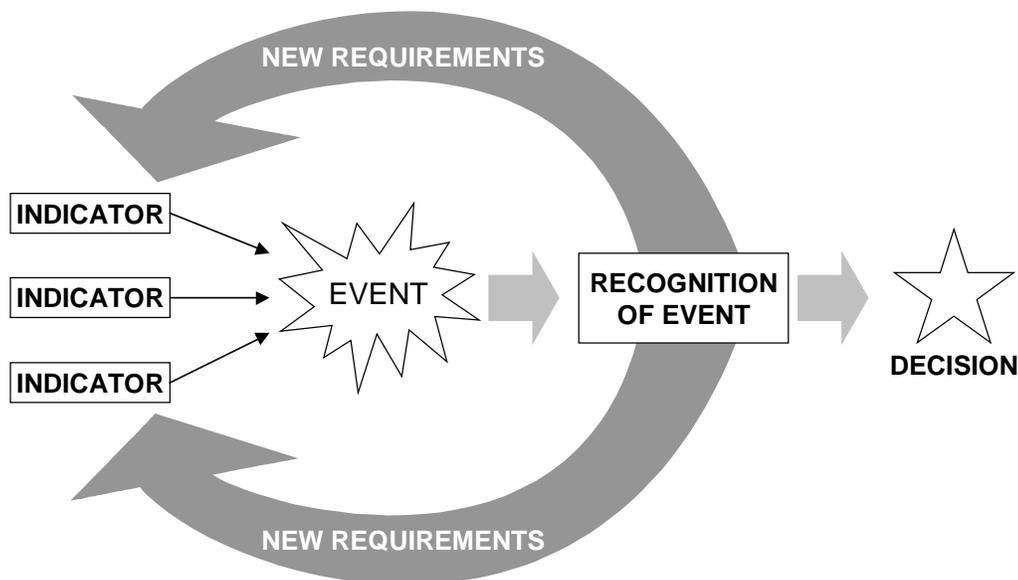


Figure 1-5 Managing information to support unplanned decisions.

This page intentionally left blank.

Chapter 2

Personnel and Duties

“Wars may be fought with weapons, but they are won by men. It is the spirit of the men who follow and the man who leads that gains victory.”

—George S. Patton

Personnel are the second element of C2. This chapter identifies the principal managers of quality information within each command and outlines their IM responsibilities. Although these individuals are key personnel with specific IM duties, all users of information should participate in the effort to manage information. Every user has an inherent responsibility to filter and fuse information for their own use and for use by others. In every command, all personnel, as information users, should support IM procedures that enhance decisions made throughout the decision cycle.

2001. Key Information Management Functions

a. Commander

The commander must not merely participate in planning—he must drive the process. His intent and guidance are key to planning. The commander uses planning to gain knowledge and situational awareness to support his decisionmaking process. His subordinate commanders use his guidance and concept of operations to accomplish the mission. The commander establishes priorities for gathering and reporting quality information needed to maintain situation awareness and achieve a level of understanding. Clear guidance, commander’s intent, and CCIRs provide a focus for the staff to identify quality information used to support key decisions. Additionally, the commander performs the following information management functions—

- Develops and approves the command IMP used to share quality information.
- Develops and approves the command communications plan that complements and supports the IMP.

b. Chief of Staff/Executive Officer

The chief of staff is responsible for coordinating the actions of the staff and ensuring that the commander is provided the information he needs to make decisions. The chief of staff directs the development of the operation order and performs the following additional information management functions—

- Directs development of and approves the daily battle rhythm.
- Implements the IMP.
- Appoints the IMO.
- Ensures IM procedures adequately share quality information used to support key decisions the commander makes to achieve desired results.

c. Primary Staff

The primary staff is the eyes and ears of the commander. They take the commander’s guidance, intent, and CCIRs and use them to collect, filter, and analyze data, and then provide the focused processed information to the commander. The principal staff members perform the following information management functions—

- Identify pertinent information used to support the daily battle rhythm.
- Establish internal staff section procedures to share quality information through the use of newsgroups, homepages, message handling, e-mail, requests for information (RFI), and suspense control measures.
- Appoint a staff section information manager as a point of contact for IM matters.
- Appoint personnel responsible for maintaining information technology and network infrastructure used to share quality information.
- Ensure training is completed for basic IM and security procedures for appropriate personnel in each staff section.
- Evaluate IM procedures to assure efficient flow of quality information.
- Establish benchmarks and conducts subjective analysis to evaluate efficiency and effectiveness of IM procedures.
- Work closely with the IMO to develop network diagrams that identify functional applications and network infrastructure required to share quality information with those that need it in a format that is clearly understood.

d. Information Management Officer

The IMO must be capable of working closely with personnel of all rank to coordinate procedures necessary to share quality information generated by the staff. These procedures should promote development and exchange of knowledge required by the commander to make decisions. At a minimum, the IMO must be aware of the following functional needs—

- Key decisions the commander is expected to make to successfully achieve desired results. These decisions are normally reflected in a DSM.
- Knowledge required by the commander to achieve the level of understanding he needs before making key decisions. This knowledge may be reflected in a daily battle rhythm matrix (DBRM).
- Information the commander needs to reduce his uncertainty about his own force, the threat and the environment. This information must be provided to the commander in a format that promotes knowledge he requires to make sound, timely decisions. Normally this information satisfies CCIR.
- Information required to satisfy established conditions for tactical operations and information the commander routinely needs on a daily basis to maintain situational awareness.
- To perform the functions listed above, the IMO must be capable of working closely with the staff to accomplish the following tasks:
 - Develop and publish the command IMP.
 - Determine information requirements necessary to satisfy CCIR, conditions and routine daily updates the commander needs to achieve understanding linked to key decisions he expects to make.
 - Publish and update the reports matrix, described in Appendix A of this manual.
 - Develop the DBRM, described in Appendix A of this manual.
 - Coordinate additional training required by staff and component elements to support production of quality information through effective IM procedures.
 - Work closely with the command CTP manager, staff, subordinate and higher headquarters IMOs to develop effective, efficient track management procedures outlined in Appendix A.
 - Work closely with information exchange technology personnel to facilitate efficient dissemination of quality information throughout the MAGTF.

e. Staff Section Information Managers

Each staff section information manager should be aware of information required by the commander, when it is required, and the desired format. Section information managers are expected to perform the following tasks:

- Monitor internal and external flow of information by their staff section.
- Ensure the command IMO is aware of information produced by each staff section to satisfy CCIR, conditions and routine daily updates that the commander requires to make sound, timely decisions.
- Provide the G/S-6 a daily update of command level information requirements that may need network infrastructure support, sharing of information, and equipment to support functional needs (to include the number and type of equipment, internet protocol (IP) accounts, computer and e-mail naming conventions, radio net and telephone requirements, and user lists for inclusion in email and telephone directories).
- Ensure compliance with IM procedures used to share quality information through the use of intranet/internet capabilities.
- Coordinate and conduct IM training for internal staff section members.

f. Request for Information Manager

RFIs are used to reduce uncertainty within the command. Questions that cannot be satisfied by organic assets are forwarded to higher headquarters in the form of a formal RFI. Answers to questions that allow the staff to promote knowledge they require to support the commander are shared through RFI responses. The RFI manager is expected to perform the following tasks:

- Receive, validate, prioritize, and submit RFIs to the appropriate authority for resolution.
- Develop and manage a tracking system to ensure RFIs are processed and responses are expeditiously disseminated to the requester and made accessible to all personnel.

See Chapter 4 for more discussion of RFI procedures.

g. Common Tactical Picture Manager

The CTP manager is responsible for the detection, reporting, and display of friendly and threat unit tracks. He is also the unit track manager. The CTP manager is expected to perform the following tasks:

- Coordinate and de-conflict all ground unit tracks with all major subordinate commands and higher headquarters. Air tracks are the responsibility of the air combat element, which provides air tracks to the command element as required.
- Work closely with the senior watch officer to ensure the location and disposition of friendly and threat ground units are visually updated as required.

h. Web Master

Intranet/intranets are a valuable resource to share quality information requirements within and external to the staff. Creation of a unit website is the responsibility of the web master. Specifically, the web master is responsible for:

- Creating the command website to support sharing of quality information. At a minimum, the website supports internal and external reporting requirements, the CCIRs, RFIs, the commander's daily brief and daily battle rhythm.
- Maintaining the website to ensure that changes to information requirements are posted in a timely manner.
- Maintaining security over the website. Ensure information contained therein is available to appropriate personnel.
- Ensuring procedures are developed, disseminated and understood for:
 - Accessing the site.
 - Uploading information.
 - Changing the site.

- Maintaining links to external sites of interest to the staff.
- Developing formatting standards, create initial pages for each staff section and train representatives from each section how to maintain their page in order to ensure uniformity of design between sections.
- Developing custom web based applications as required.
- Advising and assisting staff section web representatives.

i. Subordinate Unit and Higher Headquarters Information Management Officers

Each major subordinate command and higher headquarters appoints an IMO as a primary point of contact for IM matters. Subordinate and higher headquarters IMOs can be expected to perform the following tasks:

- Review/update information reflected by the reports matrix and daily battle rhythm.
- Conduct liaison with the higher headquarters and adjacent IMOs.
- Coordinate and assist personnel training required to produce quality information throughout the MAGTF.
- Ensure appropriate management personnel are designated within the command to address technical support if the MAGTF chooses to use automated or electronic means to share and manage command information (i.e., web site, newsgroup, public folders, shared directories).

2002. Organizations that Influence Information Management

a. Combat Operations Center

The COC supports current operations. Personnel operating in the COC conduct the following information management related activities:

- Assess information flow to support operations.
- Review and record incoming message traffic to filter and fuse information in accordance with the commander's guidance and intent. Reports information responding to CCIRs and DPs to the commander.
- Manage the CTP through commonly understood track management procedures outlined by Appendix A.
- Monitor the efficiency, effectiveness, and accuracy of the CTP to provide enhanced situation awareness of friendly and threat forces.
- Maintain a master suspense action log/journal.
- Maintain a chronological record of significant events.
- Direct production of the commander's daily briefings and fragmentary order production.
- Work closely with the G/S-2 at the combat intelligence center (CIC) to assess, update, and integrate priority intelligence requirements.

b. Combat Intelligence Center

The CIC is the overarching intelligence operations center established within the main command post. It performs the following functions:

- Review, assess, and disseminate threat related information in a format that is quickly understood by those needing the information. This provides a common understanding of the threat within the designated battlespace.
- Monitor the efficiency, effectiveness, and accuracy of the threat assessment determined by the common tactical picture parameters.
- Work closely with the COC, future operations and future plans to ensure threat assessments satisfy designated planning horizons and are updated accordingly.

- Develop, monitor, and update priority information requirements and RFIs. Respond to priority information requirements and RFIs of the commander, staff, and subordinate commands.

c. Future Operations

Future operations personnel develop courses of action to support the next stage or phase of the operation. IM supports the following future operations activities:

- Collaborative planning. Sharing quality information through the use of collaborative capabilities and commonly understood procedures outlined in Appendix B.
- Visual display tools and overlays that describe fire support coordination measures, boundaries, maneuver, logistics/sustainment, decisions, and intelligence requirements.
- Planning tools that are capable of supporting COA development.
- Filtering tools and procedures to assess measures of effectiveness for conditions tethered to key decisions required to support execution and transition to the next stage or phase of the operation.

d. Future Plans

Future plans personnel develop the next phase of the operation. Future plans is normally closely tethered to higher headquarters. IM supports the following future plans activities and tools:

- Collaborative planning. Sharing critical and relevant information through the use of collaborative capabilities and commonly understood procedures.
- Visual display tools and overlays that describe fire support coordination measures, boundaries, maneuver, logistics/sustainment, decisions, and intelligence requirements.
- Planning tools that are capable of supporting the development of the next phase of the operation.

2003. Information Management Coordination Cells

To ensure IM procedures are in compliance with those established by the joint task force (JTF), IM coordination cells are recommended at the Marine component and MAGTF level. These ad hoc cells may also be established at lower levels of command and are convened as required. Coordination cells are also activated at the JTF to ensure IM procedures by each component are able to support JTF commander and the supported combatant commander's information requirements.

a. MARFOR Computer Network Defense Augmentation Cell

The computer network defense augmentation (CNDA) cell assists the commander, via the G/S6, with developing and maintaining an information assurance picture (IAP), a computer network defense picture (CNDP), and a common network management picture (CNMP).

b. Information Management Board

The IM board acts as the focal point for coordinating IM issues within the command. It convenes during the development of the IMP, and as required thereafter. The IM board operates under the supervision of the chief of staff, or appropriate staff directorate, as best meets the commander's mission needs. Facilitated by the command IMOs, it is composed of the senior IMO from each major subordinate command and IMO representative from appropriate staff sections as required. The IM board is actively involved in resolving cross-functional and contentious information management issues. Personnel who administer information exchange technologies may also attend.

c. Common Tactical Picture Board

The CTP board acts as the focal point for coordinating the CTP within the command. It is headed by the CTP manager who is responsible for working closely with the IMO, the primary battle staff, and subordinate and higher headquarters IMOs to develop CTP procedures to maintain situation awareness of friendly and threat forces. The CTP board operates closely with the IMO, the COC and CIC watch officers, and appropriate staff sections. It is composed of the friendly air, land, maritime, and threat force track managers and is actively involved in resolving all cross-functional CTP issues.

d. Information Assurance Picture Board

The IAP board acts as the focal point for coordinating information assurance issues within the command. It operates under the direction of the defense information officer (DIO) and the Marine component, and coordinates with the CNDP board, CNMP board and IM board as required. The IAP board is composed of the senior DIO or information systems security officer (ISSO) from each major subordinate command, the special security officer (SSO), the ISSO, the IMO, and an IMO representative from appropriate staff sections as required. The Marine component CNDA cell may augment the IAP board when necessary.

e. Computer Network Defense Picture Board

The CNDP board acts as the focal point for coordinating computer network defense issues within the command. It operates under the direction of the DIO and the Marine component and coordinates with the IAP board, CNMP board, and IM board as required. It is composed of the senior DIO or ISSO from each major subordinate command and IMO representative from appropriate staff sections as required. The Marine component CNDA cell may augment the CNDP board when necessary.

f. Common Network Management Picture Board

The CNMP board acts as the focal point for coordinating network management within the command. It operates under the direction of the G/S6 and coordinates with the IAP board, CNDP board, and IM board as required.

2004. Security Personnel

a. Information Security Manager

The information security manager is responsible for the proper accountability, control, personnel access, and physical security/storage of noncompartmented classified data, in both hard and soft copy forms. This includes the TOP SECRET Control Officer's responsibility for the JTF TOP SECRET registry's accountability, control, and access.

b. Special Security Officer

The SSO is responsible for sensitive compartmented information (SCI) management, control, and access and is normally a G/S-2 function.

c. Defense Information Officer

The DIO is the primary staff officer charged with computer network defense. The DIO develops plans, policies, and procedures to ensure the reliability, availability, integrity, confidentiality, and protection of data and information. Additionally, the DIO develops plans, policies and procedures to verify the authenticity and non-repudiation of personnel accessing such data and information. As a member of the G6 staff, the DIO's primary responsibilities include—

- Information assurance.
- Network security management.
- Intrusion detection.
- Vulnerability assessments.
- Assisting in the network accreditation process.

d. Information Systems Security Officer

The ISSO is responsible for safeguarding the information systems of the command. This is done by conducting site surveys and accrediting systems to process classified and sensitive information. The ISSO also enhances the information security knowledge, skills and abilities of the command through education and training programs that are command-wide in focus. The ISSO performs the following information management functions--

- Maintain a plan for site security.
- Ensure the information system is operated, used, maintained, and disposed of in accordance with security policies and practices.
- Ensure the information system is accredited and certified if it processes sensitive information.
- Ensure users and system support personnel have the required security clearances, authorization and need-to-know; are indoctrinated; and are familiar with internal security practices before access to the information system is granted.
- Enforce security policies and safeguards on all personnel having access to the information system for which the ISSO is responsible.

e. Operations Security Officer

The operations security officer is responsible for oversight and implementation of the command operations security program, ensuring the protection against compromise of friendly force information. This position is normally a G/S-3 function, and will receive support from the G/S-2 (counterintelligence officer).

2005. Information and Information System User Responsibilities

The following duties and responsibilities are incumbent upon all users of information to ensure proper information flow—

- Report information as required by the command CCIRs.
- Ensure accuracy and relevance of information before further dissemination. Clearly differentiate between original information and previously reported information to avoid duplicative reporting.
- Properly control, classify, protect, and archive all information and information systems for which they are responsible. This requires a clear understanding of approved control measures for various classifications of information.
- Read and complies with the information requirements published by the IMP. (See Appendix A of this manual).
- Do not prematurely destroy information. When conducting an initial analysis and correlation of data, set aside but do not destroy irrelevant or conflicting data. This information may become useful when combined with additional facts.

This page intentionally left blank.

Chapter 3

Command and Control Support Structure Development

“Final decisions are made not at the front by those who are there, but many miles away, by those who can but guess at the possibilities and potentialities ...”

—Douglas A. MacArthur

C2S structure is the third element of C2. C2S structure is more than advanced technology and equipment—it is the integrated use of organizations, people, capabilities, training, procedures, doctrine, and network infrastructure to support the process of C2 and decisionmaking. An effective C2S structure produces information that promotes understanding of the situation or event and allows the commander to be better prepared to direct and coordinate actions in the execution of a decision. This chapter discusses several C2S structure considerations, and then lays out a number of IM tools and procedures that improve the effectiveness of a command’s C2S structure.

3001. Advantages

An effective C2S structure provides the following benefits—

- **Labor/Time Savings.** Capabilities and commonly understood procedures are able to perform intensive calculations very quickly that otherwise might take several people much longer to complete.
- **Dissemination.** Networked C2S structure capabilities allow the user to transfer information and knowledge simultaneously to many users even if they are not in the same geographic location.
- **Graphics Support.** An effective C2S structure can be used to take volumes of tabular data and transform it into graphics or visualization products that enable personnel to quickly gain meaningful and comprehensive understanding of the situation or event. As an example, a graphic intelligence summary overlaid on a digital map is more quickly understood than a multi-page textual message. See Appendix B for examples of visual-mapping products that support each step of the Marine Corps Planning Process (MCPPE).

3002. Information Flow

When developing a C2S structure that enhances the flow of information across warfighting functions (maneuver, fires, logistics, force protection, intelligence, command and control) and across traditional staff section boundaries, the following factors should be considered—

a. Location of Information

The location for specific types of information is often predictable, especially if the “process” to support the information requirement is understood. Prepositioning required information at anticipated point(s) of need speeds up the flow of information, reduces demands on communication networks, and provides required information to those that need it in a timely manner. This consideration is especially important when units are highly dispersed.

b. Mobility

Reliable and secure flow of information must be commensurate with the commander's mobility and tempo of operations requirements. Capabilities and procedures necessary to support effective information flow must be flexible enough to adjust immediately to support low footprint and highly mobile command posts, as well as the mobility requirements of the subordinate units.

c. Accessibility

All levels of command must have access to the information they require to support concurrent and/or parallel planning, mission execution and assessment. The C2S structure can provide access to information to required user(s) via automated means to reduce time, people and cost, while increasing efficiency and dissemination of quality information. (Example: automated, dynamic visual display of forces in a CTP environment).

d. Filter/Fusion

Information is received from many sources, in many mediums, and in different formats. Filtering occurs when information is evaluated/assessed to be of value and irrelevant data is discarded. Fusion is the logical blending of information from multiple sources into accurate, concise, and complete summary. The C2S structure must permit analysts and decisionmakers the ability to quickly filter and fuse information.

e. Push Versus Pull

IM uses two basic approaches to share information. C2S structure must incorporate the most appropriate approach based on the commander's information requirements.

- **Supply-Push.** A supply-push methodology relies heavily on information being pushed from the source to the user, either as the information becomes available or according to a schedule. The advantage of supply-push is that the commander normally does not need to request quality information. Quality information is delivered to the user in a timely manner, but there is always the danger of producing information overload because producers of information may not completely understand user information requirements.
- **Demand Pull.** In contrast to supply push, in a pure demand-pull system the user initiates the flow of information, seeking out information required. If the information is readily available—already resident in some database—the requirement can be quickly satisfied. If not, the requirement must move through the chain of command until it reaches the appropriate level. Information can be tailored specifically to support the identified requirement, avoiding overload. The disadvantage to demand-pull is the cost in time, since the search for information may not begin until the commander or user has identified the need.

3003. Process Flow

The first step in the development of an IM C2S structure is to identify the process flows that support each warfighting function. A process flow diagram identifies the series of tasks necessary to support each warfighting function. Information management is process-centric, focused on supporting the processes that satisfy information requirements essential to the warfighting functions. MCDP 1-2, *Campaigning*, identifies six basic warfighting functions: intelligence, maneuver, fires, logistics, command and control, and force protection. An information process supports each warfighting function. Each process captures the step-by-step tasks necessary to collect, analyze, and disseminate the information. Understanding the process flow (how information is physically transmitted and processed) that supports each warfighting function enables the IMO to work closely with the staff and commander to develop effective IM procedures. The warfighting processes are unique to each warfighting function and level of command. An effective C2S structure is characterized by a clear definition of the type of capabilities, procedures, training, personnel, and network infrastructure necessary to support those processes.

Figure 3-1 is an example of a completed process flow diagram. This example delineates the tasks required to provide the information to support the “collect intelligence.” Overlaid on the process flow is a depiction of the organizations within a MAGTF responsible for the appropriate components of the process flow.

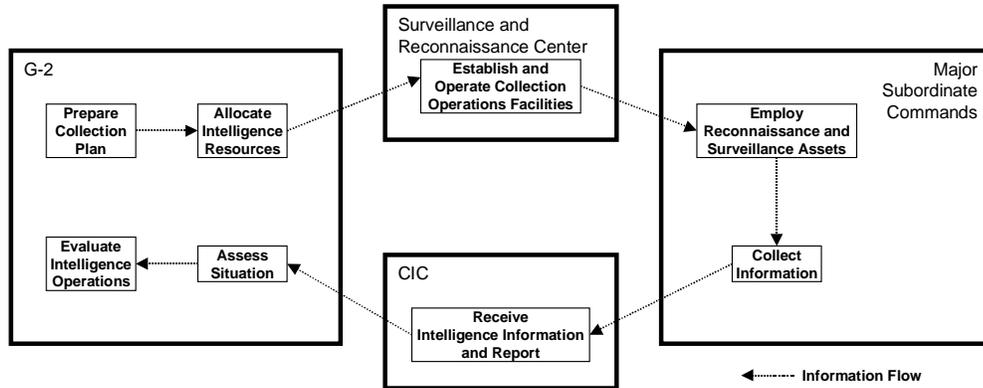


Figure 3-1. Process flow for collect intelligence.

3004. Configuration Flow

Once the process flow diagrams have been created, the next step in the development of an IM C2S structure is the development of the configuration flow diagrams. A configuration flow diagram describes the configuration of systems necessary to support the tasks in the process flow diagram. A configuration flow diagram is established by performing the following actions—

- Determine the system required performing each task identified by the process flow diagram.
- Identify the network infrastructure necessary to disseminate information produced by personnel performing each task identified by the process flow diagram.

Figure 3-2 describes a configuration flow diagram to support the process flow described by figure 3-1. Each system is placed in the appropriate command element organization linked by the proper network infrastructure. Current command relationships and task organization of forces are taken into consideration to develop the configuration flow diagram. This methodology permits a command to identify system and network shortfalls or potential vulnerabilities.

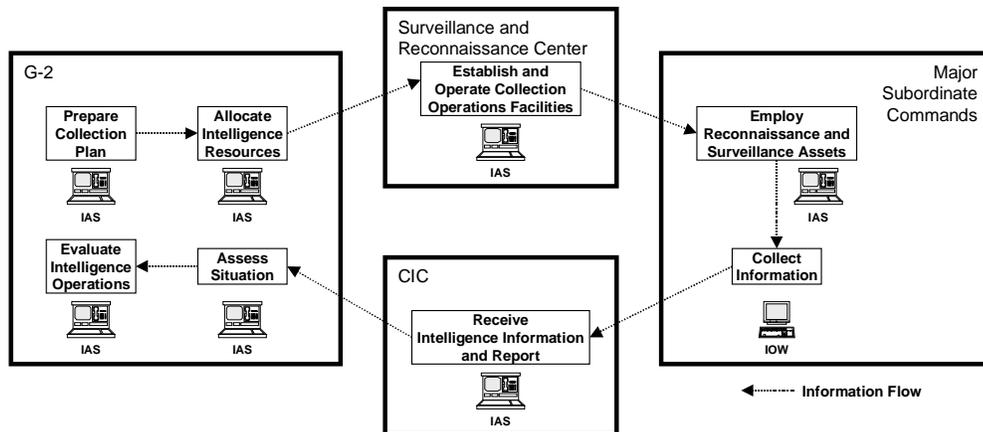


Figure 3-2. Configuration flow for collect intelligence.

3005. Personnel Requirements

In the final step of developing a C2S structure, the command identifies personnel requirements from the configuration flow diagram, determining the number of personnel, skill sets (training), and procedures necessary to support each warfighting function. These requirements are then measured against what is currently being used by the command. This action enables the command to clearly identify deficiencies and implement corrective action. The result is an efficient flow of information within the command C2S structure and effective decisionmaking. Figure 3-3 demonstrates a personnel requirements diagram to support the configuration flow diagram described by figure 3-2.

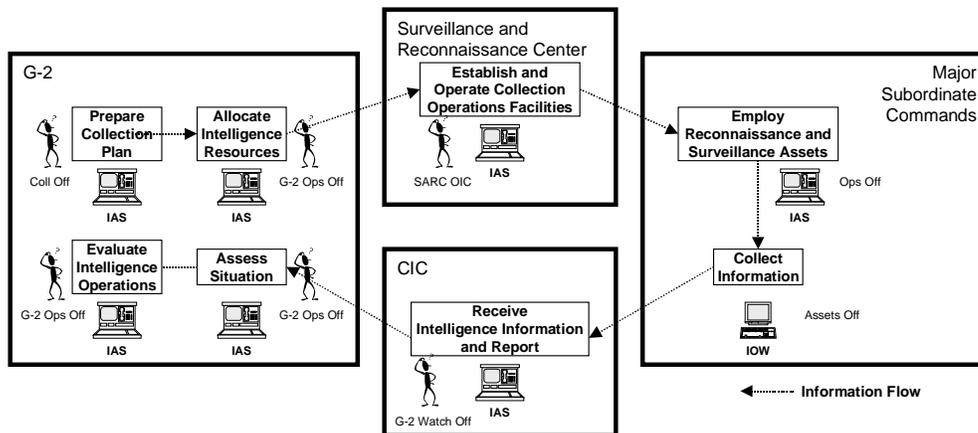


Figure 3-3. Personnel requirements for collect intelligence.

3006. Documentation

Capturing the IM decisions and plans in documentation facilitates a common understanding of IM throughout the command. The following tools are useful for dissemination.

a. Information Management Matrix

The IM matrix records all information requirements, the user(s), the recipients, capabilities used to process the information, and the pathways necessary to pass information. It is a powerful planning tool to support execution, to determine the source of information flow problem(s), and correct them through appropriate action/coordination. A carefully designed IM matrix will significantly enhance the efficiency and effectiveness of staffs and decisionmakers. The staff determines the content of the reports matrix. Appendix A provides an example of a report matrix to support intelligence functions and a more detailed explanation as to how the report matrix supports the commander and his entire battle staff.

b. Daily Battle Rhythm Matrix

The DBRM is a listing of key daily events that involve the commander and staff. These events can include staff briefings, updates, visits, reports and products (air tasking order, intelligence summary, etc.). These events are extracted from the IM matrix and placed on the DBRM. The purpose of the DBRM is to disseminate the schedule and facilitate the integration of the various events. Commanders and staff are responsible for identifying which event needs to be placed on the DBRM. Chief of staff/executive officer manages the DRBM. See Appendix A and MCRP 6-23 (E) for format and a sample DBRM.

3007. Request for Information Management

RFIs are specific, time-sensitive ad hoc requirements for information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. RFIs are generated to answer questions that cannot be resolved with organic assets, and when the information does not exist within internal databases or cannot be satisfied by resident subject matter experts. The RFI process is shown in Figure 3-3 and amplified below.

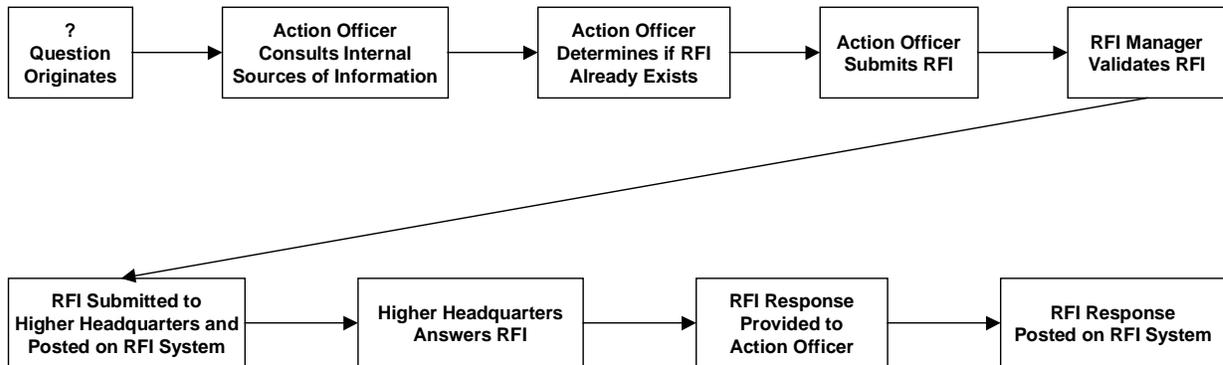


Figure 3-4, Example of a process flow used to support request for information management.

a. Command Request for Information Manager

The RFI manager is the focus of information requirements from multiple sources: the operational planning team (OPT), the primary staff sections, and the major subordinate commands. All RFIs are submitted to the RFI manager who validates the RFI, assigns priorities, and submits the RFI for resolution. The RFI manager applies the commander's guidance and intent, CCIR, and good judgement to guide validation and prioritization of each RFI. CCIRs should guide the RFI manager in determining the importance of each RFI—those RFIs directly tied to CCIRs should be assigned the higher priority.

b. Submission Guidelines

An RFI requestor will first search local information and the RFI database to ensure that the information is not available locally or has already been submitted. If the information cannot be found, an RFI will be submitted to the appropriate RFI manager. All intelligence related requests are processed through a G-2 RFI manager and all non-intelligence related requests for information are processed by the G-3 RFI manager. The following guidelines will apply to the drafting and submission of RFIs—

- Limit RFI to one question per request. Multiple questions can increase response time and add confusion as multiple agencies answer the questions from one RFI.
- State RFI as a specific question. Provide sufficient detail so that the receiving action officer will completely understand the request and the nature of the requirement.

c. Validation

When an information requirement is identified, the action officer should first exhaust all locally available resources to include other staff officers, other command sections, on-line services (libraries, databases, repositories), and other organizations (higher, adjacent, subordinate, supporting). If the information requirement cannot be satisfied locally, the action officer must next determine if this requirement has already been submitted and being addressed by another staff section. If the information requirement has not been addressed, it is submitted through the local planning cell for

submission as a formal RFI. Each RFI should be recorded, managed, tracked and sent to higher, subordinate, or adjacent headquarters or to another agency for the desired information

Validation screens RFIs to ensure that redundant RFIs are not processed. Validation includes—

- Determining if the requested information is resident within the command.
- Determining which agency to forward the RFI for action.
- Approving the request. If not approved, the request should be returned to the originator for appropriate justification.
- Assigning a tracking number to all validated RFIs.
- Logging in the RFI on the RFI tracking sheet and posting the RFI to the MAGTF RFI database. If there is a duplicate request, the RFI manager will provide all originators with the appropriate RFI tracking number.
- Forwarding the request to the appropriate headquarters, staff sections or agency for action and confirming receipt of the request by the action addressee.

d. Submission to Higher Headquarters

Once validated, the RFI manager generates an RFI to higher headquarters containing the approved formal command RFI. Only the RFI manager is authorized to submit the RFIs to higher headquarters. All other information requests to higher headquarters (through normal staff action) are not RFIs and should not use that term. This RFI process reduces formal RFIs to the few that are critical to the planning or execution and warrant command-level attention. The intent is to send a clear message that the command has determined a critical need for information and needs higher headquarters assistance. Upon receiving information that satisfies an RFI (i.e., via message or report from higher headquarters or an outside agency), the RFI manager immediately transmits the response to the originator of the RFI. Additionally, the RFI manager updates the status for that RFI on the RFI tracking system.

e. Responses

RFI responses will be sent to the respective RFI manager. The RFI manager will post the response to the RFI database and notify the requester that a response has been received. The RFI tracking log will be updated to reflect that a response was received and that the requester was notified. It is the responsibility of the individual that initiated the RFI to screen the response and determine if it is adequate or whether an additional RFI should be generated to acquire the desired information. If the RFI is not answered completely or additional information is desired, the requestor should resubmit the RFI with appropriate comments or clarification.

f. Major Subordinate Command Procedures

Major subordinate commands shall institute a mechanism to manage RFIs within their command. Upon confirming that an information requirement is critical to the planning or execution and that the information requirement cannot be satisfied at their level, major subordinate command RFI managers then submit their RFI to their higher headquarters for resolution.

3008. Information Management Plan

The IMP is the expression of the command's concept of how it will manage and control information. The IMP reflects all three elements of C2—information, people, and C2S structure. The IMP assigns responsibilities and provides instructions for personnel that manage information. IM responsibilities identified by unit standing operating procedures (SOP) do not need to be duplicated in the IMP. Development of an IMP is a vital step to ensure decisionmakers have the information they require, when they need it, in a format that they quickly understand. Each command must develop an IMP tailored to manage its information in the context of its mission and the current situation or event.

An effective IMP provides guidance to ensure “quality” information is provided to those that need it in a form they quickly understand. The IMP should cover IM filtering tools; unique IM personnel needs (duties, responsibilities, and skill requirements); C2S structure requirements (processes and procedures); and IM system protection. The IMP should include specific guidance for management of the CTP, the collaborative planning system, RFI management procedures, and network applications utilized to share critical and relevant information. This action may be accomplished through the use of news groups, web pages, or other applications.

The development and execution of an effective IMP requires the participation and interaction of all staff sections. Once each staff section identifies their information requirements, warfighting process and configuration flow diagrams, and personnel requirements, the appropriate information is incorporated into the IMP.

Information management policy and procedures are top-down in nature and the IMP should include considerations for joint interoperability. JTF IM practices will nest within those already established by the supported combatant commander. Likewise, component, MAGTF, and major subordinate IM practices must nest within those of the JTF. In fact, commanders and staffs at all levels must have a common understanding of joint information management policy and procedures. See Appendix A for a sample IMP.

3009. Networks

At present, numerous capabilities are being used to support functional requirements, but the information generated by all of the functional capabilities and the personnel that use those capabilities use primarily only five different *networks* to share and disseminate information determined to be critical and relevant. A brief explanation of those five networks are provided below:

- **Joint Worldwide Intelligence Communications System (JWICS).** A classified network used to process and disseminates information classified as SCI.
- **SECRET Internet Protocol Router Network (SIPRNET).** Classified networks authorized to process and disseminate information classified as Secret or below.
- **Nonsecure Internet Protocol Router Network (NIPRNET).** A sensitive but unclassified network able to process and disseminate sensitive but unclassified information and below.
- **Allied Networks.** Networks already established and maintained by our allies. These networks are normally made available to US Forces to maintain interoperability when conducting operations. Control measures are normally the same as that of all information releasable to that allied nation.
- **Coalition Networks.** Interoperable networks that are established by combined forces as required supporting a specific operation. The JTF commander and appropriate classification authorities determine the control measures used to protect and disseminate classified information disseminated by this network.

This page intentionally left blank.

Chapter 4

Security

“If I can deceive my own friends, I can make certain of deceiving the enemy.”

—Thomas “Stonewall” Jackson

Security of information is critical to information management and the effective conduct of operations. Accurate information serves as an enabler to enhance operations; however, rapidly evolving technologies have made this same information vulnerable. To safeguard against unauthorized access or modification of information, each command must protect and detect against information compromise. Proper security enables commanders to sustain tempo by monitoring the status of friendly information, any outside attempts to penetrate or attack friendly force information, and the location and type of threat involved. Armed with that information, commanders can determine appropriate passive or active measures to deter further intrusion or initiate actions to deceive or possibly terminate the threat as appropriate. The security goal of IM is to maintain and ensure integrity of information within the command.

4001. Information Assurance

Information assurance is the joint term applied to those security actions taken to protect friendly information and information systems. It is “all information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities” (Joint Pub 1-02).

4002. Protection

A key component of the IMP is information protection. Mission accomplishment depends on protecting information and information systems from destruction as well as safeguarding against intrusion and exploitation. All users share responsibility for information protection. Information security is a force protection issue and all users should be extremely vigilant in the use of any form of communication. It is imperative to use established security protocols and procedures for successful mission accomplishment.

The first step to defeating a network intruder is preparing defenses. But like all defenses, network defenses only buy time and not full protection. Given enough time, an intruder can eventually acquire information that could be detrimental to friendly force operations/mission objectives. The second step to defeating these intruders, then, is to have the ability to detect when and where an intrusion attempt is being made and the type of capability being used to perform the intrusion. The third step is to have a contingency plan in place to meet and defeat this threat based on time and planning considerations established by the commander. This capability allows the commander to choose when and where to degrade, defeat, deceive, or possibly destroy the threat once it is detected. Only through a comprehensive plan to defend against, detect, deceive, and defeat hostile intrusion can a network and functional capabilities that process information be truly protected. The IMO must work closely with each of the staff to ensure critical databases and networks are adequately protected.

4003. Virus Attack

Virus attack is the most serious threat to information protection. A computer virus, by definition, is any program (or code) that replicates itself by attaching a copy of itself to another file. A virus is particularly dangerous because users typically do not know their functional capabilities or networks are being infected until the virus reveals itself (the consequences of which can range from annoying to catastrophic.) The NIPRNET, SIPRNET, and JWICS are becoming more popular as file and e-mail transfer medium and users are at a growing risk. Network server solutions are ineffective at stopping the spread of infected e-mail attachments because the Internet connection bypasses network server virus protection. As modem/internet file transfers become a more commonplace, viruses are a more common source of infection.

At the most basic level, viruses can be categorized as one of two types: file or boot. File viruses reside inside .exe or .com files, gain control of the computer system when that file is executed, and attach a copy of themselves to other files after they gain control. Boot viruses reside in the section of the floppy disk or hard disk that is loaded into memory at boot time, and hence, are loaded into memory before other programs. This enables these viruses to re-infect floppy disks inserted in the disk drive. In the past, 80 percent of all viruses and the great majority of infections involved boot viruses and spread by attaching themselves to executable files (e.g., .exe and .com files). The following subsets of file type viruses resist easy detection:

- **Stealth Viruses.** These viruses avoid detection via file size monitoring in various innovative ways that exploit disk operating system interrupts.
- **Polymorph or Mutation Viruses.** Now emerging in large numbers, polymorph virus copy modified versions of themselves each time they spread to other files.
- **Macro-Type Virus.** A new type of file virus is spreading rapidly—macro-type viruses that infect everyday document and spreadsheet files. This virus type, which exploits the small macro executable code inside word processing or spreadsheet files and is spread through e-mail attachments, is the most infectious of all.

4004. Virus Protection

The first tier of virus detection and elimination is the server level. A server is generally a more powerful computer which stores and accesses data, and performs processing tasks on behalf of a users computer. In this context, it receives, transmits, and routes e-mail between individual computers. At this level, the server's networked-shared drive is scanned for viruses on an automatic basis. The server level is handled by the network system administrator and is transparent to the user. Servers should run anti-virus software periodically to catch any infected files placed on the shared drive. The G-6/S-6 is responsible for server protection. Unfortunately, servers themselves can be susceptible to infection by viruses. Some viruses can bypass server protection entirely. System administrators have little control over the type of data or files their users are exchanging between networks. With the advent of macro-type viruses, a user can receive and unknowingly unleash a virus hidden in a simple text file attached to e-mail. Viruses received from the SIPRNET currently are not intercepted by server-based anti-virus software. This allows viruses to flow into the internal LAN unchecked. Once inside the LAN, e-mail and attachments are encrypted in ways that vary as a function of the e-mail system used (e.g., cc mail, Eudora, MS Exchange, and DaVinci). This encryption blocks virus scanning of e-mail attachments while they are still in mail form. Only after the attachment has been "saved as" (and hence decrypted) to a hard disk can virus scanning take place.

The second tier of virus defense is the desktop workstation. At this level, the user accomplishes virus detection and elimination. All workstations should have anti-virus software that runs when the user boots up the system or when the user runs the software to perform a virus check on a hard disk or floppy disk. Individuals check for viruses on the local drive by "cold booting" their workstations off and on at shift change. When the computer is turned on, virus detection software automatically runs on the workstation to detect a virus. The computer locks up if a virus is

detected. To unlock the computer the user should contact the designated help desk. Combat operations run twenty-four hours a day—virus detection and anti-virus software must be initiated daily (minimum). Users should initiate a virus check at the start of each shift.

The last tier of virus detection and elimination is the individual diskette. Diskettes can easily act as hosts for the virus to travel from machine to machine, and re-infect machines after they have been scanned. Unless you know otherwise, assume diskettes are infected. As with the desktop workstation, the user is responsible for using virus detection software to scan diskettes for infection. Always scan diskettes before use.

4005. Information Security

Information security is the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. (Joint Pub 1-02).

a. Access to Classified Information

The information security manager establishes procedures to verify security clearances for assigned and augmentation personnel. Actual access, regardless of clearance, should be based on a “need to know” basis that is consistent with operational requirements and requirements. The final responsibility for granting access rests upon the individual who has authorized possession, knowledge, or control of the information and not upon the prospective recipient. Cleared personnel should not be permitted access to classified information and information systems until briefed on IM and information security procedures.

b. Security Marking of Documents

All users must ensure they properly mark all documents with the appropriate classification level. Header and footer markings should be included as well as paragraph markings, even though some viewers do not display header and footer text. Do not rely solely on header and footer comments for proper marking of electronic documents.

c. Computer Disk Classification

- Diskettes will be labeled with the appropriate operational classification. They have either the SF 710 (1-87) UNCLASSIFIED Sticker (Green) or the SF 707 (1-87) SECRET Sticker (Red).
- Diskettes used in a SECRET computer system, regardless of the classification of the files loaded on the diskette, are classified SECRET and marked appropriately.

d. Classified Destruction

Classified documents and other material shall be retained only if they are required for effective and efficient operation of the organization or if law or regulation requires their retention. Documents that are no longer required for operational purposes shall be disposed of in accordance with the provisions of the Federal Records Act (44 USC 21 and 33) and this publication. Material that has been identified for destruction shall continue to be protected as appropriate for its classification until it is actually destroyed. Destruction of classified documents and material shall be accomplished by means that eliminate risk of reconstruction of the classified information they contain.

Crosscut shredders are the preferred method of destroying classified information. If authorized shredders are not available, burn bags will be used. Burn bags should be placed throughout the unit workspace, with particular attention to areas that include printers and copiers. Users must be cognizant of the potential for an adversary to piece together

the mission of the unit and concept of operations from minor or seemingly insignificant revelations concerning organizational or unit plans and intent. Dispose of unneeded written materials via an authorized shredder or dispose of the information by placing it in a burn bag.

When burn bags are used for the collection of classified material that is to be destroyed at central destruction facilities, such bags shall be controlled in a manner designed to minimize the possibility of their unauthorized removal and the unauthorized removal of their classified contents prior to actual destruction. When filled, burn bags shall be sealed in a manner that will facilitate the detection of any tampering with the bag. Sealed bags must be marked with an office symbol and the highest classification of the information contained therein.

Records of destruction are not required for Secret material except for NATO and foreign government documents. For NATO or foreign government secret material, two signatures are required on the record of destruction. Records of destruction are not necessary for confidential material unless required by the originator. Any questions regarding classified destruction see the unit information security manager or SCI SSO as appropriate.

If no longer required, diskettes and removable hard drives will be physically destroyed to prevent unauthorized access to the classified material recorded upon them. If the diskettes and hard drives are still useful, then once the classified material has been removed by authorized degaussing and erasure programs (wiping), they may be treated as unclassified material and used appropriately.

4006. Future Initiatives

a. Network Multi-level Security

The competing demands of security and wide dissemination require databases and networks with different levels of classification and access. Currently, different networks include the NIPRNET, the SIPRNET, and the JWICS. However, in any given scenario a command may also need to operate on an Allied or Coalition classified network. Passing information from a network to another network of higher classification is usually achievable and secure. However, sharing information from a protected network to another network of lower classification is a much more difficult feat and is currently not possible in an automated fashion. Operators must take great care to ensure that information protected at the higher level is not compromised and inadvertently placed into the network with lower classification. Operators can use local procedures to manually verify that information is appropriate for release, and then use some manually managed procedure (i.e., copying to a known clean disk and moving that disk to the network of lesser classification) to disseminate the information.

b. Multi-level Workstation

The ability to exchange various classifications of information between different networks on one workstation is not currently authorized. As a result, organizations are required to use redundant systems to perform the same functions conducted at different classification levels. As an example, the all-source fusion center requires three different workstations to perform intelligence assessment: one terminal to access SCI, one terminal to access secret information, and one terminal to collect, analyze, and disseminate open-source information. Once multi-level workstations are approved to process and disseminate different classifications of information, the use of redundant systems to support information requirements will reduce.

c. Ability to Protect, Detect and Defeat Hostile Intrusion

The first step to defeating a network intruder is preparing defenses. But like all defenses, network defenses only buy time and not full protection. Given enough time, an intruder can eventually acquire information that could be detrimental to friendly force operations/mission objectives. The second step to defeating these intruders, then, is have the ability to detect when and where an intrusion attempt is being made and the type of capability being used to

perform the intrusion. This leads to the third step, which is to have a contingency plan in place to meet and defeat this threat based on time and planning considerations established by friendly force commanders. This allows friendly force commanders to choose when and where to degrade, defeat, deceive, or possibly destroy the threat once it is detected. Only through a comprehensive plan to defend against, detect, deceive, and defeat hostile intrusion can a network truly be protected. The IMO must work closely with each of the primary battle staff to protect functional databases/capabilities and the G-6/ISMO to ensure critical data networks are adequately protected.

This page intentionally left blank.

Appendix A

Information Management Annex Format

The following information provides an overview of what should be considered when developing an IMP. The following IMP is focused on supporting a Marine expeditionary force (MEF)-level MAGTF, but the same principles are applicable for all commands. Procedures normally found in unit SOP would not normally be contained in the IMP, but this format provides amplifying information to promote unity of effort throughout the Marine Corps.

This page intentionally left blank.

CLASSIFICATION

Copy no. ____ of ____ copies
 OFFICIAL DESIGNATION OF COMMAND
 PLACE OF ISSUE
 Date/time group
 Message reference number

ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
 INFORMATION MANAGEMENT ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

1. () Information Management Overview. Present an overview of the IM procedures described in this annex. Address actions that support managing quality information using the appropriate mix of personnel, equipment, procedures, training and communication, through the use of tools such as—

- CCIRs.
- Daily battle rhythm.
- Track management procedures.
- Intranet management procedures.
- RFI management.

2. () Purpose. Describe the purpose of the IM plan and how it will implement IM principles and procedures. Focus on information required to satisfy CCIR to improve the commanding general's situational awareness and facilitate rapid decisionmaking. IM procedures are used to manage quality information needed to support the CTP, share information through the use of intranet/internet, and reduce uncertainty through the use of RFI management. The SIPRNET will provide the backbone for connectivity among all participants.

3. () Information Management Points of Contact. List key IM personnel and summarize their roles. Provide further details in Appendix 3 to this Annex:

- a. () MEF Information Management Officer: Rank/Name
- b. () Staff Section Information Managers
- (1) () G-1, Personnel: Rank/Name
- (2) () G-2, Intelligence: Rank/Name
- (3) () G-3, Fires: Rank/Name
- (4) () G-4, Logistics: Rank/Name
- (5) () G-5, Plans: Rank/Name
- (6) () G-6, Communications: Rank/Name

CLASSIFICATION

- (7) () G-7, Assessment: Rank/Name
- c. () CCIR Manager: Rank/Name
- d. () MEF Web Master: Rank/Name
- e. () RFI Managers
- (1) () G-2, Intelligence: Rank/Name
- (2) () G-3, Operations: Rank/Name
- f. () Common Tactical Picture Managers: Rank/Name
- g. () Major Subordinate Command IMOs
- (1) () Ground Combat Element: Rank/Name
- (2) () Aviation Combat Element: Rank/Name
- (3) () Combat Service Support Element: Rank/Name
4. () Commander's Critical Information Requirements. Describe the role and importance of CCIRs in the management and filtering of information. The assistant chief of staff, G-3 is responsible to the commanding general for managing CCIRs and the actual CCIRs will be listed elsewhere in the order. Use Appendix 1 to this annex for additional details regarding the CCIR validation process.
5. () Reports Matrix. Describe the role and importance of reports in the command's IM concept, and outline in general terms the schedule by which reports are developed and delivered. The paragraph will describe how the reports matrix is used by the staff to monitor the delivery of required by the commanding general to maintain situation awareness of key events and issues. Actual report formats will be listed elsewhere in the order. Additional details will be contained in Appendix 4, Tab B to this annex.
6. () Daily Battle Rhythm Matrix. Describe how the commanding general uses the DBRM to focus his staff on the quality information he needs to achieve understanding for decisionmaking. Information contained in the daily battle rhythm is normally extrapolated from the reports matrix, while timelines are established by the CG. Events scheduled throughout each day (briefs, huddles, updates, visits, boards, etc.) are reflected in the matrix. Include additional information such as when reports are due from major subordinate commands, when reports are due to higher headquarters, and key command events such as air tasking order input/publication, shift changes, and other essential information needs. Use Appendix 4, Tab C to this annex to provide the format and actual matrix.
7. () Intranet Management. Provide general guidance regarding the management of the intranet by the MEF throughout the operation. Details will be listed in the following sub-paragraphs:
- a. () Location of MEF planning web site (list SIPRNET address here).
- b. () Describe how requests for additions to the MEF operational main home page will be submitted.
- c. () List the staff section web masters and their responsibilities:
- (1) () Staff Secretary: Rank/Name
- (2) () G-1: Rank/Name
(Page number)

CLASSIFICATION

CLASSIFICATION

- (3) () G-2: Rank/Name
- (4) () G-3: Rank/Name
- (5) () G-4: Rank/Name
- (6) () G-5: Rank/Name
- (7) () G-6: Rank/Name
- (8) () G-7: Rank/Name

8. () Request for Information Management. Describe the RFI process in general terms, and refer to Tab D, Appendix 4 for additional details.

9. () Track Management. Describe the track management system in general terms, and refer to Tab E, Appendix 4 to this annex.

10. () Exercise Design. This paragraph will be used only in an exercise environment. It describes how communication, equipment, procedures and modeling, and simulation capabilities will be integrated during the exercise, to include how time zones will be used by the C2 systems. Use Tab F, Appendix 4 to this annex for a matrix of game time, real time, computer system time, ZULU time, and time zones for different operating areas.

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

APPENDIXES:

- 1 — Management of Commander’s Critical Information Requirements
- 2 — Information Needs
- 3 — Duties and Responsibilities for Personnel Supporting Key IM Functions
- 4 — Procedures

OFFICIAL:

s/
Name
Rank and Service
Title

CLASSIFICATION

Copy no. ____ of ____ copies
 Official Designation of Command
 Place of Issue
 Date/time group
 Message reference number

APPENDIX 1 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
 MANAGING COMMANDER'S CRITICAL INFORMATION REQUIREMENTS ()

- () REFERENCES:
- a. Any relevant plans or orders.
 - b. Required maps and charts.
 - c. Other relevant documents.

1. () CCIR Management Procedures. Summarize how the command will develop, disseminate and task, report, and answer CCIRs. Address any specific information that bears directly on the planned operation.

2. () Tools to Manage CCIRs. Identify the capability/system here and the tool used to manage CCIRs and the information responding to the CCIR. Provide a detailed description of the system and all procedures related to the input, update, and maintenance of the information on the system.

3. () CCIR Development. Provide a detailed description of how CCIRs will be developed and reviewed, to include the following:

- Who is authorized to submit new CCIR or changes to existing CCIR?
- How and where are CCIR and subsequent changes submitted?
- Who reviews and approves CCIR?
- How are CCIR and subsequent changes and updates disseminated and tasked?

4. () Reports Matrix. The reports matrix is a tool for the staff to identify information they need to satisfy CCIR, conditions and routine daily updates that the commanding general needs to gain knowledge he requires to make sound, timely decisions.

- Describe how the MEF IMO works with each staff section IM representative to ensure the reports matrix is correct and updated as required. Discuss primary means of dissemination, verification of information, and the impact of the urgency of the decision supported by the information to be provided.
- Outline procedures to acknowledge receipt of information by the proper people with the authority to implement required actions. A more detailed description can be inserted in the Reports Matrix Tab.
- Describe the role of the MEF web master in the dissemination of reports using intranet/internet capabilities. Discuss further in Tab B, Appendix 4 to this Annex.

5. () Routine Daily Update Folder. The commanding general will occasionally ask questions of his staff that must be answered, but which, by definition, are not CCIR. Nevertheless, the fact that the commander has asked a question makes it important enough for the battle staff to collect, process and evaluate information that satisfies those questions. For these questions, create a routine daily update folder; it provides a place to store questions the commander has asked until the responsible staff section answers them. This process, although similar to the RFI

(Page number)

CLASSIFICATION

CLASSIFICATION

mechanism, is different in that these are information needs initiated by the commander. These questions may develop into RFIs or CCIRs. The management of the routine daily update folder should be outlined here as well.

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

TABS: As appropriate

OFFICIAL:

s/

Name

Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
Official Designation of Command
Place of Issue
Date/time group
Message reference number

APPENDIX 2 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
INFORMATION NEEDS ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

1. () Quality Information Needs. Define quality information as required by the command. Describe the sources of this information and how it will be presented, to include the following:

- a. () Commanders Critical Information Requirements. Define CCIRs.
- b. () Conditions. Define the conditions used to support each stage and/or phase of the operation.
- c. () Routine Daily Update. Define the information the commanding general needs on a routine basis to maintain situational awareness.

2. () Methodology. Summarize the process the command will use to recognize “quality” information the commanding general needs to achieve understanding. Identify decisions from reference (c) that form the basis to determine information used to support the commanding general and his staff. Describe the role of the DSM and other supporting in assessment, to include—

- a. () Measures of Effectiveness
- b. () Indicators
- c. () Pertinent Information

3. () Action. Address the role of the key IM personnel in defining, reviewing, modifying, and supporting MOEs, indicators, and pertinent information. These personnel should include—

- a. () The Chief of Staff
- b. () Primary Staff
- c. () Information Management Officer
- d. () Staff Section Information Managers

ACKNOWLEDGE RECEIPT

CLASSIFICATION

Name
Rank and Service
Title

TABS: As appropriate

OFFICIAL:

s/

Name

Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
Official Designation of Command
Place of Issue
Date/time group
Message reference number

APPENDIX 3 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
DUTIES AND RESPONSIBILITIES FOR PERSONNEL SUPPORTING KEY IM FUNCTIONS ()

- () REFERENCES: a. Any relevant plans or orders.
- b. Required maps and charts.
- c. Other relevant documents.

Normally duties and responsibilities for key personnel involved with managing information would be found in a unit SOP. If the unit SOP does not contain this information, provide it in this appendix for the following personnel—

1. () Chief of Staff/Executive Officer
2. () Primary Staff
3. () Information Management Officer
4. () Staff Section Information Managers
5. () Request for Information Managers
6. () Common Tactical Picture Manager
7. () MEF Web Master
8. () Subordinate Unit and Higher Headquarters Information Management Officers

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

TABS: As appropriate

OFFICIAL:

s/
Name
Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
 Official Designation of Command
 Place of Issue
 Date/time group
 Message reference number

APPENDIX 4 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
 PROCEDURES ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

Procedures from the unit SOP do not need to be duplicated in this appendix or supporting tabs. The procedures in this appendix are provided to support key decisions reflected by the DSM. Procedures are adjusted based on changes with information needs influenced by decisions the commanding general expects to make. Tabs A through F of this Appendix describe procedures needed to share quality information throughout the command.

ACKNOWLEDGE RECEIPT

Name
 Rank and Service
 Title

TABS: As appropriate

- A — Intranet/Internet Management
- B — Reports Matrix
- C — Daily Battle Rhythm
- D — RFI Management
- E — Track Management

OFFICIAL:

s/

Name

Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
 Official Designation of Command
 Place of Issue
 Date/time group
 Message reference number

TAB A TO APPENDIX 4 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
INTRANET/INTERNET MANAGEMENT ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

1. () General. Summarize the role of the MEF internet, intranet, and SIPRNET web site and how they will provide operational information to the staff and the major subordinate commands. Outline responsibilities of the information manager from each staff section or major subordinate command.

2. () Site Description. Describe the SIPRNET web site and the responsibilities for creation, management, and updating of the various pages outlined in paragraph 4 below.

3. () Key Web Personnel. Describe the intranet/internet role of the following personnel—

a. () MEF RFI Managers

b. () COC/CIC Senior Watch Officers. Include a list of inter/intranet items that the senior watch officer is responsible for keeping updated, such as—

- CCIRs posted as HTML.
- Commanding general's brief.
- Daily situation report.
- RFIs.
- Command journal.
- Operational templates and execution checklists.

c. () Staff Section Information Managers. At a minimum, the following sections require a section information manager: G1, G2, G3, G4, G5, G6, public affairs officer, staff judge advocate, comptroller, chaplain, surgeon, and all major subordinate commands assigned to the MEF for operations.

c. () Web Server Administrator

4. () Web Page Architecture. Summarize the structure of the command web site and include a description information contained, format, and location. Include the following web pages and links—

a. () Orders Page. Describe the page containing the command order, including its' two usual links—

(1) () Operation Order

CLASSIFICATION

- (2) () Warning Order/Fragmentary Order
- b. () CCIRs
- c. () Directories
- d. () Staff Sections/Major Subordinate Commands Describe the requirements for each staff section and major subordinate command, to include the associated links. Each staff section page has at least four links—
 - A current list of CCIRs, conditions, and routine daily updates that the commanding general needs to gain knowledge.
 - Information needed to update the MEF reports matrix.
 - Information that needs to be highlighted on the DBRM.
 - A link that allows users to request for information.
- e. () Command Journal
- f. () AUTODIN Messages. Include a description of how to gain MS Outlook access to SIPRNET and NIPRNET message traffic as text files.

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

EXHIBITS: As appropriate

OFFICIAL:

s/
Name
Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
 Official Designation of Command
 Place of Issue
 Date/time group
 Message reference number

TAB B TO APPENDIX 4 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
 REPORTS MATRIX ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

Provide the format for the reports matrix. The reports matrix identifies information the staffs need to respond to CCIRs, conditions, and routine daily updates for the commanding general to gain the understanding he requires to make sound, timely decisions. Using the methodology described in Appendix 2, each staff section ensures information required by the reports matrix is updated accordingly. The MEF IMO will work closely with each staff section IM representative to requirements for the reports matrix. Reports that are not linked to decisions should be eliminated unless the staff section determines a justified need.

Information relevant for specific planning horizons determined by the commanding general will be highlighted for inclusion in the DBRM.

INFO NEEDED	ORIGINATOR	RECIPIENT	MODEs OF DISSEMINATION	REPORT FORMAT (text, imagery, voice, visual, data, etc.)	TIME REQUIRED	REMARKS

ACKNOWLEDGE RECEIPT

Name
 Rank and Service
 Title

EXHIBITS: As appropriate

OFFICIAL:
 s/
 Name
 Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
 Official Designation of Command
 Place of Issue
 Date/time group
 Message reference number

TAB D TO APPENDIX 4 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
 REQUEST FOR INFORMATION MANAGEMENT ()

- () REFERENCES: a. Any relevant plans or orders.
 b. Required maps and charts.
 c. Other relevant documents.

1. () General. Summarize the process by which RFIs will be drafted, processed, submitted, validated, and submitted. Include a description of responsibilities for personnel associated with RFI management.

2. () RFI Tools. Describe the purpose and function of manual and automated support tools and processes that will be used to manage RFIs, to include—

- RFI tracking numbers.
- Tracking sheets.
- RFI database.

3. () RFI Submission Guidelines. Outline the requirements for submission of RFIs, to include—

- Number of questions per request.
- How RFIs should be stated and degree of desired detail.
- Who can originate RFIs.
- Where RFIs are submitted.
- Validation authority for RFIs.

ACKNOWLEDGE RECEIPT

Name
 Rank and Service
 Title

EXHIBITS:

- A — RFI Flow Diagram

CLASSIFICATION

OFFICIAL:

s/

Name

Rank and Service

(Page number)

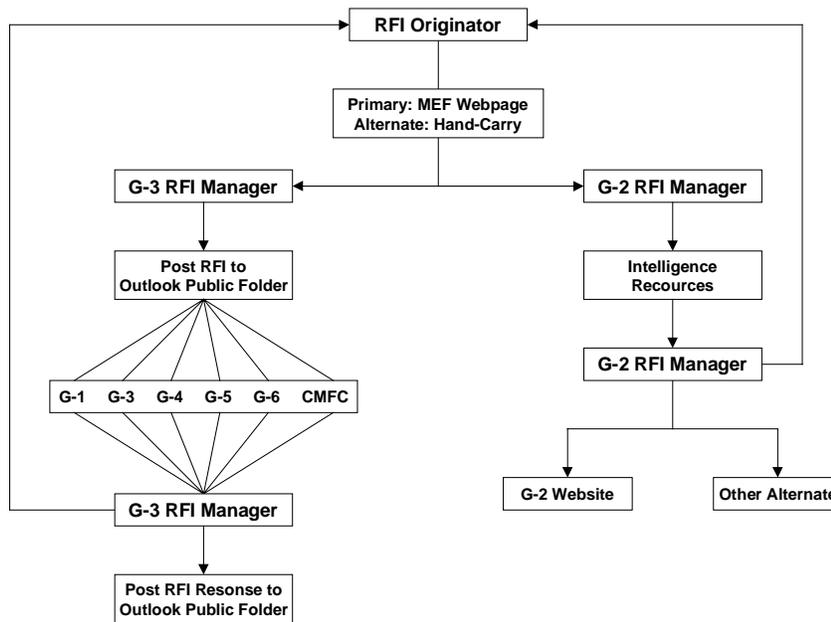
CLASSIFICATION

CLASSIFICATION

Copy no. ____ of ____ copies
Official Designation of Command
Place of Issue
Date/time group
Message reference number

EXHIBIT 1 TO TAB D TO APPENDIX 4 TO ANNEX U TO OPERATION ORDER OR PLAN (Number)
(Operation CODEWORD) ()
RFI FLOW DIAGRAM ()

- () REFERENCES:
- a. Any relevant plans or orders.
 - b. Required maps and charts.
 - c. Other relevant documents.



ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

ATTACHMENTS: As appropriate

OFFICIAL:

s/
Name
Rank and Service

CLASSIFICATION

Copy no. ____ of ____ copies
Official Designation of Command
Place of Issue
Date/time group
Message reference number

TAB E TO APPENDIX 4 TO ANNEX U TO OPERATION ORDER OR PLAN (Number) (Operation CODEWORD) ()
TRACK MANAGEMENT ()

- () REFERENCES:
- a. Any relevant plans or orders.
 - b. Required maps and charts.
 - c. Other relevant documents.
1. () General. Summarize the process by which the command will manage unit track data. Discuss display systems, automated support systems, controlling authority, and frequency of updates.
2. () Procedures. Describe the track management process in more detail. Include the following major topics--
- a. () Personnel. Responsibilities of personnel such as the track manager and system administrator.
 - b. () Blue Force Tracks. Management of friendly unit track data, to include data systems, update schedule, and amplifying data.
 - c. () Overlays. Required operational and intelligence overlays to depict scheme and control measures for the operation being executed. List established overlay standards such as—
 - Color of lines and arrows.
 - Color and size of symbols.
 - Color and shape of polylines.
 - Maneuver and restrictive fire control measures.
 - Amplifying remarks.
 - Map data.
 - f. () Miscellaneous. Discuss additional track issues as required, such as
 - Software.
 - Chat rooms.
 - Public folders.
 - Trouble shooting and coordination.
 - Passwords.

CLASSIFICATION

3. () Tactical Combat Operations System. Outline detailed procedures for origination and manipulation of unit track data with the tactical combat operations system.

4. () Broadcast Times. Provide a table showing the schedule for updating tracks, and guidance for frequency of backup of data.

UNIT	TIME INTERVAL

5. () Command and Control PC. Outline command and control personal computer (C2PC) procedures, to include—

- Gateway IP addresses.
- Login/passwords.
- “Read only” and “edit” accounts.
- User accounts.
- Multi-tiering.
- Number of C2PC Gateways to the track database management.

6. () Trouble Procedures. Outline procedures to be followed in the event of data, system, network or software problems. Include points of contact.

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

EXHIBITS: As appropriate

OFFICIAL:

s/

Name

Rank and Service

Appendix B

Information Management Support to Planning

Planning centers on the commander's intent and guidance and requires immense amounts of focused information to be successful. IM tools and procedures provide commanders and planners the information in a form they quickly understand. IM tools and procedures also facilitate the exchange of information throughout the command, which in turn enhances the ability to plan at all levels of command and promotes unity of effort throughout the MAGTF.

The MCPP establishes procedures for analyzing a mission, developing and analyzing COAs against the threat, comparing friendly COAs against the commander's criteria and each other, selecting a COA, and preparing an operation order for execution. The MCPP organizes the planning process into six manageable, logical steps (see figure B-1). It provides the commander and his staff a means to organize their planning activities and transmit the plan to subordinates and subordinate commands. Through this process, all levels of command can begin their planning effort with a common understanding of the mission and commander's intent. Interactions among the various planning steps allow a concurrent, coordinated effort that maintains flexibility, makes efficient use of time available, and facilitates continuous sharing of critical and relevant information. This appendix provides examples of IM tools and procedures and an explanation of how they can be used to support each step of the planning process. Additional details can be found in MCWP 5-1, *Marine Corps Planning Process*.

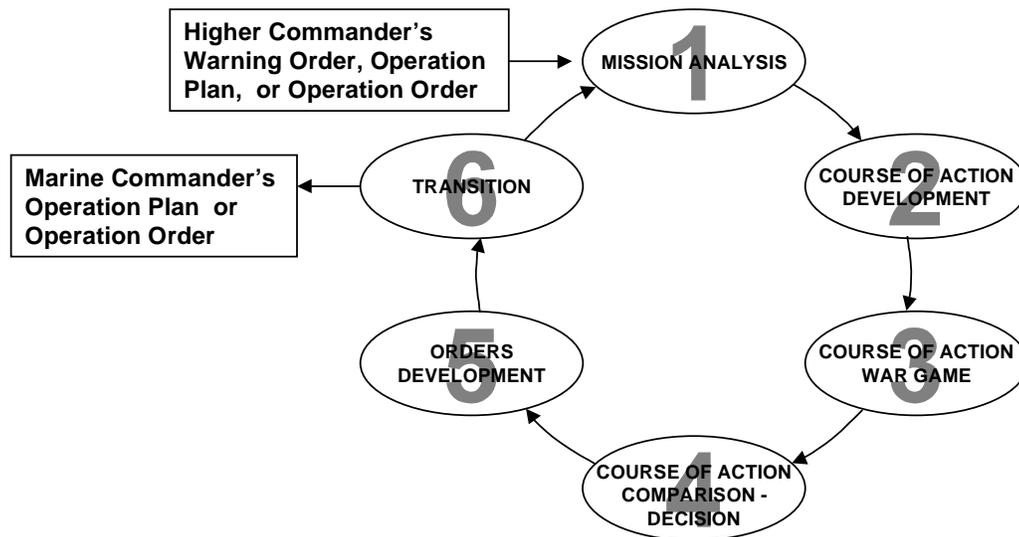


Figure B-1. The Marine Corps Planning Process.

B-1. Mission Analysis

The purpose of mission analysis is to review and analyze orders, guidance, intent, and other information provided by higher headquarters to produce a unit mission statement. This step forms the foundation for the remainder of the planning process. Figure B-2 describes basic input, the process, and output for mission analysis. IM tools and procedures can assist in the development and dissemination of mission analysis products.

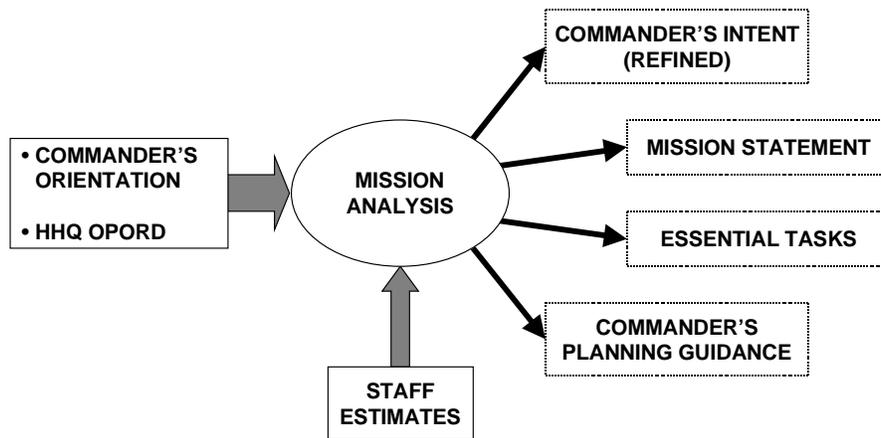


Figure B-2. Mission analysis.

The commander's battlespace area evaluation (CBAE) is the commander's personal vision based on his understanding of the mission, battlespace, the threat, and the environment. The commander uses CBAE to develop, assess, and communicate knowledge to the staff to support all four aspects of the decisionmaking process, which includes planning, decision, execution, and assessment. Figure B-3 provides an example of how IM procedures can use current capabilities such as MS Office to record and disseminate CBAE in text form to many personnel simultaneously.

A	B	C
1	TITLE	Tunisia: Stage A of JTF Phase 2
2	GEOMETRY	I'm originally satisfied with the boundary with XVIII AB Corps. It gives us maneuver room. However, as we move towards Phase Line Green, we really get channelized. And look at PL Green as the initial limit of advance. Does it give us enough room to reach out and shape II Corps? Also, with the size of XVIII AB Corps' zone, can they stop the Algerians from linking up with the Libyans? I don't know, but that is the most dangerous enemy COA as I see it.
3	INTENT	(1) The defeat of the Libyan I Corps; by defeat I mean incapable of continued coordinated operations above brigade level. (2) The Mezzouna Oil Fields secured; by secured I mean no organized resistance above the company level. (3) The key choke points and bridges on the MSR in coastal mobility corridor vicinity of GABES secured. (4) Our forces postured to continue the attack to restore the Tunisian / Libyan border if so ordered. (5) SFAX secured; by secured I mean CSS established enabling throughput to support follow-on operations.
4	CCIRs	I need to know when fuel becomes critical. I will provide additional CCIRs after reviewing our assigned mission, and I expect the OPT to provide other recommended CCIRs during their mission analysis.
5	COGs	I see the enemy's tactical center of gravity (COG) as the Libyan I Corps. I believe two of the I Corps' critical capabilities (CCs) to be the CAR (1st Artillery Regiment) and the Mahgreb Brigade. Use the Red Cell to tighten this area.
6	ENEMY	
7	FRIENDLY	Additionally, I see our ability to conduct air operations as our COG.
8	GUIDANCE	Decisive operations are defined as the defeat of the Mahgreb Brigade of the Libyan I Corps. By defeat I mean the inability to conduct continued, coordinated combat operations. Shaping, primarily with aviation and including indirect fires and C2W, against the CAR and the Mahgreb Brigade begins to establish the conditions enabling decisive operations.
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		

Figure B-3. Using MS Exchange to record commander's battlespace area evaluation.

Figure B-4 is an example of how current capabilities, such as intelligence operations workstation (IOW) can be used to record CBAE through the combined use of visual display products and text information. Through the use of effective IM procedures, current capabilities can be used to record and release this information to designated recipients or disseminate the information to many personnel simultaneously. The originator possesses the ability to control access and dissemination.

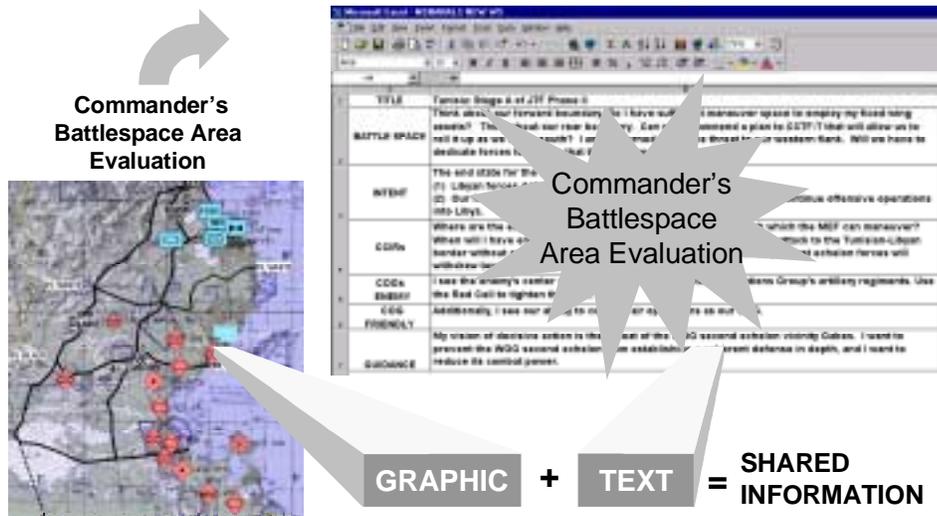


Figure B-4. Visual display product.

Using collaborative tools, MAGTF planners record text information that describes the commander’s orientation, which includes higher headquarters plans, orders, estimates, availability and suitability of forces, and results of personal reconnaissance. This information is recorded using MS Office capabilities (Excel spreadsheet) along with MS Exchange server capabilities. Automated visual display mapping capabilities are used to record analysis of the threat and associated intelligence preparation of the battlespace (IPB) products, to include environmental concerns (see to figure B-5 for an example of text and visual display products recorded during mission analysis).

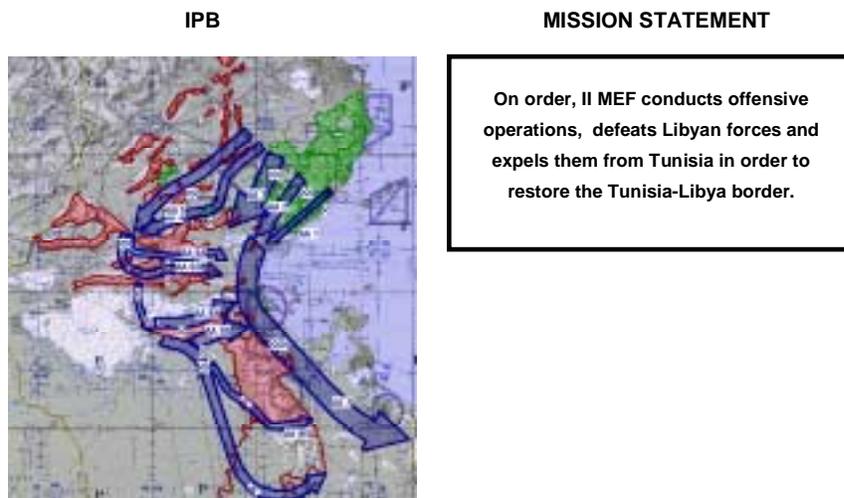


Figure B-5. Mission analysis products.

With a thorough understanding of higher headquarters’ orders and intent and an understanding of their own CBAE and initial guidance, planners identify and record the specified, implied, and essential tasks using MS Office products developed through the use of current IM capabilities. Essential tasks form the foundation for the mission statement. The commander’s intent, the mission statement, essential tasks, and commander’s planning guidance are recorded using MS Office products specifically designed to store and easily retrieve this information. Staff estimates are continuously updated and provided to planners using various forms of information, to include voice, text, and visual display products. The mission statement is generated and recorded using MS Office capabilities. Throughout the

planning process planners maintain situation awareness of current operations by monitoring a dynamic visual display of the common tactical picture that depicts current status of friendly and threat forces and relative environmental concerns. The visual display is provided through the use of IOW (a PC based platform that uses MS Exchange and C2PC capabilities) linked to the MAGTF CTP Unix server using a tactical combat operations system or Global Command and Control System (GCCS) terminal.

B-3. Course of Action Development

The mission statement, commander's intent and commander's planning guidance are used to develop several COAs that are suitable, feasible, acceptable, distinguishable, and complete with respect to current and anticipated situation, the mission, and tasking/intent from the higher headquarters commander.

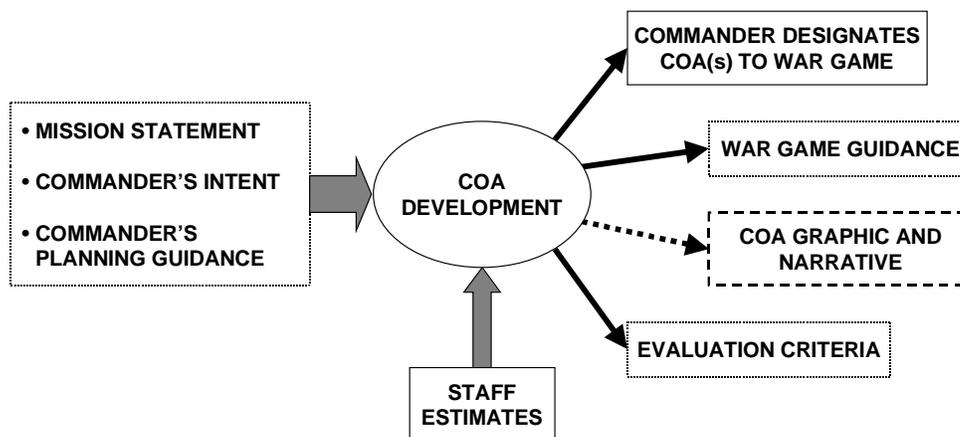


Figure B-6. Course of action development.

During COA development, IM tools and procedures are used to record specified tasks, implied tasks, essential tasks, warning order, restraints and constraints, assumptions, resource shortfalls, subject matter duty expert shortfalls, COG analysis (friendly and threat), CCIR, request for information, initial staff estimates, and IPB products. MS Office capabilities are tailored to record information for each COA developed. Staff estimates, relative to the time established by the planning horizons for that particular mission, provide planners updated information in both text and visual display products that describe friendly and threat force disposition and array of forces and other pertinent information concerning terrain and weather. Using that information and an array of employment possibilities, planners design a broad plan of “how” they intend to accomplish the mission. “How” they intend to accomplish the mission becomes the COA.

Planners can use a combination of IM text and visual display mapping products to document the following elements of a COA—

- Commander's planning guidance.
- Forms of maneuver
- Type of attack.
- Designated main effort.
- Requirement for supporting effort(s).
- Scheme of maneuver (land, air, and maritime).
- Sequential and simultaneous operations.
- Sequencing essential task accomplishment.

- Task organization.
- Use of reserves.
- Rules of engagement.

Figure B-7 shows how currently fielded IM tools can be used to display graphic and text information created during COA development.

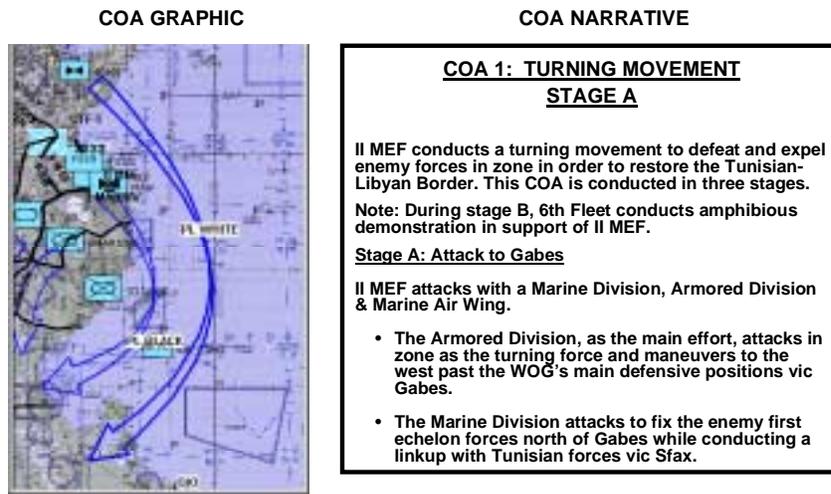


Figure B-7. Course of action development products.

B-4. Course of Action Wargame

The COA wargame involves a detailed assessment of each COA as it pertains to the threat and the battlespace (refer to figure B-8). Each friendly COA is wargamed against selected threat COAs. COA wargaming assists the planners in identifying relative strengths and weaknesses, associated risks, and asset shortfalls for each friendly COA. Additionally, COA wargaming identifies branches and potential sequels that may require additional planning. Short of actually executing the COA, COA wargaming provides the most reliable basis for understanding and improving each COA.

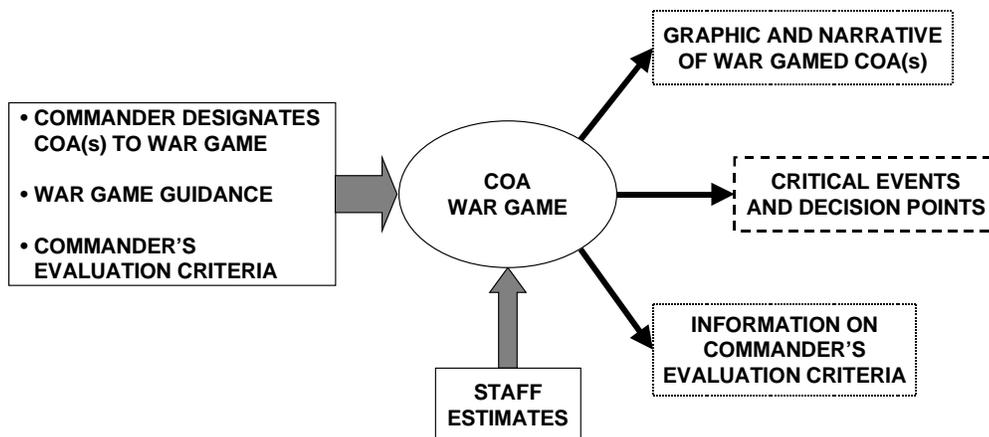


Figure B-8. Course of action war game.

COA wargaming allows the staff and subordinate commanders to gain a common understanding of friendly and possible threat COAs. This common understanding allows those personnel to determine the advantages and disadvantages of each COA and form the basis for the commander’s COA comparison and decision.

COAs designated by the commander to war game are easily retrieved using effective IM procedures that use a standard naming convention to record text and visual display mapping products/overlays for each COA developed. Using visual display mapping products, the staff conducts a war game using the threat’s most likely, most dangerous, and most advantageous (to friendly forces) COAs. Actions, reactions, and counteractions are recorded in both text and visual display products. During the war game, the commander’s staff and subordinate commands continue to refine their staff estimates and estimates of supportability. Figure B-9 shows how currently fielded IM tools can be used to display graphic and text information created during COA wargaming.

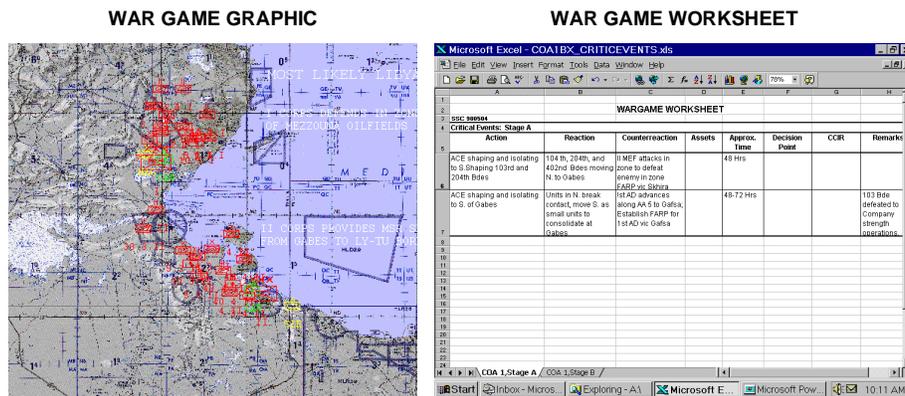


Figure B-9. Course of action war game products.

B-5. Course of Action Comparison and Decision

The commander’s evaluation of friendly COAs, first against established criteria, then against each other. Based on this comparison, intuitive reasoning is used to select the COA that he deems will best accomplish the mission. Figure B-10 identifies the input, process, and output for COA comparison and decision.

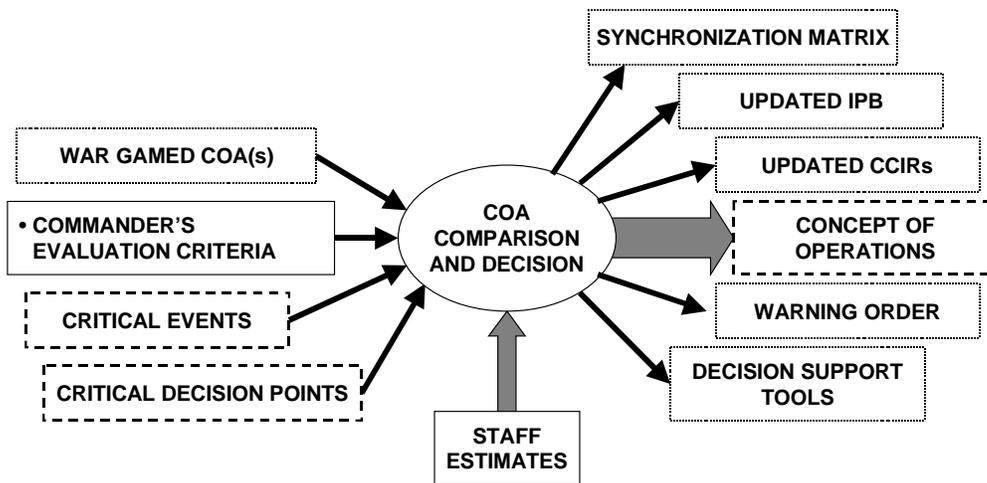


Figure B-10. Course of action comparison and decision.

COA comparison and decision requires wargamed COAs with graphic and narrative, list of critical events and decision points, and information on the commander’s evaluation criteria. Other outputs useful in COA comparison and decision may include; wargamed products (COA war game worksheet, synchronization matrix, event templates, decision support tools), war game results (initial task organization, identification of assets required and shortfalls, and updated CCIR), and staff estimates, subordinate commander’s estimates of supportability.

Figure B-11 shows how currently fielded IM tools can be used to display graphic and text information created during COA comparison and decision.

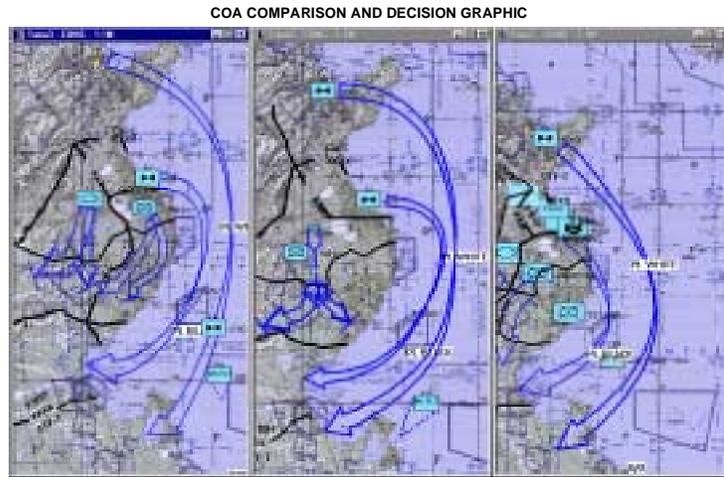


Figure B-11. Course of action comparison and decision products.

B-6. Orders Development

During orders development, the staff takes the commander’s COA decision, mission statement, commander’s intent and guidance, and develops orders to direct the actions of the unit. Orders serve as the principal means by which the commander expresses his decision, commander’s intent and guidance. Figure 12 identifies input, process and output to support orders development.

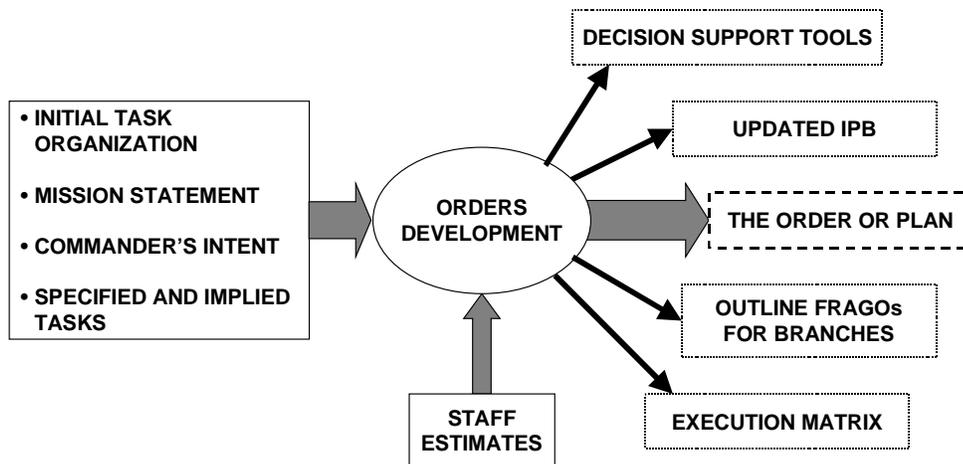


Figure B-12. Orders development.

The initial task organization, mission statement, commander’s intent, concept of operations, and specified and implied tasks, along with the information developed throughout the planning process, form the input for orders development. Other inputs can be recorded using current IM procedures and capabilities, which may include; updated intelligence and IPB products, decision support tools, updated CCIR, staff estimates, synchronization matrix, commander’s identification of branches for further planning, warning order, existing plans, and SOPs/orders. Figure B-13 shows how currently fielded IM tools can be used to support orders development.

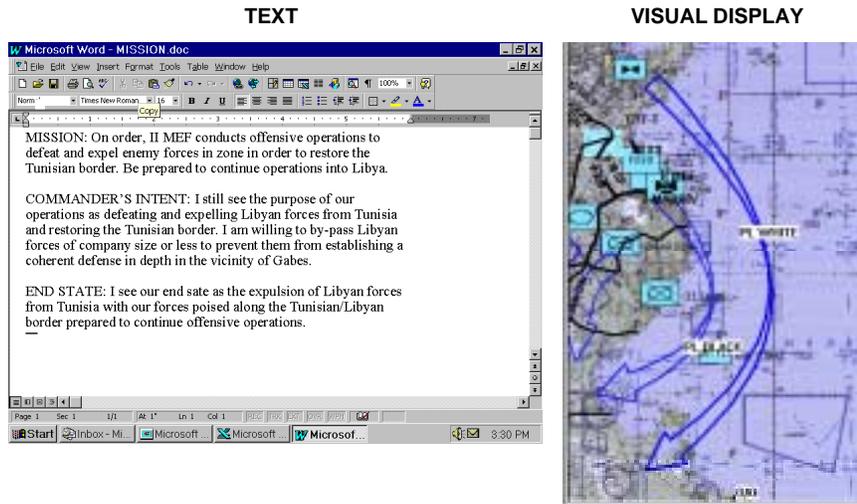


Figure B-13. Orders development products.

B-7. Transition

During transition, an orderly handover of a plan or order is conducted with those tasked with execution of the operation. Transition provides those who will execute the plan or order the situation awareness and rationale for key decisions necessary to ensure there is a coherent shift from planning to execution. Ideally, one of the planners will accompany the orders to assist staff principles and watch standers understanding specifics and gain familiarity with tools and concepts supporting the plan and to provide situation awareness. Figure B-14 describes input, process, and output to support transition.

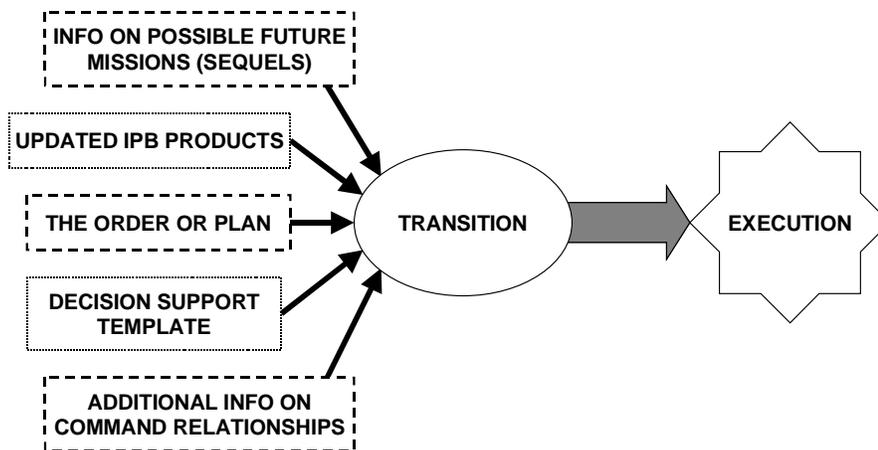
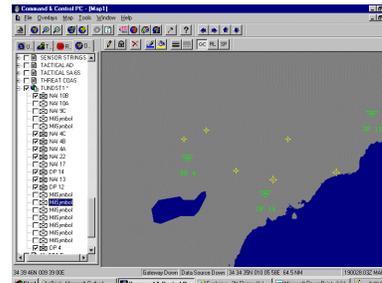


Figure B-14. Transition.

Transition is a continuous process that requires a free flow exchange of information between commanders and staffs to ensure critical and relevant information is being shared and clearly understood. IM procedures and capabilities enable personnel to share critical and relevant information through the use of collaborative planning tools, Intranet management, and common tactical picture procedures. Figure B-15 provides examples of transition products that can be created through the use of IM tools.

DP	EVENTS & INDICATORS	METABE	COLLECTION ASSETS
M12	ICORPS ATTACK ON SFAX: (1) INCREASED REGION ACTIVITY (2) INTENSE ARTY BOMBARDMENT (3) ATTEMPT TO SEIZE SFAX BY MULTIBN ATTACK	H1R5-H124	SIGINT, BMMT, AD, RECON, SCAMP, HMMNT
M4	MANGREB BDE COMMITMENT: (1) TACTICAL MOVEMENT OF MANGREB BDE FROM CURRENT POSITION/ASSEMBLY AREAS (2) UNUSUAL COMMS ACTIVITIES	H112H+36	SIGINT, BMMT, AD, RECON, SCAMP, HMMNT
M14 (M4)	WITHDRAWAL OF ICORPS 100, 13, 14 (1) LOG AND COMBAT UNITS DEPART PREPARED POSITIONS (2) REAR GUARD MOVES INTO VACATED POSITIONS (3) HQ AND LOG UNITS LEAD WITHDRAWAL ALONG MAJOR LOGS	SET DEP	SIGINT, BMMT, AD, RECON, SCAMP, HMMNT

DECISION SUPPORT MATRIX



DECISION SUPPORT TEMPLATE

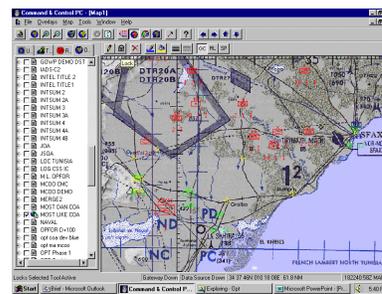
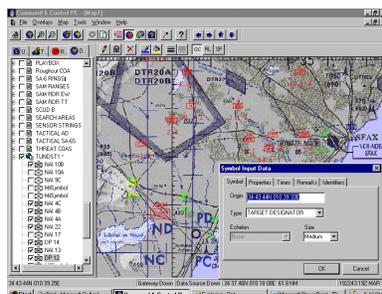


Figure B-15. Transition products.

This page intentionally left blank.

Appendix C

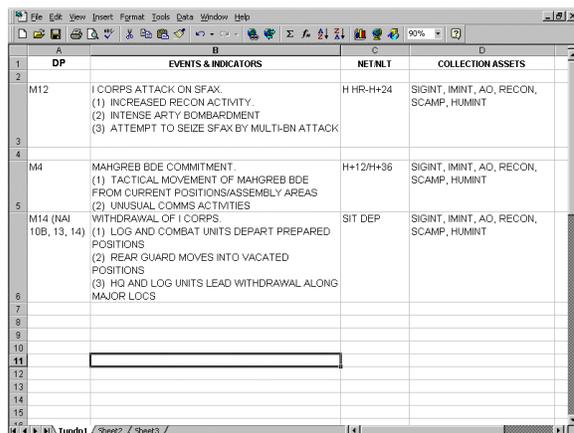
Information Management Support to Execution

Execution is the implementation of the plan developed during the planning process. However, no plan is perfect, and modifications must be made as the operation unfolds and the enemy reacts. Accurate and timely information is key to successful execution. This appendix discusses how IM tools and procedures support execution.

C-1. Information Management Execution Tools

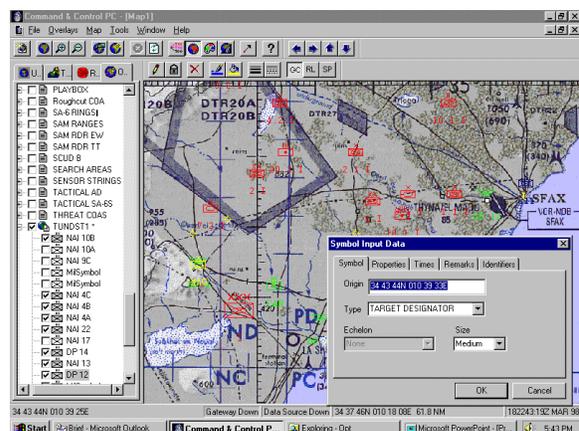
Planners transition various planning tools used to record the plan. These tools may include overlays that depict boundaries, fire support coordinating measures, intelligence collection plans, fire support plans, key decisions, and the information requirements and actions tethered to those decisions. Planning tools are often used to support execution, even when unexpected actions/activities occur.

Tools developed during the Marine Corps planning process include the DSM and DST. The DSM provides textual information that identifies key decisions, actions and information required to support those decisions, and actions expected to occur as a result of those decisions. Placing the text information from the DSM in visual form creates a DST. The DST provides a visual display of key decisions and the actions associated with those decisions. Figure C-1 is an example of how a DST (a visual product) is created from a DSM (a text product). Placing the DST on the same visual display capabilities used to maintain a common tactical picture provides each watch officer enhanced situation awareness of key situations or events. These tools enable watch officers to alert commanders of impending key decisions, and provide early warning to units executing those decisions.



A	B	C	D	
1	DP	EVENTS & INDICATORS	NET/MLT	COLLECTION ASSETS
2	M12	I CORPS ATTACK ON SFAX. (1) INCREASED RECON ACTIVITY. (2) INTENSE ARTY BOMBARDMENT (3) ATTEMPT TO SEIZE SFAX BY MULTI-BN ATTACK	H HR-H+24	SIGINT, IMINT, AO, RECON, SCAMP, HUMINT
3				
4	M4	MAHGREB BDE COMMITMENT. (1) TACTICAL MOVEMENT OF MAHGREB BDE FROM CURRENT POSITIONS/ASSEMBLY AREAS (2) UNUSUAL COMMS ACTIVITIES	H+12/H+36	SIGINT, IMINT, AO, RECON, SCAMP, HUMINT
5	M14 (NAI 10B, 13, 14)	WITHDRAWAL OF I CORPS (1) LOG AND COMBAT UNITS DEPART PREPARED POSITIONS (2) REAR GUARD MOVES INTO VACATED POSITIONS (3) HQ AND LOG UNITS LEAD WITHDRAWAL ALONG MAJOR LOCS	SIT DEP	SIGINT, IMINT, AO, RECON, SCAMP, HUMINT
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Decision Support Matrix



Decision Support Template

Figure C-1. Example of a decision support matrix used to develop a decision support template.

C-2. MCRP 6-23(E)

The fast moving world of IM does not easily mesh with the slower pace of doctrine development. In order to make the latest IM technologies available to the operating forces, an on-line electronic version of MCWP 6-23 has been developed. MCRP 6-23(E) is used to disseminate IM tools and procedures that are quickly evolving and changing. Detailed IM techniques are described in Volume 1, MCRP 6-23(E). Further information on execution tools, to include procedures for sharing information across all planning horizons, is described in detail in Volume 2, MCRP 6-23(E). Detailed procedures to maintain a CTP of friendly and threat ground, air, maritime units and key environmental concerns that enhance MAGTF situation awareness can be found in Volume 3, MCRP 6-23(E). Reducing uncertainty through the use of RFI management procedures is described in detail in Volume 4, MCRP 6-23(E).

C-3. MSTP Pamphlets

The MSTP has developed detailed “how to” IM procedures and is publishing them in pamphlet form. Each pamphlet will cover a specific IM topic and is intended to reflect emerging doctrine that is still under development, but for which the operating forces have expressed a need for interim guidance.

a. MSTP Pamphlet 6-1, MAGTF Information Needs

This TTP describes information needs used to support each echelon of command. The information needs identified by 6-1 will form the foundation for the development of detailed “how to” TTP that will describe how those information needs will be satisfied by a MAGTF supporting a joint/combined operation. The information needs are derived from the baseline list of tasks that are in the process of being verified by the operating force to support MAGTF operations. The list of tasks will be derived from the formal results of the Studies and Analysis, MCCDC sponsored functional assessment.

b. MSTP Pamphlet 6-2, Track Management Procedures

This TTP describes an overarching concept of employment for the integrated use of warfighting capability sets to satisfy MAGTF operations in a joint/combined operation. The TTP describes "how" understanding is achieved by the USMC component and subordinate echelons of command and "how" the component is able to share quality information with other components, the JTF and the combatant command in a COP environment. This TTP will include actions required to achieve understanding of location and disposition of friendly and threat forces within the battlespace and required coordinating measures used to enhance situation awareness. This TTP will describe the detailed “how to” to create and maintain the CTP in a COP environment.

c. MSTP Pamphlet 6-3, FDP&E in Support of MAGTF Operations

This TTP defines force deployment planning and execution (FDP&E), identifies the joint operations planning and execution system, time-phased force deployment data development through the use of MAGTF II and key pillars of the GCCS. The best results are achieved from focusing on the process and not the plan. The plan provides the framework to open the dialogue on process improvement. It provides general directional guidance; the process yields the results. Our planning process will be a continuous effort where we plan for the future, implement the plan, assess the outcome and then act on the information to adjust the plan. The Global Command and Control management structure provides the means for the process and the planning. This TTP describes “how” FDP&E provides detailed planning criteria used to support MAGTF operations.

d. MSTP Pamphlet 6-4, Intranets in Support of MAGTF Operations

This TTP describes “how” intranet and internet can be used to share “quality” information needed to support MAGTF operations. Intranet will focus on information needed to support each echelon of command, whereas Internet will

focus on quality information needed to be shared with external units/organizations. It is understood that both Intranet and Internet are not used to share time-sensitive information.

e. MSTP Pamphlet 6-5, The Planners Guide to C2PC

This TTP provides detailed “how to” for sharing quality information in the form of visual display products to those that need it, in a timely manner. This TTP concentrates on the use of personal based (PC based) platforms used to satisfy warfighting functions through the use of UNIX terminals that primarily perform the functions of a server.

f. MSTP Pamphlet 6-6, LOGAIS in Support of MAGTF Logistics

This TTP provides the detailed “how to” for the use of currently fielded logistics capability sets (LOGAIS, etc.) needed to support logistics and sustainment functions in a CTP supporting a COP environment.

g. MSTP Pamphlet 6-7, C2 Support to MAGTF Intelligence

This TTP provides the detailed “how to” for the use of currently fielded intelligence capability sets (such as intelligence analysis system, IOW, etc.) to maintain understanding of threat related information in a CTP supporting a COP environment.

h. MSTP Pamphlet 6-8, C2 Support for Force Fires

This TTP provides the *detailed* “how to” for the use of currently fielded fires capability sets used to maintain understanding of fires functions needed to support a CTP in a COP environment. The pamphlet will provide a basic “how to” guide on the use of the Contingency Theater Automated Planning System and Advanced Field Artillery Tactical Data System.

i. MSTP Pamphlet 6-9, Assessment

This TTP provides the detailed “how to” as to how currently fielded capability sets can be used in an integrated manner to reduce uncertainty (RFI management), manage critical information (CCIR management), manage quality information (IMP), support decisionmaking (DSM/DST) in a CTP supporting a COP environment.

C-4. Information Management During Joint and Combined Operations

IM procedures must be capable of providing a framework for rapid and effective exchange of information that enables the Marine Corps component to share critical and relevant information in support of joint/combined operations. Although each service possesses service unique capabilities, joint operations require IM procedures that are commonly understood by all components/services. For example, even though each service currently uses different tools to perform intelligence assessment, dissemination of relevant threat locations is conducted using track database management on the “chart” application of GCCS. Below corps-level, each component/service utilizes their unique service functional capability to conduct intelligence assessment, but GCCS (chart) is used by all components/services at corps-level and above. Consequently, the joint commander and each component commander are able to share critical and relevant information. The joint force is able to maintain a CTP with each component commander and share the CTP with the supported theater commander’s COP. Effective IM procedures ensure all essential information requirements and the processes necessary to support those information requirements are understood by each component supporting the joint force.

This page intentionally left blank.

Appendix D

Integrated Training

Traditionally, personnel receive training tailored to provide skills sets necessary to support a specific functional area. This specialized instruction generates “duty experts” in a particular field. However, this narrowly focused training does not provide a common understanding as to how functional capabilities and procedures need to be utilized in an integrated manner to support decisionmaking. Understanding the processes that support essential information requirements enable personnel to clearly identify functional capabilities, procedures, personnel, and training (skill sets) necessary to produce critical and relevant information that supports decisionmaking. It is critical that the following personnel within an organization possess the requisite skills necessary to work in an integrated manner to effectively manage critical and relevant information:

- Commander and primary battle staff.
- Watch officers, section chiefs, planners, and information management officers.
- System/functional capability operators.
- Network and system administrators.

D-1. Integrated Training Programs

The following classes are provided to each MEF by the MSTP during the C4I for the Warrior mobile training team (MTT) block of instruction. This training is designed to enable all personnel to understand the importance of commonly understood procedures that provides critical and relevant information to commanders in a form they quickly understand, thus promoting decisionmaking. These classes are currently provided to each MEF, but as time progresses and training adjusts, the required training will be updated and maintained in MCWP 6-23(E).

a. Common Operating Picture Overview

- **Training Audience.** Commanding general, battle staff, watch officers, section chiefs, information management officers, and planners.
- **Description of Class.** This class provides an overview of the MTT, discusses common tactical picture and common operating picture, provides a methodology for identifying essential information requirements, and discusses information management and the role of the information management officer to ensure effective and efficient procedures are utilized within the unit. A demonstration is provided of collaborative planning, intranet management, and RFI management tools.

b. Network Training

- **Training Audience.** Network and system administrators.
- **Description of Class.** The following subjects are covered by this class:
 - **UNIX.** Introduction to the VI editor and UNIX networking. Students will learn the location of critical network configuration files and commands enabling them to temporarily or permanently change a UNIX host’s IP address, netmask, and routing information.
 - **Routers.** All aspects of CISCO Routers and their configuration and includes TCP/IP.

- **Outlook.** Installation, administration, and maintenance of OUTLOOK to support collaborated integrated planning.
- **NT Exchange.** Installation, administration, and maintenance of NT Exchange to support collaborative integrated planning.

c. Command and Control Personal Computer

- **Training Audience.** Watch officers, section chiefs, and planners.
- **Description of Class.** This class is presented twice during the MTT. It is an introduction to the use of C2PC software and includes practical application. The training is designed to provide the students with the basic skills required to support planning and execution of operational requirements.

d. Track Management

- **Training Audience.** Tactical combat operations system operators and intelligence analysis system operators.
- **Description of Class.** This class provides advanced instruction on the skills required to maintain location and disposition of friendly and threat ground, air and maritime units within the designated battlespace. Instruction will concentrate on the use of GCCS (CHART), tactical combat operations system, intelligence analysis system, and C2PC to support unit disposition and location.

e. Information Management Officer

- **Training Audience.** Unit IMOs.
- **Description of Class.** This is an interactive discussion of the role and responsibilities of the information management officer to support effective and efficient procedures for the integrated use of systems and personnel to support decisionmaking. Throughout the week, the information management officers will develop an information management plan that will support the final guided scenario and be used as a start point to develop procedures to support the command information management plan.

f. Collaborative (Integrated) Planning

- **Training Audience.** Planners, staff, watch officers, section chiefs, IMOs, and planners.
- **Description of Class.** A demonstration of a collaborative integrated planning system using current systems, applications, and tools designed to support all four aspects of decision making; planning, decision, execution, and assessment. The procedures outlined in this class are only “techniques” that use current C4I technologies to support the MCPP in a shared collaborative environment.

g. Final Guided Scenario (Practical Application)

- **Description of Class.** An exercise to demonstrate why it is imperative to have the proper equipment, procedures, personnel, and training to support operational requirements through the integrated use of C4I. Terminal equipment, operators, watch officers, and staff will replicate a COC, all-source fusion center, and OPT at the MEF level. The major subordinate commands will provide personnel to support the wing, division, and FSSG functions, and MSTP will provide personnel to act as the MEF higher headquarters. Due to limited space and time, a small cadre of personnel and equipment will role-play their organic functions, replicating all organizations listed above. Using a guided scenario, information will be passed in a shared collaborative environment to highlight the importance of the skills taught during the MTT.

D-2. Additional Mobile Training Team Classes

The following classes stress the use of warfighting functions in an integrated manner—

- Command and Control: The Process.
- Common Tactical Picture Overview.
- Common Tactical Picture Refresher.
- Command and Control Personal Computer Training.
- Track Management.

This page intentionally left blank.

Appendix E

Information Management in an Exercise Environment

Although the focus of this publication has been on support to operations, the IM tools and procedures can easily be adapted to support exercises as well. This appendix concentrates specifically on exercises and provides some IM tools that are tailed to exercise support.

E-1. Real Time to Game Time Matrix

Conducting operations in multiple time zones can be confusing. In computer-driven exercises, the potential for confusion is increased by the requirements of game time. The following matrix can be used to describe the relationship between game time, real time, and ZULU time for an exercise.

Time Conversion Matrix for MEFEX 00-1						
MEF Local Time		ZULU Time		Game Time		Remarks
DDMMYY	0800	DDMMYY	1500	DDMMYY	0800	STARTEX
	1200		1900		1200	
	1900	DDMMYY	0200		1900	End of Work Day
	2400		0700			
DDMMYY	0800		1500		1900	Start of Work Day
	1200		1900		2300	
	1900	DDMMYY	0200	DDMMYY	0600	End of Work Day
	2400		0700			
DDMMYY	0800	DDMMYY	1500	DDMMYY	0600	Start of Work Day
	1200		1900		1000	
	1900	DDMMYY	0200		1700	End of Work Day
	2400		0700			
DDMMYY	0800		1500		1700	Start of Work Day
	1200		1900		2100	
	1900	DDMMYY	0200	DDMMYY	0400	End of Work Day
	2400		0700			
DDMMYY	0800		1500		0400	Start of Work Day
	1200		1900		0800	
	1900	DDMMYY	0200		1500	End of Work Day
	2400		0700			
DDMMYY	0800		1500		1500	Start of Work Day
	1300		2000		2000	ENDEX

Table E-1. Real time to game time matrix.

E-2. Exercise Design

Most computer-driven exercises use response cells to simulate the activities of command elements without the personnel and logistics burdens of actually fielding the command element. To accommodate the use of response cells, the flow of information must be clearly defined and understood by all. As an example, figure E-1 and the discussion

below describe how information will flow in an MSTP MEF-level exercise. Similar procedures should be developed prior to every exercise.

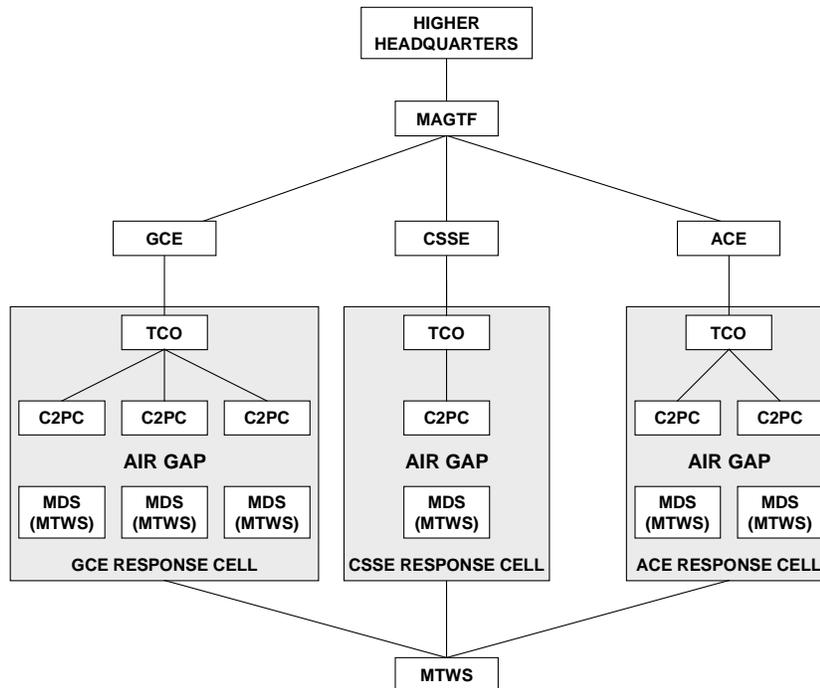


Figure E-1. Configuration to support an exercise.

a. Blue Force Information

Prior to and during the exercise, every effort will be made to make the model as transparent as possible to the exercise players. Response Cell personnel will receive ground truth model data via a Marine Tactical Wargame System (MTWS) Display System (MDS) that will be located in their response cell. The MDS filters information specifically focused to support the organization/units being simulated by the gamers in each response cell. Each MDS filters data into information (standard military reports) that are required by the players to satisfy training/learning objectives. To replicate specific real world conditions, MTWS will be used to generate subordinate Blue Force position reports for each major subordinate command supporting the MEF. This blue force data will be sent to each MDS located in each response cell. Players in each response cell will be responsible for sending unit location reports to each major subordinate command. Players will use C2PC that is connected to a tactical combat operations system. The tactical combat operations system will automatically send unit reports to each major subordinate command CTP manager. Each major subordinate command CTP manager will then filter the reports and send them up to the MEF CTP manager. The CTP manager will broadcast the reports out to all major subordinate commands and higher headquarters according to the common tactical picture (track management) procedures contained in Tab E to Appendix 4 of the IMP.

b. Threat Force Information

Threat data will be provided to the appropriate intelligence staff section per the procedures described by the reports matrix. Raw data produced by MTWS and scripted information provided by the intelligence coordination cell will be provided to the MEF and major subordinate command intelligence staff sections based upon their organic intelligence collection plan, surveillance and reconnaissance plan, and formal requests for information submitted by the staff.

c. Voice Communication

Interactive White Board and secure telephone requirements will be clearly defined at the initial planning conference. Internal and external telephone requirements will be defined based on user/functional needs. Normally MSTP will work closely with the supported unit to determine/establish an internal telephone network at the supported unit and at the distant/remote location. An exercise phone directory will be developed and published before start of the exercise.

d. Exercise Control (White Cell)

A White Cell performs the functions of external elements answering questions that ensure the supported unit meets all training/learning objectives. The White Cell influences information flow to support training/learning objectives. Through responses and reports generated by the White Cell, the Director, MSTP can influence actions that enable the supported unit to successfully achieve stated training objectives. Information provided by the White Cell should be listed in the reports matrix and be supported by the equipment, procedures, and communication described by the exercise design.

e. Higher Headquarters

This organization allows the Director, MSTP to influence exercise play. By utilizing the capabilities described in this section, higher and adjacent headquarters can interface with the MEF to keep the exercise on game path, thereby attaining the MEF's exercise objectives. This interface will be primarily by messages, secure voice, and reports required from the MEF, with video teleconferencing (VTC) used as necessary to highlight key points. Every member of the higher and adjacent headquarters will be familiar with capabilities used by the MEF to exchange required information. Refer to the DBRM for a sample of the reports that will be required to support one game day. Refer to the exercise control plan for a detailed explanation of the higher and adjacent headquarters. Personnel performing this job function will normally require training on the capabilities used to support the following functions:

- E-mail functions.
- Equipment used to generate required reports.
- Equipment used to develop required overlays.
- Equipment used to maintain a common tactical picture.
- Equipment used to de-conflict information.
- Equipment used to generate an air tasking order.
- Equipment used to support battle damage assessment.

f. Opposing Forces

Personnel performing the role of the opposing force provide realistic threat actions to counter the supported unit. Members of the opposing force (OPFOR) provide realistic enemy actions via the model. These individuals are in constant communication through various capabilities such as VTC, secure telephone, the NIPRNET or SIPRNET to ensure training/learning objectives are satisfied. They adjust their actions based on the guidance provided by exercise control (EXCON). EXCON ensures the supported unit stays on the projected game path, based on the results of the MAPEX and a close review of actions required to meet the stated training/learning objectives. All personnel from OPFOR receive required training prior to startex.

g. Video Teleconferencing

VTCs will be scheduled in accordance with the priorities established by EXCON. VTC will be available to support the entire CPX.

h. WEB Site

Higher and adjacent headquarters will establish an exercise home page on the SIPRNET. A member of the higher and adjacent headquarters, assigned by the OIC, Higher and Adjacent headquarters, will administer these pages. MSTP personnel will provide higher and adjacent headquarters personnel initial assistance in the development of an exercise homepage if required.

i. Internet

EXCON and the designated MEF exercise representative will exchange information concerning the initial planning conference as soon as practical. Then immediately after the initial planning conference, information concerning the exercise will be exchanged via the Internet. The SIPRNET will be utilized to support this exercise. It is imperative that exercise role players/participants are identified and given SIPRNET access (e-mail accounts). The C2S branch networking officer will coordinate the assignment of access. All Marine Corps Reserve participants will receive exercise billet accounts and will not be granted individual accounts.

Appendix F
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*.

C2	command and control
C2PC	command and control personal computer
C2S	command and control support
CBAE	commander's battlespace area evaluation
CCIR	commander's critical information requirement
CIC	Combat Intelligence Center
CNDA	computer network defense augmentation
CNDP	computer network defense picture
CNMP	common network management picture
COA	course of action
COC	combat operations center
COP	common operational picture
CTD	common tactical dataset
CTP	common tactical picture
DIO	defense information officer
DP	decision point
DSM	decision support matrix
DST	decision support template
EXCON	exercise control
FDP&E	force deployment planning and execution
GCCS	Global Command and Control System
IAP	information assurance picture
IM	information management
IMO	information management officer
IMP	information management plan
IOW	intelligence operations workstation
IP	internet protocol
IPB	intelligence preparation of the battlespace

ISSO	information systems security officer
JTF	joint task force
JWICS	Joint Worldwide Intelligence Communications System
MAGTF	Marine air-ground task force
MCDP	Marine Corps doctrinal publication
MCPP	Marine Corps Planning Process
MCWP	Marine Corps warfighting publication
MDS	MTWS display system
MEF	Marine expeditionary force
MOE	measure of effectiveness
MTT	mobile training team
MTWS	Marine Tactical Wargame System
NAI	named area of interest
NIPRNET	nonsecure internet protocol router network
OPFOR	opposing force
RFI	request for information
SCI	sensitive compartmented information
SIPRNET	SECRET Internet Protocol Router Network
SOP	standing operating procedures
SSO	special security officer
TAI	target area of interest
TTP	tactics, techniques, and procedures
VTC	video teleconferencing

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 military 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*.

C

commander's critical information requirements—A comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decision making process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements. Also called **CCIR**. (Joint Pub 1-02)

common operational picture—The common operational picture is the integrated capability to receive, correlate, and display a common tactical picture (CTP), including planning applications and theater-generated overlays/projections (i.e., Meteorological and Oceanographic (METOC), battleplans, force position projections). Overlays and projections may include location of friendly, hostile, and neutral units, assets, and reference points. The COP may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, any geographically oriented data, planning data from JOPEs, readiness data from SORTS, intelligence (including imagery overlays), reconnaissance data from the Global Reconnaissance Information System (GRIS), weather from METOC, predictions of nuclear, biological, and chemical (NBC) fallout, and air tasking order (ATO) data. (CJCSI 3151.01)

common tactical dataset—The common tactical dataset (CTD) is a repository of data that contains all the information available to the JTF that will be used to build the COP and CTP. The CTD is not fused, correlated, or processed data in the sense that the information has not been scrutinized by the CCM or track managers for time value, redundancy, or conflicts. However, the CTD may contain processed intelligence data. The CTD is a major sub-component of the COP and refers to: the CINC designated repository for current battlespace information including disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war for the entire area of responsibility (AOR). Upon discretion of the CINC, the CTD may be a logical database vice physical if there are several JTFs or activities that will necessitate COP reporting. In these cases there may be more than one location of database storage. (CJCSI 3151.01)

common tactical picture—The common tactical picture (CTP) is derived from the CTD and other sources and refers to the current depiction of the battlespace for a single operation within a CINC's AOR including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war. The CTP includes force location, real time and non-real-time sensor information, and amplifying information such as METOC, SORTS, and JOPEs. (CJCSI 3151.01)

I

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 assurance—Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called **IA**. (Joint Pub 1-02)

information-base processes—Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, comprise a larger system or systems of processes. (Joint Pub 1-02)

information environment—The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (Joint Pub 1-02)

information filter—Accessing the value of information and culling out that which is not pertinent or important. (MCPR 6-23A.)

information flow—Term used to describe movement of information. (MCPR 6-23A.)

information fusion—The logical blending and integration of information from multiple sources into an accurate, concise, and complete summary. (MCPR 6-23A.)

information management—The processes by which information is obtained, manipulated, directed, and controlled. IM includes all processes involved in the creation, collection and control, dissemination, storage and retrieval, protection, and destruction of information. (MCPR 6-23A.)

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 security—Information security is the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called **INFOSEC**. (Joint Pub 1-02.)

information superiority— The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Joint Pub 1-02)

information system—The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (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 confirm or deny a particular enemy course of action. Also called **NAI**. (MCRP 5-12C)

R

request for information—1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. Also called **RFI**. (Joint Pub 1-02)

S

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)

Appendix G

References

1. Joint Publications

Joint Pub 0-2	Unified Action Armed Forces (UNAAF)
Joint Pub 1-02	Department of Defense Dictionary of Military and Associated Terms
Joint Pub 3-0	Doctrine for Joint Operations
Joint Pub 6-0	Doctrine for C4 Systems Support to Joint Operations
Joint Pub 6-02	Joint Doctrine for Employment of Operational/Tactical C4 Systems

2. Marine Corps Publications

MCDP 1	Warfighting
MCDP 1-1	Strategy
MCDP 1-2	Campaigning
MCDP 1-3	Tactics
MCDP 4	Logistics
MCDP 5	Planning
MCDP 6	Command and Control
MCWP 0-1	Marine Corps Operations
MCWP 5-1	Marine Corps Planning Process
MCRP 6-23A	Multi-Service Procedures for Joint Task Force - Information Management