
MAGTF Communications System



US Marine Corps

DISTRIBUTION STATEMENT C: Distribution authorized to US Government agencies and their contractors.



USMC

PCN 143 000042 00

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in Marine Corps Order 3900.15_, *Marine Corps Expeditionary Force Development System*, which can be obtained from the Marine Corps Publications Electronic Library Online (<http://www.marines.mil/news/publications/Pages/Publications137.aspx>).

The UNS recommendation should include the following information:

- Location of change
 - Publication number and title
 - Current page number
 - Paragraph number (if applicable)
 - Line number
 - Figure or table number (if applicable)
- Nature of change
 - Addition/deletion of text
 - Proposed new text

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the MCCDC Doctrine World Wide Web home page: <https://www.doctrine.usmc.mil>.

**Unless otherwise stated, whenever the masculine gender is used,
both men and women are included.**

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

8 January 2010

FOREWORD

Marine Corps Warfighting Publication (MCWP) 3-40.3, *MAGTF Communications System*, presents doctrine, tactics, techniques, and procedures (TTP) for the employment of the communications system to support Marine air-ground task force (MAGTF) command and control. It builds on the philosophy in Marine Corps Doctrinal Publication 6, *Command and Control*, and links that philosophy to the detailed TTP in MCWP 3-40.1, *MAGTF Command and Control*, and MCWP 3-40.2, *Information Management*.

MCWP 3-40.3 is written for all MAGTF commanders, staff officers, and Marines who support command and control.

This publication supersedes MCWP 6-22, *Communications and Information Systems*, dated 16 November 1998.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS



GEORGE J. FLYNN

Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration
Marine Corps Combat Development Command

Publication Control Number: 143 000042 00

DISTRIBUTION STATEMENT C: Distribution authorized to US Government agencies and their contractors. Other requests for this document will be referred to Marine Corps Combat Development Directorate, Command and Control Integration Division.

MAGTF COMMUNICATIONS SYSTEM

TABLE OF CONTENTS

Chapter 1. Command and Control and the Marine Air-Ground Task Force Communications System

Command and Control Environment	1-1
Information Management	1-2
MAGTF Communications System Characteristics	1-6
MAGTF Communications System Responsibilities.	1-7

Chapter 2. Organizations

Section I. Marine Corps Organizations	2-1
Operating Forces.	2-1
Marine Corps Forces	2-1
Marine Air-Ground Task Forces	2-2
Marine Corps Forces Reserve.	2-4
Marine Special Operations Command	2-4
The Supporting Establishment	2-5
Section II. MAGTF Communications System Organizations	2-6
Communications Battalion	2-6
Marine Wing Communications Squadron	2-8
Communications Company, Headquarters Battalion, Marine Division	2-9
Communications Company, Combat Logistics Regiment, Marine Logistics Group	2-9
Communications Platoons, Branches, and Sections.	2-10
Special Security Communications Teams	2-10
Amphibious Communications Teams	2-11
Section III. Command and Control Organizations	2-12
Marine Expeditionary Force Command Element.	2-12
Ground Combat Element	2-14
Aviation Combat Element	2-14
Logistics Combat Element	2-17
Intelligence Command and Control	2-18
Fire Support Centers.	2-19
Rear Area Operations Centers	2-19
MAGTF Communications System Control	2-20
Amphibious Command and Control Facilities	2-22
Mobile Command Posts	2-24

Chapter 3. Global Information Grid

Components	3-1
Planning	3-4
Access Services.....	3-4
Voice Services.....	3-5
Data Services.....	3-5
Applications	3-6
Video Services	3-7
Satellite Communications Services.....	3-7
Manangement of the Global Information Grid.....	3-11
Electromagnetic Spectrum Management	3-14

Chapter 4. MAGTF C2

What is MAGTF C2?	4-1
MAGTF C2 Capabilities.....	4-3

Chapter 5. MAGTF Communications Network

Communication and the Electromagnetic Spectrum.....	5-1
Elements of a MAGTF Communications Network	5-9

Chapter 6. Communications Planning

Planning for a Dynamic Network.....	6-1
Marine Corps Planning Process	6-3
Communications Control	6-4
Commander's Intent	6-6
Center of Gravity Analysis	6-6
Commander's Critical Information Requirement.....	6-6
Communications Control Agencies	6-8

Chapter 7. Information Systems Security

Section I. Communications Security.....	7-1
Responsibilities.....	7-2
Cryptosecurity.....	7-3
Transmission Security.....	7-3
Emission Security	7-4
Physical Security.....	7-4
Section II. Computer Security.....	7-6
Threat to Computer Security.....	7-6
Protection	7-7
Section III. Incident Response	7-10
Marine Corps Network Operations and Security Command and Expeditionary Support Center	7-10
Naval Network Warfare Command	7-10

Appendices:

A	MAGTF Single-Channel Radio Nets	A-1
B	Communications Symbology and Diagrams	B-1
C	Transmission System Link Designator Numbering	C-1
D	Command Communications Service Designator	D-1
E	Communications Planning Checklist	E-1
F	Sample Annex K.	F-1
G	Information Systems Directory	G-1
H	Example of a Guard Chart	H-1

Glossary

References

CHAPTER 1

COMMAND AND CONTROL AND THE MARINE AIR-GROUND TASK FORCE COMMUNICATIONS SYSTEM

This publication, Marine Corps Warfighting Publication (MCWP) 3-40.3, *MAGTF Communications System*, outlines the responsibilities of the MAGTF communications system (MCS) personnel and users to ensure that those systems provide effective command and control (C2) support. This publication is written, to the extent possible, in nontechnical language; however, chapters 3, 4, and 5 contain many communications system and networking terms that may be unfamiliar to most Marines. These terms are defined in the glossary.

The MCWP 3-40.3 focuses on the communications system used to support the Marine air-ground task force (MAGTF) in the operational environment. It addresses the MCS's employment to support the Marine Corps component headquarters (HQ). This publication also discusses how the Marine Corps establishes command relationships and organizes to provide communications system support to the MAGTF. It describes the information systems and services that support command and control and the employment of communications systems and networks to link these information systems.

This publication emphasizes the impact of the rapidly evolving joint C2 environment of the MCS. It identifies approved doctrine for communications system support of joint operations and outlines the responsibilities of the Marine Corps to ensure effective communications support to commanders. It addresses how communications systems support the conduct of joint operations, including how systems are to be configured, deployed, and employed. Finally, this publication provides the guidance necessary to plan, manage, employ, and execute communications system support at the MAGTF operational and tactical levels.

Command and Control Environment

The C2 environment is characterized by rapid change and continuous challenge. Implementation of maneuver warfare doctrine, with its emphasis on speed and tempo, demands compressed planning, decisionmaking, execution, and assessment cycles. At the same time, the volume of information that needs to be processed and analyzed to support decisionmaking is ever increasing and threatens to overwhelm commanders and staffs. The MAGTF must employ limited communications system resources to meet these challenges. To help satisfy the operational requirement, the Marine Corps is changing its manpower structure, its education and training processes, and its doctrine through the combat development process.

Developments in the joint C2 arena are another significant factor in the C2 environment. The Department of Defense (DOD) is significantly enhancing the C2 capabilities of the armed forces by rapid exploitation of advanced information technologies and significant improvements in interoperability. The objective of the joint communications system is to assist the joint force commander (JFC) in the command and control of military operations. Effective command and control is vital for proper integration and employment of operational capabilities. The communications system supporting the JFC is the Global Information Grid (GIG). The GIG includes all joint and Service communications systems, and interfaces with non-DOD and multinational users.

One of the most difficult C2 issues the Marine Corps now faces is the requirement to support a deployable Marine Corps component HQ with MCS personnel and equipment. The primary source of support is the communications battalion (COMM BN). The requirement to provide support to a deployed Marine Corps component HQ can have a significant effect on the availability of MCS resources to support the MAGTF.

The MCS must be able to satisfy the C2 requirements of the expeditionary battlefield. It must provide MAGTF commanders and their staffs with the tools necessary to collect, process, analyze, and exchange information rapidly in support of operations planning and execution. These systems must make the necessary information available when and where it is needed on the battlefield. Employment of these systems must not adversely affect the MAGTF's freedom of action and mobility, and they must be reliable, flexible, responsive, and configurable to mission needs. The success of the MAGTF on the modern battlefield depends on designing, planning, and employing a communications system that satisfies the information needs of the MAGTF process.

Information Management

Much of the information obtained for any endeavor or purpose is incomplete. This is especially true in a battle of wills between opposing forces in military or political conflicts in which each side seeks to deceive the other with false information. The commander cannot, therefore, be certain that the information obtained depicts the situation with absolute certainty, only that it provides an approximation of reality.

Generally, the level of accuracy of the commander's estimate of reality can be increased with more time to collect and analyze additional

information. However, reality also changes with time because of enemy and friendly actions and the environment. These changes then introduce additional information that requires processing and analysis. At some point, the commander must make decisions based on the best information available. Although the MCS provides useful tools, the application of sound information management principles is required to satisfy the commander's information requirements. Information management principles address information relevance, timeliness, accuracy, completeness, objectivity, and usability.

Information Defined

In this publication, the term **information** refers to all information that is needed to support the decisionmaking process on the battlefield—that information required to execute the planning, decision, execution, and assessment cycles in combat. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, provides two definitions for information: (1) facts, data, or instructions in any medium or form, and (2) the meaning that a human assigns to data by means of the known conventions used in their representation.

It is important to understand that information, in its broadest sense, includes everything from raw data such as a radar signal or a suspected enemy sighting by an observation post, to data that has been extensively processed to be meaningful to a decisionmaker. Ultimately, study and analysis of information lead to an understanding of the situation—a situational awareness. Naval Doctrine Publication 6, *Naval Command and Control*, and Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*, describe a 4-step cognitive process by which the transformation from raw data to situational awareness takes place (see fig. 1-1). These four steps may be viewed as defining an information hierarchy.

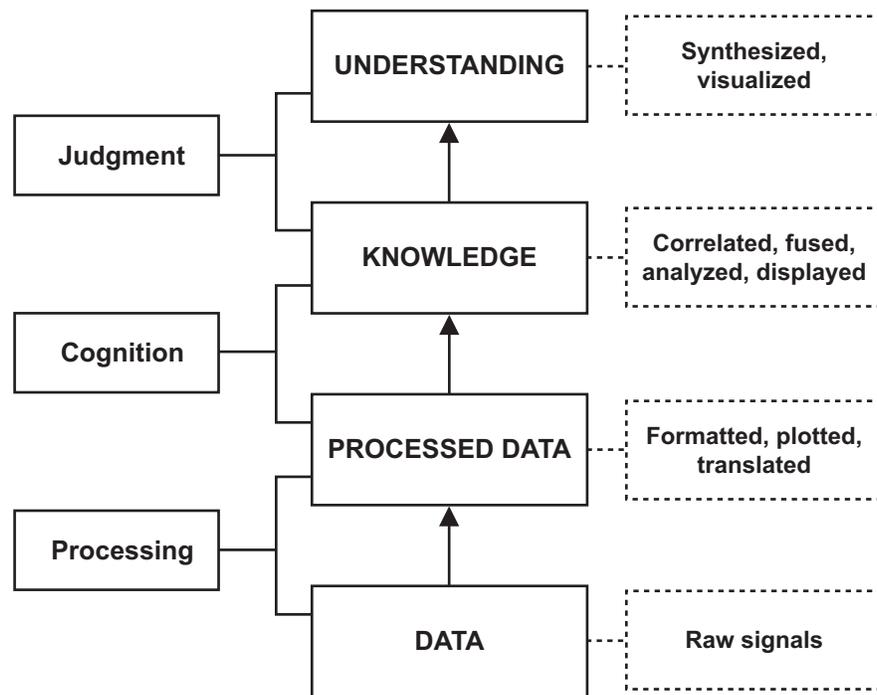


Figure 1-1. Information Hierarchy.

Data

The first step in the cognitive process is to collect raw data. The raw data can take many forms: radar signals, intercepted radio signals, meteorological data from a weather balloon, or even bar-coded logistic data scanned from the side of a container. This data may be transmitted by telephone, radio, or facsimile; transferred between computers over local area networks (LANs); or sent by messenger as rolls of undeveloped film or digital media. Regardless, to be useful, this raw data must be processed into a form that can be understood by the end user.

Processed Data

The second step, processing data, involves a wide range of functions, such as decoding and translating intercepted communication, filtering and correlating sensor returns, and developing film. Processing is putting information into a readily interpretable form, such as a graphical display or

a formatted message. Some information will come to the MAGTF in processed form and will not require further processing. Once data has been processed, it is referred to as information in the cognitive process. At this point, some information may have immediate value for Marines in close contact with the enemy. Such information is known as combat information. It is usually extremely perishable and should be disseminated to units needing it as rapidly as possible.

Knowledge

In the third step, information is analyzed and evaluated to produce knowledge. For example, the analysis of intelligence information helps build a picture of the enemy situation.

Understanding

The fourth and last step in the process is developing an understanding of the situation based on the information available. Understanding is the result

of applying human judgment based on individual experience, expertise, and intuition to gain a full appreciation of the battlefield. This understanding is situational awareness and provides a sound basis for operational decisions. It allows the commander to anticipate events and to uncover critical vulnerabilities for exploitation. As the commander strives to gain an understanding of the situation, however, he must recognize that time is working against him. He may not be able to gain complete situational awareness before he has to act. Developing situational awareness with limited and uncertain information under severe time constraints is the fundamental C2 challenge.

Information Quality

Information quality and availability have a direct effect on the commander's capability to effectively command and control forces. Good information reduces confusion and contributes to situational awareness. It is essential to plan, monitor, and influence operations effectively. Information quality cannot be taken for granted and must be assessed with care.

The following paragraphs identify criteria for determining information quality, they are neither exhaustive, of equal importance, nor are they independent of each other. It is counterproductive to seek complete information if the search for completeness makes the information untimely. Irrelevant information is worse than none and false information can be disastrous, especially if it is part of an enemy deception.

Relevance

Information must apply to the mission, task, or situation. Exhaustive, unfiltered information often detracts from the commander's ability to make timely, effective decisions. Furthermore, the transmission and processing of exhaustive information burdens the MCS unnecessarily.

Timeliness

Information must be available at the appropriate place and time to be useful. Information management procedures and techniques must ensure the following: the timely, unimpeded flow of relevant information; a well-planned and implemented communications system; clearly identified information requirements; effective collection, reporting, and dissemination; and decisiveness by commanders and their staffs.

Accuracy

Information must be as accurate as possible. Although information systems can collect, transport, process, disseminate, and display information, Marines must still evaluate the information and decide whether it is accurate, timely, and relevant.

Completeness

Information about a situation may be useful only when it is complete; however, by the time complete information is obtained, it may no longer be timely. If subordinates are aware of the commander's intent and critical information requirements, they can provide only those information fragments needed for situational awareness.

Objectivity

Information must be provided in the most undistorted, factual, and unbiased way possible. Any interpretation should be highlighted.

Usability

The display or presentation of information to the user must be understandable and useful. Standard, clearly understandable information formats, symbols, and terms should be used to exchange information and present it to users. Information exchanged and presented in non-standard forms causes delays in interpretation and is easier to misunderstand, leading to longer decision and execution cycles and, ultimately, to less reliable decisions.

Types of Information and the Commander's Critical Information Requirement

The information required for situational awareness falls into three general categories: information about the enemy, information about the environment, and information about friendly forces. The identification of the commander's critical information requirement (CCIR) is a way to focus and direct the collection and processing of information into those categories. The CCIR is the information regarding the enemy, friendly activities, and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Designation of the CCIR reduces the volume of information to a manageable level and helps to ensure the accuracy, relevance, and timeliness of that information. The CCIR consists of priority intelligence requirements (PIRs), friendly force information requirements (FFIRs), and essential elements of friendly information (EEFI). Clearly defining these information requirements is one of the most difficult and important tasks of command. The CCIR will not only govern the quantity and quality of the information available to support decisionmaking, but also will have a direct effect on the workload of the staff and subordinate units.

PIR

The PIRs are associated with a decision that will affect the overall success of the command's mission. They include information about the enemy and the environment. Information about enemy capabilities and intentions is critical for commanders to anticipate and analyze possible enemy courses of action (COAs). Information on the environment includes reports on the weather, the terrain, the local population, the local communications and transportation infrastructures, and a host of other factors that may affect the conduct of military operations. Through identification of PIRs, commanders ensure they direct limited intelligence resources to obtaining intelligence information essential for decisionmaking.

FFIR

To complete the picture of the situation, the commander requires information on friendly forces. The FFIRs are the pieces of information about friendly forces the commander needs to be able to develop plans and make effective decisions. Depending on the circumstances, any information acquired on unit location, composition, readiness, personnel status, and logistic status could become FFIRs. Just as it is essential for the commander to use PIRs to identify the most important requirements for information on the enemy, it is also necessary that the commander specify what critical friendly force information is required to support planning and execution. The commander must have real-time or near real-time information on the location, status, and capabilities of friendly forces; however, he must prioritize FFIRs to limit and focus the collection and processing effort. It is easy to overburden subordinate units and to overload communications networks with requests for nonessential information. The FFIRs help commanders, staffs, and subordinate units understand precisely what information is needed to support the planning, decision, execution, and assessment cycles.

EEFI

The EEFI are specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. These EEFI may be viewed as representing the opposing commander's PIR. Identification of the EEFI is vital to planning effective information security (INFOSEC), operations security (OPSEC), and other force protection operations.

Flow of Information

The goal of information management is to facilitate a rapid, unconstrained flow of information throughout an organization from its source, through intermediate collection and processing nodes, to its delivery to the end user. The CCIR serves as a necessary filter to ensure that only

relevant information is delivered to prevent information overload. Information must flow in all directions to support a common operational picture of the battlefield among all units senior, subordinate, adjacent, supporting, and supported. A flexible, responsive C2 architecture is required that pushes relevant, time-sensitive information to the user while allowing the user to pull additional detail as required. This C2 architecture consists of the C2 facilities, information systems, and communications networks that are described in chapters 2, 3, 4, and 5.

A number of information-sharing techniques are widely used to improve the flow of information, both within and among Marine Corps organizations. These techniques support improved situational awareness and collaborative planning. Networking also offers tremendous opportunities for electronic reachback. The concept of electronic reachback may reduce the size of deployed staffs through the use of specialists, the military, Government civilians, or consultants located in garrison.

The most widely used information-sharing technique is electronic mail (e-mail), which provides a convenient way to exchange information between organizations and individuals. It is a highly effective means of communication, supporting rapid dissemination of time-critical information between HQ and subordinate organizations and across staff sections. E-mail permits a single user to disseminate information to one or several users simultaneously; however, in a deployed environment, the potential to overload the communications system requires a disciplined approach to the establishment and use of e-mail accounts.

Other networking techniques, such as using Web pages or shared network drives on a LAN, support the concept of information pull and have the potential to reduce the load on the communications network to improve information flow. These techniques, however, are no guarantee of receipt by the intended audience.

Pull techniques are generally unacceptable for the promulgation of time-sensitive, critical information such as fragmentary orders (FRAGO) or warning orders. Although brief messages could be sent indicating that the order had been posted and requiring addressees to acknowledge and comply, the order normally would not have been lengthy enough to make this an efficient approach. On the other hand, when selective access to information in large databases is required to support an analysis, pull techniques are more efficient than push techniques.

MAGTF Communications System Characteristics

It would be impossible to provide adequate C2 support on the modern battlefield without the MCS. This publication defines the MCS as any system that primarily functions to collect, process, or exchange information. The MCS should be reliable, secure, timely, flexible, interoperable, and survivable.

Reliability

The MCS should be available when needed and perform as intended with low failure rates and few errors. Reliability is also attained by standardizing equipment and procedures and by building necessary electronic jamming and deception. Systems should perform reliably on board ships and aircraft, in garrison, and in austere field environments.

Security

The MCS should provide security commensurate with the user's requirements and with the vulnerability of the transmission media to interception and exploitation. Security is achieved by using appropriate protection and cryptographic systems and transmission security techniques. It is also achieved by educating and training personnel in operational, management, and technical security procedures.

Timeliness

The MCS should process and transfer information among decisionmakers rapidly enough to maintain a high tempo of operations. It should ensure that our decision and execution cycles remain ahead of any potential adversary's.

Flexibility

The MCS should be capable of being reconfigured quickly to respond to a rapidly changing environment. Flexibility can be obtained through system design or by using commercial facilities, mobile or transportable systems, or prepositioned facilities.

Interoperability

The MCS should enable information to be exchanged among all of the commanders and forces involved in an operation. The MCS also should possess the interoperability required to ensure information exchange in joint and multinational operations and in operations with other government agencies.

Survivability

In the context of communications, survivability refers to the measures taken to prevent disruption of the MCS by enemy interference or natural disaster. Survivability can be enhanced by the dispersal and protection of key nodes, physical and electromagnetic hardening, and redundancy of communication paths and information processing nodes.

MAGTF Communications System Responsibilities

The communications officer, officer MOS [military occupational specialty] 0602, is responsible for the MCS and responsibility for this functional area has been assigned to the communications officer (G-6/S-6). Since the technology associated with such systems and networks continues to

evolve, specific responsibilities continue to evolve as well. Already, it is clear that the responsibility for installing and operating information systems will be shared among MCS specialists and functional area users. For example, the command and control personal computer (C2PC) system will be operated by personnel from the operations office (G-3/S-3) who will be assisted by MCS personnel with its installation and interface with LAN and wide-area networks (WANs).

Just as important as the responsibility for installing, operating, and maintaining MCS is that of managing the information processed and exchanged by those systems. Each staff section will be responsible for the quality of the information in the databases of the systems that support that particular staff section. However, overall information management policies and procedures will be under the staff cognizance of the chief of staff (C/S) or the executive officer (XO).

Commander

The commander is responsible for the planning and employment of the MCS within the command, although the authority to plan and employ communications and information systems may be delegated. The commander must provide the G-6/S-6 adequate authority commensurate with the responsibilities expected or assigned, and adequate guidance, including necessary assumptions and constraints. The commander is also responsible for providing the focus for information management throughout the organization and participating directly in the information management process by establishing the CCIR discussed in this chapter.

Communications Officer

The communications officer is responsible to the commander for all matters concerning the planning and employment of MCS within the command. As a general or executive staff officer, the communications officer serves as an

advisor, planner, supervisor, and coordinator. Specific responsibilities include the following:

- Providing the commander and other staff officers with—
 - Advice on information management policies and procedures.
 - Estimates of the supportability of COA.
 - Estimates of requirements for MCS resources, including personnel, equipment, supplies, and facilities.
 - Recommendations for the allocation and use of MCS resources.
 - Recommendations for MCS training for the command.
 - Recommendations on the location, echelon, and displacement of the command post and C2 facilities.
 - Advice on operational aspects of information assurance (IA). (See chapter 7 for detailed G-6/S-6 responsibilities.)
- Preparing MCS plans, orders, and standing operating procedures (SOPs) to implement the commander's policies and decisions on MCS employment.
- Assisting the staff in the area of the MCS to prepare studies, estimates, plans, orders, instructions, and reports.
- Employing of MCS personnel.
- Installing, operating, and maintaining communications networks.
- Managing LAN and WAN, including Internet protocol (IP) address and routing management.
- Providing technical and system administration support for functional users in the installation, operation, and maintenance of information systems hardware and common user software.
- Providing communications systems training and, in coordination with functional users, information systems training.
- Supplying and maintaining the MCS.
- Complying with SOP and interoperability standards.
- Providing MCS security in coordination with the other staff sections.
- Coordinating MCS matters with related staff sections and with staffs of other units, as required.
- Establishing MCS liaison with senior, subordinate, adjacent, supported, and supporting units.

Unit Information Management Officer

The unit information management officer is a special staff officer operating under the staff cognizance of the C/S or XO. If an information management officer is not designated, then this duty is the responsibility of the C/S or XO. The information management officer is responsible for establishing the policy and procedures for information management within the command. Responsibilities include—

- Coordination, with the assistance of the information management officers of each staff section and subordinate units, of information management efforts throughout the organization.
- Development and publication of the information management plan. The information management plan establishes policies and procedures for ensuring the quality and flow of information within the organization.
- Coordination of the CCIR process: the nomination of the CCIR; approval of the CCIR by the commander and collection and reporting of the CCIR by the staff; dissemination of the CCIR to higher, adjacent, and subordinate commands; and maintenance of the CCIR.
- Development and implementation of effective information dissemination techniques in close coordination with the communications officer,

other staff principals, and the information management officers of subordinate units.

- Development of training programs on information management procedures.
- Coordination with the unit security manager in the development and implementation of INFOSEC procedures.
- Coordination with the communications officer on LAN management and networking issues, communications channels prioritization, and traffic management.

Staff Section Information Management Officer

Each staff section should appoint an information management officer. The staff section information management officer is responsible for—

- Coordinating the internal and external information flow for the staff section and its integration with the information flow of other staff sections, including identifying and prioritizing information management requirements.
- Providing the unit information management officer with input to the information management plan.
- Coordinating information management training for section personnel with the unit information officer.
- Coordinating the identification and processing of all CCIRs within the staff section's area of operations (AO).

Functional User Responsibilities

On the modern battlefield, it is essential that functional users of information be able to operate the information systems supporting their functional area. Such ability facilitates increased speed and operator knowledge in establishing a distributed network. It also ensures that functional area users are able to best exploit and control the capabilities

of systems that support their needs. Functional users include every staff section supported by the MCS. Consequently, all staff principals have functional user responsibilities for the functional areas over which they have staff cognizance. For example, the G-3/S-3 has functional user responsibilities for C2PC. Functional user responsibilities include—

- Identifying the primary point of contact (POC), both internal and external to the command, for issues affecting information systems that support the functional area.
- Serving as the configuration manager for information systems that support the functional area.
- Conducting routine information user administration, such as performing user data/file storage and management and conducting file backups.
- Coordinating with the G-6/S-6 to ensure that adequate hardware, software, trained personnel, and procedures are in place before implementing a new system or system modification.
- Coordinating with the G-6/S-6 to develop and maintain user training programs for the MCS.
- Identifying to the G-6/S-6 information system support requirements.
- Identifying to the G-6/S-6 specific communications requirements, including requirements to interface with other information systems and potential interface problems.
- Complying with applicable MCS security measures.
- Reporting malfunctions and outages and coordinating with the G-6/S-6 to restore service.

Communication Between Commands

The responsibility for establishing communication between units must be clearly delineated.

These responsibilities are a cornerstone of communications doctrine; however, when supporting combat operations, unit communications capabilities may be destroyed and responsibility may become unclear or irrelevant. Flexibility, common sense, initiative, cooperation, and mutual assistance must prevail in these instances. Communication responsibilities are as follows:

- Communication between a senior and subordinate unit is the responsibility of the senior commander.
- Communication between adjacent units is the responsibility of the first common senior commander.
- Communication between a supporting and supported unit is the responsibility of the supporting unit commander.

- Communication between a reinforcing and reinforced unit is the responsibility of the reinforcing unit commander.
- Communication between a unit and an attached unit is the responsibility of the commander of the unit to which the attachment is made.

G-6/S-6 Staff Cognizance and Technical Direction

Communications units and detachments operate under the staff cognizance and technical direction of the supported unit's G-6/S-6. The Marines assigned to these units, in concert with personnel assigned to G-6/S-6 sections and functional area users, are responsible for employing the MCS to support command and control. Accordingly, commanders should ensure that the staff principal G-6/S-6 have the authority commensurate with the responsibility assigned or expected.

CHAPTER 2

ORGANIZATIONS

SECTION I. MARINE CORPS ORGANIZATIONS

The MCS is employed to support the command and control of Marine forces. To understand the requirements for MCS support, it is necessary to understand the organization and mission of those forces. Marine forces are organized, trained, and equipped under a total force concept to conduct a wide range of expeditionary operations. The Marine Corps total force consists of three components: the operating forces, the Marine Reserve, and the supporting establishment. The operating forces are expeditionary forces-in-readiness, providing forward presence, crisis response, and rapid power projection capabilities to warfighting combatant commanders (CCDRs). The United States Marine Corps Forces Reserve (MARFORRES) is an integral part of the total force team. It continuously trains and operates with the active forces and is fully prepared to augment or reinforce them in times of crisis. The supporting establishment is responsible for recruiting, training, equipping, and sustaining the force, both active and reserve.

Operating Forces

The two major components of the operating forces are United States Marine Corps Forces Command (MARFORCOM) and United States Marine Corps Forces, Pacific (MARFORPAC), together constituting the expeditionary combat power of the Marine Corps. Other elements of the operating forces include the Marine Corps Security Forces at naval installations; United States Marine Corps Forces, Special Operations Command (MARSOC) at Camp Lejeune, NC; and the Marine Corps Embassy Security Command with

detachments at embassies and consulates. Consistent with doctrine in JP 1, *Doctrine for the Armed Forces of the United States*, each CCDR is assigned a Marine Corps Service component for the planning and execution of various operation plans (OPLANs). The MARFORCOM, headquartered in Norfolk, VA, is the Marine Corps Service component for the US Joint Forces Command, the US Southern Command, and the US European Command. The MARFORPAC, headquartered at Camp Smith, HI, is the Marine Corps Service component for the US Pacific Command and the Commander, United Nations Command/Combined Forces Command.

Marine Corps Forces

Marine Corps forces (MARFOR) is the designation given all Marine component commands. A Marine Corps component command consists of all MARFOR assigned to a joint force. There are two levels of Marine Corps components: those assigned to a CCDR or a subordinate unified commander and those assigned to a joint task force (JTF). A Marine Corps Service component may consist of one or more MAGTFs and other required theater-level organizations, such as a Marine logistics command (MLC). Normally, a JTF Marine Corps component will only include one MAGTF and no additional Marine Corps organizations. A MAGTF commander may be dually designated as the Marine Corps Service or JTF Marine Corps component commander.

Unless higher authority establishes otherwise, the Marine Corps component commander commands all assigned MARFOR and exercises operational

or tactical control over other assigned or attached forces. The Marine Corps component commander deals directly with the JFC in matters affecting assigned MARFOR. The Marine Corps component commander commands, trains, equips, and sustains all MARFOR. Combat operations are executed by assigned MAGTFs.

When designated by the joint commander, a Service or JTF Marine Corps component commander may also serve as a functional component commander. A functional component command normally comprises forces of two or more Military Departments that may be established to perform particular operational missions. Functional component commanders are normally selected from among Service component commanders who provide the preponderance of the functional capability in question.

A Service component commander who has been designated as a functional component commander retains Service component responsibilities. A Marine Corps component commander is more likely to be designated a functional component commander in smaller scale contingencies where MARFOR constitute a large portion of the joint force. The Marine Corps component commander could be designated as the joint force maritime component commander, joint force land component commander, or joint force air component commander.

MCWP 3-40.8, *Componency*, describes three possible staff organizations for the component HQ:

- One commander and one staff—A single commander is designated as both the Marine Corps component and MAGTF commander. Likewise, a single staff executes both component and MAGTF functions.
- One commander and two staffs—A single commander serves as both component and

MAGTF commander; however, the commander is supported by two separate staffs.

- Two commanders and two staffs—This organization provides for two separate commanders, each with a dedicated staff. Although this is the most effective arrangement, it is also the most costly in terms of personnel, equipment, and facilities.

Marine Air-Ground Task Forces

Marine Corps operating forces are further organized into MAGTFs. These MAGTFs are organized, equipped, and trained to conduct forward-presence and crisis-response missions anywhere in the world. They can conduct expeditionary operations across the full range of military operations, including forcible entry by amphibious assault, and are also capable of noncombat operations such as noncombatant evacuations and disaster relief. Because MAGTFs are task-organized, they differ in organization, but retain the same basic structure.

Core Elements

Each MAGTF has four core elements: a command element (CE), a ground combat element (GCE), an aviation combat element (ACE), and a logistics combat element (LCE). This structure is carefully designed to provide operational flexibility and coordinated execution, maximizing the contribution of each element to the overall mission.

CE

The CE is the MAGTF HQ. It is task-organized to provide the C2 capability necessary for the effective planning and execution of operations. The CE, with the HQ staff, includes units and detachments that provide the MAGTF with communications, information systems, and intelligence support.

GCE

The GCE is task-organized to conduct ground operations to support the MAGTF mission. It is formed around an infantry organization and reinforced with artillery, reconnaissance, armor, engineers, and other forces as needed. The GCE can vary in size and composition: as small as a reinforced infantry battalion or as large as one or more Marine divisions. During amphibious operations, it projects ground combat power ashore by using transport helicopters from the ACE, organic assault amphibious vehicles, and Navy landing craft.

ACE

The ACE is task-organized to perform all or part of the six functions of Marine aviation in support of MAGTF operations. The six functions of Marine aviation are: offensive air support, antiair warfare (AAW), electronic warfare (EW), assault support, control of aircraft and missiles, and reconnaissance. During amphibious operations, the ACE can vary in size and composition, from a reinforced aviation squadron or detachment with appropriate air command and control and logistics to one or more Marine aircraft wings (MAWs).

LCE

The LCE is task-organized to provide the full range of combat service support (CSS) capabilities necessary to support and sustain MAGTF operations. During amphibious operations, the LCE may vary in size and composition, from a task-organized CSS detachment to one or more Marine logistics groups (MLGs).

Types of MAGTFs

All MAGTFs are expeditionary forces that are task-organized for a specific mission and they vary greatly in size and composition according to the mission. Marine Corps doctrine categorizes MAGTFs into Marine expeditionary forces

(MEFs), Marine expeditionary brigades (MEBs), Marine expeditionary units (MEUs), and special purpose MAGTFs (SPMAGTFs).

MEFs

Most Marine Corps operating forces are assigned to the three standing MEFs (see table 2-1). These standing MEFs can deploy as a MEF that is normally in echelon. They may also deploy subordinate units task-organized for assigned missions. All three MEFs provide MEUs for service afloat.

Table 2-1. Standing Marine Expeditionary Forces.

	MARFORPAC	MARFORCOM
I MEF	III MEF	II MEF
Based in California	Forward based in Okinawa, mainland Japan, and Hawaii	Based in North and South Carolina

The MEF is the principal Marine Corps warfighting organization for larger crises or contingencies. Normally commanded by a lieutenant general, it is capable of a full range of military operations, including amphibious assault and sustained combat operations ashore. Consisting of a permanent CE, one Marine division, a MAW, and an MLG, each of the three standing MEFs forward deploys MEUs continuously. The size and composition of a deployed MEF can vary greatly, depending on the mission, from elements consisting of less than a full division, MAW, or MLG to elements consisting of more than a full division, MAW, or MLG. A MEF can deploy with forces attached from the other standing MEFs as well as from the Marine Reserve. With accompanying supplies for 60 days, MEFs are capable of both amphibious operations and sustainment ashore. With appropriate augmentation, especially in the area of C2 capability, the CE can perform the mission of a JTF HQ, with the MEF as its nucleus. The MCS requirements associated with such taskings are significant.

A MEF normally deploys in echelon and designates its lead element as the Marine expeditionary force (Forward) (MEF [Fwd]). The deployment of the MEF (Fwd) does not automatically trigger the deployment of the entire force. This would occur only if the crisis is large enough to require the entire MEF.

MEBs

The MEB normally consists of a reinforced infantry regiment, a combat logistics regiment (CLR), a composite Marine aircraft group (MAG), and a CE. A MEB, commanded by a general officer, is task-organized to meet the requirements of a specific situation. It can function as part of a JTF, as the lead echelon of the MEF, or alone. It varies in size and composition, but is larger than a MEU and smaller than a MEF. The MEB is capable of conducting missions across the full range of military operations.

MEUs

The MEU is normally composed of a reinforced infantry battalion; a reinforced helicopter squadron, which may include vertical/short takeoff and landing attack aircraft; a MEU combat logistics battalion (CLB); and a CE. The MEU is commanded by a colonel and deploys with supplies for 15 days. The MARFORCOM and MARFOR-PAC routinely forward deploy MEUs on board amphibious ships in the Mediterranean Sea, Indian Ocean, Persian Gulf, and Western Pacific. When deployed as part of an expeditionary strike group (ESG), the MEU provides a combatant or operational commander with a sea-based, rapid-reaction force for a wide variety of missions. The MEU has a limited forcible entry capability and can facilitate the employment of follow-on forces, including joint and combined forces as well as a MEF.

SPMAGTFs

A SPMAGTF may be formed to conduct a specific mission that is limited in scope, focus, and, often, duration. It may be any size, normally the

size of a MEU or smaller, with narrowly focused capabilities chosen to accomplish a limited mission. Common missions include raids, peacekeeping, noncombatant evacuation, disaster relief, and foreign humanitarian assistance.

Marine Corps Forces Reserve

Rapid force expansion is possible through the activation of the MARFORRES. The Marine Reserve, like the active forces, consists of a balanced combined-arms team with ground, aviation, and logistic units. Organized under the Commander, MARFORRES, units are located at 185 training centers in 48 states, Puerto Rico, and the District of Columbia. The MARFORRES is closely integrated with the active component under the Marine Corps total force concept. The Marine Reserve provides individuals and specific units to augment and reinforce active capabilities.

Marine Special Operations Command

Established February 24, 2006, the MARSOC is the Marine Corps' component of US Special Operations Command (USSOCOM). It is headquartered at Camp Lejeune, and includes approximately 2,500 Marines, Sailors, and civilian employees.

It performs the functions of manning, organizing, training, and equipping Marine special operations forces to accomplish its mission. The MARSOC HQ is responsible for identifying the unique requirements of Marine special operations; developing MARSOC tactics, techniques, procedures, and doctrine; and executing assigned missions in accordance with designated conditions and standards.

A Marine Corps major general commands MARSOC with a supporting staff designed to be compatible in all functional areas with USSOCOM and Headquarters, Marine Corps (HQMC).

Although the MARSOC HQ is a nondeployable unit, the MARSOC commander and staff may “battle roster” as needed to deploy in support of USSOCOM tasks to form, deploy, and employ a joint special operations task force.

The MARSOC includes five subordinate units: The Foreign Military Training Unit; two Marine special operations battalions (MSOBs), one at Camp Pendleton, CA, and the other at Camp Lejeune; the Marine Special Operations Support Group; and the Marine Special Operations School.

The Supporting Establishment

The supporting establishment consists of 16 major bases, training activities, formal schools, the Marine Corps Recruiting Command, the Marine Corps Combat Development Command, the Marine Corps Systems Command, and HQMC. The supporting establishment’s contributions are vital to the overall combat readiness of the Marine Corps. Furthermore, because of the interconnected nature of the MCS support infrastructure, the supporting establishment plays a direct role in supporting the command and control of all MAGTFs. This support is necessary to effectively deploy and implement modern information technology in support of the MAGTF,

both in garrison and when deployed. In particular, the Marine Corps Network Operations Center and the Marine Corps Tactical Systems Support Activity (MCTSSA) provide essential support to the operating forces in the employment and operation of the MCS.

The Marine Corps Network Operations and Security Command (MCNOSC) located in Quantico, VA, acts as the focal point for technical support of Marine Corps data networks. This activity provides assistance in planning for and maintaining data networks for the MAGTF by coordinating with external agencies, such as Defense Information Systems Agency (DISA); advising operational planners; providing software support including contact teams; and providing Marine Corps-wide network operations management.

The MCTSSA, located at Camp Pendleton, provides support to the operating forces for the operation and maintenance of the fielded MCS. As the designated post-deployment system support activity for most of the MCS, MCTSSA receives trouble reports, analyzes problems, and takes corrective action. The Fleet Marine Force Support Division of MCTSSA provides direct, continuous liaison with the operating forces to identify and resolve problems. It provides training and operational support for exercises and actual contingencies.

SECTION II. MAGTF COMMUNICATIONS SYSTEM ORGANIZATIONS

Marines dedicated to using the MCS are organized by table of organization (T/O) into the units described in the following paragraphs. The units may deploy and be employed as a complete unit or they may provide task-organized detachments to support elements of a MAGTF. These units and detachments operate under the staff cognizance of the G-6/S-6 of the supported unit. Separate units and detachments will be found only at higher echelons. At regiments and below, the communications unit will be an integral part of the HQ, and the communications unit commander may also serve as the S-6. The Marines assigned to these units, in concert with personnel assigned to G-6/S-6 sections and functional area users, ensure that an effective MCS network is planned, installed, operated, and maintained. Communications units and the detachments they deploy are crucial to providing MCS capability for the MAGTF elements that they support. Missions, tasks, and concepts of organization and employment of these units are identified in their T/O and summarized in this section.

Communications Battalion

The mission of the COMM BN is to provide communications support to a MARFOR component HQ, a MEF CE or a MEF (Fwd) CE, a component HQ deployed simultaneously with a MEF CE and a MEF (Fwd) CE, or two MEF (Fwd) CEs. An additional mission is to provide support to three MEU CEs. The COMM BN provides—

- Command element communications for the supported CE: MEU, MEF (Fwd), MEF, and component HQ.
- Communications connectivity between the supported CE and senior, adjacent, and subordinate HQ.
- The supported CE with an entry into the GIG.

The battalion's command and control is exercised through the battalion commander and the executive staff. The COMM BN consists of the HQ company, a service company, three direct support communications companies, and a general support company. Elements of COMM BN may be employed separately as task-organized detachments to support organizations smaller than a MEF CE, or the entire battalion may be employed to support larger MAGTF CEs. The HQ company includes the structure necessary to provide detachments to support two MEU CEs.

The COMM BN normally deploys as a task-organized unit or deploys task-organized detachments in support of MAGTF CEs. Upon notification and before deployment of a MEF CE, COMM BN task-organizes to support the deployment. Upon notification and before the deployment of a MEF (Fwd) CE or a component HQ, a direct support communications company is task-organized to support the deployment. The MAGTF CE G-6/S-6 exercises staff cognizance over MAGTF communications. To facilitate system planning and engineering, COMM BN conducts concurrent planning with the component MAGTF G-6/S-6.

Headquarters Company

The mission of the HQ company is to provide organic command, administration, logistic, and other required support for a COMM BN. It also supports system planning and engineering for operating MAGTF communications networks as required. The HQ company—

- Plans and engineers the MCS for the MAGTF CEs as required.
- Installs, operates, and maintains network and system control facilities for the component HQ

and MAGTF CEs that are MEF (Fwd) size and larger.

- Installs, operates, and maintains message centers, radio links, and tactical switchboard/telephone systems for two MEU CEs.

The HQ company is organized into functional groups to provide for a battalion and company HQ and support the primary mission and tasks. The company normally collocates with the battalion HQ and operates in support of the battalion. As required, the various sections can be assigned to task-organized COMM BN detachments in support of deployed MAGTFs.

Direct Support Communications Company

The mission of the direct support communications company is to install, operate, and maintain the communications system for a MEF (Fwd) CE, MEF CE, or component HQ. The direct support communications company—

- Installs, operates, and maintains communications center facilities for the supported CE/HQ.
- Maintains radio stations on the MCS and on administrative, logistic, and other radio nets as required. See appendix A for an explanation of the various types of nets.
- Installs, operates, and maintains switchboard and telephone services for the supported CE/HQ.

The direct support communications company is organized into a company HQ and three platoons along functional lines, tailored to support the primary mission and tasks listed above. The direct support communications company operates under the direct control of the COMM BN. When operating in support of a MEF CE, the company deploys and collocates with the COMM BN. When in support of a MEF (Fwd) CE or component HQ, the company, with reinforcements, can deploy as a separate unit.

General Support Communications Company

The mission of the general support communications company is to install, operate, and maintain the component HQ, MEF CE, and MEF (Fwd) CE message and voice switches and links to JTF HQ, major subordinate commands (MSCs), adjacent units, and the GIG. The general support communications company—

- Installs, operates, and maintains the MEF digital transmission backbone by using cable and multichannel radio (MCR) equipment.
- Installs, operates, and maintains digital switches to provide secure and nonsecure voice, facsimile, message, and data service to the MEF CE command posts.
- Interfaces the component and MEF CE MCS with national systems; naval telecommunications system; commercial telecommunications systems; and senior (CCDR/JTF), adjacent, and subordinate systems and networks as required.
- Installs, operates, and maintains tactical WANs/LANs for MAGTF CEs of MEF (Fwd) size or larger.
- The general support communications company is organized into a company HQ, a switching platoon, a satellite communications platoon, and a terrestrial communications platoon. It operates under the direct control of the COMM BN. When operating in support of the MEF CE, the general support communications company deploys and collocates with the COMM BN. When in support of a MEF (Fwd) CE or component HQ, detachments from the general support communications company augment a task-organized direct support communications company to provide a switched communications hub for an area communications network. Simultaneously, ground mobile forces (GMFs) satellite communications teams and terrestrial transmission teams, as required, deploy as attachments to MSCs to connect the MEF CE with subordinate commands.

Service Company

The mission of the service company is to provide the following services for a COMM BN:

- Heavy transportation support to operating companies.
- Communications-electronics equipment maintenance support to operating companies.
- Primary electrical power distribution and service for the battalion.
- Materiel handling support to the battalion.
- Combat trains in support of the battalion.

The service company is organized into a company HQ and the following three platoons:

- A motor transport platoon to provide the operation and maintenance of heavy motor transportation equipment organic to the battalion.
- A communications-electronics maintenance platoon capable of performing third-echelon maintenance on digital switches, telephones, cables, computers, cryptographic equipment, and radio equipment, including high frequency (HF), very high frequency (VHF), ultrahigh frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF) single and multichannel assets organic to the operating companies of the COMMBN.
- An engineer platoon that installs, operates, and maintains power distribution, air conditioning, refrigeration systems, and materiel handling equipment organic to the COMM BN.

When the COMM BN is deployed as a unit, the service company normally collocates with the battalion HQ and provides support. As required, personnel and equipment from the service company can be assigned as part of task-organized COMM BN detachments.

Marine Wing Communications Squadron

The mission of the Marine wing communications squadron (MWCS) is to provide expeditionary communications for the ACE of a MEF, including communications support for the deployment of task-organized elements of a MAW. The MWCS—

- Assists in the system planning and engineering of ACE communications and installs, operates, and maintains expeditionary communications to support the command and control of the MEF ACE.
- Provides operational systems control centers, as required, to coordinate communications functions internally and externally to the ACE.
- Provides maintenance support for ground-common communications equipment in the MAW.
- Provides the digital backbone communications support for the ACE HQ, forward operating bases, and Marine air command and control system (MACCS) agencies for up to two airfields per detachment. The MACCS agencies include the tactical air command center (Marine TACC), tactical air operations center (TAOC), direct air support center (DASC), early warning/control (EW/C) sites, low altitude air defense (LAAD) teams, and Marine air traffic control detachments (MATCD).
- Provides tactical, automated switching and telephone services for the ACE HQ and Marine TACC.
- Provides electronic message distribution for the ACE HQ, primary MACCS agencies, and tenant units.
- Provides external, single-channel radio (SCR), MCR, and radio retransmission communications support for ACE operations as required.

- Provides deployed WAN and LAN server support for the ACE HQ and primary MACCS agencies.
- Provides the support cryptographic site for all ground-common and MACCS-assigned communications security (COMSEC) equipment within the ACE.

The MWCS consists of one HQ element and one or two detachments. It provides communications support for the ACE HQ and Marine TACC. Each detachment may be independently deployed to provide external communications for up to two airfields and four forward bases.

Communications Company, Headquarters Battalion, Marine Division

The mission of the communications company is to install, operate, and maintain the communications system for a Marine division HQ. The communications company—

- Installs, operates, and maintains communications center facilities for the division HQ.
- Maintains radio stations on the MCS, administrative, logistic, and other radio nets as required.
- Installs, operates, and maintains switchboard and telephone services for the division HQ.
- Installs, operates, and maintains MCR terminals for support of internal division communications links as required.
- Provides, in coordination with the artillery regiment, communications support for the division naval gunfire (NGF) officer, division air officer, and division fire support coordination center (FSCC).
- Installs, operates, and maintains enhanced position location reporting system in support of MAGTF operations. The division communications company consists of a company HQ and seven platoons organized by function to support the assigned mission.

The division communications company furnishes communications capability for the division main, the division rear, and the alternate command post. It provides multichannel communications to the three infantry regiments; the artillery regiment, which may act as the alternate division command post; and to the DASC. The MCR is the primary means of communication with major subordinate units. Wire communications will not normally be installed to major subordinate units, but may be installed to separate battalions if located within approximately 1 mile of the division HQ. Otherwise, wire service is restricted to internal HQ installations for local telephone and multichannel lines. Multichannel communications service will be disrupted during displacement of the division HQ.

Communications Company, Combat Logistics Regiment, Marine Logistics Group

The mission of the communications company is to provide communications support to the HQ of the MLG, subordinate battalions, and LCEs. The communications company—

- Provides communications support to the MLG HQ/force CSS area and other LCEs established to support MAGTF operations.
- Provides communications support for the MLG HQ; forward CLR; and maintenance, supply, and dental battalions.
- Augments the communications needs of the direct support CLR, engineer support, and medical battalions.
- Installs, operates, and maintains communications control facilities.
- Installs, operates, and maintains tactical automatic switching and wire communications for the MLG HQ/force CSS area. When required, provides small-scale automated switching within maintenance, supply, medical, and dental battalions; the explosive ordnance disposal platoon and bulk fuel company; the engineer support battalion; and the MLG.

The communications company is structured to provide communications support to the MLG HQ in MEF operations and task-organized detachments to the HQ of LCEs deployed with MAGTFs smaller than a MEF. Augmentation from the MEF COMM BN is required if a dedicated naval telecommunications system/defense communications system entry is required.

The communications company provides the primary communications support for the MLG HQ and other LCE HQ.

Communications Platoons, Branches, and Sections

Communications platoons, branches, and sections provide communications support at the regimental/group, battalion/squadron, and, in some instances, company/battery levels of the MAGTF. These communications units are organized to support the communications networks and command posts of their parent organizations. The artillery unit communications platoons are further required to provide support for establishing the communications links to the units receiving their artillery support. The radio battalion communications platoon provides special intelligence communications support for the MAGTF CE. Communications platoons, branches, and sections are found in the following organizations:

MEF CE

- Headquarters and service (H&S) company, radio battalion.

Marine Division

- HQ company, infantry regiment.
- H&S company, infantry battalion.
- HQ battery, artillery regiment.
- HQ platoon, artillery battery.
- HQ battery, artillery battalion.
- H&S company, tank battalion.
- H&S company, assault amphibian battalion.
- H&S company, combat engineer battalion.
- H&S company, light armored reconnaissance battalion.

MLG

- H&S company, engineer support battalion.
- H&S company, medical battalion.
- HQ company, direct support CLR.

MAW

- Marine air support squadron, Marine air control group (MACG).
- H&S battery, LAAD battalion, MACG.
- Marine air control squadron, MACG.
- Airfield operations division, Marine wing support squadron, Marine wing support group.

MEU

- MEU CE communications platoon.
- H&S company, battalion landing team.
- Communications detachment, CLB.
- Communications section, MACG, ACE.

Special Security Communications Teams

The mission of the special security communications teams is to provide special intelligence communications support to the MAGTF. The special intelligence communications support for the MAGTF CE is provided by special intelligence communications personnel organic to the radio battalion or radio battalion detachment. The special intelligence communications support for the division and MAW HQ is provided by special security communications teams—small force units organic to each division and MAW. These teams operate under the staff cognizance of the assistant chief of staff, intelligence officer (G-2)/special security officer. The special security communications element or team provides the personnel and equipment to install, operate, and maintain special intelligence communications terminals. Communications circuits are provided by the communications unit supporting the HQ—the COMM BN for the MAGTF CE, the communications company for the division HQ, and the communications squadron for the MAW HQ. Close coordination is maintained with supporting systems control (SYSCON) and technical control (TECHCON) to ensure adequate support and circuit priority.

Amphibious Communications Teams

In 1998, Marine communications detachments and Marine tactical C2 sections were reorganized into amphibious squadron deployment teams to provide support for landing forces on board all amphibious ships. In 2003, amphibious squadron deployment teams were split into two landing force system teams to work for the amphibious group commander at the amphibious group in support of the landing force. In 2007, the amphibious group was called the ESG. The amphibious communications teams were assigned to naval units on the waterfront to provide the same level of support. As the naval architecture migrates toward a more standardized, network centric environment, it is critical to look at all amphibious platforms as a node in the

GIG and provide the proper personnel support to facilitate these requirements.

Amphibious communications teams provide the required expertise and leadership to maintain current Marine Corps situational awareness by continually evaluating and providing feedback for future amphibious communications systems. The Marine Corps communications staffing billets, as part of the Commander Naval Surface Forces staffs, will facilitate essential amphibious communications and networks planning, coordination, installation, and maintenance. In addition, the amphibious communications teams provide appropriate manpower to address critical deficiencies in amphibious requirements determination, programming at flag and staff levels, and necessary operational support.

SECTION III. COMMAND AND CONTROL ORGANIZATIONS

To exercise command and control in combat, all MAGTF units establish command posts, HQ from which the commander and staff operate. Battalion-sized or larger units may divide the HQ into echelons—main, rear, and tactical. The command post then becomes the echelon at which the commander is physically located. The main echelon (main) is where the commander and those elements of the staff required to plan and direct operations and control forces are normally located. In a large geographic area, a unit may establish a rear echelon (rear) to serve principally as an administrative and logistical support base. To be in close proximity to subordinate units and more directly influence tactical actions, the commander may create a tactical echelon (tactical command post). The tactical echelon is mobile and contains a minimum number of personnel and equipment, including the commander, the MCS operator(s), the G-2/S-2, the G-3/S-3, and the fire support coordinator.

Marine Expeditionary Force Command Element

The MEF staff and supporting CE units are task-organized to exercise command and control and to support the MEF's assigned mission. The MEF includes standard components as well as components that are used only for certain missions. Standard components include the principal staff sections and future and current operations cells within the operations section. Additional components may be added, based on the mission, to support functions needed in a particular operation. For example, in a foreign humanitarian operation, the MEF commander may organize an agency or section to coordinate with other foreign or domestic governmental or nongovernmental agencies and organizations.

Another example is the establishment of a consolidated military engineering group to provide centralized planning and manage Marine Corps, US Army (USA), and US Navy (USN) engineering assets assigned to the MEF.

Future Plans

The MEF planning officer (G-5) establishes a future plans cell to conduct long-range planning. Future plans works closely with the JTF HQ to ensure that the MEF is prepared for its next major mission. Products from future plans provide the basis on which future operations will develop the operation order (OPORD).

Future Operations

The MEF G-3 establishes a future operations cell that is responsible for planning operations in support of the current mission. The future operations cell receives an initial plan and related material from future plans and begins detailed planning. It consists of several full-time personnel from the G-3 who form the core of an operational planning team. When the operational planning team is formed, it includes members of the G-1, G-2, G-4, G-5, and G-6 sections. Other appropriate staff sections join the planning team as needed, as do representatives from subordinate units and designated functional experts. The operational planning team remains together through mission analysis and COA development, analysis, and comparison/decision. They then return to their respective work sections, complete annexes and appendices to the OPORD as required, and resume normal duties.

Current Operations

The MEF G-3 establishes a current operations cell responsible for executing operations. Current

operations personnel receive the plan from future operations and execute it. Current operations personnel staff the MEF combat operations center (COC) from which they monitor MEF operations and respond to situations as needed. The COC consists of a G-3 watch officer, a G-2 watch officer, a senior watch officer, and a situation report watch officer. A number of enlisted Marines assist in operating tactical information systems and maintaining situation displays.

The G-2 and G-3 watch officers receive information from collocated MAGTF all-source fusion center personnel, the surveillance and reconnaissance center (SARC), force fires coordination center (FFCC), ground and air representatives, and subordinate and adjacent units. The G-2 and G-3 watch officers filter this information and forward important pieces to the senior watch officer. The senior watch officer also receives information that affects current operations from other principal staff sections, such as G-1, G-4, and G-6, and evaluates that information in the context of current operations to determine whether action is required.

Depending on the situation, the senior watch officer may be assisted in this process by other officers from current operations. On the basis of authority delegated by the MEF commander, the senior watch officer acts by either issuing orders or briefing the MEF commander and recommending action.

Command and Control Facilities

Watch officers and supporting personnel from the staff sections and supporting units establish and operate centers within the HQ from which the day-to-day activities of the MEF are coordinated, controlled, and supported. These C2 centers sometimes, especially when dealing with air command and control, are referred to as C2 agencies. In this publication, these centers and agencies, both at the MEF level and at the subordinate unit

level, are referred to as C2 facilities. These facilities include the personnel, software, hardware, shelters, and ancillary equipment needed to support command and control. The key C2 facility in the MEF is the COC. In most cases, the COC is located with the FFCC and the MAGTF all-source fusion center. These three C2 facilities work together closely, focusing on current operations and responding to the immediate needs of the MEF commander. In all cases, information system support and LAN connectivity within and among these three facilities are essential for efficient execution of MEF operations. The FFCC, the MAGTF all-source fusion center, and other MEF C2 facilities are discussed under the functional area they support.

Marine Expeditionary Force Rear

The MEF rear may perform several functions within the MEF AO. A MEF rear may be established to coordinate administrative and logistical activities while the MEF maneuvers forward. The MEF rear may also be assigned responsibility for rear area operations. Rear area operations are extremely complex at the MEF level. Joint doctrine currently defines eight rear area functions that must be coordinated: area management, movements, infrastructure development, host-nation support, security, communications, intelligence, and sustainment. The MEF commander may assign some or all of these functions to the MEF rear and others to the wing and the MLG. If assigned overall responsibility, the MEF rear would require the capability to plan and conduct rear area operations. In this instance, the MEF rear would establish a rear area operations center to facilitate the command and control of operations within the rear area. In situations where the main HQ does not move forward and the MEF retains responsibility for rear area operations, the rear area operations center becomes another element of the MEF.

Ground Combat Element

Division Main

The division main serves as the division commander's primary HQ. Both current and future operations planning are accomplished in the division main. Division personnel monitor and, if the commander is located in the division main, direct current operations from the division main. Although smaller than the MEF, the division main is organized for command and control in a similar manner, including a future operations cell within the G-3 section. Current operations are directed from the division COC (which is typically staffed by G-3 and G-2 personnel; the division engineer; the division air officer; and chemical, biological, radiological, and nuclear personnel). The FSCC is usually physically collocated with the COC. The DASC is either physically or electronically collocated with the FSCC.

Division Rear

If the division is spread over a large geographic area, the division commander may establish a division rear. The division rear may serve principally as an administrative and logistical support base for the division. In this arrangement, the division main may consist of the COC and FSCC with the collocated DASC. The division rear would then include principal staff elements not required to plan and execute current operations, such as G-1, G-4, or staff judge advocate. This arrangement allows the division main to maneuver rapidly in high-tempo operations.

Division Tactical Echelon

The division commander may establish a small, highly mobile, tactical echelon to remain in close proximity to the battle, gain first-hand situational awareness, and more directly influence tactical operations at critical times. Depending on the situation, either surface or air platforms are appropriately configured to provide mobility and

communication for the tactical echelon. The division commander prescribes which staff members constitute the tactical echelon. A nominal tactical echelon would include the division commander, the MCS operator(s), G-2, G-3, and a fire support coordinator.

Regiment/Battalion

Regiments and battalions also use the main, rear, and tactical echelon structure and establish a COC to coordinate and direct operations. These operations centers and echelons are much smaller than those at the division level because regiments and battalions have fewer subordinate units and fewer functions to support.

Tactical Air Control Party

Tactical air control parties (TACPs) provide coordination among GCE units and supporting aviation assets. They exist at the infantry division, regiment, and battalion levels. Depending on the command level, a TACP contains a combination of air officers, forward air controllers, and enlisted radio operators. Air officers serve at the division, regiment, and battalion levels. These officers serve as special staff officers to their respective commanders. Additionally, they may serve within the FSCC to assist with planning and deconfliction functions related to air support for the assigned unit. Forward air controllers provide terminal control of close air support aircraft that are passed to them by the DASC. These officers also advise GCE commanders on aviation capabilities and limitations and prepare requests for air support.

Aviation Combat Element

Wing Main

The wing main serves as the principal HQ for the wing commander. Like the MEF and division main, most principal staff members are located in the wing main where future planning is done. The

wing rear area operations center is often collocated with the wing main. Unlike the MEF and division main, however, the wing main may be located outside the MEF AO. The wing commander often locates the wing main at a large airfield, especially if this airfield houses most of the wing's fixed-wing aircraft. Wing future and current operations functions occur within the Marine TACC, which may or may not be collocated with the wing main.

Marine Tactical Air Command Center

The mission of the Marine TACC is to function as the senior MAGTF air C2 agency and to serve as the command post for the ACE commander. The Marine TACC provides the facility from which the ACE commander and battle staff plan, supervise, coordinate, and execute all current and future MAGTF air operations, including the planning and execution of the current ACE operation or FRAGO. The Marine TACC will be organized with a battle staff consisting of four mutually supporting organizations:

- Air combat intelligence—responsible to the ACE G-2 for producing and disseminating aviation-tailored, all-source intelligence required for decisionmaking during the planning and execution of MAGTF air operations.
- Future plans—responsible to ACE G-3 for aviation planning in support of the next MEF mission change.
- Future operations—responsible to ACE G-3 for developing MAGTF future air tasking orders, writing of the OPOD/FRAGO for the next ACE mission change, and for conducting current planning.
- Current operations—the current operations officer is in charge of the current operations section and is responsible to the ACE G-3 for the overall combat operations of the ACE to include execution and assessment of the current air tasking order.

Aviation combat intelligence is imbedded within the Marine TACC. Timely, tailored, and fused intelligence is integral to the functioning of future plans, future operations, and current operations. Aviation combat intelligence is the focus of all aviation intelligence activities supporting the ACE. It produces and disseminates aviation-specific, all-source intelligence, including assessments of adversary capabilities and vulnerabilities, target analysis, battle damage assessment, and the current status and priority of assigned targets to assist in execution day changes. The Marine TACC uses specialized information systems and equipment to display a common operational picture of the aviation situation received from tactical digital information links. Each Marine aviation function—AAW, assault support, EW, air reconnaissance, offensive air support, and control of aircraft and missiles—provides representation to the Marine TACC.

Tactical Air Operations Center

The TAOC is the principal air defense agency that conducts real-time surveillance and positive aircraft control of its assigned airspace within the MACCS. The TAOC normally deploys as a part of the MACCS within the MAGTF, but, if the mission dictates, it may deploy independently or as part of a combined or joint force. Personnel and equipment are provided by the Marine air control squadron.

Through radar inputs from its organic sensors and data link information from other military radar units, the TAOC provides real-time surveillance of assigned airspace in addition to air direction, positive aircraft control, and navigational assistance to friendly aircraft. Its primary function, to conduct and coordinate AAW, is accomplished through the direction, coordination, and employment of various air defense weapons systems that include interceptor aircraft and ground-based air defense weapons.

Marine Air Traffic Control Detachment

The MATCD provides friendly aircraft with continuous all-weather radar/nonradar approach, departure, tower, and en route air traffic control (ATC) services within assigned controlled airspace. It is the primary terminal air control agency within the MACCS. The MATCD is organized and equipped to satisfy the ATC requirements for virtually any type of forward operating base.

Low Altitude Air Defense Battery Command Post

The LAAD battalion, usually collocated with the TAOC, establishes a COC for the exercise of battalion operations. The LAAD battalion commander exercises overall command and control of LAAD battalion operations from the COC. The commander obtains and relays intelligence and combat information on friendly and enemy operations to the two subordinate LAAD battery COCs. The LAAD battery COCs maintain situational awareness of MAGTF and other air operations and plan and control employment of LAAD teams.

Direct Air Support Center

The DASC is equipped and operated by the Marine air support squadron. Typically the first major air control agency landed ashore during an amphibious operation, the DASC normally lands in the same serial as the senior GCE FSCC. The DASC processes immediate air support requests; coordinates aircraft employment with other supporting arms; manages terminal control assets supporting GCE and LCE forces; and controls assigned aircraft, unmanned aircraft systems, and itinerant aircraft transiting through DASC-controlled airspace. The DASC, when practical, physically collocates with the GCE's senior FSCC. An electronic link may be an acceptable alternative in situations where DASC siting requirements differ from FSCC requirements.

Airborne Coordinators/Controllers

Tactical Air Coordinator (Airborne)

A tactical air coordinator (airborne) (TAC[A]) is an officer who, from an aircraft, coordinates the actions of combat aircraft engaged in close support of ground or sea forces. Within the MACCS, the TAC(A) is a naval aviator or naval flight officer. The TAC(A) is the senior air coordinator and has air authority over all aircraft operating in an assigned area. The TAC(A)'s primary mission is to act as an airborne extension of the DASC, Marine TACC, or FSCC. The TAC(A) helps to coordinate TACPs, forward air controllers (airborne) (FAC[A]s), and the fire direction of artillery and NGF.

Forward Air Controller (Airborne)

A FAC(A) is a specifically trained and qualified aviation officer who, from the air, exercises control of aircraft engaged in close air support of ground troops. The FAC(A) is normally an airborne extension of the TACP. Within the Marine Corps, the FAC(A) is a naval aviator or flight officer who is specifically trained, qualified, and designated to perform air reconnaissance and surveillance, conduct terminal control of aircraft engaged in offensive air support operations, control artillery and naval surface fire support missions, act as a radio relay, and control landing zone operations.

Assault Support Coordinator (Airborne)

An assault support coordinator (airborne) (ASC[A]) is an aviator who, from an aircraft, coordinates the movement of aviation assets during assault support operations. The ASC(A) is an experienced aviator with extensive knowledge of the MACCS who acts as an airborne extension of the DASC. This individual assists in providing situational awareness to the assault force, relays requests to the DASC, exercises launch authority for immediate and on-call missions, coordinates with the TAC(A), and provides routing recommendations to the air mission commander.

Airborne strike coordination and reconnaissance is a means to efficiently focus aviation fires in the deep area of the battlespace. This function, usually performed by an F/A-18 aircrew, allows real-time reconnaissance to locate the MEF commander's high-priority targets. Once located, the strike coordination and reconnaissance aircrew control attack aircraft in much the same manner as a tactical air coordinator: by cycling and deconflicting multiple strike packages as they ingress to the target area. Using an aircrew to extend the C2 system allows them to position themselves to effectively control multiple aircraft missions while maintaining communication with the aircraft they control and ground-based C2 facilities.

Logistics Combat Element

Marine Logistics Group Main

The MLG main is task-organized by the MLG commander to enable him to control and coordinate logistic support of the MEF. An MLG main includes the principal staff sections, a future plans and deployment section, and the logistics operations center (LOC). The future plans and deployment section ensures that the MLG is prepared to support the next major mission of the MEF. Often, this new mission involves a deployment or redeployment. The LOC monitors current operations and plans near-term future operations. The MLG main is typically located near sea or aerial ports of debarkation in the MEF's AO. Subordinate regiments and battalions establish their own HQ close by the MLG main.

Logistics Operation Center

The LOC serves as the hub for future and current operations planning within the MLG main. Each logistic functional area—supply, maintenance, transportation, engineering, health, and other services—provides representation to the LOC. Under the supervision of a G-3 watch officer,

these personnel monitor current operations and maintain status displays of friendly and enemy situations. Additionally, LOC personnel handle requests from subordinate units and keep the MEF informed of the logistic situation. The MLG commanders may choose either a centralized or decentralized configuration for their LOCs.

Combat Logistics Battalions and Combat Logistics Companies

Depending on the situation, the MLG commander establishes forward elements to provide direct support to the GCE. A CLB is the standard element that provides direct support to an infantry regiment. The lowest echelon of support would come from the combat logistics company. The CLB commanders may establish small facilities to coordinate support and monitor logistic communications nets. A mobile CLB possesses the least capability to establish an operations center. In this instance, the LOC could resemble a mobile, tactical echelon. Communications connectivity would be predominantly through SCR.

Movement Control Center

Movement control centers support the deployment of the MEF from the home station, through intermediate bases, to the destination. The commander, MARFOR establishes the HQ movement control center, which provides connectivity to United States Transportation Command and keeps the MEF force movement control center informed about strategic movement issues. The force movement control center controls and coordinates all movement support. It serves as liaison with the Air Mobility Command, the Military Sealift Command, and the Military Surface Deployment and Distribution Command. The force movement control center supervises efforts of unit movement control centers of the division, wing, and MLG. The division, wing, and MLG provide transportation and communications assets in support of deployment activities. Bases and air stations from which Marine units deploy establish base or station operations support groups to coordinate their

efforts with those of deploying units. These bases also provide their transportation and communications assets in support of deploying units. These units augment unit movement control centers to ensure that all personnel and materiel arrive at sea and aerial ports of embarkation.

Marine Logistics Command

The commander, MARFOR may establish an MLC and assign it responsibility for establishing the theater general support structure to facilitate arrival/assembly reception, staging, onward movement, and integration operations. The MLC may also be assigned responsibility for providing operational logistic support to Marine forces as the Marine component operational-level logistic agency in theater. The MLC is a task organization option, not a standing organization. The commander, MARFOR may assign a specific MLG responsibility for MLC functions. Then, on the basis of the operational situation, theater geography, operations and logistics, command and control, and infrastructure requirements, commander, MARFOR will assign Marine Corps component resources to the MLG for detailed task-organizing and conducting MLC theater-support operations.

Intelligence Command and Control

The intelligence operations center is established under the G-2/S-2 within the MAGTF HQ to provide centralized direction for the overall MAGTF intelligence effort. This organization serves the entire force by consolidating, validating, and prioritizing intelligence requirements from all MAGTF elements. The intelligence operations center links the MAGTF to JTF, theater, and national and allied intelligence assets. The intelligence operations center is supported by the reconnaissance operations center, surveillance and reconnaissance center, and the operations control and analysis center (OCAC).

Surveillance and Reconnaissance Center

The SARC is the primary intelligence C2 node used to direct, coordinate, monitor, and supervise MAGTF collection operations. The MAGTF collection operations include intelligence collection operations conducted by organic, attached, and direct support assets. The SARC is located close to the MEF COC. The SARC coordinates collection and operations tasks to various MEF assets, including force reconnaissance, the ground sensor platoon, the unmanned aircraft squadron, the radio battalion, and counterintelligence detachments.

Reconnaissance Operations Center

The reconnaissance operations center serves as a focal point for monitoring and supervising force reconnaissance operations. Located in or near the SARC, this facility gathers information from dispersed teams, decrypts reports, and forwards information for fusion into the overall MAGTF intelligence situation display. Personnel manning the reconnaissance operations center assist reconnaissance teams with movement and other activities as needed.

Operations Control and Analysis Center

The OCAC provides centralized direction, management, and control of signals intelligence and EW activities within the MAGTF and coordinates with external theater and national assets. Assigned personnel process, analyze, and disseminate collected information. The OCAC is located within the MAGTF HQ compound near other intelligence C2 facilities.

Intelligence Centers

The G-2/S-2 establishes intelligence centers at all echelons of the MAGTF down to the battalion level. Personnel assigned to the intelligence center collect, process, integrate, analyze, evaluate, and interpret intelligence, continuously updating

the enemy situation and rapidly providing that information to current and future operations. These centers are collocated with the COC whenever possible.

Fire Support Centers

The C2 facilities are established to coordinate the overall fire support effort and to exercise tactical and technical fire support direction.

Force Fires Coordination Center

The FFCC is established at the MEF level to assist the MEF commander in planning and coordinating deep fires. The FFCC performs three primary functions for the MEF: planning, acquiring, and maintaining target information; coordinating and integrating MAGTF-level fires with future operations; and coordinating and integrating MAGTF-level fires into current operations. Located within the MEF, this facility assists both future operations and current operations with targeting functions. Additionally, the FFCC provides coordination between the MEF and JTF targeting boards and centers. Watch standers may be collocated with the COC to facilitate rapid deep fires coordination.

Fire Support Coordination Center

Each Marine ground combat organization from division to battalion employs an FSCC as an advisory and coordination agency. The FSCC is collocated with the COC. The senior FSCC coordinates and deconflicts fire support efforts among subordinate units and centers. The FSCC includes the fire support coordinator, artillery liaison, TACP personnel, mortar unit liaison when appropriate, and a naval surface fires liaison. At the division level, the division artillery officer or artillery regiment commanding officer serves as the fire support coordinator. At lower levels, each commander appoints a fire support coordinator from his staff who is usually the weapons company commander.

Fire Direction Center

Fire direction centers (FDCs) exist at artillery regiments, battalions, and batteries. These organizations permit respective commanders to plan and control fires. Fire direction activities may be centralized or decentralized. At regimental and battalion levels, the FDC exercises tactical fire direction, and battalion FDC personnel supervise, advise, and augment battery personnel as required. Battalion personnel also assist by troubleshooting gunnery problems, which enables battery FDC personnel to focus on delivering artillery fires. The battery FDC provides technical fire direction by evaluating information received by forward observers and determining firing data. This firing data is issued to artillery sections through fire commands. Battery FDCs are also capable of tactical fire direction and would perform this function in cases, such as MEU deployments, when the battery operates independently.

Electronic Warfare Coordination Center

The EW coordination center facilitates coordination of EW operations with other fires and the MCS. This center coordinates efforts by the G-2, G-3, and G-6 to eliminate conflicts between these overlapping warfighting functions. The EW coordination center is under the staff G-3's cognizance. Assigned personnel identify potential conflicts in planned operations and work to resolve these issues. The EW coordination center includes an EW officer, an MCS representative, and other liaison officers as needed. Liaison could include radio battalion representation, EA-6B electronic countermeasures officers, a MACG radar officer, and other Service representatives.

Rear Area Operations Centers

A rear area operations center facilitates C2 operations within the rear area(s). Responsibility for rear area operations may be tasked to the MEF rear. It may also be shared with or assigned to

the MLG and the wing, especially when the MSCs are widely dispersed geographically. The rear area operations center contains personnel to monitor and coordinate the varied activities occurring in the MEF rear area. For MSCs, the size and scope of a rear area operations center would be driven by the unit's mission and rear area activities. At a minimum, the wing and MLG would use one or more rear area operations centers to coordinate security for the bases they occupy. Personnel serving in these facilities must be knowledgeable in all functions performed by the facility. To support the security function, a fire support coordinator must be assigned to plan and coordinate fires in the rear area. All rear area operations centers should be linked and should coordinate activities across the entire MEF rear area.

MAGTF Communications System Control

At the MAGTF CE level, the G-6/S-6 exercises overall staff cognizance and technical direction of the MAGTF communications system and personnel. The G-6/S-6 also coordinates with the controlling authorities of external networks. The G-6/S-6 is assisted by personnel from the communications battalion to exercise operational systems control. Operational systems control is exercised at levels lower than the MAGTF down to the battalion/squadron level by the G-6/S-6 of that organization. The G-6/S-6 is supported by organic communications units or detachments.

Operational Systems Control Center

The functions of an operational systems control center (OSCC) exist at all levels of MCS control. At the higher echelons of MSC and above, specific agencies are established to conduct these functions. At the lower echelons of the battalion and squadron, the functions are still performed,

but they are performed at the S-6/communications unit level. Figure 2-1 details a typical joint operational systems control model. The OSCC functions consist of the four elements discussed in the following paragraphs.

Systems Planning and Engineering

The systems planning and engineering (SPE) element performs future operations functions for communications operations. The SPE at any echelon consists of MCS network design. These networks are designed and subsequently engineered to meet the operational requirements as determined by the communications officer. Circuits are determined by type and number to meet both internal and external command communications requirements. The SPE personnel normally perform their duties in a suitable facility as part of the G-6/S-6 staff in the main command post. The MAGTF G-6/S-6 is the senior Marine communications officer who directs the overall SPE effort at the MAGTF level. The G-6/S-6 at lower echelons, with the assistance of their supporting communications unit/detachment, performs appropriate level SPE functions in accordance with the overall MAGTF communications plan.

Systems Control

The SYSCON performs current operations functions for communications operations. It is established by the operations officer of each communications unit to maintain current information on availability and operational readiness of the MCS and to set priorities and resolve conflicts. The SYSCON receives direction from the SPE and coordinates directly with senior, subordinate, and adjacent SYSCONs as required. Its personnel perform their duties in an appropriate facility in the vicinity of the supported command post and must have the technical expertise and experience to coordinate the resolution of complex communications problems.

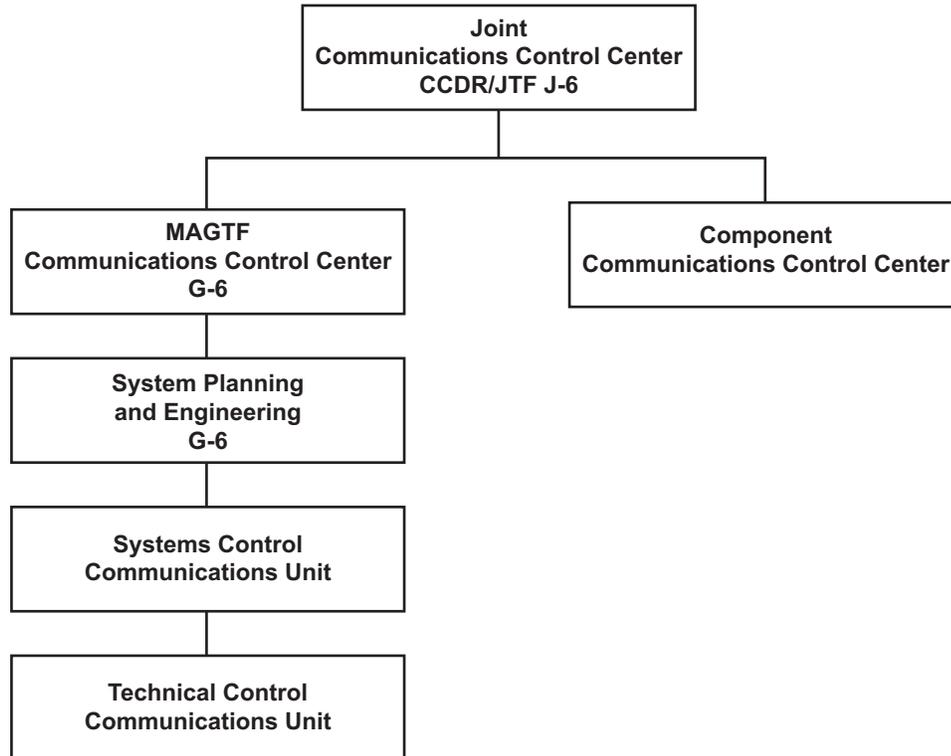


Figure 2-1. Joint Operational Systems Control Model.

Technical Control

The TECHCON element provides centralized technical supervision over the installation, operation, and maintenance of SCR, wire, multichannel, and data communications systems. Its functions are performed from a specially-designed TECHCON facility, the network operations center, maintenance facilities, and communications centers when established. The TECHCON facility provides a means to conduct and coordinate circuit troubleshooting and restoration. The facility's size and scope are driven by the size of the communications organization and types of services being provided. All TECHCON personnel must have the technical expertise and experience to resolve complex communications problems.

Joint Communications Control Center

The joint communications control center (JCCC) is the operational systems control agency of the JTF or CCDR communications system staff officer (J-6). According to the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231.07D, *Manual for Employing Joint Tactical Communications - Joint Network Management and Control*, the JCCC provides theater or JTF planning level and supervision of component communications control centers (CCCs). Normally, liaison officers from each Service component command are provided to the JCCC as subject matter experts and participate in JCCC functions as watch members. See figure 2-1.

MAGTF Communications Control Center

The MAGTF G-6 employs the MAGTF CCC as the MAGTF operational systems control center. Subordinate communications battalion/company staffs augment the MAGTF CCC. The MAGTF CCC coordinates external communications control with the JTF or CDR J-6 through the JCCC. The MAGTF CCC also may be required to support a Marine component HQ.

Component Communications Control Centers

Each component of the joint force or theater command, whether USA, US Air Force (USAF), USN, or Marine Corps, establishes some form of an OSCC to perform component-level operational systems control functions. The components of the designated Army theater signal command normally support the Army component command and augment the JTF/theater-level operational systems control agency. The MAGTF CCC coordinates OSCC functions with joint and Service component CCCs to maintain the joint network.

Amphibious Command and Control Facilities

When the MAGTF is aboard amphibious ships, the MAGTF commander serves concurrently as the commander, landing force (CLF). While embarked, the MAGTF commander and staff direct the actions of the MAGTF from C2 facilities aboard the amphibious ships. Under the operational maneuver from the sea concept, MAGTF command and control may remain afloat throughout the amphibious operation. Many of the shipboard C2 facilities also support the commander, amphibious task force (CATF), who is normally located with his staff in the flag plot area aboard the flagship.

Flag configured ships and LPD [Amphibious Transport Dock]-17 class ships will have a troop operations area used for planning and control

similar to that of the landing force operations center (LFOC). Non-flag configured ships on the LPD-4 class and LSD [Landing Ship Dock] class have only a tactical-logistical group (TACLOG) for command and control.

Landing Force Operations Center

The LFOC is the shipboard space allocated to the CLF and staff to plan and execute landing force operations. The LFOC is normally located on the ESG. The LFOC also staffs the MAGTF COC when it is phased ashore in an amphibious operation. The functions of the LFOC mirror those of the COC. This center controls and monitors the activities of the landing force until the CLF establishes command ashore.

Joint Intelligence Center

The joint intelligence center (JIC) is a single, naval intelligence facility formed during a pre-assault phase of amphibious operations. It supports the requirements of the CATF and the CLF. The JIC is usually located aboard the amphibious flagship and is staffed by Navy and Marine intelligence personnel. Intelligence resources available to the JIC include national, joint, combined, and organic naval force assets. Some of these assets may already be forward deployed prior to assault operations. Landing force intelligence personnel and their organic information systems, such as the intelligence analysis system and the technical control and analysis center workstations, are integrated in the JIC operations while afloat. Additionally, the ship's signals exploitation spaces are within the JIC and contain ESG special security communications terminals and processing facilities.

Supporting Arms Coordination Center

Commander, amphibious task force exercises overall coordination of supporting fires within the amphibious objective area through the supporting arms coordination center (SACC). This center, located aboard the amphibious flagship,

consists of a supporting arms coordinator, NGF, air support, and target information sections. The ESG operations, intelligence and communications, and landing force fire support personnel perform the functions of the SACC. These functions are similar to those performed by the FFCC and FSCC that may be subsequently established ashore. A landing force liaison is established in the SACC if the responsibility for coordination of supporting arms is passed ashore.

The SACC provides the commanders of the amphibious task force and the landing force with information concerning the requirements and developments that affect coordination of fire delivery by NGF units, support aircraft, and artillery units. Fire support requests received from the landing force are coordinated from this center to ensure that all fires are integrated to achieve the maximum effect against their targets. Current fire support information is continually updated and displayed while direction for the execution of restrictive fire plans and instructions concerning troop safety are promulgated. The NGF plans are prepared and their execution is supervised by the SACC staff. This center also coordinates air support operations with appropriate amphibious task force and landing force air control agencies. Records of targets in the objective area are maintained, and appropriate fire support activities in the amphibious objective area are monitored when responsibility for the coordination of fires is passed to the CLF ashore.

Tactical Air Direction Center

The tactical air direction center (TADC) is organized and located in the flagship of the CATF. The TADC provides the means to direct and coordinate all tactical air operations in an objective area, including AAW, until this responsibility is transferred to the Marine TACC ashore. The TADC consists of a tactical air controller; air support controller; AAW coordinator; and appropriate operations, intelligence, and communications personnel

and equipment. Personnel and equipment are provided by the flagship, the staff of the CATF, and a designated tactical air control squadron.

Helicopter Direction Center

The helicopter direction center (HDC) is organized aboard the flagship of the helicopter transport group to provide the means to direct and control helicopters during the ship-to-shore movement. It consists of a helicopter director, who is accountable to the tactical air commander for direction of all helicopters and supporting aircraft; a helicopter direction net officer; a helicopter air controller; and other appropriate air operations and communications personnel and equipment. Personnel and equipment are normally provided by the flagship on which the HDC is established.

To effect the direction and control of helicopter movement in an objective area, the HDC must operate under the overall direction of the TADC for coordinating air operations with other agencies and under the operational control (OPCON) of the helicopter transport group commander. The HDC advises the TADC on all matters pertaining to helicopter movement that require coordination with supporting arms. The HDC provides information as directed by the TADC and the helicopter transport group commander and maintains availability and location status of assigned helicopters. The HDC also receives requests for helicopter support, designates units to provide helicopters for specific missions, and directs their employment. The HDC further controls the movement of helicopters, both transport and escort, from wave rendezvous to the initial point, and from takeoff at the landing zone to the breakup point. The HDC also controls movement of helicopters between platforms and assists the DASC in controlling helicopters between ship and shore after the control of helicopters has been passed ashore.

Tactical-Logistical Group

Tactical-logistical groups are temporary agencies organized as required by ground combat organizations of a landing force to assist the naval control organization in the ship-to-shore movement of troops, equipment, and supplies. They are normally established aboard control ships at each echelon of the MAGTF, along with the naval control agency exercising control over the ship-to-shore movement of that echelon during a waterborne landing. They are also established aboard each helicopter transport carrier during vertical assaults. A TACLOG consists of operations, CSS, embarkation, and communications personnel provided by the parent ground combat organization.

The TACLOG assists the corresponding naval control agency in handling landing force requirements during the ship-to-shore movement. It is task-organized to inform the naval control agency about the location of units, equipment, and supplies, and to monitor their regulated movement ashore. The TACLOG maintains a detailed record of the unloading and landing status, provides information to appropriate commanders concerning the progress of the ship-to-shore movement, and responds to routine requests received from units by coordinating with the naval control agency. It further advises the naval control

agency when the tactical situation ashore dictates an adjustment to the prescribed landing sequence.

Mobile Command Posts

Mobile command posts provide means for commanders at all levels to keep pace with rapidly maneuvering elements. They are essential for conducting maneuver warfare. These mobile command posts are usually mounted in vehicles, but may be airborne or footmobile. Various configurations exist depending on the availability of C2 platforms. The C2 variants of the amphibious assault vehicle, expeditionary fighting vehicle, utility helicopter, and light armored vehicle are specifically designed for the mobile command post purpose. Units also use organic vehicles in various arrangements to form mobile command posts. Mobile command posts normally consist of the commander accompanied by a few key personnel from the tactical echelon. At the small unit level, such as a rifle company or platoon, the command post is often footmobile. In some situations, the tactical echelon of a larger unit may also be footmobile, such as when operating in terrain that precludes using vehicles. However, given restrictions on the amount of equipment that can be carried, a footmobile command post is usually impractical above battalion level.

CHAPTER 3

GLOBAL INFORMATION GRID

The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel used for acquiring, processing, storing, transporting, controlling, and presenting information on demand to joint forces and support personnel. The GIG includes all owned and leased communications and computing systems and services, software and applications, data, security services, and other associated services necessary to achieve information superiority as defined in the Clinger-Cohen Act of 1996 (Sec. 5142). The GIG supports all war and peacetime DOD, national security, and related intelligence community missions and functions, including those of a strategic, operational, tactical, and business nature. The GIG provides capabilities from all operating locations, such as bases, posts, camps, stations, facilities, mobile platforms, and deployed sites. The GIG provides interfaces among multinational and non-DOD users and systems. For the purposes of the GIG, raw sensor data is not considered to be “information” until it is transported to the communications system or processing node and converted to a file format that can be used by an information consumer.

The GIG is evolving rapidly. This chapter focuses on the doctrine and general characteristics of the communications system portion of the GIG. The GIG interacts with and provides connections to both the national and global information infrastructures. The DOD’s strategy is to empower joint forces with the information needed to achieve successful military operations by integrating the seven components of the GIG described in this chapter. The GIG supports the JFC throughout the range of military operations. Offensive actions that affect an adversary’s information environment must be routinely explored and analyzed as a part of the full range of alternatives during the joint operation planning process.

Components

The seven components of the GIG are: warrior, global applications, computing, communications, network operations (NETOPS), information management, and foundation.

Warrior Component

The joint force is directly connected to the network by the GIG warrior component. The warrior component comprises computers, software, display devices, and radios that can be personal; shipboard; or track-, vehicle-, and aircraft-mounted. This equipment directly contributes to situational awareness, collaboration, and access to information critical to combat operations and the individual decisionmaker/shooter. All components of the GIG support the warrior component.

Global Applications Component

The global applications component is the set of information applications used by the joint force over the GIG. It provides the information needs of the force and includes applications for use in fire support, weather, logistics, medical, and business.

Computing Component

The computing component includes the automatic acquisition, storage, manipulation, management, control, and display of data or information. Its primary emphasis is on DOD enterprise hardware, software operation systems, and hardware/software support that enable the GIG enterprise. The DISA defense enterprise computing centers provide a significant portion of this support to the joint force.

Communications Component

The communications component provides common-user information, transport, and processing services to all DOD users. It extends from the local base post, camp, station, and ship, through the strategic networks, to the “first tactical mile.” To achieve this, Service frequency management offices work directly with combatant command frequency management offices to coordinate and negotiate the electromagnetic spectrum supportability of the communications components, such as electromagnetic spectrum dependent devices. The communications component includes a blend of DOD and commercial communications including satellite communications (SATCOM), global fiber, wireless, radio frequency nets, and standardized tactical entry point (STEP) sites that are evolving to more capable DOD teleports. The STEP/teleports connect the joint force to the Defense Information Systems Network (DISN) long-haul services to provide a reachback capability for DISN voice, data, and video services across all frequency bands. The DISN provides the JFC with the ability to access needed capabilities worldwide.

Network Operations Component

The NETOPS mission is to operate and defend the GIG. The NETOPS provides integrated, end-to-end management of networks, global applications, and services across the GIG. This management offers network visibility to enable commanders to manage their networks as they would other battle systems. The Global NETOPS command center provides worldwide network monitoring, contingency support, network crisis action support, network resolution management, and network GIG defense integration. United States Strategic Command (USSTRATCOM) executes DOD global network operations through the Joint Task Force-Global Network Operations (JTF-GNO). The USSTRATCOM JTF-GNO is collocated with the Global NETOPS command center.

The NETOPS component provides integrated network visibility and end-to-end management of networks, global applications, and services across the GIG and facilitates network enabled operations. Its goals are to provide assured system and network availability, assured information protection, and assured information delivery. The NETOPS operational construct consists of situational awareness, the essential tasks, and command and control.

The NETOPS is a supporting enabler in achieving shared situational awareness of the GIG system, network, and information availability. That support comes from the integrated capability to receive, correlate, and display a functional or theater-level view of systems and networks such as voice, video, and data. The primary purpose is to enhance knowledge of the GIG to collaboratively improve the quality and speed of decisionmaking with regard to the employment, protection, and defense of the GIG.

The JTF-GNO was established by the Commander, USSTRATCOM, to facilitate operating and defending the GIG. The JTF-GNO commands and controls the operation and defense of the GIG in support of the President, Secretary of Defense, joint staff, CCDRs, Services, and DOD agencies. It collaboratively conducts operations through a tiered construct of NETOPS centers.

The three joint mission-essential tasks of NETOPS (see fig. 3.1) are GEM [GIG Enterprise Management], GND [GIG Network Defense], and information dissemination management/content staging (CS). They are defined as follows:

- The GEM task is the technology, processes, and policy necessary to effectively operate the systems and networks that comprise the GIG. This essential task merges information technology services with the NETOPS critical capabilities.
- The GND task incorporates protection, detection, and response of any unauthorized activities against the GIG. It ensures data

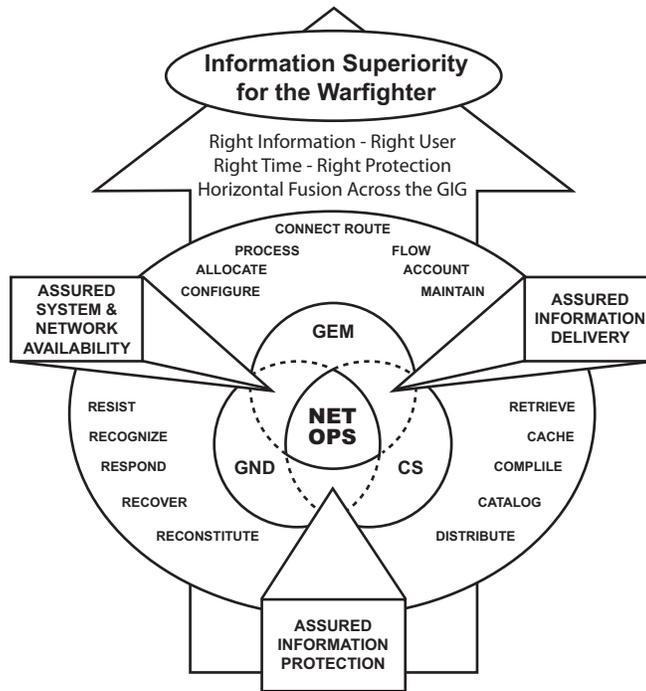


Figure 3-1. Joint Network Operations Essential Tasks.

quality and protection against unauthorized access and inadvertent damage or modification. The GIG Network Defense incorporates IA protection activities, computer network defense (CND), and critical information protection. Additionally, GIG constituent systems that meet the definition of a national security system must follow the appropriate IA guidelines and policies for national security systems. Other GIG systems not designated as national security systems must be provided adequate IA so as not to jeopardize the security of GIG national security systems.

- Information dissemination management/CS is the technology, processes, and policy necessary to provide awareness of relevant, accurate information; automated access to newly discovered or recurring information; and timely, efficient, and assured delivery of information in a usable format. As information dissemination management/CS become more mature, the complete complement of its services will be available for use by all authorized DOD GIG users as a network-enabled service. This

essential task merges core services with the NETOPS critical capabilities.

Information Management Component

The information management component provides relevant information to the right person at the right time in a usable format for situational awareness and decisionmaking. It allows the joint force to access needed data with appropriate permissions anywhere in the world, and dynamically tailor and prioritize their information requirements to support the mission and environment. Information management is facilitated by a variety of common information-sharing services such as messaging, discovery and delivery of information, collaboration, and directory services that are managed and assured through the NETOPS component.

Foundation Component

The foundation component includes doctrine, policy, compliance, architectures, testing, electromagnetic spectrum, and host nation approval. It

anchors and defines the GIG through policy and standards and provides the basis for an interoperable, secure, DOD-networked enterprise. The GIG integrates all DOD requirements—strategic, operational, tactical, and base/post/camp/station/shipboard—providing flexible, assured bandwidth regardless of environment.

Planning

The planning of GIG support of the JFC is a fundamental activity in the contingency and crisis action planning process. Planning has evolved from the traditional determination of numbers, types, and locations of communications system elements to a more comprehensive determination of the JFC's information needs.

The complexity of joint operations coupled with finite communications system resources may require the JFC to adjudicate or assign subordinate command responsibilities for extending the GIG's reach into an operational area. This assignment is normally done in an OPLAN; however, in the absence of such a plan, communication is planned and employed as follows: senior to subordinate, supporting to supported, reinforcing to reinforced, left to right, between adjacent units as directed by the first common senior, or by the unit gaining an attachment. This order is more common to ground forces, but it may have application to space, special operations, naval, and air forces as well. These rules are generally followed except when sound military judgment dictates otherwise.

Access Services

The DISN is the major element of the GIG. It has three segments: sustaining base, long-haul, and deployed. It is DOD's worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer for supporting military operations. For the most part, it is transparent to the joint force. The

DISN facilitates the management of information resources and responds to national security and DOD needs. It provides GIG network services to DOD installations and deployed forces. Those services include voice, data, video, and ancillary enterprise services such as directories and messaging. The DOD policy mandates the use of the DISN for wide-area and metropolitan networks.

In concert with military and commercial communications segments that support DOD missions, the primary interface point between the sustaining base and deployed forces is the STEP and its upgrade, the teleport. The STEP concept and program were designed to meet a specific requirement: the provision of prepositioned, sustainable DISN services. An equally important result of this upgrade to the DISN has been the improvement and standardization of the JFC's access to the DISN, which has facilitated interoperability.

The STEP program enhances the ability of the DISN to respond to the needs of the joint force. It provides predefined and tailored support packages on a predefined timeline. This support is extended via common user transports and includes voice, data, and video services. These services are extended directly to deployed naval forces and to each component of a JTF, if employed. Voice services include access to the Defense Switched Network (DSN) and the Defense Red Switched Network (DRSN). Data includes access to the SECRET Internet Protocol Router Network (SIPRNET) and the Non-Secure Internet Protocol Router Network (NIPRNET). Video services include access to DISN video services. It will also support the Joint Worldwide Intelligence Communications System (JWICS), a sensitive compartmented information (SCI)-level data, voice, and video services network.

Although the STEP concept was implemented globally under a single executive agent, JFCs and their staffs play important roles in STEP employment. Entry point access and procedures

are coordinated by the tactical communications system planners. Defense Information Systems Agency plays a major role in the planning process and uses regional contingency exercise planning branches and USSTRATCOM-operated global and theater NETOPS centers to facilitate that interaction with the joint force. The STEP concept has evolved to incorporate additional satellite connectivity through the teleport program. This connectivity provides greater flexibility when using DOD and commercial SATCOM resources. Flexibility, in this sense, does not imply additional bandwidth for the deployed joint force; however, quad-band terminals provide the joint force with more flexible means of SATCOM support.

The DOD teleport expands upon existing STEP capabilities by providing satellite connectivity to deployed tactical communications systems operating in the X-band, C-band, Ku-band, Ka-band, UHF, and EHF portions of the radio spectrum.

Voice Services

Defense Switched Network

The DSN is a standard, unclassified voice network supporting DOD.

Defense Red Switched Network

The DRSN is a classified voice network supporting DOD.

Enhanced Mobile Satellite Services

Enhanced Mobile Satellite Services are commercial, portable satellite systems, such as international maritime satellite (INMARSAT) or Iridium satellite, capable of voice and data transmission.

Tactical Voice

Tactical voice is a military-specific switching system capable of operating in austere areas.

Data Services

Joint Data Network

The joint data network (JDN) is a compilation of subnetworks comprised of a wide variety of data systems. These systems carry a broad range of tactical information on tactical digital information links within a theater in support of joint and multinational warfighting. These subnetworks are the multi-tactical data information link network, the ground network, the intelligence network, and the sensor networks. Information is passed over the JDN in real, near-real, and non-real time. The JDN is the primary feed to generate a common tactical picture. The common tactical picture enables command and control, situational awareness, and combat identification. Effective design and implementation of the multitactical data information link network are critical in managing the complexities of the electronic battlefield to improve the JFC's ability to engage hostile forces and prevent fratricide.

Non-Secure Internet Protocol Router Network

The NIPRNET is a computer network for unclassified, but sensitive information supporting DOD.

SECRET Internet Protocol Router Network

The SIPRNET is a computer network for classified information (up to SECRET) supporting DOD.

Coalition/Multinational Wide-Area Network

Coalition/multinational WAN is a computer network supporting the combined/multinational operations that may be unclassified or classified.

Joint Worldwide Intelligence Communications System

The JWICS is a computer network for classified information, including SCI, supporting DOD.

Applications

The following paragraphs discuss the Global Command and Control System (GCCS), the theater battle management core system (TBMCS), the defense message system (DMS), the Army Battle Command System (ABCS), and the Defense Collaboration Tool Suite (DCTS), which only represent a few of the available communications applications. There are literally thousands of applications in such areas as command and control, fire support, weather, logistics, medical, and business managed by various organizations supporting the JFC and DOD over the GIG.

Global Command and Control System

The GCCS is a suite of software applications and hardware designed for planning, execution, command and control of forces, and multidiscipline intelligence processing. The system receives multiple sensor feeds and reports that assist in the development of the common operation picture. Planning and execution applications also support supply, maintenance, transportation, acquisition, finance, personnel, engineering, and force health protection. As a system, it supports the Joint Chiefs of Staff and CCDRs through the JOPES [Joint Operation Planning and Execution System] in contingency and crisis planning.

Theater Battle Management Core System

The TBMCS is used by the joint force air component commander and other component commanders to collaboratively plan, direct, and control joint air operations in support of JFC objectives. This automated system facilitates the development, deconfliction, dissemination, and execution of the air operations plan, air tasking order, airspace control order, and air defense tactical operations data message. It also supports collaborative target management and force- and unit-level joint forces throughout all phases of

military operations. It is interoperable with other GIG systems including GCCS, ABCS, and Global Combat Support System/Command and Control Integrated Planning System. The TBMCS is used by the USAF, USN, and the Marine Corps.

Army Battle Command System

The ABCS is the Army's approach to automating its tactical C2 systems for component and joint operations. It is intended to give commanders from unit of employment to brigade/brigade combat team and below a common operational picture of the battlespace and to facilitate synchronization of combat forces in joint environments. The ABCS consists of several major warfighting functional C2 systems intended to improve interoperability among Army, joint, and multinational forces. The subsystems include the Maneuver Control System, Force XXI Battle Command Brigade and Below, the Forward Area Air Defense Command and Control System, the All Source Analysis System, the AFATDS [Advanced Field Artillery Tactical Data System], and the Combat Service Support Control System.

Defense Message System

The DMS is a secure system for transmission of record message traffic in support of DOD. Critical systems supporting command and control may be designated for DMS applications in support of specified message handling functions. The DMS high grade service has replaced the Automated Digital Network as the organizational message system of record. Its high-grade service allows joint forces to communicate and share information quickly and securely with any DOD or intelligence community organization using inherent global directory services.

Defense Collaboration Tool Suite

The DCTS is a DOD tool suite for interoperable collaboration. It provides combatant commands, Services, and agencies with an interoperable,

real-time asynchronous collaboration capability that includes voice and video conferencing, document and application sharing, instant messaging, virtual meeting, and whiteboard capability in support of DOD planning.

Video Services

Defense Video Teleconferencing System – Global

The video teleconferencing (VTC) system is a classified, closed video network capable of voice, image, and data exchange supporting C2 functions of DOD.

Sensitive Compartmented Information-Level Video Teleconferencing

The SCI-level VTC is a classified, closed video network capable of voice, image, and data exchange. It supports intelligence and C2 functions of DOD and is typically carried over the JWICS network.

Commercial News Feed

Commercial news feeds may be rebroadcast over the DOD communications system or received via a commercially leased terminal in support of C2 functions.

Satellite Communications Services

The SATCOM systems normally consist of three segments:

- The space segment includes military or leased commercial satellites.
- The ground segment includes fixed and deployable terminals.
- The control segment includes hardware distributed among control centers, satellites and terminals, and software to evaluate the status of

the system stations. This software is capable of monitoring, operating, and positioning the satellite; near real-time allocation of satellite power; antenna orientation/nulling; and terminal monitoring and control.

The DOD SATCOM architecture is flexible and adaptable. Current investment strategies attempt to find the right mix between DOD-owned and commercially-leased services, while balancing mobility, survivability, capacity, and assured access. Emphasis is focused on using SATCOM to support the deployed joint force by providing reach-back to the sustaining base portions of the GIG. In addition to these needs, SATCOM also supports a broad range of other missions and C2 requirements.

The SATCOM provides instant global reach to widely-dispersed, small, and mobile forces. It covers polar, open ocean, and remote areas of the world and has a nuclear-survivable component with appreciable capacity. The SATCOM supports a wide range of narrowband/wideband services for voice, data, video, and paging and is especially well suited for netted and broadcast services. It keeps en route forces and support systems supplied with critical information while deploying into an operational area. The SATCOM can immediately tie sensors to shooters and provide beyond line-of-sight (LOS) control of remote sensors and remote or in-flight weapons. It is also essential to intelligence and diplomatic communities, providing worldwide transmission of critical intelligence data and sensitive diplomatic traffic over communications paths that remain under the direct control of the United States, especially during times of political tension or crisis.

While it is clearly desired that DOD take full advantage of the commercial sector's capabilities and offerings when it is affordable, not all communications needs can or should be met by commercial means, especially in an unpredictable threat environment. There is an enduring need for DOD-owned SATCOM because military and commercial communications needs and uses are not convergent. Specific military needs

include nuclear survivable and antiscintillation communications, antijam or covertness, globally assured and immediate access, and netted voice and data. In some cases, commercial SATCOM coverage is not available over the objective area nor is it available for lease. Additionally, the military's need to support rapid deployment of large infrastructure contrasts sharply with the relatively static commercial environment.

There is, however, a genuine need for military use of commercial SATCOM. Its access to advanced capabilities of future commercial systems will provide faster access to new technologies or services. There is little DOD infrastructure needed to build or maintain access to commercial systems, which results in reduced acquisition, operations and maintenance, and manpower investment. Along with these efficiencies, DOD benefits by only acquiring commercial capacity as it is needed.

The SATCOM resources are inherently flexible and well suited to supporting mobile operations. They provide the global reach necessary for DOD's global mission. Some of the advantages of the GIG's SATCOM architecture are the inherent ability to share resources over large geographic areas by individual satellites, the ability to provide worldwide or nonpolar global coverage with a few assets, the capability to quickly service isolated areas, and the ability to extend new LOS communication to mobile platforms rapidly. Currently, the three main subcomponents of the GIG's SATCOM architecture are wideband, protected, and narrowband services. Commercial services augment military wideband and narrowband services.

Wideband

Wideband services providing high-capacity and broadcast communications coverage to meet increasing demands for information include military-owned and commercially-leased satellite systems. Military-owned wideband systems include the Wideband Global Satellite Communications (WGS) System, the Defense Satellite Communications System (DSCS), and the Global Broadcast System (GBS).

WGS

The WGS supports DOD's warfighting information exchange requirements, enabling the execution of tactical C2, battle management, and combat support information. It also augments the existing GBS by providing additional information broadcast capabilities. The wideband global SATCOM system comprises space, terminal, and control segments. The WGS satellites support communication at X-band and Ka-band with an onboard channelizer. The channelizer supports the cross-banding of uplink/downlink signals and establishes signal paths among a dispersed user community that may be deployed across multiple coverage areas. The WGS provides 4.875 GHz of instant switchable bandwidth, supplying more than 10 times the capacity of a DSCS III Service Life Enhancement Program satellite. The first WGS satellite was launched in October 2007.

DSCS

The DSCS provides a GIG transmission backbone of high capacity C2, intelligence, and multichannel communications service for CCDRs, Services, and agencies. Although not formally considered part of the architecture's protected communications capabilities, DSCS has a credible antijam capability with sophisticated satellite survivability features. The satellites are nuclear-hardened, providing secure voice and high data rate, long-haul, worldwide communication. The DSCS satellites support deployed forces and ships.

GBS

Global Broadcast System is a DOD program for wide-area broadcast of commonly shared information. It is capable of providing a wide range of video and data services on a broadcast-only basis to widely dispersed elements. Critical nodes are typically receiving terminals in support of designated C2 operations, but may include in-theater injection, or transmission points. The GBS provides a high-capacity, near-worldwide, military-owned SATCOM broadcast capability for dissemination of information products. The broadcast signals are transmitted to a large inventory of

user-receive units worldwide. This capability makes possible a high data rate bit stream of video, data, imagery, and other information from high-powered broadcast satellites to a large section of the force structure and numerous warfighting platforms. The broadcast is transmitted from a limited number of fixed and deployable injection terminals controlled by the CCDRs and managed by a broadcast management segment in each satellite field of view. The information being transmitted is collected from numerous sources and packaged for broadcast injection by the satellite broadcast manager or theater injection points. The CCDR theater information managers nominate and monitor CCDR priorities, authorize user access, coordinate broadcast schedules, and allocate resources. The three primary injection points support the Pacific, European, and Central Command theaters.

Commercial Wideband Services

Commercial wideband services are procured by DISA under such contract vehicles as the Managed Transponder Contract and the DISN Satellite Transmission Services-Global. All Services and agencies are required to procure their long-haul communications services through DISA unless a waiver is granted by the Office of the Secretary of Defense. Currently, the DISN Satellite Transmission Services-Global contract can provide—

- Fixed satellite bandwidth.
 - Bandwidth and service management.
 - Leased earth terminal services.
 - Purchased earth terminals, if approved by Army Communications-Electronics Command.
 - Global on-site earth terminal operation and maintenance.
 - Commercial teleport services.
 - US and foreign bandwidth and terminal licenses and approval.
 - Terrestrial interconnection services to support satellite service.
 - Host nation agreement-negotiating support.
- Systems-engineering support.
 - First right of refusal and guaranteed reservations.
 - DISN common-user hub services.
 - Multiple location turnkey satellite systems.

Protected Services

Protected and survivable services provide anti-jam, nuclear-survivable, low probability of detection (LPD), low probability of intercept (LPI), and exploitation of communications capabilities. These military-owned and operated systems include the Advanced Extremely High Frequency (AEHF) System, the Air Force satellite communications (AFSATCOM) system, the military strategic and tactical relay system (Milstar), and the Interim Polar System (IPS).

AEHF

The AEHF system is a joint service satellite communications system that provides global, secure, protected, and jam-resistant communication for high-priority military ground, sea, and air assets. The system consists of 4 satellites in a geosynchronous earth orbit that provides more than 10 times the capacity of the legacy Milstar satellites. Advanced EHF allows the National Security Council and unified CCDRs to control their tactical and strategic forces at all levels of conflict through general nuclear war and supports the attainment of information superiority. The AEHF system provides communication across a specified set of data rates from 75 bps to approximately 8 Mbps. The space segment consists of a cross-linked constellation of satellites. Each AEHF satellite responds directly to service requests from operational commanders and user terminals, providing real-time, point-to-point connectivity and network services on a priority basis. The AEHF system is backward compatible with Milstar's low data rate and medium data rate capabilities, while providing extended data rates and larger capacity.

AFSATCOM

Air Force satellite communications payloads, intended for nuclear wartime communication, are hosted on a variety of satellites providing global coverage. Some DSCS satellites accommodate an enhanced single-channel AFSATCOM payload as an alternative path for emergency action message dissemination and force direction. Other AFSATCOM payloads include Package-D and Satellite Data System payloads on hosts providing polar capabilities. The AFSATCOM constellation has outlived its planned life expectancy; therefore, most AFSATCOM users are migrating to Milstar.

Milstar

Milstar is designed to support strategic and tactical missions through secure global communications systems that are jam-resistant and survivable with LPI and LPD. It supports both single-channel and multichannel communication with low data rates from 75 bits per second up to 2.4 kilobits per second (Milstar-I). It supports medium data rates up to 1.544 megabits per second (Milstar-II). Crosslinks between the satellites permit worldwide communication without the use of ground stations. The use of EHF frequencies provides for narrow antenna beams for LPD and antijam capability. Additionally, EHF frequencies provide wide bandwidths for nuclear effects mitigation and antijam capability. Both wide and narrow spot beam satellite antennas provide appropriate power levels for a variety of user terminals. Milstar is the core DOD C2 communications system for US strategic and tactical combat forces in hostile environments. Additionally, some small-scale EHF payloads are hosted on some fleet satellite and ultrahigh frequency follow-on (UFO) satellites to provide a contingency/surge capability for strategic and tactical users.

IPS

The IPS provides EHF low data rate (75 bits per second to 256 kilobits per second) communication to users above 65 degrees north latitude. It

supports combatant commands and North Atlantic Treaty Organization (NATO) missions with C2, DISN, and essential targeting information.

Narrowband Services

Narrowband and mobile services provide phone and data transfer capability for netted, mobile, hand-held, paging, and low speed broadcast. Some of the GIG's key systems in this category include military-owned Mobile User Objective System (MUOS), UFO, fleet satellite communications (FLTSATCOM), and commercially-available mobile satellite services, such as Iridium and INMARSAT.

MUOS

The MUOS is the narrowband military satellite communications component that will replace the existing UFO constellation. Its primary user community will be the air, land, and maritime tactical warfighter who is typically on-the-move, beyond-line-of-sight, in difficult terrain conditions, and using small, disadvantaged terminals. In order to satisfy increases in UHF SATCOM requirements, MUOS will provide "bandwidth-on-demand," which is the ability to dynamically allocate the system's throughput capacity to users only when required.

Each MUOS satellite will contain two communications payloads: a legacy UFO payload and an advanced Wideband Code Division Multiple Access payload. This design was chosen to allow continued use of legacy terminals and to enable a gradual transition from legacy UHF SATCOM to Wideband Code Division Multiple Access communications. The legacy payload will support all legacy UHF SATCOM waveforms including integrated waveform, which will more efficiently use the on-orbit 5/25 kilohertz channels. As an end-to-end capability, MUOS comprises three interdependent, but separately procured, systems: the MUOS satellites and ground support infrastructure; the teleport, such as the DISN interface; and the Joint Tactical Radio System. The MUOS is

scheduled to achieve initial operating capability in 2010, with a final operating capability in 2014. Complete constellation consists of four primary satellites and one on-orbit spare.

UFO and FLTSATCOM

The UFO and FLTSATCOM systems provide small, lightweight, low-cost user terminals that can be used while on the move, under adverse weather conditions, and in dense foliage. However, these UHF systems yield low data rates and are susceptible to both detection and jamming. Limited numbers of channel accesses available, coupled with limited earth coverage satellite beams, result in competition for access over wide geographic areas. This competition requires adjudication at the highest levels within DOD.

INMARSAT

The INMARSAT, a commercial SATCOM service, provides bulk use and pay-per-use alternatives that support information transfer requirements during both normal operations and periods of contingency or crisis. The INMARSAT does not provide the survivability, LPI, or antijam capabilities required in tactical applications. It may be subject to electromagnetic interference, jamming, or intrusion.

Iridium

Iridium, also known as Enhanced Mobile Satellite Services, provides secure and nonsecure voice and data services to DOD tactical and nontactical users. Although Iridium is considered a commercial SATCOM service, DOD has procured and installed an Iridium gateway that provides direct connection to DSN and NIPRNET services. The DISA has contracts in place from which DOD and other US Government users can obtain service.

Trojan

The Trojan network is the primary tactical extension of the JWICS network. The system consists of secure voice, data, facsimile, video,

and secondary imagery dissemination capabilities. The system receives, displays, and transmits digital imagery, weather and terrain products, templates, graphics, and text between bases and deployed forces within and outside the continental United States.

Management of the Global Information Grid

The USSTRATCOM has overall responsibility for global network operations and defense in coordination with the Chairman of the Joint Chiefs of Staff (CJCS) and the other combatant commands. Because the GIG represents the entire DOD communications system, there remain many decisions regarding planning and design that fall under the purview of the Assistant Secretary of Defense (Networks and Information Integration) (ASD[NII]), who is also designated DOD's chief information officer (CIO). Many of those decisions involve the insertion of new technology as well as various other architectural standards, which may impact DOD's interoperability.

Global Information Grid Configuration Management Responsibilities

The GIG is essentially a global DOD federation that combines the specific communications system capabilities of DOD components. Operation and defense of the GIG is largely a matter of overarching common processes, standards, and protocols orchestrated by USSTRATCOM. The purposes of this framework are to govern common activities by all subscribers, deal with competing demands for service, and solicit essential joint force support from relevant agencies.

Department of Defense Chief Information Officer Responsibilities

The DOD CIO ASD(NII) is responsible for developing, maintaining, and enforcing compliance with the GIG architecture. Inherent in the CIO's architecture responsibility is enforcing

interoperability, sharing IA network-centric data, using enterprise services, and synchronizing the GIG program.

Uniform configuration management of the GIG ensures interoperability and survivability of the DOD information infrastructure. In addition to the expected adherence to DOD policy, GIG configuration is controlled through compliance with GIG architecture. The GIG assets, including commercial off-the-shelf, are to be configured in accordance with approved capabilities documents and standards and compliant with the operational, system, and technical views of the GIG's architecture. DOD has created various forums to assist the CIO and the CJCS in compliance determination.

Operational assets are also uniformly configured to ensure architecture standards compliance, INFOSEC, operational effectiveness, efficiency, and quality of service across the GIG. Configuration control boards are often used to determine and regulate actual communications system configurations. The theater joint tactical networks (TJTNs) configuration control board seeks to coordinate initiatives and the fielding of software and hardware products associated with the deployed networks of the GIG. The Army is the Executive Agent for TJTNs. Together with the TJTNs configuration control board, the Army oversees and coordinates development and life-cycle enhancement of the theater-deployable networked communications system. They do this to achieve DOD compatibility, interoperability, and integration objectives for systems composing the TJTNs. The ASD(NII) participates in an advisory capacity.

Chairman of the Joint Chiefs of Staff and Other Agency Responsibilities

The CJCS, DISA, and the Services ensure that commanders at each echelon have the necessary capabilities to employ the GIG to accomplish their assigned missions (DOD Directive [DODD] 5105.19, *Defense Information Systems Agency [DISA]*). According to Chairman of the Joint Chiefs of Staff Instruction 6211.02B, *Defense*

Information Systems Network (DISN): Policy, Responsibilities, and Processes, the CJCS is responsible for operational network policy and overall direction of the DISN as DOD's primary and global provider of GIG joint information services and information systems. This oversight responsibility does not imply command authority and is executed and facilitated through the assistance of the National Military Command Center and USSTRATCOM's Global NETOPS C2 structure.

The non-DOD intelligence community agencies retain command and control of their respective networks and assets, which interface with the GIG in support of warfighting and other national interests. They interface at the SCI level via JWICS, in compliance with the guidance and directions of the Director, Central Intelligence Agency. The GIG networks are controlled within a tiered management hierarchy consisting of global, regional, and local control centers to enable a survivable, flexible, and disciplined C2 capability for DOD's GIG.

The JTF-GNO has, in some theaters, established theater NETOPS centers to provide a single POC for theater network services, operations status, and communications system anomalies. These control centers also serve as a central POC for operational matters in support of a geographic CCDR. In some theaters, CCDRs have established a theater NETOPS control center or equivalent organization, as an adjunct to the joint operations center, to gain network situational awareness and to assess operational impact when network anomalies arise. These organizations interface with component control centers within the theater. At the joint force level, the J-6 establishes a joint network operations control center to manage and control joint networks. Another local control center in the GIG operational hierarchy, it also interfaces with Service component control centers in the operational area. The grid's assets of the combatant commands, Services, and agencies are configured generally to meet the requirements of the command being served; however,

the priority requirement is to support the National Military Command System. The GIG assets of a combatant command also include the GIG assets of subordinate unified commands and JTFs when such organizations are established, assigned, or attached.

Combatant Commander Responsibilities

Regardless of the source, GIG resources assigned to CCDRs operate under their combatant command (command authority) (COCOM) and are an integral part of their C2 system until such time as the President, Secretary of Defense, or the CCDRs determine that further support is no longer needed or a higher priority necessitates redeployment of the assets. The command authority and responsibilities of the CCDRs include control, review, and coordination of assigned GIG resources and actions affecting such resources within the CCDRs' areas of responsibility (AORs).

Combatant commanders coordinate and direct NETOPS activities consistent with USSTRATCOM guidance to ensure the availability and protection of the GIG. Geographic CCDRs have the authority to change information operations conditions (INFOCONs) within their AORs. Functional CCDRs have the authority to change INFOCONs for the unique systems and networks supporting their mission areas. Local commanders on bases, posts, camps, stations, or vessels have the authority to change INFOCONs for their information systems and networks.

The CCDRs normally develop plans that integrate the DISN, National Communications System (NCS), and commercial and multinational systems. They organize joint and Service organic and component tactical GIG assets into interoperable and compatible theater networks to support their missions. As a part of their planning, CCDRs determine priorities for information flow and allocate network resources, such as bandwidth, within the AOR of their commands and

those required by component and other subordinate commands. The CCDRs oversee their theater portion of the GIG through their support relationship with DISA regional offices and those forces assigned to them in the Secretary of Defense's "Forces for Unified Commands" memorandum, or as modified by deployment orders. Operating elements of the DISN are subject to authoritative direction from different sources because of ownership.

However, in accordance with DODD 5105.19, DISA field organizations, under the command of the Director, DISA, exercise operational direction over the DISN operating elements. This operational direction is the authoritative direction necessary to ensure the effective operation of the DISN. Directors of DISA field organizations and Service component commanders, though, will be responsive to the operational needs of the CCDRs, who exercise COCOM over the Service component operating elements of the DISN. The CCDRs develop agreements that clearly delineate the commanders' relationships with the DISA field organizations within their AORs.

In exercising COCOM, the CCDRs are cognizant of DISN support to the President and the Secretary of Defense, DOD agencies, and other CCDRs. They preserve DISN integrity and standards to the maximum possible extent. With respect to the DISN, DISA coordinates and controls the provision of network services across the DISN transport network and service delivery points or demarcation lines associated with the ownership and subsequent technical control of GIG resources, in accordance with CCDR requirements. The CCDR planners must acknowledge the highly integrated nature of their theater network as a part of the GIG. Consequently, development of communications system annexes to their campaign plans and OPLANs requires close coordination among their components, including DISA field operating commands, to ensure interoperability among forces.

Electromagnetic Spectrum Management

Critical to success in communications system support to joint operations is DOD electromagnetic spectrum management. Electromagnetic spectrum management is a specialized area that relies heavily on systems engineering support and modeling to ensure electromagnetic spectrum-dependent systems are mission-ready and compatible with the intended electromagnetic environment. It is DOD's responsibility to obtain, control, and ensure the effective and efficient use of the electromagnetic spectrum through the development of policy, practices, and procedures.

Joint electromagnetic spectrum operations apply DOD electromagnetic spectrum management functions of electromagnetic spectrum operations, electromagnetic spectrum supportability, and strategic management of the electromagnetic spectrum. Each of these functional areas must abide by international, national, and military electromagnetic spectrum laws, regulations, and policies. The functional areas must take into account other existing and planned electromagnetic spectrum-dependent systems and the environmental attributes of the intended operational areas.

Strategic management of the electromagnetic spectrum requires national and international long-term planning of strategies, policies, practices, and procedures. This planning is for the expressed purpose of obtaining and maintaining necessary access to electromagnetic spectrum and capital investments of electromagnetic spectrum-dependent systems.

Electromagnetic Spectrum Operations

Electromagnetic spectrum operations consist of electromagnetic spectrum operational planning and frequency management:

- Electromagnetic spectrum operational planning is the ability to proactively combine military forces' electromagnetic spectrum-dependent systems in support of the commander's

mission, so that the mission can execute free of unintended friendly or harmful interference.

- Frequency management comprises requesting, recording, deconflicting, and authorizing the use of frequencies or operation of electromagnetic spectrum-dependent systems. Frequency management also includes monitoring and interference resolution processes.

Electromagnetic spectrum supportability is an engineering process that is focused on the development of technologies that match electromagnetic spectrum attributes with desired system(s) characteristics. Equipment and systems certification and host nation coordination processes are considered part of electromagnetic spectrum supportability. The goal of electromagnetic spectrum supportability is to provide functional electromagnetic-compatible systems in support of combatant command missions. To facilitate these functional areas, DOD electromagnetic spectrum management is comprised of two primary activities: national defense electromagnetic spectrum management and joint electromagnetic spectrum operations. Both of these, to varying degrees, apply elements of strategic management of the electromagnetic spectrum; electromagnetic spectrum operations, including electromagnetic spectrum operational planning and frequency management; and electromagnetic spectrum supportability.

National Defense Electromagnetic Spectrum Management

National defense electromagnetic spectrum management comprises those activities carried out by the national defense electromagnetic spectrum management establishment, which includes the Office of the Secretary of Defense, joint staff, combatant commands, Military Departments, DOD agencies, and others. It is oriented toward the planning, programming, budgeting, and execution activities for electromagnetic spectrum within DOD and national and international electromagnetic spectrum legal, regulatory, and policy coordination.

Joint Electromagnetic Spectrum Operations

Joint electromagnetic spectrum operations are those activities in the joint warfighting arena carried out by joint electromagnetic spectrum operators, who include combatant command staffs, the JTF, and others. Their objective is to plan and

execute joint or multinational operations across the operational environment successfully. Assured access to the electromagnetic spectrum and compatibility are key enablers to joint or multinational mission success and the focus of joint electromagnetic spectrum operations.

CHAPTER 4

MAGTF C2

What is MAGTF C2?

As the premier expeditionary total force in readiness, the Marine Corps requires a robust C2 capability to execute actions across the range of joint and coalition military operations. This capability increases strategic agility, operational reach, and tactical flexibility. MAGTF C2 enhances lethality and effectiveness across the range of military operations through better decisionmaking and shared understanding. It is an intuitive and holistic environment of people, processes, and technology enabling network centric operations throughout the enterprise and empowering the initiative of warfighters at all levels in the context of the commander's intent. It is a strategy to harmonize all aspects of command and control concepts, requirements, training, and doctrine; an integrating process to provide governance over the C2 community to ensure that it meets the objectives of the strategy across the enterprise; and a capability that will provide common, modular, and scalable material solutions from the lowest tactical level across the MAGTF at all echelons.

MAGTF C2 is the strategy by which the Marine Corps implements the ideas in *Command and Control Joint Integrating Concept*, *Net-Centric Operational Environment Joint Integrating Concept*, and *FORCEnet: A Functional Concept for the 21st Century*. It is the functional and conceptual equivalent to other Services' network centric concepts, such as the Army's LandWarNet and the Air Force's C2 Constellation. The Marine Corps is fully engaged with the development of the joint command and control (JC2) and network centric concepts to ensure that Marine Corps

requirements are fully considered and that Marine Corps programs align to these concepts. The Marine Corps is currently involved in the development of C2 concepts with the other Services to ensure that MAGTF C2 is fully employable in the littorals, from the air, on land, and at sea. The ability to engage in the joint arena and to function effectively within the labyrinth of interdependencies that exist is of key importance. Integrated with formal alliances such as NATO, MAGTF C2 facilitates command and control within less formal coalitions.

Creating networked capabilities is the basis of the MAGTF C2 approach to commanding and controlling Marine forces. Every node in the network—commander, staff, unit, rifleman, supporting organization, platform, piece of equipment, or item—can be a producer, processor, and user of information. All information must be readily available to nodes without overloading or paralyzing them with irrelevant information. Further, many of the nodes in the network are required to perform multiple functions, so the essence of MAGTF C2 is decentralized and highly adaptive. It uses the digital, global network to foster and exploit the human capacity for mutual understanding, implicit communication, and intuitive decisionmaking. The cumulative network effect, achieved by organizing all nodes into an information-rich, collaborative, global network, is expected to enhance these inherently human qualities. The goal of MAGTF C2 is to ensure that the entire Marine Corps and its supporting elements become nodes in the network that can share information seamlessly and attain true, end-to-end capability, fundamental to the future network centric environment.

Future MAGTF C2 will provide its capabilities from the sea base. Within the construct of the FORCEnet functional concept and MAGTF C2, the sea base is a node within the larger network that can produce, process, and consume information in support of C2 functions. In strategic and operational terms, seabasing, as one of the three key pillars of *A Cooperative Strategy for 21st Century Seapower*, serves as the foundation from which offensive and defensive fires are projected, making the two companion concepts of sea strike and sea shield realities. In direct support of Marine Corps concepts such as operational maneuver from the sea, seabasing accelerates expeditionary deployment and employment timelines by prepositioning vital equipment and supplies in-theater, preparing the United States to take swift and decisive action during crises. Seabasing capabilities include providing Marine Corps and JFCs with global command and control and extending integrated logistical support to other Services. Afloat positioning of these capabilities strengthens force protection and frees airlift-sealift to support missions ashore.

Commander centric, MAGTF C2 enhances the ability of commanders at all levels to gain and maintain situational awareness and shared understanding, to make better decisions at an increased tempo, and to exercise authority through commander's intent and mission-type orders. It facilitates planning and execution by providing the warfighter with distributive and collaborative planning tools. It also provides an accurate, user-defined, fused, common operational picture of the battlespace to facilitate more rapid decisionmaking through increased situational awareness and shared understanding. The intent is to increase freedom of action and small unit initiative through decentralized command and control while minimizing the requirement for specified and implied linear control measures that limit the initiative of subordinates in a complex and increasingly ambiguous battlespace.

To exploit the power of the network centric environment is also to consider the potential needs levied by operations in an austere battlespace, or when disconnected from the network. All Marine operations must be equally capable of operating either within the GIG or without the benefit of its full range of services. As a result, it is critical to ascertain the proper balance between GIG services and organically deployable networking capabilities.

As stated in the *Marine Requirements Oversight Council (MROC) Decision Memorandum (DM) 29-2005*, MAGTF C2 includes both C2 and communications systems that provide "end-to-end, fully integrated, cross-functional, reachback as well as a deployed set of C2 capabilities." Therefore, MAGTF C2 is an all-encompassing system of systems, which includes families of systems in layers that aggregate applications, enterprise services, network services, and transmission service capabilities (MROC DM 39-2004).

To maintain the superiority of these MAGTF C2 capabilities, the Marine Corps must have a plan to continually integrate new and proven technologies as they become viable and affordable. Often, these solutions only become apparent during ongoing operations, so the plan must allow the Marine Corps to leverage technologies in the near-term with a consistent, repeatable process that will continue to meet the long-term goals of interoperability and cross-functional integration.

The increasing numbers of C2 support systems that are not integrated place an ever increasing burden on the time and funding required for operations, maintenance, and training. These burdens impact the ability of the Marine Corps to support troops on the front lines as it transforms to meet the challenges of the future. Two of the key near-term goals of MAGTF C2 are to reduce the operating and maintenance requirements of C2 systems and to support the overall transformation of DOD.

MAGTF C2 Capabilities

Today's MAGTF commanders have access to a wide range of nonstop, in-depth information produced by a variety of human and machine collection nodes. The commander has access to so much information that it is difficult to sort out the key decisions that need to be made. The explosion of information is due, in large part, to the rapid technological advances that continue to provide more and more complex data gathering and correlation capabilities. The MAGTF C2 operation must manage this flow of information so the commander gets only the information needed to be effective, but also has access to the wider information flow when required.

Marine Corps C2 consists of the means and methods by which a commander recognizes what needs to be done in any given situation, and then sees to it that appropriate actions are taken. Further, the foundations of Marine Corps C2 are rooted in the warrior ethos and warfighting philosophy of expeditionary maneuver warfare. When pursuing MAGTF C2, however, the term "command" refers to all of the functionality that supports the commander's contribution to the planning phase and his decisionmaking processes from pre-deployment planning to execution and redeployment. Regarding "control," MAGTF C2 captures feedback—the continuous flow of information about the unfolding situation—returning to the commander. This philosophy imbeds captured feedback into all planning, execution, and specified or implied reporting functionality.

Effective and timely decisionmaking using C2 and communications systems is one of the primary

objectives of MAGTF C2. The MAGTF structure assures unity of command and facilitates the full integration of air, ground, and logistic operations in support of the commander's overall mission. The scope of MAGTF C2 requires providing the capabilities necessary for the full range of Marine Corps operations: joint and multinational enabling, strategic agility, operational reach, tactical flexibility, and support and sustainment. The MAGTF C2 capabilities must be developed across the following areas:

- The fully scalable MAGTF, from MEF to MEU, including units such as distributed operations platoons and individual fire teams.
- All warfighting functions—command and control, fires, maneuver, intelligence, logistics, and force protection.
- Quadrennial Defense Review quadrants—traditional, irregular, catastrophic, and disruptive.
- Levels of warfare—strategic, operational, and tactical.
- Joint and multinational involvement—USAF, USA, USN, alliance, coalition, multinational, interagency, joint force component, and special operations forces.
- Operational phases of warfare—planning, deterrence, employment, execution, and redeployment.
- The expansion of MAGTF C2 to include the nonwarfighting or business operations of the Marine Corps will likewise require greater exploitation of the network, integration of additional processes, and vastly improved interoperability.

Commander Centric

Marine Corps command and control is commander centric. Command and control is essentially about people; the system exists to facilitate the needs of its users. According to MCDP 6, *Command and Control*, “An effective command and control system must account for the characteristics and limits of human nature and at the same time exploit and enhance uniquely human skills. At any level, the key individual in the command and control system is the commander who has the final responsibility for success.” The MAGTF C2 system supports the individual styles of commanders with the flexibility and adaptability necessary to enhance their skills and accommodate their preferences.

Marine leaders use MAGTF C2 to issue broad mission intent, and then maintain “control” through improved situational awareness and shared understanding. A shared appreciation of the situation is supported by common information that enables rapid collaborative maneuver, engagement, and support. The fog of war can never be eliminated, nor will it ever achieve perfect clarity. Therefore, the aim of MAGTF C2 is to empower Marine Corps leaders at every level to make more effective decisions despite this uncertainty by focusing resources upon a mission and enabling the creativity and initiative of subordinates.

Network Centric

As described in the DOD Office of Force Transformation’s *Network Centric Operations Conceptual Framework* document, the United States is facing an unprecedented transformation in its national security landscape that has been accelerating over the past decade. With the decline of traditional peer adversaries has come the rise of new irregular threats and enemies, capable of carrying out attacks such as those of September 11, 2001.

In addition to these irregular threats, the US military is also widely engaged across the globe in foreign humanitarian assistance, peace enforcement, and foreign military assistance missions.

As Marine Corps operations in Afghanistan, Iraq, and the January 2005 post-tsunami operations in Southeast Asia demonstrated, there is a growing need to transform MAGTF C2, warfighting, and other business functions into a network centric environment. This is necessary to implement electronic and streamlined processes that allow decisions to be made rapidly, transparently, and across disparate platforms, systems, and domains.

The Marine Corps has always defined itself in terms of the capabilities it provides, rather than the specific mission Marines are deployed to accomplish. So far, this self-perception has enabled the Marine Corps to be relatively agile in transforming to meet the changing strategic landscape, as defined by the Quadrennial Defense Review released in 2006. However, this holds critical lessons for the development of MAGTF C2 information technology programs. To avoid obsolescence and irrelevancy, these programs need to be defined in terms of capabilities rather than around specific missions or threats.

A robustly networked force uses network centric warfare to improve information sharing and collaboration and enhance the quality of information and shared situational awareness. This capability enables further collaboration and self-synchronization and improves sustainability and speed of command, ultimately resulting in dramatically increased mission effectiveness.

Figure 4-1 depicts how network centric operations increase command and control and force agility. When Information Age technologies are paired with transformational changes in organizations and processes, dramatic improvements in effectiveness can be achieved. These improvements can

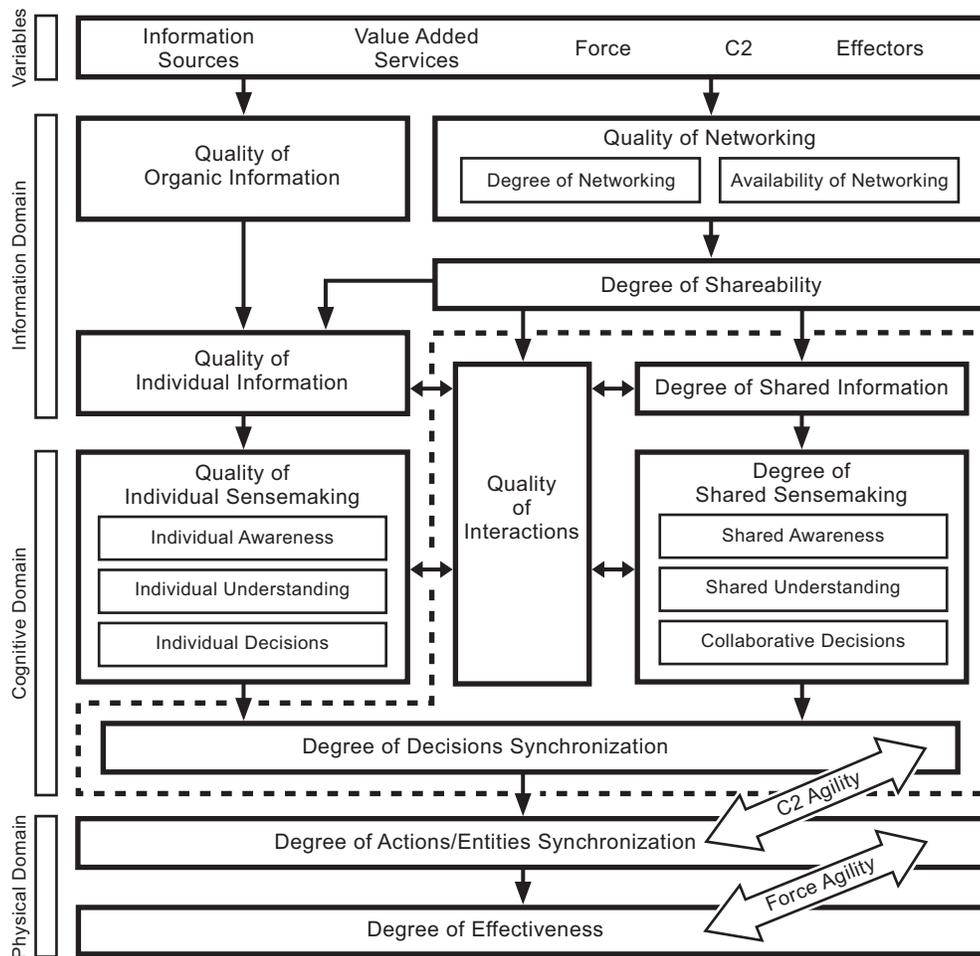


Figure 4-1. Framework for Network Centric Operations.

be applied in any operational environment and across different warfare levels—tactical, operational, and strategic—because mission effectiveness is greatly enhanced by agility and the ability to be quick, nimble, adaptive, responsive to changing circumstances, and innovative problem-solvers on demand.

Integrated

Marine Corps Strategy 21 states, “Marines instinctively understand the logic and synergy behind joint and multinational operations. Based on our experience operating as combined-arms, multidimensional MAGTFs, Marines seamlessly integrate into and operate as part of a joint or

multinational force.” However, the growing number of C2 and communications systems that are not integrated place an increasing burden on the Marine Corps for both time and funding required for operation, maintenance, and training. These burdens impact the ability of the Marine Corps to support troops on the front lines at the same time as it transforms to meet the challenges of the future. Two of the key near-term goals of MAGTF C2 are to reduce the operating, maintenance, and training requirements of C2 systems and to support the overall transformation of DOD.

Joint concepts describe the capabilities that military forces must acquire or exhibit in future

operations, and they serve to guide capability development toward an end state of integrated people, processes, and technology. For MAGTF C2, the joint command and control and FORCEnet concepts provide the primary guidance for developing new capabilities. Communicating closely with other Services and their respective C2 systems commands will help ensure that MAGTF C2 is well integrated into the next generation of JC2 initiatives.

Supportive of Command and Control Principles

While command and control is complex, it contains a number of timeless principles. These must be recognized and understood within any future concepts, including MAGTF C2. They include the following:

- Command and control is always commander centric. Its purpose is to give the commander the best possible understanding of the situation, support effective decisionmaking, ensure effective implementation, and provide feedback on the progress of the operation.
- Command and control always occurs in an operational environment. The operational environment consists of several connected elements—both physical, such as terrain and weather, and social, such as the political and economic environment.
- Every military organization’s mission operates within rules of engagement. Commanders are often included in the discussions that define their missions but ultimately must operate within the boundaries of those missions and the constraints associated with them.
- Throughout history, the essence of command and control has been the reduction of uncertainty, including uncertainty about the environment, the adversary, and our own forces—
 - Uncertainty is inherent in military operations and will never be removed completely, regardless of the technologies employed or the quality of the forces and their commanders.
- Manipulation of uncertainty is always an element of command and control. This manipulation of uncertainty is achieved by reducing our own, increasing the adversary’s, and managing and operating with the uncertainty that remains.
- Command and control above the simplest tactical level is always a complex adaptive system—
 - The goal of command and control is to select crucial aspects of the operating environment and establish control over them.
 - Because the operating environment is complex and dynamic and because each adversary, neutral, or friendly pursues individual missions or goals, control is transitory until one side is victorious. For that reason, military operations are organized into phases and campaigns.
- Leadership is an essential element of command and control. The presence of the commander—whether physical or virtual—and the quality of the communication between the commander and the force are core elements of command and control. Leadership is necessary to create trust and understanding in an organization. It is necessary to enlist the committed, enthusiastic, and loyal performance of subordinates. Leadership is also important in coordinating the actions of multinational and interagency peers.
- Because command and control is a dynamic interaction between a military organization and its operating environment, it can be understood as a cyclic process. The observe, orient, decide, act (OODA) loop reflects this process:
 - Observe refers to obtaining the best information available.
 - Orient refers to bringing together what is known about the military situation and the knowledge—developed through training, experience, and intuition—of the commander and senior staff to understand that situation.

- Decide refers to the process of selecting a COA, which includes consideration of alternatives as well as adversary reactions to them.
- Act refers to implementing decisions in the battlespace. It also initiates a new cycle of observation.
- The HQ organizes and prepares its forces for warfighting. It provides guidance and plans that support subordinate forces and the commander's leadership responsibilities and decisionmaking.
- The C2 element relies on the best available information systems, but sometimes they must sacrifice the number of users who may participate and the quality of the information content and the user interaction. These sacrifices, however, are likely to diminish over time as new technology is developed

CHAPTER 5

MAGTF COMMUNICATIONS NETWORK

The MAGTF communications network supports information exchange requirements—voice, data, video, and imagery—both internal and external to the MAGTF. For external, long-haul communication, the communications network interfaces with the DISN. The MAGTF tactical communications network must also interface with the tactical communications networks of the other Services. The symbology, diagrams, and designator information used to represent these networks can be found in appendices B, C, and D.

Communication and the Electromagnetic Spectrum

The basic concept of communications theory is that an electronic signal can be modified so that at least two different states of that signal can be detected. The two states represent a zero or one, mark or space, on or off. As soon as two or more different states can be detected, the capability for moving information exists. This movement occurs within the electromagnetic spectrum.

The electromagnetic spectrum defines the range of different types of electromagnetic radiation, from visible light, to gamma rays, to heat, to audio signals. This energy travels through space at or near the speed of light. The primary way in which the military communicates is over radio frequency (RF) waves, which form a portion or band of the spectrum.

Technically, communications is the process of converting data into a signal, a form of energy that occupies a slice of the electromagnetic spectrum. Once converted, the information can be passed to a distant point. At its destination, the energy is changed back to its original form.

Where the slice falls in the RF band determines its transmission characteristics.

Frequency

Radio wave energy is identified by its frequency, or the amount of time it takes a wave to complete a sine wave cycle. Hertz, or cycles per second, measures a signal's frequency. Each frequency has a discrete wavelength, or how far the wave travels in space within a given frequency. Frequency and wavelength are inversely proportional: the higher the frequency, the shorter the wavelength, and vice versa. This relationship is important because knowing where in the RF band a piece of communications equipment functions allows for an accurate prediction of the behavior of that equipment as well as the different properties that influence to what extent a signal can support the exchange of information. Frequency, more than any other characteristic, determines range; throughput, or ability to carry information; physical makeup, or size and configuration, of equipment; and susceptibility to interference that may be manmade, electrical, or atmospheric.

The RF portion of the spectrum is divided into well defined frequency bands that correspond to a discrete frequency range. These bands are assigned unique designations, such as HF, VHF, UHF, SHF, and EHF. They have their own specific capabilities and limitations related to the characteristics of those frequency groupings. A typical SCR, for instance, transmits in the VHF range. Radios operating here can be lightweight, can use simple and relatively short wire antennas called whips, and can easily be transported by an individual. On the other hand, a typical multichannel satellite radio transmits in the SHF range, which requires complex and relatively bulky combinations of equipment that must be transported by vehicle.

Three types of electromagnetic propagation are common: ground wave, sky wave, and free space. At lower frequencies, radio ground waves travel great distances along the surface of the earth. Ground waves attenuate, or lose signal strength, as frequency increases. At higher frequencies, losses along the surface become so great that the ground wave is limited to short distances. Sky waves occur at medium to high frequencies, where reflection from the ionosphere permits radio communication over great distances. At frequencies above 30 MHz, these reflections are not dependable. Communication above this band depends upon LOS and tropospheric scatter, also called troposcatter, equipment to reach beyond the horizon. Atmospheric interference, however, tends to degrade sky wave propagation. At EHF, for example, there may be wave attenuation caused by rain-fall or absorption by dust and water vapor.

Finally, as frequency increases, required transmitter output power decreases. Transmitter output power is important because it determines how much input power is required for the radio system to operate properly. A 5-watt UHF radio will transmit and receive for many hours on small dry-cell batteries. An HF radio with a 1-kW transmit power, conversely, requires a relatively high amperage constant power source, such as that provided by tactical generators or commercial power sources. Another consideration is that the higher the output power, the easier it is to find the transmitter using direction-finding techniques.

Signals and Encoding

There are two basic types of signals that are used to send information from one point to another. An analog signal is a continuously varying electromagnetic wave, typically represented by a sine wave. A digital signal is a sequence of voltage pulses: a positive voltage level may represent a one and a negative voltage may represent a zero. Data, such as the human voice, e-mail, or files, can be electronically represented by the sequencing of these voltage pulses.

Encoding

Encoding is the process by which analog or digital data is impressed onto an analog or digital waveform for the purpose of transmission and utilization at a destination. In other words, encoding is how data is put onto a waveform by the originator so that it can be sent to a destination. At the destination, the waveform must be decoded in order for the data to be extracted from the waveform for use. Putting data onto a signal permits it to be transmitted at greater distances than it could go in its original form, such as voice versus phone. The signal allows data to be amplified or manipulated at the received end to overcome distortion, such as in forward error correction. It also lets information move quicker and more efficiently, as in electronically transmitting a 4-page file vice reading it over a radio net.

Modulation

The impressing of analog or digital data onto an analog waveform is known as modulation. The most common application of modulation is applying sound, such as the human voice, to a radio wave for transmission. The radio wave, onto which the data is impressed, is called a carrier. One of the wave characteristics of the carrier—frequency, amplitude, or phase—is varied to represent the data to be transmitted. A modem (“modulator” and “demodulator”) converts signals from one format to another.

Transmission

Transmission is the process of conveying a signal from point to point along a path. This path, or the transmission medium, is either guided or unguided. Unguided transmission media can be either SCR or MCR.

Guided

Guided transmission media use physical conductors, such as metallic wire, coaxial cable, and fiber optic cable, to guide signals along a specific path.

Two-wire or 4-wire field wire and multipair cable exhibit good transmission qualities over short distances. Field wire generally is used for local distribution systems to connect users to a central facility and to interconnect communications sites located at a single node or installation. Coaxial cable has excellent transmission qualities for several miles and is suitable for connecting major nodes as a short-hop substitute for multichannel radio. Optical fiber can transmit significantly more data than coaxial cable, is lightweight, and is almost impervious to the electromagnetic jamming and interference problems associated with metallic conductors.

Unguided

Unguided transmission media use electromagnetic waves that propagate through the atmosphere, but are not guided down a specific path. Radio systems provide this capability and operate point-to-point when signals are transmitted and received between two locations. They broadcast point-to-multipoint when signals serve a broader community of users with one station functioning as the originator or as net control. These signals can be categorized as either single-channel or multichannel.

Unguided SCR

Single channel radios typically operate at half-duplex, meaning that a user may transmit or receive at any given instant, but may not do both simultaneously. They primarily provide the ability to exchange voice with a potentially broad range of users while on the move (OTM). It can also support the exchange of low bandwidth data, but not at the same time as voice. Typically, SCRs, based on the portion of the RF band in which they operate, are smaller and easier to install than multichannel radios. Table 5-1, on page 5-4, discusses the employment considerations and requirements for each SCR frequency range.

Because of its great flexibility and quick installation, SCR is the principal means of communication for maneuvering and OTM units, and is normally the first means of communication established upon occupation of a site. SCRs have both positives (capabilities) and negatives (limitations):

Capabilities

- Provides secure voice and limited data exchange, such as files and chat.
- Supports OTM communication.
- Installs and operates faster and easier than other means of communication and is more responsive.
- Spans great distances, overcoming physical obstacles.

Limitations

- Is susceptible to enemy EW and electrical, physical, atmospheric, and space weather interference.
- Has lower data throughput than multichannel radio systems.
- Operates at half-duplex—a user can only transmit or receive at any given moment, not both simultaneously.

Unguided MCR

All MCRs operate at full-duplex; information can be transmitted and received simultaneously. Unlike SCR, however, MCR provides multiple channels over a single pathway, accommodating multiple users and services simultaneously. It is generally used for connecting different nodes within a network, such as a MEF CE with its MSCs.

Because of its high bandwidth capability, MCR systems operate in different portions of the electromagnetic spectrum than SCR, using frequencies in the UHF, SHF, and EHF bands. Table 5-2, on page 5-7, discusses the employment considerations and requirements for each MCR frequency range. Additionally, MCR pathways are both terrestrial- and space-based.

Table 5-1. Employment Considerations and Requirements for SCR HF, VHF, UHF, and Satellite Signals.

Frequency	Frequency Range	Employment Considerations	Requirements
HF	2-9.9999 MHz	<p>Provides short-range, long-range, or over-the-horizon, secure voice and limited data exchange.</p> <p>Uses ground-wave propagation for short distances.</p> <p>Uses sky-wave propagation for long distances and overcoming obstacles (usability of certain frequencies are dependent upon ionospheric conditions, transitions between day and night, seasonal changes, and solar activity).</p> <p>Provides automatic link establishment equipment to maintain communication during adverse conditions.</p> <p>Requires deliberate radio operator procedures to mitigate lower voice quality.</p> <p>Represents hazards to personnel, depending on power output of antenna elements.</p> <p>Requires antenna site selection to ensure proper antenna separation, remoting from COC, and, depending upon antenna type, large physical space.</p>	<p>Multiple, varied frequencies that span the HF portion of the electromagnetic spectrum.</p> <p>Propagation analysis and prediction to determine optimum frequencies.</p> <p>COMSEC keys.</p> <p>Data network interfaces.</p> <p>Proper site reconnaissance and selection.</p> <p>Field expedient antenna planning and employment.</p>
VHF	30-88 MHz	<p>Is the primary means of OTM communication.</p> <p>Employs frequency hopping to mitigate effects of enemy jamming.</p> <p>Provides short-range (radio LOS), secure voice and, compared with HF, improved voice quality and data exchange to about 15 miles, depending upon radio type, power output, and environmental conditions.</p> <p>Is susceptible to terrain, particularly foliage.</p> <p>Offers increased range and reliability through use of retransmission sites.</p> <p>Requires antenna site selection to ensure proper antenna separation and remoting from the COC.</p>	<p>Hop-set data for frequency hopping, ordinarily generated by MSC spectrum managers and net identifications.</p> <p>Propagation analysis to determine LOS coverage as well as locations for retransmission sites.</p> <p>COMSEC keying material.</p> <p>Data network interfaces.</p> <p>Proper site reconnaissance and selection, particularly for antenna stand-off distance from terrain and obstacles.</p>

Table 5-1. Employment Considerations and Requirements for SCR HF, VHF, UHF, and Satellite Signals. (Continued)

Frequency	Frequency Range	Employment Considerations	Requirements
UHF	225–400 MHz	<p>Is the primary means of ground-to-air communication.</p> <p>Employs frequency hopping to mitigate effects of enemy jamming.</p> <p>Provides short-range, secure voice and, compared with HF, improved voice quality and data exchange.</p> <p>Offers critical LOS range with both transmitting and receiving antennas having a clear LOS.</p> <p>Is susceptible to terrain and obstacles.</p>	<p>Hop-set data for frequency hopping.</p> <p>COMSEC keying material.</p> <p>Proper site reconnaissance and selection.</p>
UHF Tactical Satellite (TACSAT)	225–400 MHz	<p>Provides long-range, over-the-horizon, secure voice and data exchange.</p> <p>Uses narrowband or wideband channels, which impact data rate. More narrowband and fewer wideband channels are available.</p> <p>Uses demand assigned multiple access equipment and allows sharing of available channels with multiple users.</p> <p>Has a limited number of satellites and channels, resulting in competition for access and user prioritization across Services and combatant commands.</p> <p>Reduces channel congestion, noise, and network saturation impact data rate.</p> <p>Has critical LOS range with reliability affected by weather, terrain, and location. Shallow look angles, or the angle at which an antenna is positioned above the horizon in order to "see" the satellite, indicate terminal placement outside of or near the edge of the satellite's footprint (occurs as terminals move closer to the earth's poles).</p>	<p>Extensive coordination and planning lead times to ensure access to satellite channels.</p> <p>COMSEC keying material.</p> <p>Look angle analysis.</p> <p>Data network interfaces.</p> <p>Proper site reconnaissance and selection.</p>
Commercial Satellite Terminals		<p>Provides worldwide secure voice, with appropriate COMSEC modules, and improved data exchange.</p> <p>Provides a first-in, redundant, or amplifying capability to tactical SCRs.</p> <p>Has a potentially significant cost.</p> <p>Has a limited number of terminals.</p>	<p>COMSEC keying material.</p> <p>Data network interfaces.</p> <p>Contractual vehicle.</p>

The demands of operating in these frequency bands as well as performing multiplexing functions require complex and relatively large pieces of equipment. The MCR systems, therefore, have considerably more logistical and operating requirements than SCR systems. MCRs have both positives (capabilities) and negatives (limitations):

Capabilities

- Provides simultaneous access to secure voice, video, and data.
- Has high bandwidth potential.
- Interfaces with the GIG.
- Extends high bandwidth connectivity.
- Spans great distances and overcomes physical obstacles.

Limitations

- Is susceptible to enemy EW and to electrical, physical, atmospheric, and space weather interference.
- Does not support OTM communication.
- Is logistically more intense than SCR and requires generator support, mobility, and more operators.
- Requires longer installation times and more coordination.
- Uses critical low-density equipment items.
- Uses satellite resources and loss of link drops all circuits.

Multiplexing

Multiplexing is the process of combining two or more discrete signals into a single, higher-capacity signal. A telephone circuit and a data circuit, for instance, are combined and then transmitted over the same path; this combination helps reduce the overall number of different transmission systems required. At the receiving end, the signal is demultiplexed and the individual circuits are routed to terminating equipment, such as a telephone switchboard or a data router. Multiplexed signals can be transmitted over guided (cable) or unguided (MCR) media.

Synchronization and Timing

Synchronization

Synchronization is a networking term that applies to a state where data or information arrives and departs from connected devices at coordinated times so that data is neither lost nor jumbled. Synchronization is critical with multiplexing and MCR, where high volumes of information are carried to multiple nodes. Communicating devices must be synchronized to know when to receive or transmit information and on which channel or path.

Timing

Timing is the glue that holds a communications network together. Timing ensures that exchanged information is synchronized across the different layers of transmissions and multiplexing. Timing sources, which are typically based on the decay of radioactive elements as they provide a high degree of accuracy, are either embedded into certain types of equipment such as an MCR. They can also serve as stand-alone devices that interface with a network. The most reliable timing scheme employs separate timing sources at each node in a network.

Switching

Users must be capable of communicating with any other user on demand. Because it is impossible to have every user linked directly to every other user, a different means of communicating—of connecting users to one another—is required. Switching provides the ability to connect many users and their terminal devices in a way that permits on-demand exchange with other users and terminal devices without having to link them individually. Switching provides the means by which traffic is routed through a communications network. From a tactical perspective, there are two types of switching: circuit and packet.

Table 5-2. Employment Considerations and Requirements for MCR UHF, SHF, and EHF Signals.

Frequency	Frequency Range	Employment Considerations	Requirements
UHF (terrestrial)	300–3000 MHz	<p>Provides medium bandwidth connectivity.</p> <p>Has LOS range to 35 miles depending on terrain, antenna, and power output. Can be extended using repeater systems.</p>	<p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Network interfaces.</p> <p>Proper site reconnaissance and selection, particularly for antenna stand-off distance from terrain and obstacles.</p>
SHF (terrestrial)	3–8 GHz	<p>Provides high bandwidth connectivity.</p> <p>Offers range to 100 miles dependent upon mode of operation, terrain, antennas, and power output.</p> <p>Can overcome physical obstacles, depending upon mode of operation.</p> <p>Power output can represent hazards to personnel and ammunition and interfere with other types of equipment.</p>	<p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Network interfaces.</p> <p>Proper site reconnaissance and selection.</p>
SHF (SATCOM)	3–30 GHz	<p>Provides high bandwidth connectivity.</p> <p>Provides LOS operation with reliability affected by weather, terrain, and location.</p> <p>Has various configurations such as point-to-point, hub-spoke, or mesh.</p> <p>Uses critical low density equipment and is expensive.</p> <p>Has limited numbers of satellites and channels, resulting in competition for access and user prioritization across Services and combatant commands.</p>	<p>Extensive coordination and planning lead times to ensure access to satellite channels and termination of services.</p> <p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Look angle analysis.</p> <p>Proper site reconnaissance and selection.</p>
EHF (SATCOM)	30–300 GHz	<p>Provides high bandwidth connectivity.</p> <p>Is jam-resistant with low probability of interception.</p> <p>Operates in a relatively noncrowded portion of the electromagnetic spectrum.</p> <p>Is more susceptible to effects of weather and atmospheric conditions than UHF or SHF.</p>	<p>Extensive coordination and planning lead times to ensure access to satellite channels and termination of services.</p> <p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Look angle analysis.</p> <p>Network interfaces.</p> <p>Proper site reconnaissance and selection.</p>

Circuit Switching

Circuit switching is the process of interconnecting a specific circuit to provide a direct connection between calling and called stations, and is historically used for telephone networks. With this type of switching, a dedicated path is established whenever a call is initiated. That path remains fixed for the duration of the connection. This constant connection ensures a degree of reliability whenever a call is placed so that, generally, the exchange of information can be guaranteed. The disadvantage, however, is that the connection dedicates bandwidth that is no longer available to other users.

Telephone switchboards enable circuit switching. A “loop” is a circuit between an individual telephone and the switch to which it is connected. A “trunk” is a channel between different switches and enables a user in one node to call a user in another node. Typically, there are multiple trunks between switches to support simultaneous calls, but this bandwidth is limited and is seized whenever a switch-to-switch call is made. Put another way, there are more loops than there are trunks, so users vie for access whenever they make calls to users on other switches.

To help compensate for this congestion potential, switches are capable of ensuring access to priority users. A 5-level precedence scheme categorizes users based on information exchange and billet requirements. This assignment of precedence allows higher priority users to preempt, if necessary, calls of lower priority users. The five levels are routine, priority, immediate, flash, and flash override.

Within a tactical circuit switch network, switchboards are identified by a unique number called the primary region switch locator (PRSL) code. The PRSL determines the dialing scheme used to call users on the same switch as well as users on

other switches in the network. Its capabilities and limitations are—

Capabilities

- Provides simultaneous access to secure voice and limited video and data.
- Interfaces with the GIG, providing worldwide connectivity.
- Supports a high volume of simultaneous users.
- Provides guaranteed capacity through fixed bandwidth.
- Enhances communications and emissions security through encrypted wireline communications.

Limitations

- Does not support OTM communication; requires a relatively static environment and increased time for installation.
- Requires generator support, mobility, operators, and maintainers.
- Offers a less efficient use of bandwidth as channels take up bandwidth whether in use or not.
- Requires extensive coordination.
- Wires are susceptible to physical damage.

Employment considerations and requirements for tactical telephone networks are as follows:

Employment Considerations

- Number of users.
- User services required, such as secure or nonsecure, precedence, call conferencing, or hotlines.
- Switch channel rates.
- Trunk requirements and channelization.
- Routing type such as flood-search or deterministic.
- Cable runs including considerations of types and lengths.

Requirements

- Wideband transmission links and network interfaces.
- Numbering scheme.
- Timing source.
- COMSEC keying material.
- Logistical support.

Packet Switching

Packet switching is fundamentally different. Instead of dedicating an entire channel to an information exchange, packet switching shares a communications path. Information is broken up into smaller units, or packets, that are routed to the destination independent of each other. At the receiving end, the packets are reassembled into the original information. Packet switching is an efficient and relatively inexpensive method of information exchange, and it is used for tactical data networks.

Routers, data switches, and bridges typically form the packet switching backbone. Just as important as the equipment, however, are the standards used to route traffic. Packet switching requires highly structured protocols to maintain network status and control of the packets. For instance, the nodal points within a network only store packets for the very brief time it takes to recognize and forward them through the network. If an incomplete message is received, the originator must retransmit the message. Protocols define these standards to ensure reliable and accurate information exchange.

While LANs generally support a single node of a network within a relatively small geographic area, WANs connect different LANs or other WANs together. Capabilities and limitations are as follows:

Capabilities

- Provides simultaneous access to secure voice, video, and data.
- Provides worldwide connectivity by interfacing with the GIG.
- Supports a high volume of simultaneous users.
- Supports collaboration and file exchange.
- Optimizes bandwidth by allowing multiple devices to use the same channel with routes that can be dynamically changed.
- Supports OTM communication such as data connectivity through SCR for lower bandwidth application.

Limitations

- Does not support OTM communication for high bandwidth applications and requires a relatively static environment and increased time for installation.
- Requires generator support, mobility, operators, and maintainers.
- Requires extensive coordination.
- Wires susceptible to physical damage.

Employment considerations and requirements for tactical data networks are as follows:

Employment Considerations

- Number of users.
- User services required such as secure or nonsecure, e-mail, World Wide Web, video, or file storage.
- Quality of service.
- Survivability such as disaster recovery, backup requirements, or threat mitigation.
- Physical and logical network design.

Requirements

- Wideband transmission links, network interfaces.
- Protocols and standards.
- Information assurance policies and procedures.
- Logistical support.

Elements of a MAGTF Communications Network

A network is the interconnected arrangement of different systems or parts of systems. From a tactical communication standpoint, several SCRs communicating together are a network. Computers sharing a common printer are a network. Telephone switchboards cabled together are a network. Any of these in isolation or connected together is a network.

A tactical communications network is the technical means by which different methods of communication are linked together. The network is designed to satisfy information exchange

requirements and provide access to networked services such as voice, imagery, and data. Services can often be segregated into different communications functional areas; however, access to those services overlaps the functional areas. E-mail, for instance, is ordinarily provided by data networks. This overlap eases and complicates the challenges faced by communicators in planning, providing, and controlling a communications network.

A MAGTF communications network contains four basic elements: services, switching networks, multiplexing networks, and transmission networks. The capabilities and limitations of these elements are summarized in table 5-3 on page 5-13.

Services

A service is the method by which a user interacts with information, that is, how information is presented, accessed, used, and exchanged. Services are divided into three broad categories:

- Voice—radio or telephone.
- Imagery—video or picture.
- Data—files, documents, e-mail, or chat.

Terminal devices are equipment through which access to services is provided, such as phones, computers, printers, or radios.

Switching Networks

Switching networks provide services and connect terminal devices. There are two types of switching networks: circuit switch and packet switch.

Circuit Switch Network

Circuit switch network (CSN) provides voice telephone services and can support imagery and data exchange. Tactical telephone connectivity is provided by a combination of both tactical and commercial circuit switches, telephone networks, data networks, telephone devices, and

transmission systems. In addition to networks established in an AO, tactical telephone networks can interface with DSN and DRSN strategic and commercial networks through DISA STEP/teleport sites in order to provide worldwide connectivity. Various types of telephones—both tactical and commercial—provide secure and nonsecure capabilities. Depending upon the switch type, other services, such as call conferencing, call forwarding, voice mail, and radio-wire interfaces, may be available.

Packet Switch Network

Packet switch network (PSN) provides imagery and data services and can support voice services. Tactical data network connectivity is provided by a combination of both tactical and commercial equipment, software, protocols, and transmission systems. In addition to networks established in an AO, tactical data networks can interface with SIPRNET, NIPRNET, Internet, and strategic and commercial networks through DISA STEP/teleport sites in order to provide worldwide connectivity. Encryption devices, secure enclaves, tunneling, and virtual private networks provide secure and nonsecure capabilities. Voice over IP technology permits telephone connectivity over data networks.

Multiplexing Networks

Multiplexing networks combine multiple circuits into a single link and layer different services together for transmission.

Transmission Networks

Transmission networks provide connectivity and extend multiplexed and other services to users and between nodes. There are two types of transmission networks:

- Wideband:
 - Guided (cable) provides cable connectivity of multiplexed links.

- Unguided (MCR) provides terrestrial- and space-based LOS and beyond LOS MCR connectivity of multiplexed links.
- Narrowband (SCR) provides OTM voice, but also can support low bandwidth imagery and data exchange.

This page intentionally left blank.

CHAPTER 5

MAGTF COMMUNICATIONS NETWORK

The MAGTF communications network supports information exchange requirements—voice, data, video, and imagery—both internal and external to the MAGTF. For external, long-haul communication, the communications network interfaces with the DISN. The MAGTF tactical communications network must also interface with the tactical communications networks of the other Services. The symbology, diagrams, and designator information used to represent these networks can be found in appendices B, C, and D.

Communication and the Electromagnetic Spectrum

The basic concept of communications theory is that an electronic signal can be modified so that at least two different states of that signal can be detected. The two states represent a zero or one, mark or space, on or off. As soon as two or more different states can be detected, the capability for moving information exists. This movement occurs within the electromagnetic spectrum.

The electromagnetic spectrum defines the range of different types of electromagnetic radiation, from visible light, to gamma rays, to heat, to audio signals. This energy travels through space at or near the speed of light. The primary way in which the military communicates is over radio frequency (RF) waves, which form a portion or band of the spectrum.

Technically, communications is the process of converting data into a signal, a form of energy that occupies a slice of the electromagnetic spectrum. Once converted, the information can be passed to a distant point. At its destination, the energy is changed back to its original form.

Where the slice falls in the RF band determines its transmission characteristics.

Frequency

Radio wave energy is identified by its frequency, or the amount of time it takes a wave to complete a sine wave cycle. Hertz, or cycles per second, measures a signal's frequency. Each frequency has a discrete wavelength, or how far the wave travels in space within a given frequency. Frequency and wavelength are inversely proportional: the higher the frequency, the shorter the wavelength, and vice versa. This relationship is important because knowing where in the RF band a piece of communications equipment functions allows for an accurate prediction of the behavior of that equipment as well as the different properties that influence to what extent a signal can support the exchange of information. Frequency, more than any other characteristic, determines range; throughput, or ability to carry information; physical makeup, or size and configuration, of equipment; and susceptibility to interference that may be manmade, electrical, or atmospheric.

The RF portion of the spectrum is divided into well defined frequency bands that correspond to a discrete frequency range. These bands are assigned unique designations, such as HF, VHF, UHF, SHF, and EHF. They have their own specific capabilities and limitations related to the characteristics of those frequency groupings. A typical SCR, for instance, transmits in the VHF range. Radios operating here can be lightweight, can use simple and relatively short wire antennas called whips, and can easily be transported by an individual. On the other hand, a typical multichannel satellite radio transmits in the SHF range, which requires complex and relatively bulky combinations of equipment that must be transported by vehicle.

Three types of electromagnetic propagation are common: ground wave, sky wave, and free space. At lower frequencies, radio ground waves travel great distances along the surface of the earth. Ground waves attenuate, or lose signal strength, as frequency increases. At higher frequencies, losses along the surface become so great that the ground wave is limited to short distances. Sky waves occur at medium to high frequencies, where reflection from the ionosphere permits radio communication over great distances. At frequencies above 30 MHz, these reflections are not dependable. Communication above this band depends upon LOS and tropospheric scatter, also called troposcatter, equipment to reach beyond the horizon. Atmospheric interference, however, tends to degrade sky wave propagation. At EHF, for example, there may be wave attenuation caused by rain-fall or absorption by dust and water vapor.

Finally, as frequency increases, required transmitter output power decreases. Transmitter output power is important because it determines how much input power is required for the radio system to operate properly. A 5-watt UHF radio will transmit and receive for many hours on small dry-cell batteries. An HF radio with a 1-kW transmit power, conversely, requires a relatively high amperage constant power source, such as that provided by tactical generators or commercial power sources. Another consideration is that the higher the output power, the easier it is to find the transmitter using direction-finding techniques.

Signals and Encoding

There are two basic types of signals that are used to send information from one point to another. An analog signal is a continuously varying electromagnetic wave, typically represented by a sine wave. A digital signal is a sequence of voltage pulses: a positive voltage level may represent a one and a negative voltage may represent a zero. Data, such as the human voice, e-mail, or files, can be electronically represented by the sequencing of these voltage pulses.

Encoding

Encoding is the process by which analog or digital data is impressed onto an analog or digital waveform for the purpose of transmission and utilization at a destination. In other words, encoding is how data is put onto a waveform by the originator so that it can be sent to a destination. At the destination, the waveform must be decoded in order for the data to be extracted from the waveform for use. Putting data onto a signal permits it to be transmitted at greater distances than it could go in its original form, such as voice versus phone. The signal allows data to be amplified or manipulated at the received end to overcome distortion, such as in forward error correction. It also lets information move quicker and more efficiently, as in electronically transmitting a 4-page file vice reading it over a radio net.

Modulation

The impressing of analog or digital data onto an analog waveform is known as modulation. The most common application of modulation is applying sound, such as the human voice, to a radio wave for transmission. The radio wave, onto which the data is impressed, is called a carrier. One of the wave characteristics of the carrier—frequency, amplitude, or phase—is varied to represent the data to be transmitted. A modem (“modulator” and “demodulator”) converts signals from one format to another.

Transmission

Transmission is the process of conveying a signal from point to point along a path. This path, or the transmission medium, is either guided or unguided. Unguided transmission media can be either SCR or MCR.

Guided

Guided transmission media use physical conductors, such as metallic wire, coaxial cable, and fiber optic cable, to guide signals along a specific path.

Two-wire or 4-wire field wire and multipair cable exhibit good transmission qualities over short distances. Field wire generally is used for local distribution systems to connect users to a central facility and to interconnect communications sites located at a single node or installation. Coaxial cable has excellent transmission qualities for several miles and is suitable for connecting major nodes as a short-hop substitute for multichannel radio. Optical fiber can transmit significantly more data than coaxial cable, is lightweight, and is almost impervious to the electromagnetic jamming and interference problems associated with metallic conductors.

Unguided

Unguided transmission media use electromagnetic waves that propagate through the atmosphere, but are not guided down a specific path. Radio systems provide this capability and operate point-to-point when signals are transmitted and received between two locations. They broadcast point-to-multipoint when signals serve a broader community of users with one station functioning as the originator or as net control. These signals can be categorized as either single-channel or multichannel.

Unguided SCR

Single channel radios typically operate at half-duplex, meaning that a user may transmit or receive at any given instant, but may not do both simultaneously. They primarily provide the ability to exchange voice with a potentially broad range of users while on the move (OTM). It can also support the exchange of low bandwidth data, but not at the same time as voice. Typically, SCRs, based on the portion of the RF band in which they operate, are smaller and easier to install than multichannel radios. Table 5-1, on page 5-4, discusses the employment considerations and requirements for each SCR frequency range.

Because of its great flexibility and quick installation, SCR is the principal means of communication for maneuvering and OTM units, and is normally the first means of communication established upon occupation of a site. SCRs have both positives (capabilities) and negatives (limitations):

Capabilities

- Provides secure voice and limited data exchange, such as files and chat.
- Supports OTM communication.
- Installs and operates faster and easier than other means of communication and is more responsive.
- Spans great distances, overcoming physical obstacles.

Limitations

- Is susceptible to enemy EW and electrical, physical, atmospheric, and space weather interference.
- Has lower data throughput than multichannel radio systems.
- Operates at half-duplex—a user can only transmit or receive at any given moment, not both simultaneously.

Unguided MCR

All MCRs operate at full-duplex; information can be transmitted and received simultaneously. Unlike SCR, however, MCR provides multiple channels over a single pathway, accommodating multiple users and services simultaneously. It is generally used for connecting different nodes within a network, such as a MEF CE with its MSCs.

Because of its high bandwidth capability, MCR systems operate in different portions of the electromagnetic spectrum than SCR, using frequencies in the UHF, SHF, and EHF bands. Table 5-2, on page 5-7, discusses the employment considerations and requirements for each MCR frequency range. Additionally, MCR pathways are both terrestrial- and space-based.

Table 5-1. Employment Considerations and Requirements for SCR HF, VHF, UHF, and Satellite Signals.

Frequency	Frequency Range	Employment Considerations	Requirements
HF	2-9.9999 MHz	<p>Provides short-range, long-range, or over-the-horizon, secure voice and limited data exchange.</p> <p>Uses ground-wave propagation for short distances.</p> <p>Uses sky-wave propagation for long distances and overcoming obstacles (usability of certain frequencies are dependent upon ionospheric conditions, transitions between day and night, seasonal changes, and solar activity).</p> <p>Provides automatic link establishment equipment to maintain communication during adverse conditions.</p> <p>Requires deliberate radio operator procedures to mitigate lower voice quality.</p> <p>Represents hazards to personnel, depending on power output of antenna elements.</p> <p>Requires antenna site selection to ensure proper antenna separation, remoting from COC, and, depending upon antenna type, large physical space.</p>	<p>Multiple, varied frequencies that span the HF portion of the electromagnetic spectrum.</p> <p>Propagation analysis and prediction to determine optimum frequencies.</p> <p>COMSEC keys.</p> <p>Data network interfaces.</p> <p>Proper site reconnaissance and selection.</p> <p>Field expedient antenna planning and employment.</p>
VHF	30-88 MHz	<p>Is the primary means of OTM communication.</p> <p>Employs frequency hopping to mitigate effects of enemy jamming.</p> <p>Provides short-range (radio LOS), secure voice and, compared with HF, improved voice quality and data exchange to about 15 miles, depending upon radio type, power output, and environmental conditions.</p> <p>Is susceptible to terrain, particularly foliage.</p> <p>Offers increased range and reliability through use of retransmission sites.</p> <p>Requires antenna site selection to ensure proper antenna separation and remoting from the COC.</p>	<p>Hop-set data for frequency hopping, ordinarily generated by MSC spectrum managers and net identifications.</p> <p>Propagation analysis to determine LOS coverage as well as locations for retransmission sites.</p> <p>COMSEC keying material.</p> <p>Data network interfaces.</p> <p>Proper site reconnaissance and selection, particularly for antenna stand-off distance from terrain and obstacles.</p>

Table 5-1. Employment Considerations and Requirements for SCR HF, VHF, UHF, and Satellite Signals. (Continued)

Frequency	Frequency Range	Employment Considerations	Requirements
UHF	225–400 MHz	<p>Is the primary means of ground-to-air communication.</p> <p>Employs frequency hopping to mitigate effects of enemy jamming.</p> <p>Provides short-range, secure voice and, compared with HF, improved voice quality and data exchange.</p> <p>Offers critical LOS range with both transmitting and receiving antennas having a clear LOS.</p> <p>Is susceptible to terrain and obstacles.</p>	<p>Hop-set data for frequency hopping.</p> <p>COMSEC keying material.</p> <p>Proper site reconnaissance and selection.</p>
UHF Tactical Satellite (TACSAT)	225–400 MHz	<p>Provides long-range, over-the-horizon, secure voice and data exchange.</p> <p>Uses narrowband or wideband channels, which impact data rate. More narrowband and fewer wideband channels are available.</p> <p>Uses demand assigned multiple access equipment and allows sharing of available channels with multiple users.</p> <p>Has a limited number of satellites and channels, resulting in competition for access and user prioritization across Services and combatant commands.</p> <p>Reduces channel congestion, noise, and network saturation impact data rate.</p> <p>Has critical LOS range with reliability affected by weather, terrain, and location. Shallow look angles, or the angle at which an antenna is positioned above the horizon in order to "see" the satellite, indicate terminal placement outside of or near the edge of the satellite's footprint (occurs as terminals move closer to the earth's poles).</p>	<p>Extensive coordination and planning lead times to ensure access to satellite channels.</p> <p>COMSEC keying material.</p> <p>Look angle analysis.</p> <p>Data network interfaces.</p> <p>Proper site reconnaissance and selection.</p>
Commercial Satellite Terminals		<p>Provides worldwide secure voice, with appropriate COMSEC modules, and improved data exchange.</p> <p>Provides a first-in, redundant, or amplifying capability to tactical SCRs.</p> <p>Has a potentially significant cost.</p> <p>Has a limited number of terminals.</p>	<p>COMSEC keying material.</p> <p>Data network interfaces.</p> <p>Contractual vehicle.</p>

The demands of operating in these frequency bands as well as performing multiplexing functions require complex and relatively large pieces of equipment. The MCR systems, therefore, have considerably more logistical and operating requirements than SCR systems. MCRs have both positives (capabilities) and negatives (limitations):

Capabilities

- Provides simultaneous access to secure voice, video, and data.
- Has high bandwidth potential.
- Interfaces with the GIG.
- Extends high bandwidth connectivity.
- Spans great distances and overcomes physical obstacles.

Limitations

- Is susceptible to enemy EW and to electrical, physical, atmospheric, and space weather interference.
- Does not support OTM communication.
- Is logistically more intense than SCR and requires generator support, mobility, and more operators.
- Requires longer installation times and more coordination.
- Uses critical low-density equipment items.
- Uses satellite resources and loss of link drops all circuits.

Multiplexing

Multiplexing is the process of combining two or more discrete signals into a single, higher-capacity signal. A telephone circuit and a data circuit, for instance, are combined and then transmitted over the same path; this combination helps reduce the overall number of different transmission systems required. At the receiving end, the signal is demultiplexed and the individual circuits are routed to terminating equipment, such as a telephone switchboard or a data router. Multiplexed signals can be transmitted over guided (cable) or unguided (MCR) media.

Synchronization and Timing

Synchronization

Synchronization is a networking term that applies to a state where data or information arrives and departs from connected devices at coordinated times so that data is neither lost nor jumbled. Synchronization is critical with multiplexing and MCR, where high volumes of information are carried to multiple nodes. Communicating devices must be synchronized to know when to receive or transmit information and on which channel or path.

Timing

Timing is the glue that holds a communications network together. Timing ensures that exchanged information is synchronized across the different layers of transmissions and multiplexing. Timing sources, which are typically based on the decay of radioactive elements as they provide a high degree of accuracy, are either embedded into certain types of equipment such as an MCR. They can also serve as stand-alone devices that interface with a network. The most reliable timing scheme employs separate timing sources at each node in a network.

Switching

Users must be capable of communicating with any other user on demand. Because it is impossible to have every user linked directly to every other user, a different means of communicating—of connecting users to one another—is required. Switching provides the ability to connect many users and their terminal devices in a way that permits on-demand exchange with other users and terminal devices without having to link them individually. Switching provides the means by which traffic is routed through a communications network. From a tactical perspective, there are two types of switching: circuit and packet.

Table 5-2. Employment Considerations and Requirements for MCR UHF, SHF, and EHF Signals.

Frequency	Frequency Range	Employment Considerations	Requirements
UHF (terrestrial)	300–3000 MHz	<p>Provides medium bandwidth connectivity.</p> <p>Has LOS range to 35 miles depending on terrain, antenna, and power output. Can be extended using repeater systems.</p>	<p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Network interfaces.</p> <p>Proper site reconnaissance and selection, particularly for antenna stand-off distance from terrain and obstacles.</p>
SHF (terrestrial)	3–8 GHz	<p>Provides high bandwidth connectivity.</p> <p>Offers range to 100 miles dependent upon mode of operation, terrain, antennas, and power output.</p> <p>Can overcome physical obstacles, depending upon mode of operation.</p> <p>Power output can represent hazards to personnel and ammunition and interfere with other types of equipment.</p>	<p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Network interfaces.</p> <p>Proper site reconnaissance and selection.</p>
SHF (SATCOM)	3–30 GHz	<p>Provides high bandwidth connectivity.</p> <p>Provides LOS operation with reliability affected by weather, terrain, and location.</p> <p>Has various configurations such as point-to-point, hub-spoke, or mesh.</p> <p>Uses critical low density equipment and is expensive.</p> <p>Has limited numbers of satellites and channels, resulting in competition for access and user prioritization across Services and combatant commands.</p>	<p>Extensive coordination and planning lead times to ensure access to satellite channels and termination of services.</p> <p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Look angle analysis.</p> <p>Proper site reconnaissance and selection.</p>
EHF (SATCOM)	30–300 GHz	<p>Provides high bandwidth connectivity.</p> <p>Is jam-resistant with low probability of interception.</p> <p>Operates in a relatively noncrowded portion of the electromagnetic spectrum.</p> <p>Is more susceptible to effects of weather and atmospheric conditions than UHF or SHF.</p>	<p>Extensive coordination and planning lead times to ensure access to satellite channels and termination of services.</p> <p>Logistical support.</p> <p>COMSEC keying material.</p> <p>Look angle analysis.</p> <p>Network interfaces.</p> <p>Proper site reconnaissance and selection.</p>

Circuit Switching

Circuit switching is the process of interconnecting a specific circuit to provide a direct connection between calling and called stations, and is historically used for telephone networks. With this type of switching, a dedicated path is established whenever a call is initiated. That path remains fixed for the duration of the connection. This constant connection ensures a degree of reliability whenever a call is placed so that, generally, the exchange of information can be guaranteed. The disadvantage, however, is that the connection dedicates bandwidth that is no longer available to other users.

Telephone switchboards enable circuit switching. A “loop” is a circuit between an individual telephone and the switch to which it is connected. A “trunk” is a channel between different switches and enables a user in one node to call a user in another node. Typically, there are multiple trunks between switches to support simultaneous calls, but this bandwidth is limited and is seized whenever a switch-to-switch call is made. Put another way, there are more loops than there are trunks, so users vie for access whenever they make calls to users on other switches.

To help compensate for this congestion potential, switches are capable of ensuring access to priority users. A 5-level precedence scheme categorizes users based on information exchange and billet requirements. This assignment of precedence allows higher priority users to preempt, if necessary, calls of lower priority users. The five levels are routine, priority, immediate, flash, and flash override.

Within a tactical circuit switch network, switchboards are identified by a unique number called the primary region switch locator (PRSL) code. The PRSL determines the dialing scheme used to call users on the same switch as well as users on

other switches in the network. Its capabilities and limitations are—

Capabilities

- Provides simultaneous access to secure voice and limited video and data.
- Interfaces with the GIG, providing worldwide connectivity.
- Supports a high volume of simultaneous users.
- Provides guaranteed capacity through fixed bandwidth.
- Enhances communications and emissions security through encrypted wireline communications.

Limitations

- Does not support OTM communication; requires a relatively static environment and increased time for installation.
- Requires generator support, mobility, operators, and maintainers.
- Offers a less efficient use of bandwidth as channels take up bandwidth whether in use or not.
- Requires extensive coordination.
- Wires are susceptible to physical damage.

Employment considerations and requirements for tactical telephone networks are as follows:

Employment Considerations

- Number of users.
- User services required, such as secure or nonsecure, precedence, call conferencing, or hotlines.
- Switch channel rates.
- Trunk requirements and channelization.
- Routing type such as flood-search or deterministic.
- Cable runs including considerations of types and lengths.

Requirements

- Wideband transmission links and network interfaces.
- Numbering scheme.
- Timing source.
- COMSEC keying material.
- Logistical support.

Packet Switching

Packet switching is fundamentally different. Instead of dedicating an entire channel to an information exchange, packet switching shares a communications path. Information is broken up into smaller units, or packets, that are routed to the destination independent of each other. At the receiving end, the packets are reassembled into the original information. Packet switching is an efficient and relatively inexpensive method of information exchange, and it is used for tactical data networks.

Routers, data switches, and bridges typically form the packet switching backbone. Just as important as the equipment, however, are the standards used to route traffic. Packet switching requires highly structured protocols to maintain network status and control of the packets. For instance, the nodal points within a network only store packets for the very brief time it takes to recognize and forward them through the network. If an incomplete message is received, the originator must retransmit the message. Protocols define these standards to ensure reliable and accurate information exchange.

While LANs generally support a single node of a network within a relatively small geographic area, WANs connect different LANs or other WANs together. Capabilities and limitations are as follows:

Capabilities

- Provides simultaneous access to secure voice, video, and data.
- Provides worldwide connectivity by interfacing with the GIG.
- Supports a high volume of simultaneous users.
- Supports collaboration and file exchange.
- Optimizes bandwidth by allowing multiple devices to use the same channel with routes that can be dynamically changed.
- Supports OTM communication such as data connectivity through SCR for lower bandwidth application.

Limitations

- Does not support OTM communication for high bandwidth applications and requires a relatively static environment and increased time for installation.
- Requires generator support, mobility, operators, and maintainers.
- Requires extensive coordination.
- Wires susceptible to physical damage.

Employment considerations and requirements for tactical data networks are as follows:

Employment Considerations

- Number of users.
- User services required such as secure or nonsecure, e-mail, World Wide Web, video, or file storage.
- Quality of service.
- Survivability such as disaster recovery, backup requirements, or threat mitigation.
- Physical and logical network design.

Requirements

- Wideband transmission links, network interfaces.
- Protocols and standards.
- Information assurance policies and procedures.
- Logistical support.

Elements of a MAGTF Communications Network

A network is the interconnected arrangement of different systems or parts of systems. From a tactical communication standpoint, several SCRs communicating together are a network. Computers sharing a common printer are a network. Telephone switchboards cabled together are a network. Any of these in isolation or connected together is a network.

A tactical communications network is the technical means by which different methods of communication are linked together. The network is designed to satisfy information exchange

requirements and provide access to networked services such as voice, imagery, and data. Services can often be segregated into different communications functional areas; however, access to those services overlaps the functional areas. E-mail, for instance, is ordinarily provided by data networks. This overlap eases and complicates the challenges faced by communicators in planning, providing, and controlling a communications network.

A MAGTF communications network contains four basic elements: services, switching networks, multiplexing networks, and transmission networks. The capabilities and limitations of these elements are summarized in table 5-3 on page 5-13.

Services

A service is the method by which a user interacts with information, that is, how information is presented, accessed, used, and exchanged. Services are divided into three broad categories:

- Voice—radio or telephone.
- Imagery—video or picture.
- Data—files, documents, e-mail, or chat.

Terminal devices are equipment through which access to services is provided, such as phones, computers, printers, or radios.

Switching Networks

Switching networks provide services and connect terminal devices. There are two types of switching networks: circuit switch and packet switch.

Circuit Switch Network

Circuit switch network (CSN) provides voice telephone services and can support imagery and data exchange. Tactical telephone connectivity is provided by a combination of both tactical and commercial circuit switches, telephone networks, data networks, telephone devices, and

transmission systems. In addition to networks established in an AO, tactical telephone networks can interface with DSN and DRSN strategic and commercial networks through DISA STEP/teleport sites in order to provide worldwide connectivity. Various types of telephones—both tactical and commercial—provide secure and nonsecure capabilities. Depending upon the switch type, other services, such as call conferencing, call forwarding, voice mail, and radio-wire interfaces, may be available.

Packet Switch Network

Packet switch network (PSN) provides imagery and data services and can support voice services. Tactical data network connectivity is provided by a combination of both tactical and commercial equipment, software, protocols, and transmission systems. In addition to networks established in an AO, tactical data networks can interface with SIPRNET, NIPRNET, Internet, and strategic and commercial networks through DISA STEP/teleport sites in order to provide worldwide connectivity. Encryption devices, secure enclaves, tunneling, and virtual private networks provide secure and nonsecure capabilities. Voice over IP technology permits telephone connectivity over data networks.

Multiplexing Networks

Multiplexing networks combine multiple circuits into a single link and layer different services together for transmission.

Transmission Networks

Transmission networks provide connectivity and extend multiplexed and other services to users and between nodes. There are two types of transmission networks:

- Wideband:
 - Guided (cable) provides cable connectivity of multiplexed links.

- Unguided (MCR) provides terrestrial- and space-based LOS and beyond LOS MCR connectivity of multiplexed links.
- Narrowband (SCR) provides OTM voice, but also can support low bandwidth imagery and data exchange.

This page intentionally left blank.

CHAPTER 6

COMMUNICATIONS PLANNING

The primary purpose of tactical communication is to enable and support command and control. Communications planning must be detailed enough to provide clarity, but also flexible enough to respond to the chaos inherent in the battlespace and during the conduct of military operations.

The relationship between command and control and communication is inextricable. The commander must recognize that command and control is the means to identify what needs to be done and then see to it that appropriate actions are taken. Information is essential: it *informs* the commander as he develops situational awareness and makes a decision, and it *informs* subordinates as they carry out the decision and provide feedback to the commander. In either case, the value of information is not derived from its mere existence, but rather from its ability to be shared and exchanged within a particular context. Isolated information is meaningless; shared information forms the basis of command and control.

Despite continued technological advances, uncertainty—the fog of war—remains and will always be the defining problem of command and control. Enabling commanders and staffs to better deal with uncertainty is the goal of a C2 system, and communications plays a pivotal role in supporting this goal.

Col John R. Boyd postulated in *Boyd: The Fighter Pilot Who Changed the Art of War* by Robert Coram that if a military force is to adapt and thrive in the chaotic conditions of combat, it must harmonize its own internal dynamics and reduce organizational friction so that it can concentrate efforts against the enemy. Failure to do so inhibits organizational freedom of action, compelling that organization to remain inordinately focused on itself and not on an adversary. The effect of excessive internal friction is a slower

OODA cycle relative to the enemy's and a necessarily reactive posture. Additionally, he describes combat—the clash of opposing OODA loops—as a strategic game in which one side must be able to diminish an adversary's ability to communicate or interact with his environment while sustaining or improving its own. Put another way, the efficient exchange of information—effective communication—helps smooth out internal dynamics and allows the commander to concentrate on the uncertainty that matters most: what are the capabilities and intentions of the enemy, and how can he be defeated?

From this perspective, planning—projecting thoughts forward in time and space to influence events before they occur—ensures that a communications network properly enables command and control and links the MAGTF together.

Planning for a Dynamic Network

Planners must understand, anticipate, and be prepared to deal with change. The fog of war, emerging threats and opportunities, and the fluidity of the battlespace require a dynamic communications network and planners who understand that—

- Communications planning—like other forms of planning—is sequential, concurrent, repetitive, scalable, and continuous. Additionally, communications planning follows the same tenets of the Marine Corps Planning Process: top-down (the G-6/S-6 drives the process and is involved at every step), single battle (action anywhere is related to action everywhere, whether related to tactical conditions or aspects of the communications network), and integrated (across staffs and across communications functional areas).

- There are discrete capabilities, limitations, and availability of strategic, operational, and tactical communications resources. Employment considerations particularly shape the means by which a network is established and help define timelines and coordination requirements.
- Designing the communications network requires a detailed understanding of the command's task organization, mission, commander's intent, and concept of operations (CONOPS). To this end, the communications planner must be "tied to the hip" of the commander, operations officer, and other staff members.
- Designing the communications network requires identification of both specified and implied information exchange requirements. Put another way, information exchange requirements must be accounted for though they are often unarticulated. Planners must forecast requirements by anticipating, interpreting, and actively discovering them within the context of current and future events in the battlespace.
- The communications network must facilitate the rapid, unconstrained flow of information to properly support command and control. A network that adheres to the principles of communication—flexibility, interoperability, reliability, survivability, timeliness, and security—is best equipped to provide that support and reliably satisfy information exchange requirements.
- Redundancy is the preeminent feature of a well-designed network and accounts for the principles of communication. The degree to which redundancy is achieved largely determines how well a network performs. Redundancy takes on many forms and reflects a defense-in-depth approach for supporting command and control:
 - Redundant capabilities are a diversity of systems that span the different means of communication and best provide alternatives for the exchange of information.
 - Redundant links are multiple pathways that provide alternate or additional routes. In the event one route fails, information can be rerouted through alternate links.
 - Redundant equipment is held in reserve accounts to be used as replacements in the case of equipment failure, degradation, or changing requirements. This applies to both communications equipment and support equipment, such as generators.
 - Redundant data are identical data stored in multiple locations.
- Information exchange requirements exist at all times during a military operation. Communications support is, therefore, persistent but may scale up or down over time. Communications resources are likely first-in and last-out.
- Communications resources are limited, frequently critical low-density, and face competing requirements. Priorities, derived from information exchange requirements, help balance available resources with demands.
- Because of the relationship between communications and command and control, limited availability of resources and the detrimental effect a disturbance in one aspect of the network may have on the force as a whole demands that the communications network be carefully and continuously monitored. Effective control processes and procedures—especially the interplay of direction and feedback—help ensure unity of effort as well as mitigate deficiencies.
- The electromagnetic spectrum is a warfighting domain in which offensive and defensive tasks can be accomplished, and which, as with other aspects of the battlespace, requires the careful coordination and deconfliction of activities within it. Competition for access in the spectrum is acute. Besides communications equipment, various systems that support warfighting functions—as well as those of other Services and coalition partners—require access to the electromagnetic spectrum; incomplete

coordination may result in adverse effects that threaten force protection and inhibit military operations. Additionally, as the electromagnetic spectrum is a global commons and has no geographic boundaries, the enemy, host nation, and civilian activities in it become crucial planning factors.

Marine Corps Planning Process

Mission Analysis

Whether deliberately as part of an operational planning team or rapidly as a communications platoon commander, the communications planner begins formulating a network by first dissecting the challenge at hand into manageable parts (see app. E). Mission analysis frames the problem and identifies information exchange requirements. The communications planner—

- Analyzes the command's mission, commander's intent, tasks (specified, implied, and essential), and purpose of the operation.
- Analyzes the friendly force task organization including higher and adjacent units.
- Evaluates and develops initial assumptions as well as constraints and restraints.
- Evaluates the battlespace with respect to friendly and enemy forces, terrain, and weather to determine how these factors and conditions may influence communication.
- Analyzes resource availability.
- Determines and assesses information exchange requirements, both specified and implied.
- Develops a communications mission statement.
- Develops, from a communications perspective, initial commander's intent and conducts a communications center of gravity analysis.

<p>End state: All information exchange requirements are identified once mission analysis is completed</p>
--

Course of Action Development

There are two complementary aspects of the role of the communications planner in COA development. First, the communications planner helps shape and influence the development of tactical COAs by providing input, from the communications perspective, regarding a COA's feasibility, acceptability, and suitability. Second, the communications planner begins developing communications concepts—potential communications networks supporting one or several COAs—that satisfy information exchange requirements within the context of resource availability. The communications planner—

- Assigns resources to meet information exchange requirements.
- Develops a communications concept in support of each COA.
- Ensures each communications concept is feasible, acceptable, suitable, and complete.
- Provides an estimate of supportability for each COA.

<p>End state: Communications concepts are developed to support each tactical COA.</p>
--

Course of Action War Game

As the tactical COAs are war gamed, the communications planner evaluates each communications concept. During this evaluation, the communications planner continually tests and “what ifs” the potential communications network in order to expose weaknesses. The communications planner—

- Compares the communications concept with the COA and evaluates whether it can effectively respond to friendly and enemy tactical events in the battlespace as they unfold.
- Evaluates the communications concept with respect to equipment failure or degradation.
- Identifies the strengths, weaknesses, risks, and shortfalls associated with the communications concept.

- Refines the communications concept.
- Identifies potential branches and sequels..

End state: Communications concepts are tested through war games and the communications concept is further refined.

Course of Action Comparison and Decision

Using both the commander's COA evaluation criteria and the principles of communications as the lens through which the communications concepts are evaluated, the communications planner assesses the supportability of each COA and the strengths of the concepts compared to one another. The best possible concept emerges and becomes the basis of the communications plan. The communications planner—

- Provides input to the commander and conveys the supportability of each COA.
- Articulates the relative advantages and disadvantages of each communications concept and provides an assessment of capabilities and limitations..

End state: The chosen communications concept becomes the basis of the final communications plan.

Orders Development

As the tactical COA is converted into the overall CONOPS and the command's OPORD is crafted, the communications planner translates the communications concept into the communications CONOPS and develops the communications plan. While the formal manifestation of a communications plan is annex K (see app. F), time available, size of the unit, and mission dictate the extent to which a plan is documented. The purpose of any order—whether delivered in a 200-page document or verbally while studying a map on the hood of a high mobility multipurpose wheeled vehicle—is to provide clarity and promote shared

understanding. Its usefulness is derived not from its collective heft but from its simplicity and brevity. The communications planner—

- Develops the communications plan.
- Works with the G-3/S-3 to develop paragraph 5 of the OPORD.

End state: Communications plan is delivered to the receiver through the most effective and efficient means.

Transition

Carrying the plan through to successful execution requires a deliberate, focused transition that enhances the situational awareness of those who will execute the plan. It also generates tempo and ensures unity of effort. The communications planner—

- Provides a confirmation brief to the commander.
- Conducts transition briefs and drills with the staff as well as with communications personnel.
- Conducts a communications rehearsal that validates the planned network..

End state: Personnel are prepared to execute the plan.

Communications Control

Understanding the relationship between communications and command and control makes it clear that the network is indispensable to those who require it to accomplish the mission. As the United States continues to adapt to the Information Age, the trend of increasingly relying upon a communications network will endure. In many respects, the Marine Corps can no longer satisfactorily conduct military operations and achieve

desired effects without the ability to rapidly and reliably exchange information. It falls on communicators to create and sustain the network despite the dynamic nature of the battlespace and the vexing circumstances within it.

Besides the effects of enemy action and equipment failure, there are many challenges that shape how the network is created and sustained. First, the overriding importance of the network in enabling command and control raises visibility of the presence and status of the network. When the network is degraded, it may detrimentally impact combat operations and expose the force to vulnerability. Consequently, its proper function becomes a concern not just for communicators but for the commander, his staff, and the Marines who rely upon it. Second, the pressure to provide a reliable, adaptable network based on frequently unarticulated requirements engenders an atmosphere of confusion. Uncertainty in a competitive environment is amplified by the need to satisfy elusive—yet essential—requirements. Third, limited resources to satisfy both known and unknown requirements create tension between ends and means. The ends, at times, appear endless, while the means, as always, are finite.

Both communicators and those who are supported face these and similar challenges: they are emblematic of the different factors and conditions that confound command and control in the broadest sense. Recognizing this, it follows that efforts to create and sustain a network are susceptible to the same kinds of philosophies, processes, and procedures that define command and control in an expeditionary maneuver warfare environment. The same C2 doctrine articulated in MCDP 6 applies to communications just as easily as it does to fires, aircraft, or maneuvering units.

There are unique circumstances associated with communications that create tension when applying mission command and control to creating and sustaining a network. A network, by definition, is the interconnected arrangement of different systems. These interrelationships call for careful

coordination, exacting attention to detail, and direction that can require high degrees of specificity. Like any complex system, the dynamic interactions of its various parts may create chaotic, seemingly uncontrollable conditions that can cascade and reverberate throughout the force. A virus, downloaded on a single computer on a data network, can quickly multiply and infect the entire network. An incorrectly performed changeover of a COMSEC key can eliminate a unit's ability to communicate on a pivotal SCR net. The loss of a generator supporting a satellite terminal can isolate a unit from external connectivity. An equipment setting configured wrongly can deactivate a redundant link that provides a key information pathway for a unit once or twice removed.

Communications cannot be viewed in isolation, as conditions affecting it in one part of the battlespace influence conditions that affect it elsewhere. Both physical and electronic interactions make communications susceptible to even the most minor problems. Priorities must be set in the type and volume of voice or data passed over networks to ensure that networks do not become taxed beyond their capabilities.

Communications control (COMMCON) represents command and control of the network. The COMMCON process controls—through decentralized execution—the organization, direction, coordination, planning, and employment of communications resources in order to plan, install, operate, and maintain a communications network responsive to MAGTF operational requirements. While COMMCON is the delegated authority of the G-6/S-6, communications is a function of command and overall responsibility is retained by the commander. The COMMCON process, then, is reflective of command requirements at each level of the chain of command.

There are three functional areas comprising COMMCON: systems planning and engineering, operational systems control, and TECHCON. In a deployed environment, COMMCON is exerted through the arrangement of communications units

and agencies throughout the chain of command to ensure MAGTF communication commonality and fulfillment of functional responsibilities. The MAGTF or major subordinate command communications control center (xCCC) represents the communications planning focal point for a MAGTF and its MSCs. Meanwhile, operational SYSCON centers and TECHCON facilities implement plans and orders and manage the day-to-day functioning of communications networks.

Commander's Intent

A mission contains two parts: the task to be accomplished and the purpose or reason behind it. The G-6/S-6, aside from the commander, plays *the* instrumental role in shaping the communications fight. A commander provides the vision that unifies the separate actions of the force. The G-6/S-6 focuses the efforts of communicators to enable and support command and control. Commander's intent from the communications perspective represents the G-6's/S-6's expression of the desired end state. Despite the technical nature of communications and despite the seeming wizardry of equipment and technology, those who create and sustain a communications network need intent that allows them to act with initiative in the face of chaotic circumstances and in the absence of situational certainty. Effective COMCON cannot exist without clearly articulated intent. Intent is the G-6's/S-6's logic, the intellectual thread that ties together the various separate actions that must occur in the creation of a communications network. Defining the purpose of the network, the method, the key tasks by which that purpose will be achieved, and the end state that determines when that purpose is fulfilled establishes effort focus and harmony.

Center of Gravity Analysis

Along with the intent, an appropriate friendly center of gravity (COG) analysis from the communications perspective illuminates not only

planning considerations but also how those considerations bear on mission execution. Distributed awareness of the G-6's/S-6's determination of the COG, which likely will change over time and as the situation dictates, provides aiming points for how to create and tend to a network given limited resources and competing requirements. An effective COG analysis should reflect the G-6's/S-6's identification of the communications network's source of strength in enabling command and control.

A thorough COG-critical/capability-critical/requirement-critical vulnerabilities construct ensures a level of precision in identifying sources of strength as well as corresponding vulnerabilities that, when properly considered, positively shape network creation and sustainment. A notional commander's intent can be constructed from the COG-critical/capability-critical/requirement-critical vulnerabilities construct and is illustrated in figure 6-1.

Commander's Critical Information Requirement

Finally, CCIR, from the communications perspective, identifies information on friendly activities, enemy activities, and the environment that the G-6/S-6 deems critical to maintaining situational awareness, planning future activities, and assisting in timely and informed decisionmaking. It focuses not only collection activities (e.g., whether related to network status reporting requirements or indications of enemy interference), but also current and future planning efforts. It also provides thresholds that, when tripped, support key decisions regarding the network. The following list is an example of a CCIR:

- PIR (information about enemy capabilities and intentions):
 - Indications and warnings of enemy network intrusion activities.

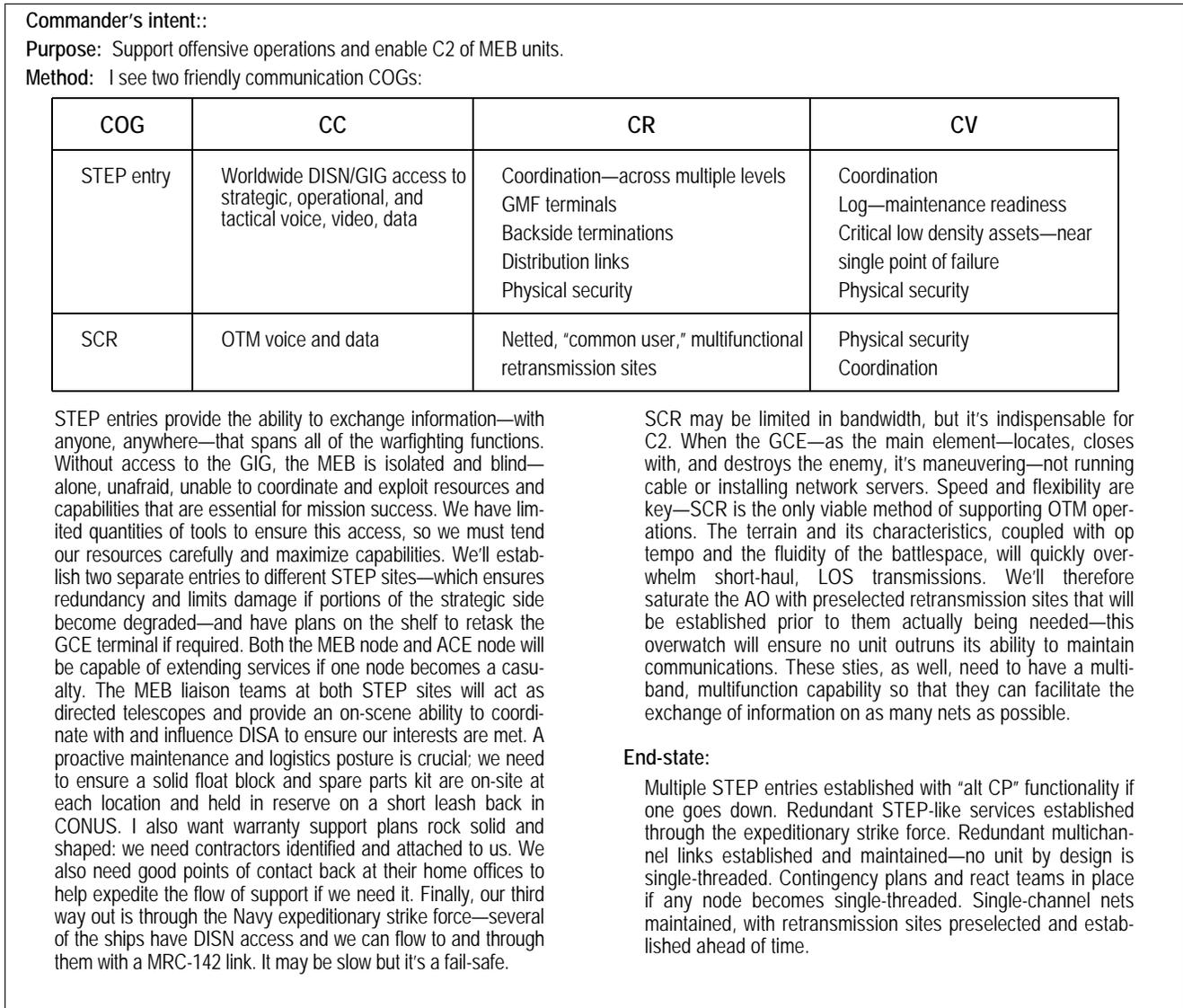


Figure 6-1. Notional Commander's Intent from Communications Perspective and COG Analysis.

- Indications and warnings of enemy jamming activities.
- Indications and warnings of enemy attacks against communications nodes or retransmission sites.
- Indications and warnings—or use—of enemy antiradiation or electromagnetic pulse weaponry.
- FFIR (information about friendly forces):
 - Loss of a key communications node, facility, or retransmission site.
 - Loss of STEP site/gateway access.
 - Loss of redundant paths that "single thread" a key node and which could lead to node isolation.
 - Maintenance readiness of critical low density assets that fall below 90 percent.
 - Inability to effect repair of deadlined or degraded GMF terminals.
 - Coordination difficulties with DISA that inhibit continued operation or shifting of GMF links.
 - Weather forecasts or actual conditions that negatively impact the operational capability of communications equipment.

- EEFI (specific pieces of friendly information to conceal from the enemy):
 - Frequencies and call signs.
 - Location of GMF terminals.
 - Location of retransmission sites.

Communications Control Agencies

Systems Planning and Engineering and xCCC

A MAGTF or MSC G-6 exerts COMMCON through the xCCC and is responsible for providing operational communication support to the MAGTF or MSC commander and directing subordinate xCCCs (see fig. 6-2). Systems planning and engineering is the primary function of the xCCC and involves current and future operations as well as future plans in order to design, implement, and responsively adjust communications networks to satisfy operational requirements. The xCCC and its systems planning and engineering cell, which is normally staffed by both G-6 and supporting communications unit personnel, designs, engineers, and adjusts aspects of the

communications network through promulgation of communications plans, orders, and technical directives, and supervision of their execution. Functions of the xCCC include—

- Producing and distributing the Information System directory (see app. G).
- Continuously capturing operational requirements and designing/modifying responsive communications networks that satisfy them; maintaining visibility and situational awareness of the operational communications network as well as the battlespace and operational picture.
- Analyzing the performance of the communications network.
- Developing and issuing communications plans, orders, and technical directives that implement or adjust a communications network; providing direction to the local SYSCON and subordinate xCCCs; and coordinating with higher, adjacent, and subordinate xCCCs as required (see fig. 6-3).
- Conducting planning as part of an operational planning team.

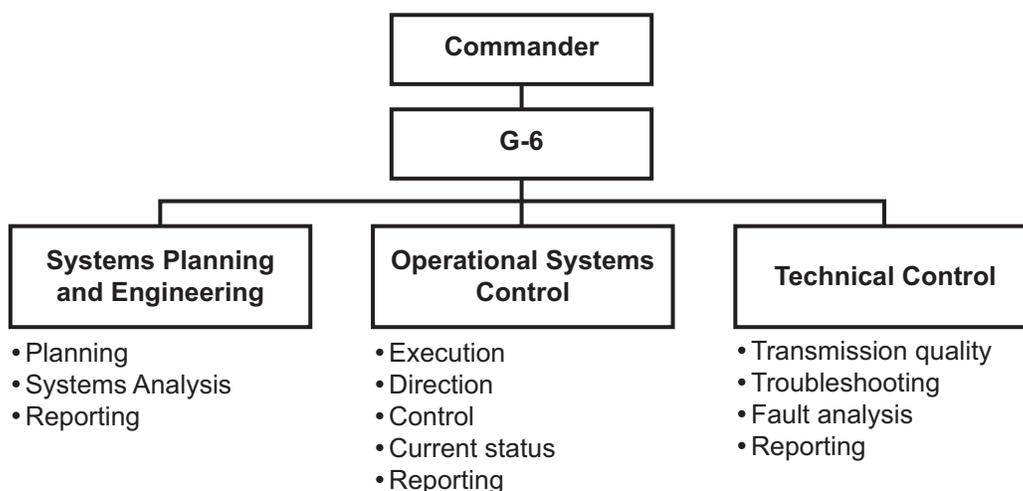


Figure 6-2. Communications Control.

- Staffing a liaison element in the MAGTF or MSC COC.
- Preparing, maintaining, collecting, and submitting reports from local facilities and subordinate xCCCs to the higher xCCC.

Operations Systems Control

Operational SYSCON represents current operations and day-to-day management of the operational communications network. The operational SYSCON center, which is normally staffed by supporting communications unit personnel, serves as the focal point for information regarding the health of the current network, maximizes the effectiveness of communications resources to meet operational demands, and remedies deficiencies and outages. Operations systems control functions are as follows:

- Maintain visibility and situational awareness of the operational communications network by monitoring system performance, collecting and

analyzing traffic data and outage reports, conducting quality checks and tests to gauge network viability, and maintaining initiative and tempo.

- Receive direction from the xCCC and higher SYSCONs.
- Implement and supervise the execution of communications plans, orders, and technical directives and provide direction to the local TECHCON facility and the subordinate SYSCONs. Coordinate with higher, adjacent, and subordinate SYSCONs as required.
- Coordinate actions for service restoration and, when required, supervise emergency adjustments to the communications network.
- Prepare, maintain, and distribute information management products related to the communications network, including information systems directories, user operating instructions, and communications-electronics operating instructions (CEOI).

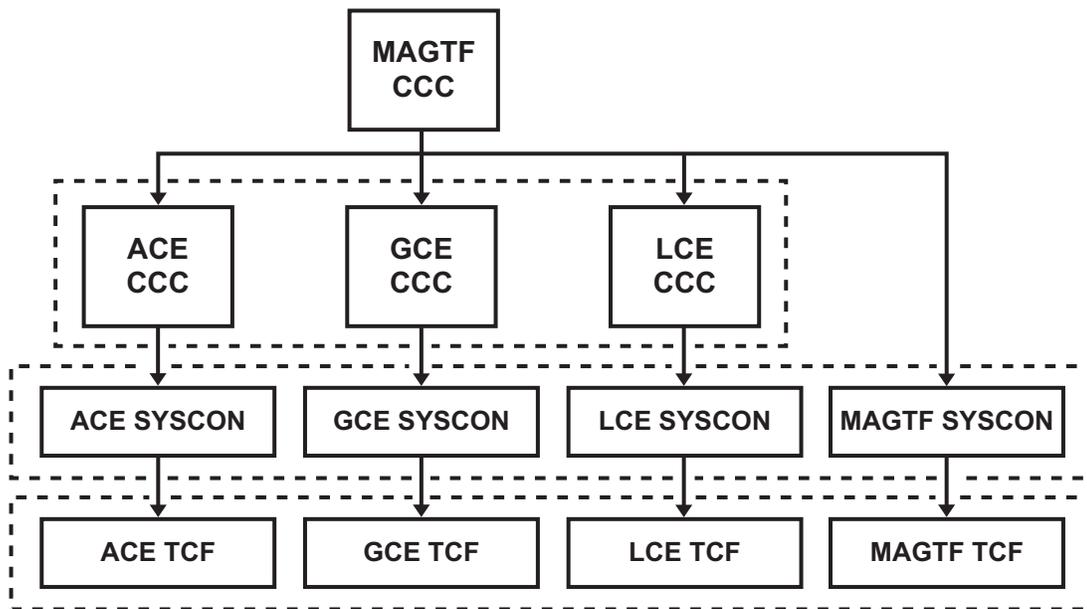


Figure 6-3. Communications Control Agency Relationships.

- Prepare, maintain, collect, and submit reports from local facilities and subordinate SYSCONs to the xCCC.
- Recommend corrective actions to the xCCC for network adjustments or changes.
- Ensure network-wide compliance with applicable security directives.

Technical Control

The TECHCON element of COMMCON is the means of exercising centralized, technical supervision and direction of the installation, operation, and maintenance of communications links, circuits, and systems. The TECHCON facility, which is normally staffed by supporting communications unit personnel, ensures the integrity of signal paths and reroutes or reconfigures portions of the communications network to rapidly respond to operational requirements. TECHCON functions include—

- Conducting monitoring, performance testing, signal conditioning, and circuit rerouting to improve and maintain circuit quality and preempt circuit degradation.
- Activating, deactivating, and reconfiguring circuits, links, and systems based on priorities established by and at the direction of the SYSCON.
- Analyzing factors involving circuit, link, or system interruptions, failures, and disturbances; recommending corrective actions to the local SYSCON for network adjustments or changes.
- Implementing and supervising the execution of technical directives and providing direction to local communications elements and subordinate TECHCONs. Coordinating with higher, adjacent, and subordinate TECHCONs as required.
- Directing troubleshooting efforts and coordinating employment of trouble teams to isolate and remedy circuit, link, or system problems.
- Preparing, maintaining, and submitting reports to the local SYSCON.

CHAPTER 7

INFORMATION SYSTEMS SECURITY

The term INFOSEC is defined in the JP 1-02 as 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. All MAGTF command and control relies on the confidentiality, availability, and integrity of tactical communications networks and information systems. Protecting these networks and systems from exploitation, disruption, and destruction is of highest priority.

Threats to the MCS originate from a variety of sources and continue to evolve. They range from conventional EW/signals intelligence techniques to newer forms such as computer intrusions by hackers; drug traffickers; foreign intelligence agencies; disaffected, disgruntled, or disloyal personnel; and, potentially, battlefield adversaries. Intruders have repeatedly demonstrated their ability to penetrate military information systems. With the increasing inter-connection of information systems, such attacks threaten the

entire Defense Information Infrastructure including all the tactical communications networks and information systems that interface with and use that infrastructure.

As with other forms of security, the first step in providing effective INFOSEC is understanding the threat. This understanding includes identifying threat objectives, capabilities, techniques, and friendly vulnerabilities. The threat's characteristics affect the way the MAGTF must defend its information systems.

At the strategic level, DISA responds to threats with a defensive information warfare strategy based on protecting the infrastructure and data, detecting and promptly reacting to attacks, and maintaining service. On the battlefield, the MAGTF responds to threats through a similar C2 protection strategy.

This chapter focuses principally on INFOSEC and two key security disciplines to counter those threats: COMSEC and computer security (COMPUSEC).

SECTION I. COMMUNICATIONS SECURITY

The communications system's COMSEC is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. It includes physical, cryptographic, transmission, and emission security. The goal of COMSEC is to protect friendly communication from enemy exploitation while ensuring unimpeded use of the assigned electromagnetic spectrum. The organization must be able to employ communications equipment effectively in the face of

enemy efforts. Its COMSEC is an integral part of electronic protection—the element of EW that focuses on shielding our capabilities. The requirements of COMSEC must be integrated into communications systems planning and must focus on providing secure communications without impairing reliability or responsiveness. Modern communications equipment includes features such as integrated encryption and frequency hopping capabilities, which contribute to communications protection. The security of our communication, however, depends on the proper operation of communications equipment and adherence to proper procedures.

Responsibilities

The responsibility for COMSEC lies with the command and with each individual user of communications systems and networks. The G-6/S-6 is responsible to the commander for the overall planning, supervision, and coordination of COMSEC matters, including the administrative, day-to-day management of COMSEC material. Specific staff responsibilities include—

G-6/S-6

- Incorporating COMSEC requirements into the communications plan.
- Supervising communications to ensure proper equipment operation and use of COMSEC procedures.
- Training communications personnel in COMSEC and electronic protection techniques.
- Promoting awareness of the enemy EW threat among all members of the command.
- Advising and assisting the unit security manager, G-2/S-2, and G-3/S-3 in matters regarding communications and information systems and electronic security and protection.
- Preparing an emission control (EMCON) plan to include employing alternate means of communications.
- Advising and assisting the G-3/S-3 in matters regarding the command's OPSEC and deception plan.
- Instructing all users on proper operation of communications systems and equipment and proper communications procedures.
- Coordinating with G-2/S-2 and G-3/S-3 for conducting COMSEC monitoring and analysis operations.
- Supervising Electronic Key Management System (EKMS) managers in the execution of their duties and responsibilities for control and accountability over classified EKMS material and equipment, including distribution and destruction of material in accordance with current directives.

- Ordering COMSEC/EKMS material and equipment for operations and exercises.
- Developing, in coordination with the unit security manager, emergency destruction plans for COMSEC/EKMS materials and equipment.

G-2/S-2

- Advising and assisting the communications officer on electronic protection techniques based on analysis of enemy signals intelligence and EW capabilities and other threats to the unit MCS and operations.

G-3/S-3

- Integrating communications information systems protection, including COMSEC and electronic protection, into the CONOPS in accordance with the commander's guidance.
- Planning and supervising the physical protection of essential communications nodes.
- Planning and supervising the overall EW effort in coordination with the G-2/S-2 and the G-6/S-6.

COMSEC Management Office

- Providing and sourcing MEF units with mission-essential contingency COMSEC material.
- Establishing EKMS policy within the MEF.
- Deploying as a MEF COMSEC management office in support of the MEF or deploying or supporting a joint COMSEC management office for a joint HQ.

Command Security Manager

- Serving as the commanding officer's advisor and direct representative in matters pertaining to the security of classified information and personnel.
- Developing written command information and personnel security procedures, including an emergency plan that integrates emergency destruction bills, where required.
- Ensuring that threats to security, compromises, and other security incidents are reported, recorded and, when necessary, investigated thoroughly. Ensures incidents falling under the investigative jurisdiction of the Naval Criminal Investigative Service are immediately referred to the nearest Naval Criminal Investigative Service office.

For a complete list of all security manager duties/requirements, refer to Secretary of the Navy instruction 5510.30B, *Department of the Navy Personnel Security Program Instruction*, and Secretary of the Navy publication M-5510.30, *Department of the Navy Personnel Security Program*.

Cryptosecurity

Cryptosecurity is the COMSEC component that results from providing technically-sound cryptosystems and properly using them. With the built-in encryption feature of the single-channel ground and airborne radio system (SINCGARS) and the widespread availability of encryption equipment for other SCRs and the switched backbone (SBB), it should be possible to cover all tactical communications. Accomplishing COMSEC requires detailed planning that is conducted as an integral part of the overall communications planning effort. The requirements for encryption must be determined and the appropriate equipment and material must be obtained to support those requirements. The CJCSM 6231.05B, *Manual for Employing Joint Tactical Communications—Joint Communications Security*, provides detailed COMSEC information and is a key reference in planning. Units must act immediately upon receipt of a COMSEC callout message to obtain the required cryptographic material. This material is to be employed in a particular exercise or operation to include, when designated, the intertheater COMSEC package. In the future, the joint key management system, which is under development, will enable the electronic distribution of keys throughout the JTF.

Modern cryptographic systems use random number generators to accomplish encryption. By initializing the random number generator with a seed number, a deterministic sequence of pseudorandom numbers is generated. Each time the same seed is used, the same sequence of numbers is generated. The pseudorandom numbers may then be used, for example, to modify a bit

stream to send over a communications network. If the receiver of the bit stream has access to the seed used by the sender, the modified bit stream can be decoded. The bit stream may consist of data, or it may be digitized voice. With this approach to encryption, it is not necessary for the equipment itself to be highly classified as was the case with World War II era encryption equipment. Only in losing the seed number, or key, will the encrypted information be compromised; therefore, the management and control of keying material is of utmost concern. Commanders should limit the holdings of keying material to the minimum required for operations. This material must be transported, stored, safeguarded, destroyed, and accounted for in strict accordance with existing regulations.

Transmission Security

Transmission security (TRANSEC) is the component of COMSEC that results from applying measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. One goal of the Marine Corps is to secure all tactical communications circuits and SCR networks, but even encrypted communication may be targeted, exploited, and disrupted by an enemy's intelligence and EW organizations via traffic analysis, direction finding, and jamming. The TRANSEC component is an important part of the unit electronic protection effort.

Single-Channel Radios

Strict radio discipline and adherence to authorized procedures are key to ensuring TRANSEC over SCR networks. Operating SINCGARS in a frequency-hopping mode provides maximum protection against enemy EW capabilities. Other TRANSEC measures include—

- Training operators thoroughly on proper communications procedures and equipment operation. This includes all Marines who may operate SCR, not just MCS personnel.

- Avoiding unauthorized transmission. Measures also include testing and maximizing use of data networks to minimize transmission time and opportunity for enemy direction finding.
- Using transmitter, antenna, and power combinations that produce minimum wave propagation and emission intensity consistent with reliable communications.
- Adhering to authorized channels/frequencies.
- Requiring user or device authentication systems to protect against imitative deception on nonsecure networks.
- Changing call signs and frequencies on nonsecure networks.
- Responding to and reporting enemy jamming promptly. Operators should continue to operate on assigned frequencies in a secure mode, unless otherwise directed by a competent authority, and they should attempt to work through the interference.
- Adhering to all EMCON restrictions and observing radio silence.
- Using communications means that do not radiate in the electromagnetic spectrum, such as messengers, visual and sound signaling, and local wire loops.
- Using terrain masking to shield transmission systems from enemy EW systems.
- Remoting transmitters and avoiding the clustering of antennas.

Multichannel Radio and Wire

Information is often compromised when wire is assumed to be secure. While wire is inherently more secure than radio, the SBB normally uses MCR to move traffic beyond the local geographic area. Furthermore, when a wire infrastructure is used over an extended area, the line can be tapped. Sensitive traffic—voice or data—should be either sent over covered circuits or encrypted prior to transmission over nonsecure circuits. Any MCR operation in close proximity to the enemy

is of concern because the transmission equipment's high-power output and the continuous mode of operation are easily detectable and could reveal the location of units and command posts. Use of terrain masking and, where possible, limiting forward and back lobe emission into enemy territory are measures that can reduce the vulnerability of MCR to enemy EW.

In addition to encryption and measures to reduce the probability of interception, traffic flow security is required. Traffic flow security conceals the presence of messages on communications circuits. Traffic flow security is normally achieved on the SBB by using trunk encryption devices to generate a continuous stream of bits, making the circuit appear busy at all times.

Emission Security

Emission security (commonly referred to as TEMPEST) is the component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from intercepting and analyzing compromising emanations from cryptographic equipment and telecommunications systems. The operation of communications and information systems may result in unintentional electromagnetic emissions. Although tactical equipment is designed to reduce the possibility of such emissions, commercial off-the-shelf (COTS) equipment is not. Unintentional emissions are extremely susceptible to interception and analysis and may disclose classified information. Commanders must follow applicable regulations, providing guidance on control and suppression of such emissions.

Physical Security

Physical security is the COMSEC component that results from all physical measures necessary to safeguard classified equipment, material, and documents from physical access or observation

by unauthorized persons. The access to classified cryptographic information must be tightly controlled. When a commander or designated representative has determined that an individual has a need-to-know and is eligible for access, then access to classified cryptographic information will be formally authorized. The authorization process must include an introduction to the unique nature of cryptographic information, its unusual sensitivity, the special security regulations governing its handling and protection, and the penalties prescribed for unauthorized disclosure. In the event of a violation of physical security, a report is required. Reportable COMSEC incidents include—

- Loss of material.
- Unauthorized viewing.
- Capture of individuals having access to COMSEC information.

Currently, fielded COMSEC equipment is unclassified for external viewing when appropriate covers are in place and no keying material is visible. Consequently, the exposure of such equipment to casual viewing by uncleared personnel, whether by accident or as the result of operational necessity, does not constitute a reportable violation.

Personnel planning for and setting up the SBB must be aware of the requirement for red/black isolation. Red/black isolation refers to the separation of circuits, systems, equipment, and areas that handle classified plain text (red) information in electronic signal form from those who handle unclassified (black) information in electronic signal form. Black signals include encrypted signals because these signals would not divulge national security information if recovered and analyzed.

SECTION II. COMPUTER SECURITY

Increasingly, command and control on the modern battlefield depends on information systems. The amount of data that is processed and the tempo of operations combine to make manual procedures inadequate except at the small-unit level. Even at the small-unit level, automated systems are proliferating, particularly in the fire support area. The increasing dependence on tactical information systems drives the requirement to protect these systems from disruption or exploitation by hostile forces. In much the same way that COMSEC provides the security for information transferred through communications systems, COMPUSEC provides the security for information that is collected, stored, processed, and displayed by computers and peripheral equipment at user locations.

Threat to Computer Security

With the openness of the Internet, intruders can inflict damage on information systems from virtually any location, with little fear of detection. Today's information systems are connected into worldwide communications networks that are only as secure as their weakest links. The enemy can easily gain access to much of the same information infrastructure used by the MAGTF. Intruders do not require sophisticated technology. A non-technical means, such as a compromised password, can bypass LAN security features. Once access is gained, the attacker can employ malicious logic to inflict tremendous damage on our information systems. Malicious logic is computer code designed to mine for data as well as deny, destroy, modify, or impede system configurations, programs, data files, or routines. Types of malicious logic include viruses, Trojan horses, logic or time bombs, and worms. The enemy will have several objectives in attacking MAGTF information systems, to include, but not limited to, information compromise, information modification, and denial of service.

Information Compromise

A major goal of threat attacks on MAGTF information systems is to gain access to classified or sensitive information. Access to this information provides the enemy insight into MAGTF, joint, and national capabilities; force and resource locations; plans and intentions; readiness status; and knowledge of what is known about the enemy. This type of information, when discovered and used to an advantage, has often decided a battle's outcome. In today's environment, this type of information is surprisingly easy to obtain. For example, careless e-mail exchanges with family and friends can reveal planned MAGTF movements and operations. E-mail is easily and readily collected by enemy agents.

Information Modification

Another objective of attacks on our information systems is information modification. Such information corruption can be used to create an electronic deception. Undetected, it can lead to incorrect assumptions and subsequent faulty decisions. In other instances, the attack may be designed to destroy information required to execute the MAGTF planning and decision cycles. In either case, the information modification attack can severely reduce confidence in the MAGTF's information systems. The MAGTF's ability to execute the OODA loop more quickly than the enemy depends greatly on the quality of the information provided by the information systems used. Reduced confidence, delays, and undetected or faulty information can all severely degrade the commander's ability to make sound and timely decisions.

Denial of Service

Still another objective of enemy attacks on our information systems is either total or partial

restriction of our ability to process, retrieve, and disseminate information. Data corruption results in lost confidence and denial of service. Successful enemy attacks on stored data, applications, or operating systems may render information systems unusable. Physical damage to or destruction of equipment, facilities, and personnel will be a high priority for the enemy because our communications systems' capabilities are viewed as critical vulnerabilities and key targets. Attackers may range from terrorist truck bombers to more technologically-advanced enemies using directed energy weapons.

The environment is also a potential disruptive force. Information systems, particularly COTS, are very susceptible to power surges; temperature extremes; and dusty, dirty, and sandy conditions encountered in the austere, littoral areas in which the MAGTF operates.

Protection

Protection of MAGTF information systems is essential and COMPUSEC is the means of providing it. This protection includes knowledge of the threat and employing operating procedures, equipment, and personnel training to counter that threat. It also includes putting measures in place to detect intrusion early, plan for immediate action to counter attacks, and, if necessary, restore lost data and service.

Chief Information Security Officer Responsibilities

A command responsibility, COMPUSEC must be understood and practiced by all MAGTF information system users. However, overall network and information systems security responsibility belongs to the communications officer. Responsibilities include the following:

- Establish policy and procedures for LAN, WAN, and information systems management. Procedures include managing user identification and assigning passwords.

- Maintain visibility and control of the operation and use of network services.
- Coordinate network management functions, including security, with the individual LAN managers and information systems coordinators.
- Provide for training and education in threat capabilities and COMPUSEC procedures, with assistance from the unit security manager, G-2/S-2, and G-3/S-3 in coordination with all LAN managers and functional information systems coordinators.

The communications officer provides overall COMPUSEC management through policies, directives, plans, and training. The communications officer guides LAN managers, information systems coordinators, and information systems users in implementing procedures necessary to maintain reliable and secure information systems. Much of the security for information systems is provided at the individual workstation through operating systems and application-specific access mechanisms. However, for networked applications and services, a well-devised network security plan is necessary to manage the various accesses and privileges that control read and write access to files and data. Monitoring the network is required to document activity and detect intruders. The COMPUSEC procedures must be integrated with and complement the overall communications information systems plan to ensure responsive service to authorized users while protecting against unauthorized access.

Implementation

The DODD 8500.01E, *Information Assurance (IA)*, and DOD Instruction 8500.2, *Information Assurance (IA) Implementation*, establish and define mandatory, minimum standards for automated information systems security. These documents promote using computer-based security features that emphasize the personal responsibility of system users. Current procedures rely on standalone workstations and system high networks, which require dedicated routers and switches, making system security management

difficult. There are many ongoing programs to provide improved security services for individual workstations, LANs, and the overall defense information infrastructure. Multilevel Information Systems Security Initiative (MISSI) products and services are being fielded incrementally as technology matures. They include cryptographic cards, firewalls, high assurance guards, in-line network encryptors, and security management services.

Cryptographic Cards

Personal computer-configured cryptographic cards are gradually being introduced to provide different levels of INFOSEC protection, including confidentiality, data integrity, identification/authentication, and nonrepudiation.

Firewalls

The Institute for Science and International Security defines a firewall as a system or group of systems that enforce an access control policy between two networks.

There are many different firewall types, but the industry-accepted monikers for these are “packet filtering firewalls” and “proxying firewalls.” Packet filtering firewalls can be either static or dynamic in nature. Proxying firewalls can proxy traffic at the circuit level or application level and can provide “store and forward” type capabilities.

Firewalls are one layer of defense used to protect a network’s critical information, information systems, and applications. If used correctly, they can prevent unauthorized ingress and egress of the network and unauthorized disclosure of the network.

Current firewall technology can provide standard firewall capability sets, such as blocking and logging of nefarious traffic; anti-spam, URL [Uniform Resource Locator] filtration, such as white listing and blacklisting; and antivirus functionality.

High Assurance Guards

High assurance guards, such as the secure network server with standard mail guard, are used to

protect against unauthorized release of classified information from a classified facility while allowing the release of unclassified information. High assurance means that the guard has been verified by the National Security Agency to be highly-resistant to penetration based on the application of rigorous security software engineering methods, extensive penetration testing, and security analysis during its development, production, and fielding. The guard is required for information processing and exchange between facilities or systems operating at different levels. The guard also ensures that external requests for access to the “guarded” higher security level locations are approved before allowing that access.

In-Line Network Encryptor

In-line network encryptors provide data confidentiality and integrity across LANs and WANs. They employ encryption and access control through cryptographic key management. Some in-line network encryptors can also provide traffic flow security services. In-line network encryptors operate with IP routers, packet switches, synchronous optical networks, and asynchronous transfer mode networks. Some of the in-line network encryptors offer combinations of these capabilities to allow for the future growth of networks based on synchronous optical network and asynchronous transfer mode technologies. A key feature of in-line network encryptors is that they encrypt only the data, not the address information. This enables the transmission of classified data on unclassified networks or SCI data on secret networks. In-line network encryptors, through software configuration and appropriate keying material, are used to link multiple sites.

Security Management Services

Security management services include security measures such as cryptographic keying, access control, authentication, and the use of passwords. These services are needed to implement effective information systems security programs

within the MAGTF. Key security management services include—

- Local authority workstations that reside on the LAN and provide security capabilities such as digital signatures, cryptographic keys, and access control permissions.
- Rekey managers that work in conjunction with electronic key management systems to provide cryptographic rekey support for MISSI products.
- Audit managers that provide support for the collection and analysis of security-relevant events that can be audited and are associated with MISSI products. Repeated failed user login is an example of a security-relevant event that can be audited.
- Directories that provide a repository for public security information essential for effective global message addressing. The public part of a user's digital signature is an example of this type of public security information.
- Mail list agents that are used by messaging systems to add security for messages that are sent to many recipients.

SECTION III. INCIDENT RESPONSE

Effective response to attacks on MAGTF information systems requires that all users and support personnel be aware of attack indicators and the procedures to be followed in the event of an attack. The network operations center (NOC) and the Marine Corps Command Center (MCCC) will exchange information in the event of an INFOSEC incident. The MCCC will act as the communications link between the NOC and HQMC throughout the incident. The NOC has the overall responsibility of managing any computer intrusion incidents in the Marine Corps.

Marine Corps Network Operations and Security Command and Expeditionary Support Center

In partnership with Marine-deployed operating forces and supporting organizations, the MCNOSC provides on-site/on-call network technical advice and assistance during the planning, execution, and maintenance phases of a deployment, exercise, or contingency, coordinating swift solutions to technical issues. Functions of the MCNOSC Expeditionary Support Center include—

- Task-organizing expertise within the MCNOSC to support Marines around the globe.
- Acting as operational forces liaison with joint or coalition committees to represent and enforce Marine Corps tactical network policies and standards.

- Providing the appropriate training and onsite technical support for the deployed security interdiction devices (DSIDs). The Marine Corps' tactical CND device provides Marine deployed forces with the same defense-in-depth, boundary-level network security architecture as the garrison commands.
- Providing information technology excellence to all deployed elements of the MAGTF.
- Supporting deploying units.

Naval Network Warfare Command

The Naval Network Warfare Command is the Navy's principal agent for developing EW tactics, procedures, and training. The center deploys personnel trained in C2 protection and is equipped with appropriate information systems security equipment to support battle group and JTF operations. It is responsible for providing computer incident response teams and is the single POC for monitoring the security of information systems. All computer incidents—break-in attempts and malicious logic—are reported to the center. The center publishes advisories containing the latest information on system vulnerabilities and effective countermeasures. These advisories are received from the center's computer incident response team by the MCNOSC and disseminated to all Marine Corps commands.

APPENDIX A

MAGTF SINGLE-CHANNEL RADIO NETS

This appendix provides examples of commonly used MAGTF SCR nets. It includes the basic description of the net, what the net is used for, and which units, or type of units, typically join the net. This list is a planning guide; it is not all-inclusive nor does it define what nets must be established. The establishment of nets is dictated by the situation, mission, and information exchange requirements of a unit in a particular circumstance.

Note: Within each net discussed, the individual units listed normally participate in the specified net as required. They do not constantly guard the net, but enter it as the operational situation requires. Where multiple frequency bands are listed in parentheses following radio net titles, the frequency band most often used is listed first.

Master Net Lists

The MEF Master Net List (MNL) is a database that facilitates the MEF's joint automated CEOI system generation. These files are unclassified and consist of every circuit within the MEF and each circuit's emission requirements, as well as grouping, call sign, and call word information. The list is important to radio network planners because it is the sole source of net assignments and net identifiers. The MEF MNL will be divided into three sections:

- Section 1: Single-channel radio nets.
- Section 2: Units/sections (if required, call sign or call word).
- Section 3: Multichannel radio networks such as Mux (multiplexer)/TRC (transcoder) links or Mk142 and/or AN/TRC-170.

The automated CEOI offers some degree of COMSEC protection and implementation of the following changes increases the difficulty for an adversary to obtain EEFI:

Call signs and call words should be changed daily on all nets/circuits not secured with an encryption device. Exceptions may be necessary when operational needs or safety of life issues outweigh the benefits of COMSEC protection. Units will maintain the capability to implement changing call signs and call words in the event that secure capability is lost.

Tactical SCRs should change frequencies daily. Exceptions to this may be necessary when operational needs outweigh the benefits of COMSEC protection or because of platform-related electromagnetic compatibility limitations, RF propagation limitations, or insufficient spectrum resources.

When using secure, frequency-hopping radio systems, such as the integrated COMSEC SINCGARS, it is not required to change call signs, call words, or frequencies daily. However, because of changes in force structure or capabilities, commanders may designate these nets as single channel, so call signs, call words, and frequencies will be changed daily.

The MEF MNL is controlled by the MEF G-6 and is managed by the MEF frequency manager. The MEF MNL will be reviewed annually for proposed modifications on the basis of input from operating force commanders. Requests for modification of the MNL will be submitted to higher HQ for consolidation and review. The MNL, and thereby CEOI net assignments, should not be modified without the review and approval of the MEF G-6.

The need to maintain consistent, standard radio network terminology demands that MEF radio

circuit assignments be regulated. Joint automated CEOI software is the joint standard and will be used to create the MNL. The electronic CEOI information can be matched to the task organization, edited, generated, and printed for an entire MEF within hours. Unit participation in MNL revisions and compliance are essential to maintaining the currency of this information.

Categories of Nets

There are three general categories of radio nets: operational nets, fires nets, and support nets. These nets are typically employed across all elements of the MAGTF and are not unique to a particular unit or type of unit. The following sections describe those standard categories and provide examples of each.

Standard Operational Nets

Operational nets are established to support the exercise of command and control during combat operations. The type of operation, commander's intent, CONOPS, environment, enemy capabilities, and task organization will influence which nets are required and established.

Command Net (UHF-SATCOM/HF)

Employed to exercise command and coordinate administrative and logistic functions with subordinate elements, command nets are used throughout all levels of command. They are designed to provide long-range communication and a redundant form of command and control for the unit commander. The following organizations are examples of those that would use the command net:

- Division command.
- MEU command.
- Regimental command.
- Reconnaissance command.

Tactical 1 Net (VHF)

Tactical (Tac) 1 nets are used throughout all levels of command to employ operational traffic between the commander and subordinate elements. They are designed to serve as the primary means of tactical control for a commander over his maneuver forces. The following organizations are examples of those that would use the Tac 1 net:

- Division Tac 1.
- Regimental Tac 1.
- Battalion Tac 1.
- Company Tac 1.
- Platoon Tac 1.

Intelligence Net (UHF-SATCOM/HF/VHF)

Used for rapid reporting and dissemination of intelligence, collaborative planning of future intelligence operations, and command and control of ongoing intelligence and reconnaissance operations, intelligence nets are seen at battalion and higher levels of command. Both organic and OPCON collections assets will use this net for reporting and command and control. The following organizations are examples of those that would use the intelligence net:

- Division intelligence.
- Regimental intelligence.
- MEU intelligence.
- Battalion intelligence.

Standard Fires Nets

Standard fires nets are established to support the request for and direction and coordination of fire support during combat operations. The type of operation, commander's intent, environment, enemy capabilities, and task organization will influence which nets are established and required.

Fire Support Coordination Net (VHF)

Fire support coordination is used to coordinate all MAGTF fires and activated at the CE when an FFCC or FSCC is established. The following organizations are examples of those that would use the fire support coordination net:

- SACC.
- FFCC and senior FSCC(s).
- Senior artillery FDC.
- Unmanned aerial vehicle (UAV) squadron/detachment.
- Supporting arms special staff.

Conduct of Fire Net (VHF)

Conduct of fire is established when fire direction is centralized and it is used by forward observers to request and adjust fire. When fire direction is decentralized, each battery in the battalion has a separate conduct-of-fire net that terminates at the battery HQ. There may be as many as four conduct of fire nets in each direct-support artillery battalion. The following organizations are examples of those that would use the conduct of fire net:

- Artillery battalion or battery HQ.
- Battery forward observers.
- Battery liaison officers.
- UAV squadron/detachment.
- Artillery battalion liaison officers.
- Attached/reinforcing artillery units.

Fire Direction Net (VHF)

Fire direction net is used to exercise tactical fire direction of subordinate units by the assignment of fire missions, designation of units of fire, and conduct of time-on-target missions. Subordinate units may use this net to request additional fires from organic and attached artillery units. This net

may also be used for the exchange of infantry fire planning data and fire support coordination information when no other means is available. The following organizations are examples of those that would use the fire direction net:

- Artillery unit HQ.
- Division FSCC.
- Subordinate artillery units.
- Attached/reinforcing artillery units.
- Supporting artillery units.

Tactical Air Request/Helicopter Request Net (HF/VHF/UHF)

Tactical air request (TAR)/helicopter request (HR) net provides a means for MAGTF units to request immediate air support from the DASC. The GCE FSCCs monitor this net and may modify or disapprove a specific request. The DASC uses this net to brief the requesting unit on the details of the mission. Additionally, battle damage assessments may be passed over this net. The following organizations are examples of those that would use the TAR/HR net:

- DASC.
- Marine TACC.
- TACPs.
- TAC(A).
- FAC(A).
- ASC(A).
- Air mission commander (AMC).
- Other MAGTF agencies.
- FSCCs.

Tactical Air Direction/Helicopter Direction Net (UHF/VHF)

The tactical air direction (TAD)/helicopter direction (HD) net provides a means for the direction

of aircraft in the conduct of close air support missions. It enables the DASC to brief support aircraft on target information or assignment to the FAC. The following organizations are examples of those that would use the TAD/HD net:

- DASC.
- Direct air support aircraft.
- TACP.
- FAC(A).
- TAC(A).

Naval Gunfire Control Net (HF)

The NGF control net is used to request, assign, and relieve fire support ships. It is also used to request general support missions and report reliefs, emergencies, and orders pertinent to the execution of scheduled fires. The CATF may establish an NGF control overload net to handle excess traffic. The following organizations are examples of those that would use the NGF control net:

- CATF/SACC.
- Fire support group and unit commanders.
- Fire support ships.
- Screen commanders.
- GCE NGF officer.

Tactical Air Control Party Local Net (VHF)

The TACP local net provides a means for coordination between the air officer at the battalion FSCC and the battalion's forward air controllers' GCE NCS. The following organizations are examples of those that would use the TACP local net:

- Battalion FSCC.
- Forward air controllers.
- FAC(A).
- TAC(A).

Shore Fire Control Party Local 1 Net (VHF)

A shore fire control party local 1 net is used to coordinate shore fire control party activities. The following organizations are examples of those that would use the shore fire control party local 1 net:

- NGF spot team.
- NGF liaison officer.

Marine Corps Standard Support Nets

Standard support nets are established to provide administrative, logistical, and technical support to requesting units during combat operations. The type of operation, commander's intent, environment, enemy capabilities, and task organization will influence which nets are established and required.

Tactical 2 (UHF-SATCOM/VHF) Net

This net exercises command and coordinates administrative and logistic functions with subordinate elements. Tac 2 nets are employed throughout all levels of command. They are designed to serve as a backup to a unit's command net. The following organizations are examples of those that would use the Tac 2 net:

- Division Tac 2.
- Regimental Tac 2.
- Battalion Tac 2.

Combat Service Support Request Net (UHF-SATCOM/VHF)

The CSS request net is used to receive requests from supported units and provide status. The following organizations are examples of those that would use the CSS request net:

- LOCs.
- CLBs.
- Supported unit(s).

Medical Evacuation Coordination (Ground) (VHF) Net

This net is used to coordinate ground medical evacuation (MEDEVAC). The following organizations are examples of those that would use the medical evacuation coordination (ground) net:

- Medical unit HQ.
- MEDEVAC ambulances/vehicles.
- Evacuation/treatment facilities.
- Requesting units.

Medical Evacuation Coordination (Air) (VHF) Net

This net is used to coordinate air MEDEVAC. The following organizations are examples of those that would use the medical evacuation coordination (air) net:

- Medical unit HQ.
- MEDEVAC aircraft.
- DASC.
- Evacuation/treatment facilities.
- Requesting units.

Communications Coordination (VHF) Net

The communications coordination net is used to coordinate the installation, operation, and maintenance of the communications network throughout all levels of command. They are designed to serve as a troubleshooting and coordination link between all communications elements. The following organizations are examples of those that would use the communications coordination net:

- Division.
- Communications company.
- Regiment.
- Battalion.

Convoy Control 1 (VHF/HF) Net

This net is used to control the various elements within a convoy. Multiple convoy control nets

may be required depending on the extent of motor march activity within the force. Convoy control nets exist throughout all levels of command and are designed to serve as a means of coordination for the convoy. Convoy control nets can be internal, designed to control the actual movement of the convoy from checkpoint to checkpoint. Convoy control nets can also be external, providing overall control of all convoys from destination to destination. These are usually controlled by a senior agency. The following organizations are examples of those that would use the convoy control 1 net:

- Convoy commander.
- Designated convoy elements.
- Artillery units and aerial observers.
- Unit HQ conducting convoy.

Helicopter Direction Net (UHF/VHF/HF)

For the Navy, these nets are used by the HDC for positive control of inbound and outbound helicopters in the amphibious objective area. The radar controller in the HDC utilizes these nets to direct flight course and altitude of helicopters, holdings, letdowns, and climb outs. For the Marine Corps, the DASC, TACP, AMC, ASC(A), and TAC(A) use these nets for procedural control of helicopters in the objective area. When both UHF/VHF and HF helicopter direction nets are employed, the HF net is a backup and provides long-range control of airborne helicopters. The following organizations are examples of those that would use the HD net:

- DASC.
- HDC.
- Helicopters.
- AMC.
- Helicopter landing zone control team (LZCT).
- TAC(A).
- ASC(A).
- TACPs.

Landing Zone Control Net (VHF/UHF)

The landing zone control net provides a means for the LZCT to control helicopters traveling between the initial point and the landing zone. The following organizations are examples of those that would use the landing zone control net:

- LZCT.
- Helicopters traveling between the initial point and the landing zone.
- DASC.
- AMC.

Nets Unique to the Aviation Combat Element

Most units use various forms of the standard nets discussed in the previous paragraphs. For example, a Tac 1 net for an infantry battalion performs a similar function as a Tac 1 net for a logistic battalion. The ACE, however, requires additional nets to effect control of aircraft and missiles. Because of the complexity of aviation command and control, the following additional nets describe general SCR requirements unique to the ACE.

Tactical Air Command Net (HF/UHF-SATCOM/Mux)

The tactical air command net is the primary means by which the tactical air commander provides operational tasking to his subordinate units/agencies to include tasking to aviation groups/squadrons to provide aircraft for missions. The following organizations are examples of those that would use the tactical air command net:

- Tactical air control center (Navy TACC)/TADC.
- Marine TACC.
- TAOC(s).
- LAAD battalion COC.
- DASC.
- MAGs/squadrons.
- ATC detachment(s).
- EW/C.

LAAD Battalion Command Net (HF)

The LAAD battalion command net provides a LAAD commander with a means to exercise command, administrative, and logistical functions with subordinate batteries. The following organizations are examples of those that would use the LAAD battalion command net:

- LAAD battalion HQ.
- LAAD battery.

Command Action Net (Mux/HF)

The command action net provides a means for command level coordination of AAW through the exchange of information pertaining to missile battery employment, assignment of air targets, and interceptor/missile coordination. The following organizations are examples of those that would use the command action net:

- Navy TACC/TADC.
- Marine TACC.
- TAOC(s) sector air defense commander.
- Other AAW agencies.

Air Operations Control Net (Mux/HF)

The air operations control (AOC) net provides a means for the TAOC to request interceptor aircraft and to report friendly air defense situation information to the Navy TACC/TADC. Information pertaining to combat air patrol availability, stationing, assignment and disposition of targets, intercept progress, surface-to-air missile (SAM) unit status and employment, and aircraft/missile weapons coordination is passed on this net. The following organizations are examples of those that would use the AOC net:

- Navy TACC/TADC.
- Marine TACC.
- TAOC(s).
- Other AAW agencies.

Antiaircraft Control Net (Mux/HF)

Antiaircraft control net provides a means to control SAM units. Types of information passed on this net include target assignments, fire control orders, weapons control status, battery status reports, and progress of engagements. The following organizations are examples of those that would use the antiaircraft control net:

- TAOC(s).
- LAAD HQ elements.
- EW/Cs.
- Other AAW agencies.

Antiaircraft Intelligence Net (Mux/HF)

The antiaircraft intelligence net provides a means for SAM missile units to report targets. Additionally, this net may be used by the TAOC to pass selected early warning contacts to missile firing units. The following organizations are examples of those that would use the antiaircraft intelligence net:

- TAOC(s).
- Other AAW agencies.
- LAAD HQ/batteries.
- EW/Cs.

Combat Information/Detection Net (HF/Mux)

The combat information/detection (CI/D) net provides a means for reporting on unidentified or hostile aircraft, including initial contact reports, tracking, amplifying, and final disposition reports. The following organizations are examples of those that would use the CI/D net:

- TAOCs.
- Navy TACC/TADC.
- Marine TACC.
- EW/C(s).

- Sector air defense facility.
- Other Service agencies.
- LAAD.
- ATC detachment(s).

Voice Product Net (HF/UHF/Mux)

The voice product net (VPN) provides a means for reporting on hostile targets in a joint environment. The following organizations are examples of those that would use the VPN:

- Other Service agencies.
- Marine TACC.
- TAOC.
- EA-6B(s).

Handover/Crosstell Net (HF/Mux)

The handover/crosstell net provides a means to prepare for the exchange of aircraft control between air control agencies. Multiple nets could be established for other elements such as TAOC-EW/C handover, TAOC-DASC handover, ATC-TAOC handover, or ground control intercept/approach handover. To conserve assets, the functions could also be combined based on expected traffic. The following organizations are examples of those that would use the handover/crosstell net:

- TAOC(s).
- EW/C(s).
- ATC detachments(s).
- Other Service agencies.
- DASC.

LAAD Command Net (HF)

The LAAD command net provides connectivity between the battery, or net control station, and subordinate platoons for administrative and logistical support and to coordinate the tactical

employment of LAAD platoons. The following organizations are examples of those that would use the LAAD command net:

- LAAD battery commanders.
- LAAD platoon commanders.

LAAD Weapons Control Net (HF)

The LAAD weapons control net provides connectivity between the platoon commander—net control—and his section leaders. Multiple nets may be required. It also provides subordinate/senior elements with current air defense warning conditions; weapon control statutes; and pertinent information on hostile, unknown, and friendly aircraft. The following organizations are examples of those that would use the LAAD weapons control net:

- LAAD platoon commanders.
- LAAD section leaders.

LAAD Team Control Net (VHF)

Each LAAD section leader—net control—uses the LAAD team control (LTC) net to control teams and to relay air defense warning conditions, weapons control statutes, and pertinent information on friendly, enemy, and unknown aircraft. Multiple LTC nets, usually one per LAAD section, are normally required. These nets may also be used by teams to pass aircraft sighting reports, engagement reports, position reports, status reports, and resupply requests to section leaders. The following organizations are examples of those that would use the LTC net:

- LAAD section leaders.
- LAAD teams.

Tactical Digital Information Link A (HF/UHF) Net

The tactical digital information link (TADIL) A net provides a secure means for exchanging automatically processed digital data among various tactical data systems. Types of data passed

include air and surface tracks, weapons status, and selected orders and functions. The TADIL A operates as a half-duplex, netted data link. The following organizations are examples of those that would use the TADIL A net:

- Marine TACC.
- TAOC(s).
- EW/C.
- Other Service air control agencies.

TADIL B (Mux) Net

The TADIL B provides a secure means for exchanging automatically processed digital data between various tactical data systems. It is operated in a point-to-point mode using a full duplex wire/multichannel path. The following organizations are examples of those that would use the TADIL B net:

- Marine TACC.
- TAOC(s).
- ATC detachment(s).
- EW/C detachment(s).
- Other Service air C2 agencies.

TADIL-J (Link 16) (UHF) Net

This net provides a secure, time division multiple access, full duplex data link between the TAOC and other LINK-16 capable platforms for automatically processed digital data. Data passed over this link includes detected air tracks, engagement commands, ground tracks of interest, voice communication, and other special information system aircraft/national source data inputs. The following organizations are examples of those that would use the TADIL-J net:

- TAOC(s).
- EWC(s).
- Other Service agencies.

Air Defense Command and Control Net (HF/UHF/TACSAT)

This net provides a means for coordination of air defense operations. The following organizations are examples of those that would use the air defense command and control net:

- Marine TACC.
- TAOC(s).
- Regional air defense commander/area air defense commander.
- Other Service air control agencies.
- SAM units.

Track Supervision Net (Mux/HF/UHF)

The track supervision net (TSN) provides a means for track surveillance personnel to exchange voice information to maintain a clear air picture. This net may assume the functions of a data link coordination net (DCN) based on equipment available. The following organizations are examples of those that would use the TSN:

- Navy TACC/TADC.
- Marine TACC.
- TAOC(s).
- Other Service air control agencies.

Data Link Coordination Net (Mux/HF/UHF)

The DCN provides a means to maintain coordination of data link operations. It may be combined with TSN for single channel operations. Generally, there is one DCN per TADIL-B. The following organizations are examples of those that would use the DCN:

- Marine TACC.
- TAOC(s).
- Other Service air control agencies.

Direct Air Support Net (Mux/HF/VHF)

The direct air support net provides a means for the DASC to request direct air support aircraft from the Marine TACC. Additionally, information pertaining to items such as aircraft stationing, fuel and ordnance status, or progress of direct air support missions, may also be passed over this net. The following organizations are examples of those that would use the direct air support net:

- Navy TACC/TADC.
- Marine TACC.
- DASC.

Tactical Air Traffic Control Net (UHF/VHF)

The tactical air traffic control (TATC) net provides a means for the Navy TACC/TADC and Marine TACC, TAOC, and DASC to exercise airspace control over all tactical and itinerant aircraft in the objective area. Types of information passed over this net include aircraft reports of launches by mission number, clearing aircraft to their assigned control agencies, diverting aircraft as necessary, aircraft completed mission reports prior to landing, and threat updates. Multiple tactical ATC nets are often required for each control agency. The following organizations are examples of those that would use the TATC net:

- TAOC(s).
- Navy TACC/TADC.
- Marine TACC.
- DASC.
- EW/C(s).
- Fixed-wing aircraft.
- Rotary-wing aircraft.
- ATC detachment(s).
- Unmanned aircraft.

Fighter Air Direction Net (UHF/VHF)

The fighter air direction (FAD) net provides a means for air control agencies and elements to control aircraft in the conduct of intercepts. Multiple fighter air direction nets are required and are assigned to major control agencies. The following organizations are examples of those that would use the FAD net:

- TAOC.
- EW/C.
- Interceptor aircraft.
- Other Service air control agencies.

TADIL-C (UHF) Net

The TADIL-C (Link-4A) is a netted data link conducted between the TAOC and F-14 and F/A-18 aircraft. TADIL-C data links can be configured for one-way, limited two-way, and full two-way communication. TADIL-C data links are conducted over UHF radio and are unencrypted. The following organizations are examples of those that would use the TADIL-C net:

- TAOC.
- Interceptor aircraft.
- Other Service air control agencies (E-2C/E-3C).
- EW/C(s).

Tanker (UHF) Net

The tanker net provides a means for in-flight refueling aircraft to communicate with the tanker. Additionally, it can be used by the TAOC to exchange information with the tanker. The following organizations are examples of those that would use the tanker net:

- Tanker.
- In-flight refueling aircraft.
- TAOC(s).
- ATC detachment(s).

Air Defense Alert Net (UHF)

The air defense alert net provides for direct coordination and exchange of critical threat information between UHF-capable, ground-based air defense systems and combat air patrols in adjacent engagement zones. It also provides verbal warning to friendly aircraft transiting minimum risk routes close to missile engagement zones. The following organizations are examples of those that would use the air defense alert net:

- TAOC(s).
- AAW aircraft.
- Non-AAW aircraft.
- EW/C.

Squadron Common Net (VHF/UHF)

The squadron common net provides a means of communication between in-flight squadron aircraft and squadron HQ. Each aircraft squadron has its own common net. The following organizations are examples of those that would use the squadron common net:

- Squadron HQ.
- Squadron aircraft.

Group Common Net (VHF/UHF)

The group common net provides a means of communication between in-flight group aircraft and the aircraft group HQ. Each aircraft group establishes its own common net. Group common net may be established in lieu of squadron commons based on communications asset availability. The following organizations are examples of those that would use the group common net:

- Aircraft group HQ.
- In-flight group aircraft.
- Squadron HQ.

Tower Primary Net (UHF/VHF)

The tower primary net provides a means for the local controller to issue traffic advisories and aircraft clearances within the airport traffic area. The following organizations are examples of those that would use the tower primary net:

- ATC detachment(s).
- Aircraft.

Ground Control Net (UHF/VHF)

The ground control net provides a means for the ground controller to coordinate the movement of all ground aircraft, vehicles, and personnel on taxiways and runways. The following organizations are examples of those that would use the ground control net:

- ATC detachment(s).
- All aircraft, vehicles, and personnel on taxiways and runways.

Approach Control Net (UHF/VHF)

The approach control net provides a means to communicate radar traffic into the terminal airspace. The following organizations are examples of those that would use the approach control net:

- ATC detachment(s).
- Inbound aircraft.

Departure Control Net (UHF/VHF)

The departure control net provides a means to coordinate radar traffic out of the terminal airspace. The following organizations are examples of those that would use the departure control net:

- ATC detachment(s).
- Outbound aircraft.

Ground Control Approach Net (UHF/VHF)

The ground control approach net provides a means for ground control approach to provide bearing and altitude information to aircraft. The

following organizations are examples of those that would use the ground control approach net:

- ATC detachment(s).
- Landing aircraft.

Guard Net (UHF/VHF/HF)

The guard net provides an emergency distress net used by aircraft to declare an emergency. It further serves as a means for air control agencies to advise aircraft of emergency conditions or serious hazards to aircraft safety. The following organizations are examples of those that would use the guard net:

- Airborne aircraft.
- All air control agencies.

Crash, Fire Rescue Net (VHF/VHF-AM)

The crash, fire rescue net provides a means to coordinate crash recoveries in and around the airfield. The following organizations are examples of those that would use the crash, fire rescue net:

- ATC detachment(s).
- Crash crew.
- Airfield operation center.
- Explosive ordnance disposal.
- Medical facility.
- Military police.

Search and Rescue Net (UHF/VHF/HF)

The search and rescue (SAR) net provides a means for the control and coordination of air rescue missions. Multiple SAR nets may be required depending on the number of concurrent SAR or tactical recovery of aircraft and personnel missions. The following organizations are examples of those that would use the SAR net:

- All elements within the air C2 system.
- Aircraft involved in search and rescue missions.

Landing Zone Control Team Local Net (VHF)

The LZCT local net provides a means for the LZCT commander to direct the activities of helicopter control personnel in each of the landing sites. Multiple LZCT local nets may be required depending on the number of zones in operation

at the same time. The following organizations are examples of those that would use the LZCT local net:

- LZTC.
- Landing site controllers.

APPENDIX B

COMMUNICATIONS SYMBOLOGY AND DIAGRAMS

Timing Symbols



General clock/timing generator

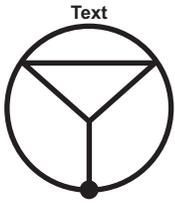


GPS stratum 1 SAASM

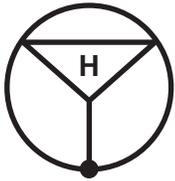


GPS stratum 1 XLDC (non-SAASM)

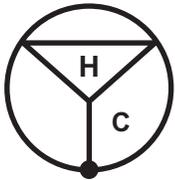
Single Channel Radio Symbols



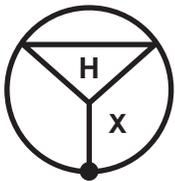
RF transceiver: Downward pointing triangle with line extending from down point. The identification of the specific RF transceiver can be entered in the Text field. Additional information may be entered within or may be placed external to the symbol.



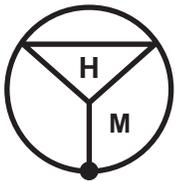
HF



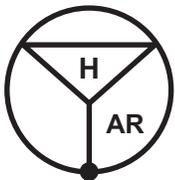
HF NCS



HF (guard)

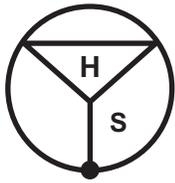


HF (monitor)

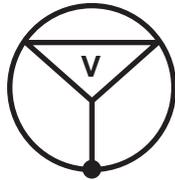


HF (as required)

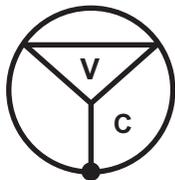
Single Channel Radio Symbols



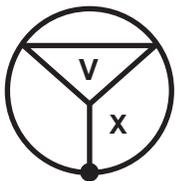
HF ANCS



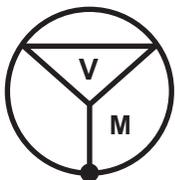
VHF



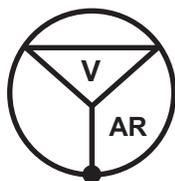
VHF NCS



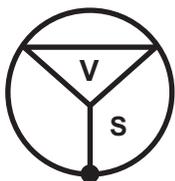
VHF (guard)



VHF (monitor)



VHF (as required)

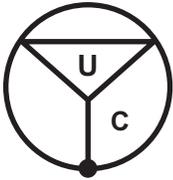


VHF ANCS

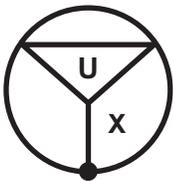
Single Channel Radio Symbols



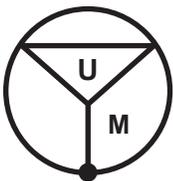
UHF LOS



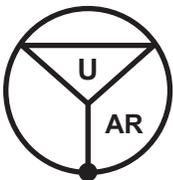
UHF LOS NCS



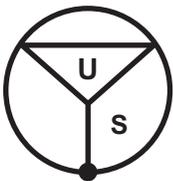
UHF LOS (guard)



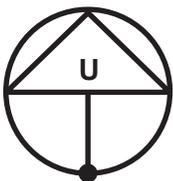
UHF LOS (monitor)



UHF LOS (as required)

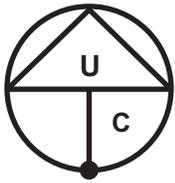


UHF Los ANCS

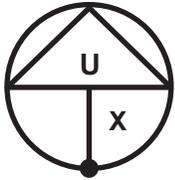


UHF TACSAT radio

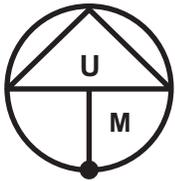
Single Channel Radio Symbols



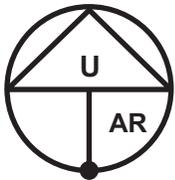
UHF TACSAT NCS



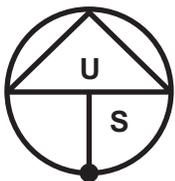
UHF TACSAT radio (guard)



UHF TACSAT radio (monitor)

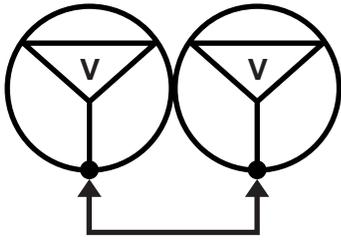


UHF TACSAT radio (as required)

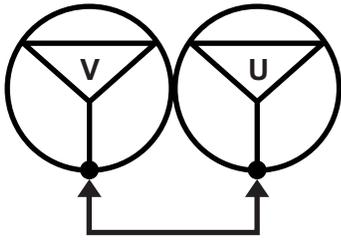


UHF TACSAT (ANCS)

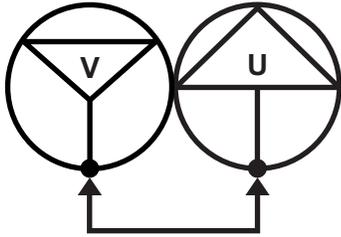
Single Channel Radio Symbols



VHF to LOS retransmission

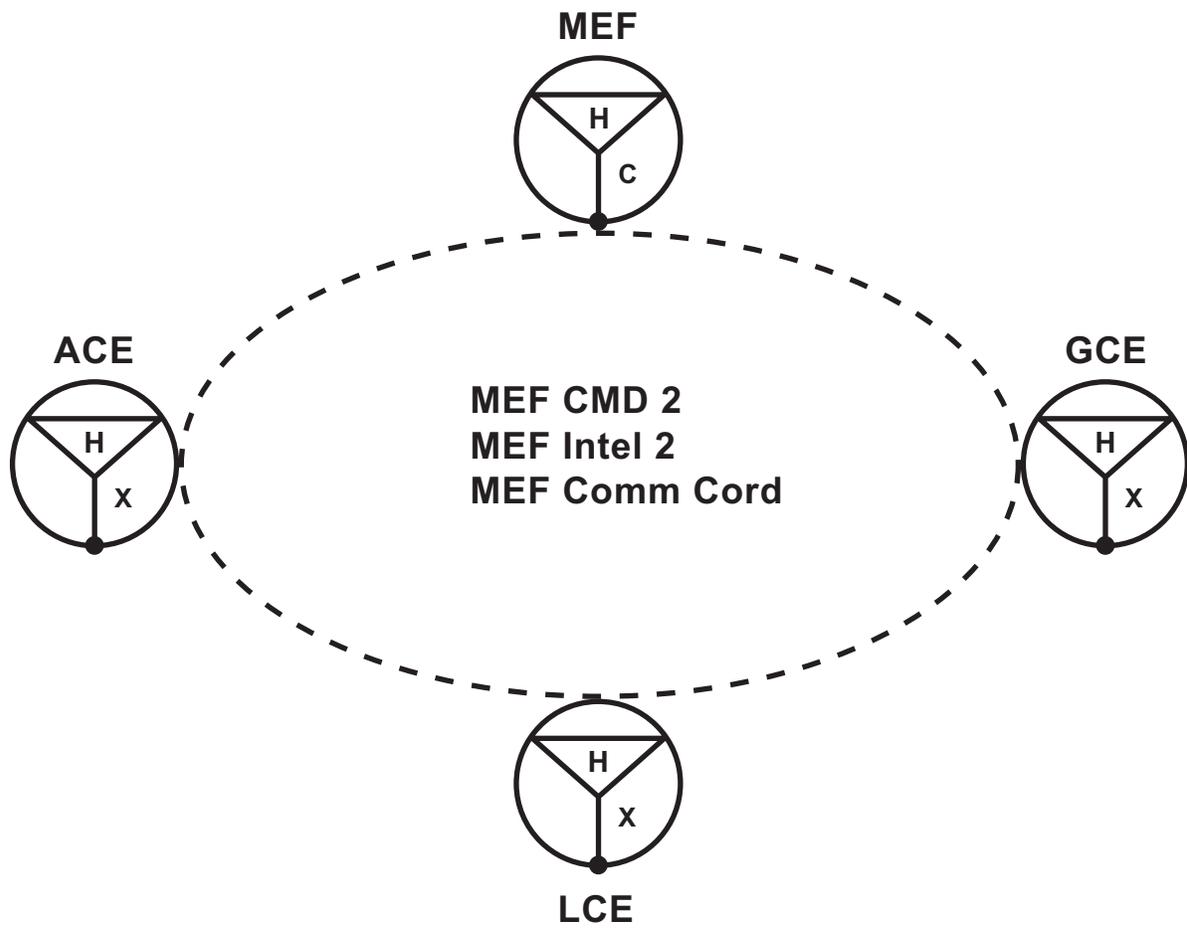


VHF to UHF LOS retransmission



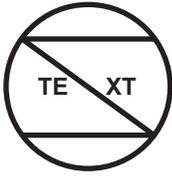
VHF to UHF TACSAT radio retransmission

Single Channel Radio Symbols



HF radio network diagram

Multichannel Radio Symbols



Satellite transceiver: Circle with a zigzag line attached to the top of the circle. The identification of the specific satellite can be entered into the text field. Additional information may be entered within or may be placed outside the symbol.



QUADBAND/LMST hub/spoke capable station

AN/USC-65v1

Symbol ID: MC-MCR

QUADBAND/LMST

#: Indicates antenna size

##: Indicates band (X, C, Ku, Ka)



QUADBAND/LMST hub/spoke capable station

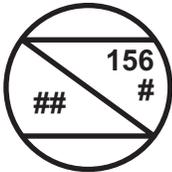
AN/USC-65v1

Symbol ID: MC-MCR

QUADBAND/LMST

#: Indicates antenna size

##: Indicates band (X, C, Ku, Ka)



QUADBAND/PHOENIX hub/spoke capable station

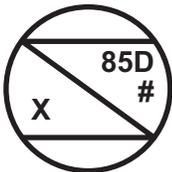
AN/TSC-156

Symbol ID: MC-MCR

QUADBAND/PHOENIX

#: Indicates antenna size

##: Indicates band (X, C, Ku, Ka)_SHF/GMF hub/spoke

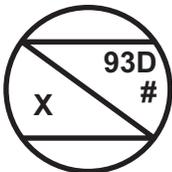


SHF/GMF hub/spoke capable station

AN/TSC-85D

Symbol ID: MC-MCR

SHF/GMF X-band hub/spoke



SHF/GMF spoke capable station

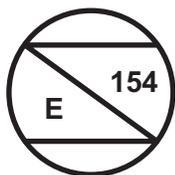
AN/TSC-93D

Symbol ID: MC-MCR

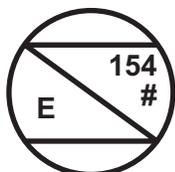
SHF/GMF X-band spoke

#: Indicates antenna size

Multichannel Radio Symbols



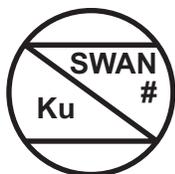
Generic EHF MCR satellite capable station
AN/TSC-154 SMART-T
Symbol ID: MC-MCR EHF



EHF MCR satellite capable station
AN/TSC-154 SMART-T
Symbol ID: MC-MCR EHF
#: Indicates terminal ID



EHF MCR satellite capable station with terminal ID



SWAN D Ku capable station
SWAN D V1/V2/V3
Symbol ID: MC-MCR SWAN D (Ku)
#: Indicates antenna size



SWAN D Ku capable station
SWAN D V1
Symbol ID: MC-MCR SWAN D (Ku)



SWAN D Kurtz-under band (Ku) capable station
SWAN D V2
Symbol ID: MC-MCR SWAN D (Ku)

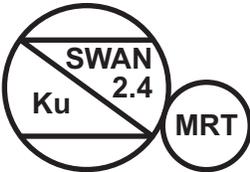
Multichannel Radio Symbols



SWAN D Ku capable station
SWAN D V3
Symbol ID: MC-MCR SWAN D (Ku)

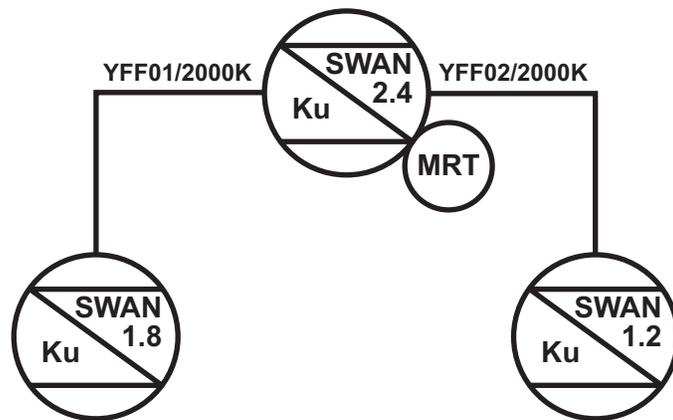


MRT - MRT is needed on each SWAN D TDMA network. MRT provides timing for SWAN network. Only one MRT per SWAN network is allowed. MRT will be located with either a SWAN V3 or SWAN V2

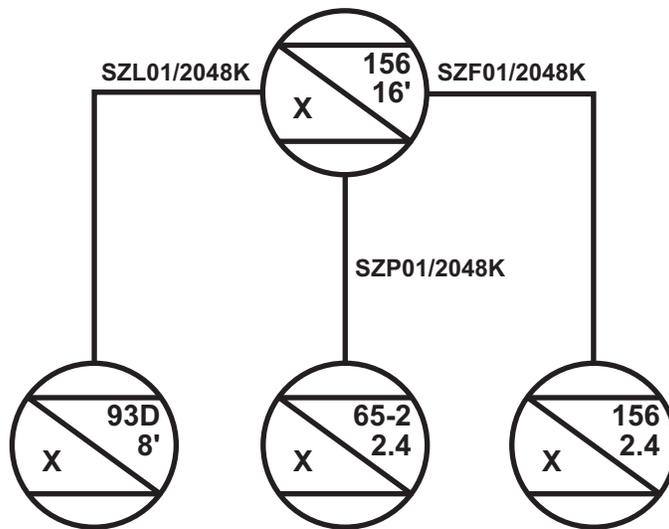


SWAN D Ku capable station
SWAN D V3 with MRT

Multichannel Radio Symbols



SWAN D Ku-band satellite with MRT

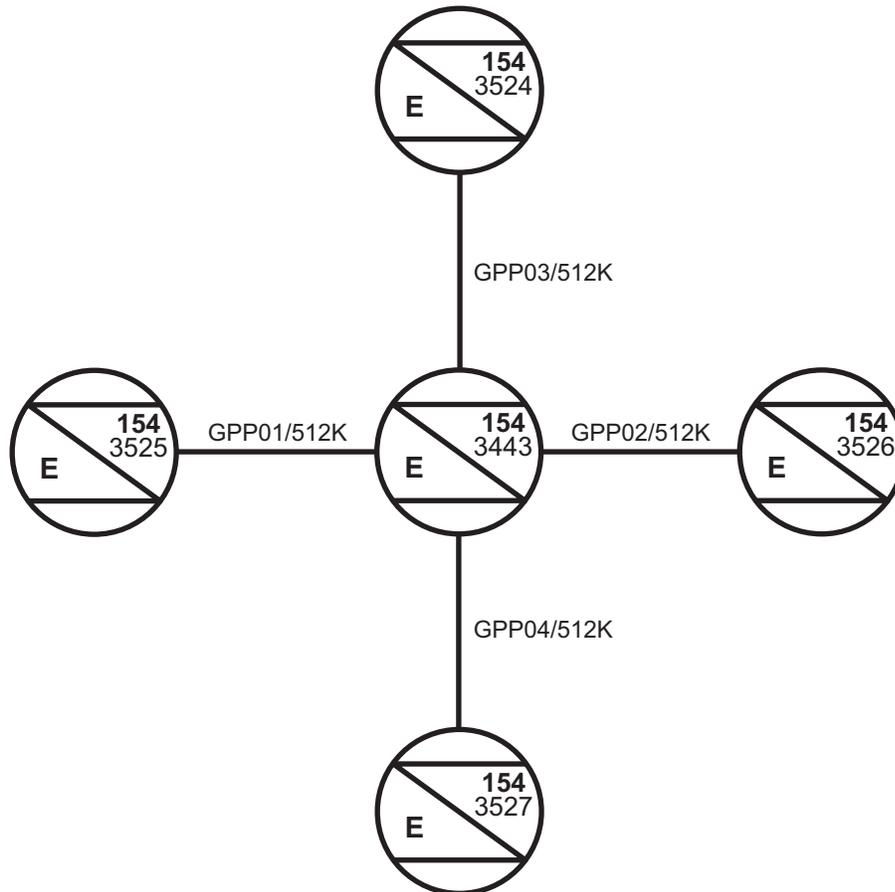


GMF/SHF X-band satellite hub/spoke link

Multichannel Radio Symbols



GMF/SHF Ku-band satellite point-to-point link

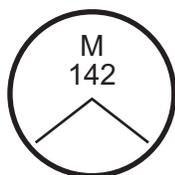


EHF band MDR satellite network

Multichannel Radio Symbols



SHF MCR TROPO/LOS station AN/TRC-170V5
Symbol ID: MC-MCR TROPO/LOS SHF
LOS/diffraction/TROPO



UHF MCR LOS station
AN/MRC-142: M(a), M(b), or M(c) are used
depending on the type of system.
Symbol ID: MC-MCR UHF LOS



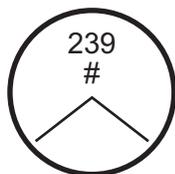
UHF MCR LOS station
AN/MRC-142A: M(a)
Symbol ID: MC-MCR UHF LOS



UHF MCR LOS station
AN/MRC-142B: M(b)
Symbol ID: MC-MCR UHF LOS



UHF MCR LOS station
AN/MRC-142C: M(c)
Symbol ID: MC-MCR UHF LOS

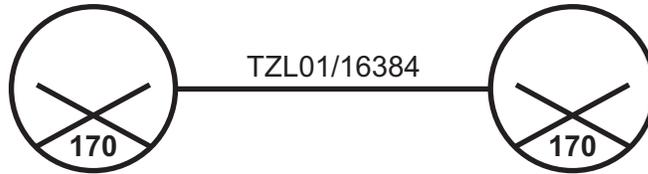


SHF MCR LOS station
AN/GRC-239 TSSR
Symbol ID: MC-MCR SHF LOS
#: Indicates antenna size
(1 ft or 2 ft)



Orthogonal frequency division Mux
WPPL
SHF LOS
#: Indicates antenna size

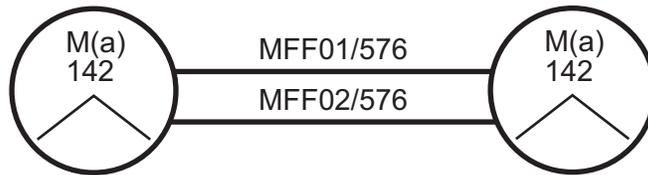
Multiplexing Symbols



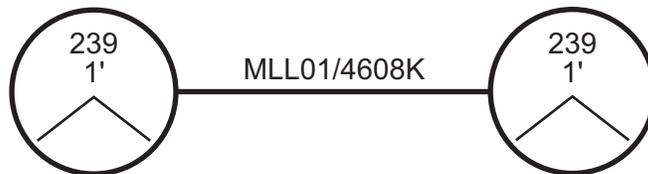
AN/TRC-170V5 TROPO/LOS single link



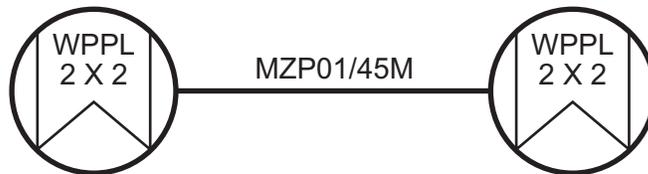
AN/MRC-142A single link



AN/MRC-142A dual link

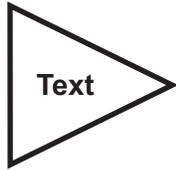


AN/GRC-239 TSSR single link



WPPL single link

Multiplexing Symbols



Multiplexer:

Right or left pointing triangle. The identification of the specific Mux (FCC-100, LRM) can be entered in the Text field. Additional information may be entered within or may be placed external to the symbol.



Smart Multiplexer:

Right or left pointing polygon. The identification of the smart Mux (IDNX, P800) can be entered in the Text field. Additional information may be entered within or may be placed outside the symbol. It is used when developing engineer-level diagrams to show circuits off back side of Mux and SA trunk aggregates off front side of Mux.



PROMINA:

Indicate model (P800, P400, P200, P100) and number of shelves.

DXX: Domain number

NXXX: Node number

It is used when developing engineer-level diagrams to show circuits off back side of Mux and SA trunk aggregates off front side of Mux.



GATEWAY NODE PROMINA:

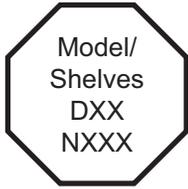
Indicate model (P800, P400, P200, P100) and number of shelves.

DXX: Domain number

NXXX: Node number

It is used when developing engineer-level diagrams to show circuits off back side of Mux and SA trunk aggregates off front side of Mux.

Multiplexing Symbols



PROMINA:

Indicate model (P800, P400, P200, P100) and number of shelves.

DXX: Domain number

NXXX: Node number

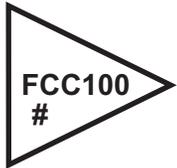


GATEWAY NODE PROMINA:

Indicate model (P800, P400, P200, P100) and number of shelves.

DXX: Domain number

NXXX: Node number



AN/FCC-100

Commercial Mux

#: Indicate version type.



Vocality Mux

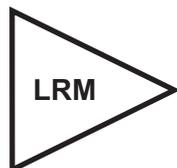
#: Indicate model (V50, V100, V150, V200) ##: Indicate node number.



TAC Mux

#: Indicate model (300, 900)

##: Indicate node number.



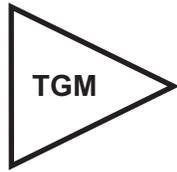
LRM

(TD-1389)

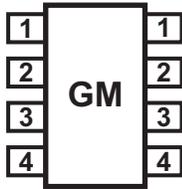


Loop group modem (TD-1235)

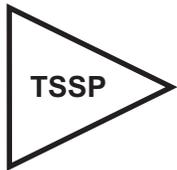
Multiplexing Symbols



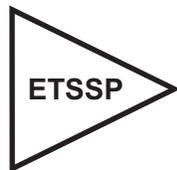
Trunk group Mux
(TD-1236)



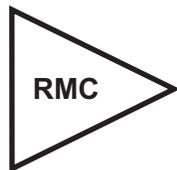
Group modem (MD-1026)



TACSAT signal processor
(TD-1337(V))



Enhanced TACSAT signal processor
(TD-1337(V))

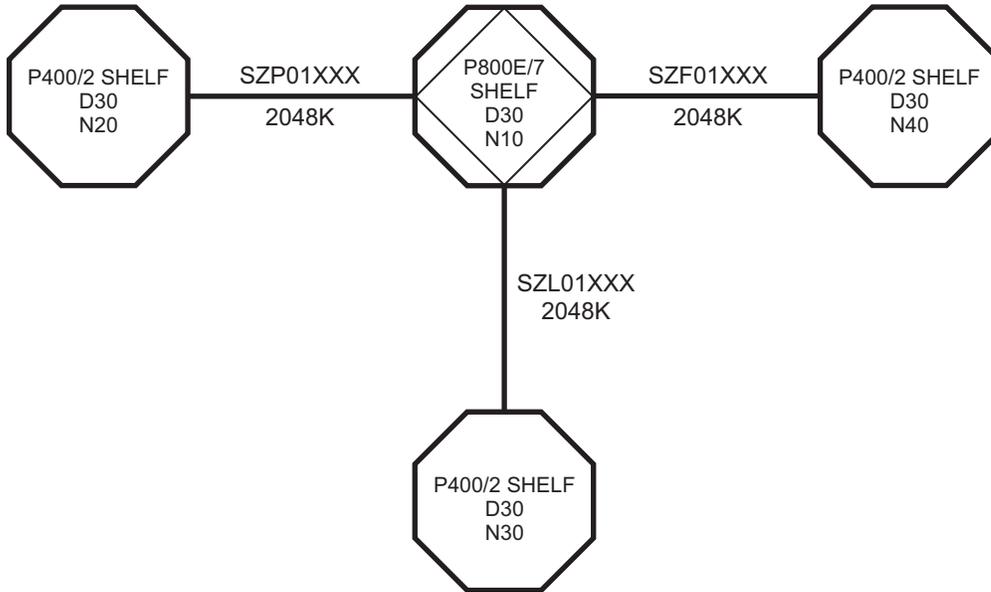


Remote Mux combiner (TD-1234)



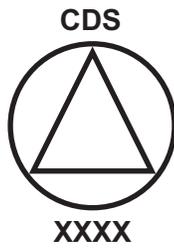
VersaMux 4000

Multiplexing Symbols



Promina architecture example with gateway node.

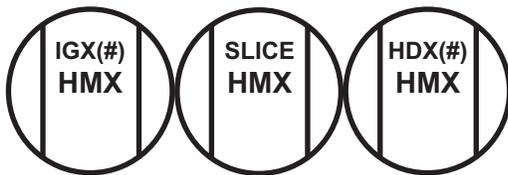
Voice Network Symbols



CDS - member of CBCS. Fielded in AN/TTQ-227 DTC facility.

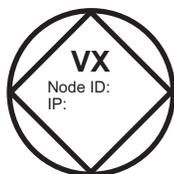


SMU is used in STEP and aboard ships. Stand alone SMUs may exist at MSC-level communications units. Member of CBCS family of switchboards.



Commercial circuit switchboards:

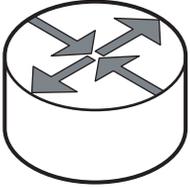
These symbols represent the REDCOM IGX, HDX and SLICE models of commercial circuit switchboards. HMXs will be labeled between the vertical lines of the symbol. The number of shelves for the HDX and IGX will be indicated next to the switch model number in parentheses. The HDX is the circuit switchboard associated with the AN/TTC-62 DEOS. The SLICE is the circuit switchboard associated with the AN/TTC-63 RSAM and the IGX is the commercial circuit switchboard associated with the AN/TTQ-227 DTC.



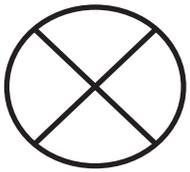
The VX 900 is a multi-service voice switch with robust gateway functionality. Currently fielded in the AN/TTC-62 (DEOS) and AN/TTC-63 (RSAM). Primarily used for conversion of DS-1 formatted trunk groups into serial or IP formatted trunk groups. Node ID will be required for BSP employment and an IP address will be required for IP trunking employments.

Data Network Symbols

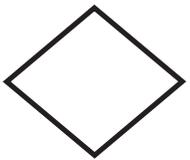
Router



USCENTCOM standard

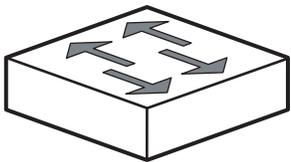


2D standard

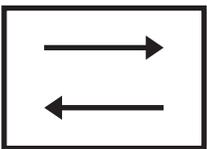


CJCS

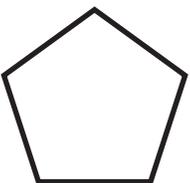
Layer 2 Switch



USCENTCOM standard



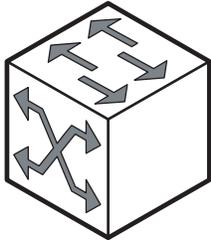
2D standard



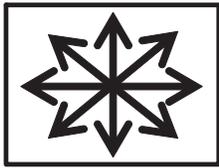
CJSC

Data Network Symbols

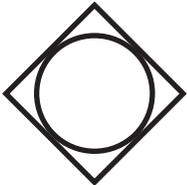
Multilayer Switch



USCENTCOM standard



2D standard



CJCS

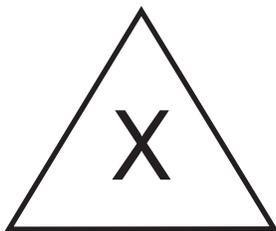
IDS Sensor



USCENTCOM standard

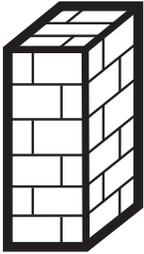


2D standard



CJCS

Data Network Symbols

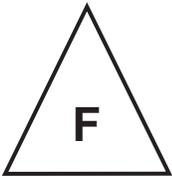


Firewall

USCENTCOM standard

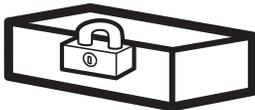


2D standard



CJCS

Encryption Device

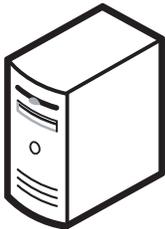


USCEN
TCOM
standard



2D standard/CJSC

Server



USCENCOM standard



2D standard



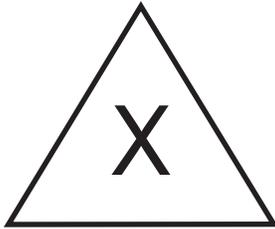
CJCS

Server name or the name of some type of application device. List inside this block the roles that the device is hosting. For example, DC or AV.

Data Network Symbols



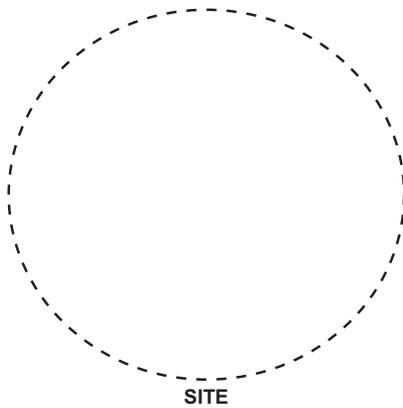
Virtual LAN or network tunnel



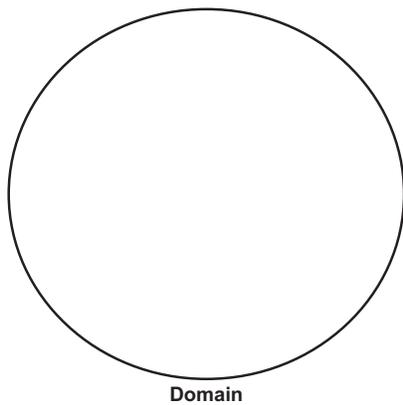
Multilevel security device
I INE
G guard
F firewall
X other



Wide-area network cloud:
Descriptor could read SIPRNET, NIPRNET, COWAN, etc.



Site

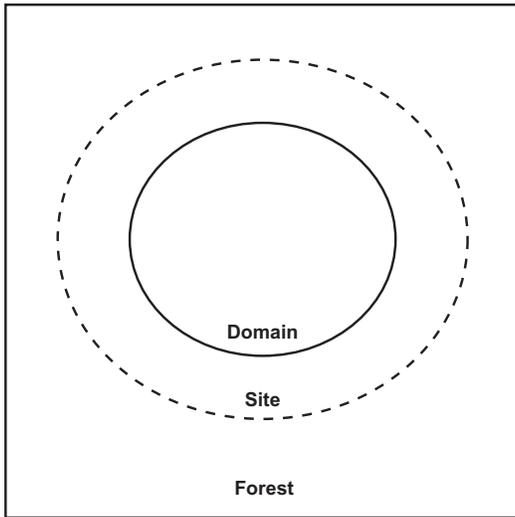


Domain

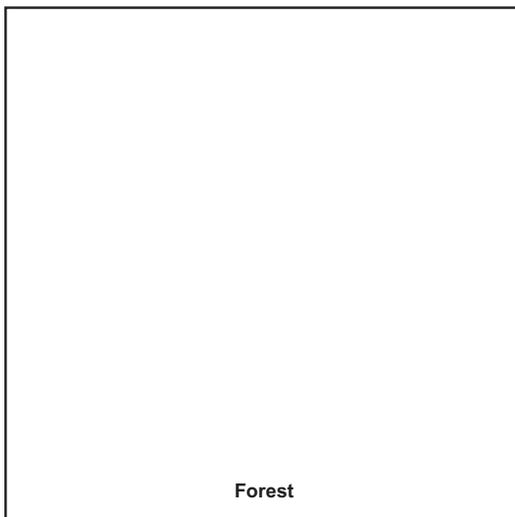


Active directory replication

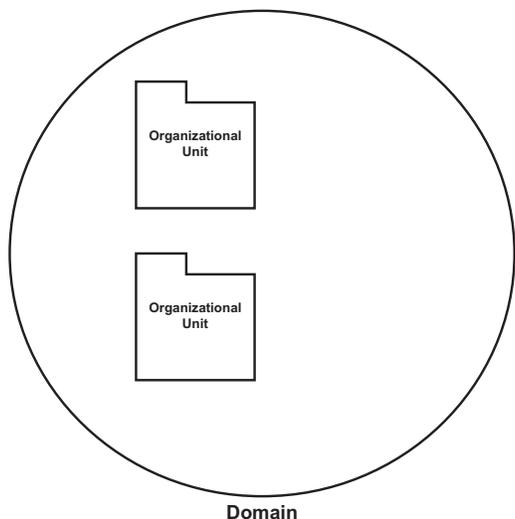
Data Network Symbols



Symbology for an entire forest that may have more than one site and domain. If the sites and domains need to be displayed in further detail—especially when displaying child domains—these symbols can be broken out as exhibits to the active directory tab.

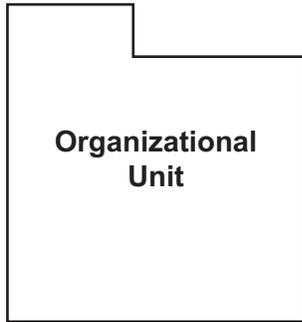


Representation of a single forest. This can be used in a multiple forest display or as the senior container for multiple sites and domains.



Representation of a single domain with multiple organizational units. This level of detail would be in an exhibit of the active directory tab. This symbol can be used in logically planning organizational units within a domain.

Data Network Symbols



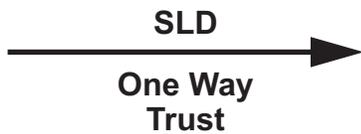
Representation of an organizational unit. This is the lowest level planning symbol of the active directory architecture. This symbol can be used to display multiple regiments within a division. Further organizational units can be used to create the regiment's logical architecture for its S-shops and battalions.



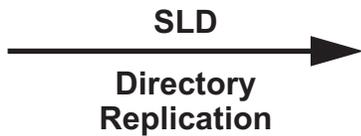
Representation of transitive trust replication.



Representation of one-way trust replication.



Representation of directory replication.



H320 VTC
EXT #



H323 VTC
EXT #

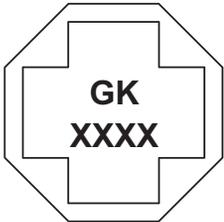


Multipoint control unit

Data Network Symbols

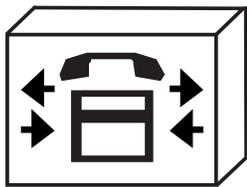


Gateway/gatekeeper zone prefix #



Gatekeeper zone prefix #

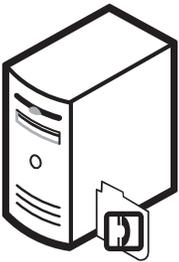
CUCM



Cisco symbol



2D symbol

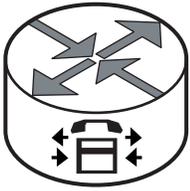


USCENTCOM VOIP CUCM

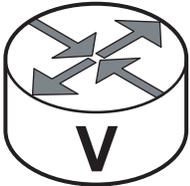


USCENTCOM VOSIP CUCM

Data Network Symbols



Cisco symbol
Cisco call manager express

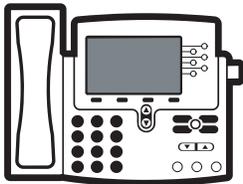


3D symbol
Cisco call manager express



2D symbol
Cisco call manager express

IP Phone



3D symbol

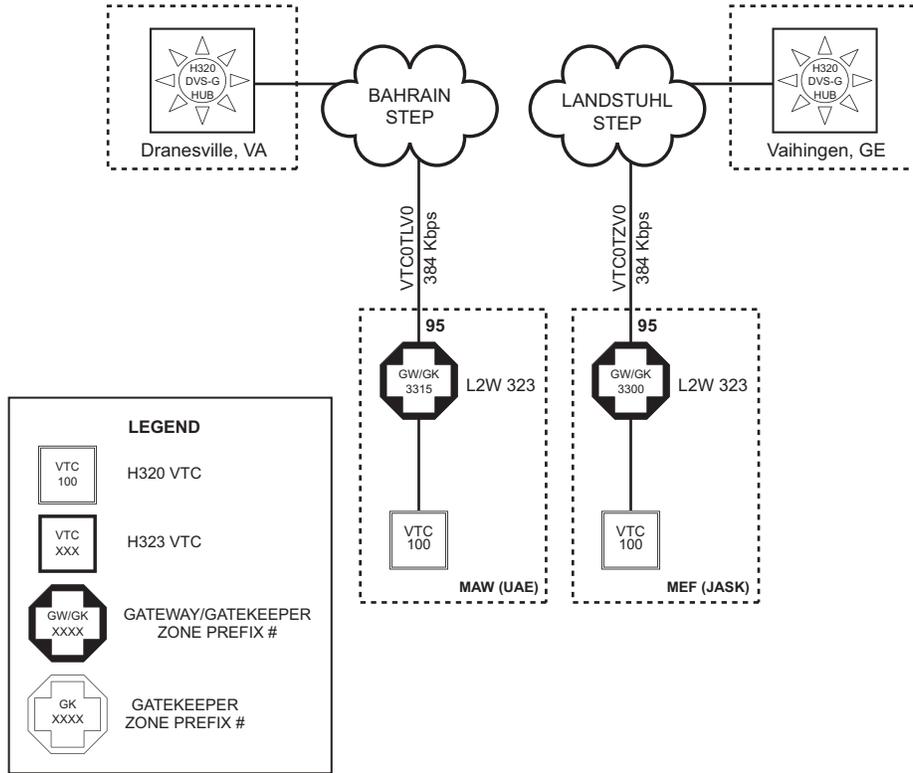


2D symbol



USCENTCOM VOSIP phone

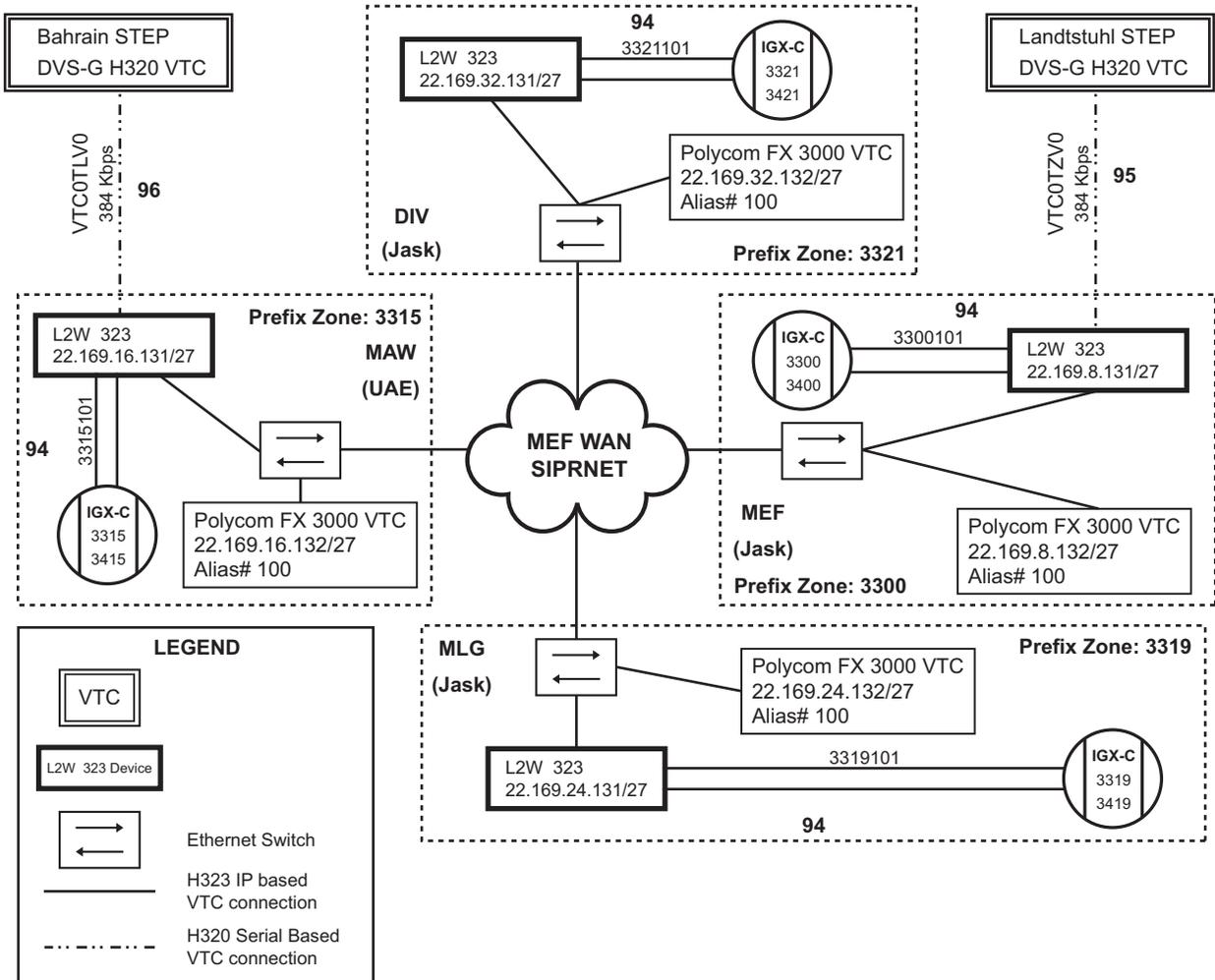
Data Network Symbols



VTC Configuration Example 1.

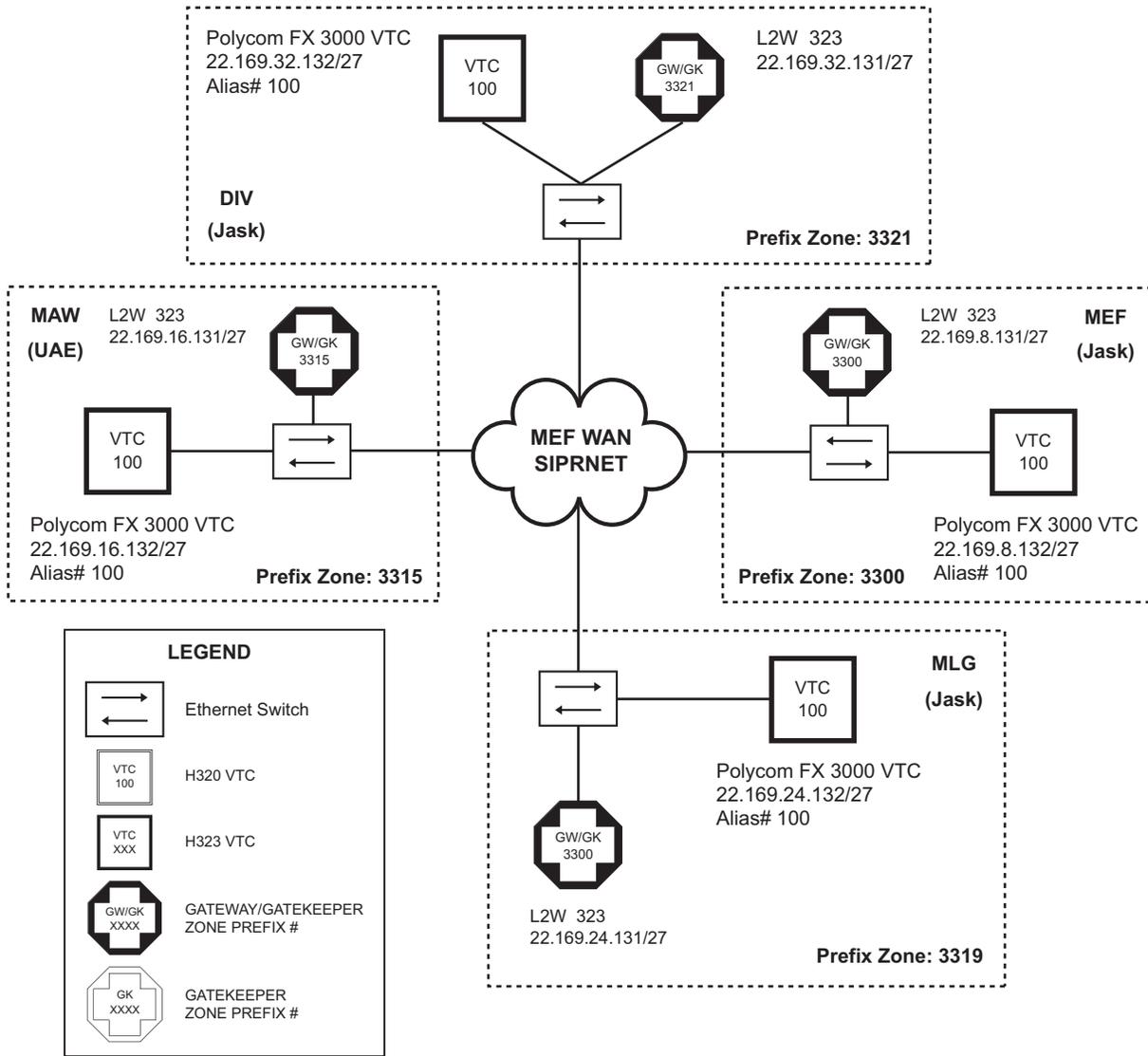
Data Network Symbols

Dialing Scheme:
 DVS-G HUB Landstuhl, dial 95 xxx
 DVS-G HUB Bahrain, dial 96 xxx



VTC Configuration Example 2.

Data Network Symbols



Legend for appendix B:

ACE	aviation combat element	HDX	high density exchange
ANCS	alternate net control station	HF	high frequency
AV	antivirus	HMX	Home exchange code
BSP	best-flow signaling protocol	ID	identification
CBCS	common baseline circuit switchboard	IDNX	Integrated Digital Network Exchange
CDS	compact digital switch	IDS	intrusion detection system
CJCS	Chairman of the Joint Chiefs of Staff	IGX	ISDN gateway exchange
CMD	command	IGX-C	ISDN gateway exchange for command and control
Comm	communications	INE	inline network encryptor
Comm Cord	communication cord	Intel	intelligence
COWAN	coalition operations wide-area network	IP	Internet protocol
CUCM	Cisco unified communications manager	IPSEC	Internet protocol security
DC	domain controller	ISDN	integrated services digital network
DEOS	deployable end office suite	JASK/Jask	Jask, Iran
DIV	division	Ka	Kurtz-above band
DS	digital signal	Ku	Kurtz-under band
DTC	digital technical control	LAN	local area network
DVS-G	DISN Video Services-Global	LCE	logistics combat element
EHF	extremely high frequency	LGM	loop group modem
ETSSP	enhanced tactical satellite signal processor	LMST	lightweight multiband satellite terminal
EXT	extension	LOS	line of sight
FCC	Federal Communications Commission	LRM	low rate multiplexer
ft	foot	MAW	Marine aircraft wing
GCE	ground combat element	MCR	multichannel radio
GK	gatekeeper	MCU	multipoint control unit
GM	group modem	MDR	medium data rate
GMF	ground mobile force	MEF	Marine expeditionary force
GPS	global positioning system	MLG	Marine logistics group
GW	gateway	MRT	master reference terminal

MSC	major subordinate command	TDMA	time division multiple access
Mux	multiplexer	TGM	trunk group multiplexer
NCS	net control station	3D	three dimensional
NIPRNET	Non-Secure Internet Protocol Router Network	TROPO	tropospheric scatter
REDCOM	REDCOM Laboratories, Inc	TSSP	tactical satellite signal processor
RF	radio frequency	TSSR	tropospheric scatter satellite support radio
RMC	remote multiplexer combiner	2D	two dimensional
RSAM	remote subscriber access module	UAE	United Arab Emirates
SA	symmetric/asymmetric	UHF	ultrahigh frequency
SAASM	selective availability anti-spoofing module	USCENTCOM	United States Central Command
SAN	subject alternative name	VERSA	VersaMux protocol converter/multiplexer
SHF	super high frequency	VHF	very high frequency
SIPRNET	SECRET Internet Protocol Router Network	VOIP	voice over Internet protocol
SLD	system link designator	VOSIP	voice over secure Internet protocol
SLICE	REDCOM switch SLICE® (SLICE 2100™)	VTC	video teleconferencing
SMART-T	secure mobile antijam reliable tactical terminal	VTI	virtual tunnel interface
SMU	switch multiplex unit	VX	voice exchange
STEP	standard tactical entry point	WAN	wide-area network
SWAN	support wide-area network	WPPL	wireless point-to-point link
TAC	tactical access concentration	XLDC	model version name of the stratum 1 device in the DTC
TACSAT	tactical satellite		

APPENDIX C

TRANSMISSION SYSTEM LINK DESIGNATOR NUMBERING

System link designator (SLD) codes are used to number joint communications systems links. The SLD consists of eight characters (see fig. C-1). Every radio transmission and cable transmission link should be assigned an SLD.

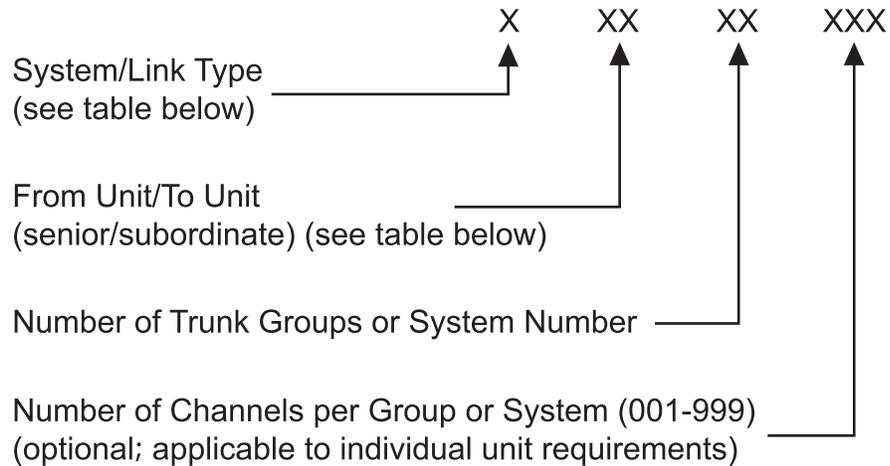


Figure C-1. System Link Designator Code.

First Character – System/Link Type

Letter Designator	System/Link Types
S	DSCS SHF satellite
E	C-band satellite
B	HF radio
V	Ka-band satellite
Y	Ku-band satellite
G	EHF satellite
A	UHF satellite
T	TROPO
M	Microwave (UHF/SHF)
H	UHF/VHF (single channel)
R or C	Cable (26 pair)
K	Cable (coaxial landline)
F or O	Cable (fiber optic)
Z	Cable (other)
L	Commercial (leased, any type)
Q	Submarine coaxial cable
U	Submarine fiber optic

Second/Third Character – User Codes

Code	User	Code	User
A	JTF	T	DISA (Reserved and assigned by DISA for tactical circuits that originate in or traverse the DCS/DISN)
B	NAVFOR	U	ARFOR
C	Army Corps Main	V	Spare
D	Army Corps Forward	W	Spare
E	Army Division	X	Spare
F	LCE	Y	JSOTF
G	Marine TACC	Z	MARFOR
H	CRC	1	ARSOF
I	Spare	2	AFSOF
J	AFFOR	3	NAVSOF
K	CRP	4	COSCOM
L	Marine Air Component	5	Spare
M	FTR Wing Operations Center	6	Spare
N	Spare	7	Spare
O	Spare	8	Spare
P	Marine Ground Component CDR	9	Spare
Q	TAOC	A	JTF
R	DCS--Central Area	B	NAVFOR
S	Navy TACC/TADC		

Examples

SZL01XXX – SHF satellite, MEF to ACE, first link, Promina Multiplexer.

TZP01016 – Tropo, MEF to GCE, first link, FCC-100 Multiplexer.

YFF02001 – Ku-band satellite, LCE to LCE, second link, one channel.

GZP03016 – EHF satellite, MEF to GCE, third link, FCC-100 Multiplexer.

KZZ01018 – Cable (coaxial), MEF to MEF, first link, 18 channels.

Legend for appendix C:

ACE	aviation combat element	HF	high frequency
AFFOR	Air Force forces	JSOTF	joint special operations task force
AFSOF	Air Force special operations forces	JTF	joint task force
ARFOR	Army forces	Ka	Kurtz-above band
ARSOF	Army special operations forces	Ku	Kurtz-under band
C	Compromise (band)	LCE	logistics combat element
CDR	commander	MARFOR	Marine Corps forces
COSCOM	Corps support command	MEF	Marine expeditionary force
CRC	control and reporting center	NAVFOR	Navy forces
CRP	combat reporting post	NAVSOF	Navy special forces
DCS	Defense Communications System	SLD	system link designator
DISA	Defense Information Systems Agency	SHF	super high frequency
DISN	Defense Information Systems Network	TACC	tactical air command center (Marine); tactical air control center (Navy)
DSCS	Defense Satellite Communications System	TADC	tactical air direction center
EHF	extremely high frequency	TAOC	tactical air operations center
FCC	Federal Communications Commission	TROPO	tropospheric
FTR	fighter	UHF	ultrahigh frequency
GCE	ground combat element	VHF	very high frequency

APPENDIX D

COMMAND COMMUNICATIONS SERVICE DESIGNATOR

The command communications service designator is an eight-character, alphanumeric code (see fig. D-1) used to identify circuits throughout the joint communications network.

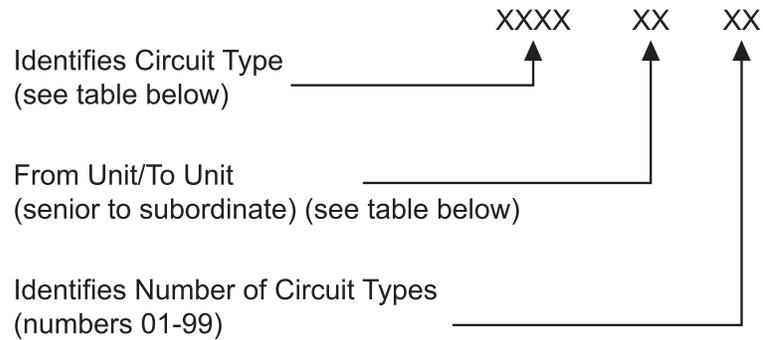


Figure D-1. Command Communications Service Designator Code.

First Four Characters

Circuits	Description
DTG8	Digital Trunk Group (Modulator 8)
DTG9	Digital Trunk Group (Modulator 9)
SIPR	SIPRNET
NIPR	NIPRNET
CAS0	Channel Associated Signaling
PRI0	Primary Rate Interface
VTC0	Video Teleconferencing (Serial H320)
VTC3	Video Teleconferencing (IP H323)
LLOC	Long Local
THOT	TECHCON Hot
DRSN	Defense Red Switch Network
JWICS	Joint Worldwide Intelligence Communications System

Fifth and Sixth Characters

Code	User	Code	User
A	JTF	T	DISA (Reserved and assigned by DISA for tactical circuits that originate in or traverse the DCS/DISN)
B	NAVFOR	U	ARFOR
C	Army Corps Main	V	Spare
D	Army Corps Forward	W	Spare
E	Army Division	X	Spare
F	LCE	Y	JSOTF
G	Marine TACC	Z	MARFOR
H	CRC	1	ARSOF
I	Spare	2	AFSOF
J	AFFOR	3	NAVSOF
K	CRP	4	COSCOM
L	Marine Air Component	5	Spare
M	FTR Wing Operations Center	6	Spare
N	Spare	7	Spare
O	Spare	8	Spare
P	Marine Ground Component CDR	9	Spare
Q	TAOC	A	JTF
R	DCS--Central Area	B	NAVFOR
S	Navy TACC/TADC		

Examples

- DTG8ZL01 Digital Trunk Group (Modulator 8), MEF to ACE, DTG, first DTG circuit.
- SIPRLP11 SIPRNET, ACE to GCE, eleventh SIPRNET circuit.
- NIPRPF03 NIPRNET, GCE to LCE, NIPRNET, third NIPRNET circuit.
- VTC0ZL01 Video teleconferencing H320 serial, MEF to ACE, VTC, first VTC circuit.

Legend for appendix D:

ACE	aviation combat element	JSOTF	joint special operations task force
AFFOR	Air Force forces	JTF	joint task force
AFSOF	Air Force special operations forces	LCE	logistics combat element
ARFOR	Army forces	MARFOR	Marine Corps forces
ARSOF	Army special operations forces	MEF	Marine expeditionary force
CDR	commander	NAVFOR	Navy forces
COSCOM	Corps support command	NAVSOF	Navy special forces
CRC	control and reporting center	NIPRNET	Non-Secure Internet Protocol Router Network
CRP	combat reporting post	SIPRNET	SECRET Internet Protocol Router Network
DCS	Defense Communications System	TACC	tactical air command center (Marine); tactical air control center (Navy)
DISA	Defense Information Systems Agency	TADC	tactical air direction center
DISN	Defense Information Systems Network	TAOC	tactical air operations center
DTG	date-time group	TECHCON	technical control
FTR	fighter	VTC	video teleconferencing
GCE	ground combat element		

APPENDIX E

COMMUNICATIONS PLANNING CHECKLIST

The purpose of this checklist is to guide communications planning for joint operations. This checklist is derived from JP 6-0, *Joint Communications System*; it is not all-inclusive. Questions should be revisited as communications planners adapt to changing operational situations. The checklist provides a framework for supporting the communications planning of each phase of an operation, which focuses communications planners on the mission and how the commander intends to accomplish it. Communications planners should also be familiar with relevant joint and naval tactics, techniques, and procedures. They should have access to communications support organizations and to pertinent publications identified in the References section of this publication.

Reference Material

- Existing OPLANs and OPORDs.
- Commander's planning guidance, estimate, intent, and CONOPS.
- Area studies.
- Unit SOPs.
- JP 6-0.
- CJCSM 6231.01C through 6231.07D.
- DISA Contingency Plan 10-95.
- *Joint Communications Support Element (JCSE) C4I Planning Guide*.
- Lessons-learned databases from previous operations and exercises.
- Time-phased force and deployment data and time-phased force deployment list.

Planning Considerations

- What is the MAGTF or unit mission?
- What is the geographic operational area?
- What are the commander's intent, CONOPS, planning guidance, and CCIR?
- What are the commander's communication and information exchange requirements?
- What are the JTF, naval strike force, MAGTF, and supporting elements' task organizations? What are the command relationships?
- How will the forces deploy—means of transportation—and what is the deployment timeline?
- Are there any transport or lift restrictions—availability of assets, departure, and arrival locations?
- Are there any satellite landing rights?
- When are the operations planning meetings scheduled? How will communications planning meetings fit into this schedule? Has DISA been involved regarding the coordination of technical requirements?
- Are there any planning constraints?
- Are there any special communications requirements? What unit requires them?
- What national space-based assets are required or available to support the operation? Has a USSTRATCOM joint space support team been contacted?
- What communications capabilities are available to the MAGTF?
- SHF or UHF commercial satellite, DSCS, and FLTSATCOM.

- Milstar satellite terminals.
- JWICS and Milstar.
- HF, VHF, and UHF radio.
- Tropospheric and LOS microwave systems.
- Local area, SBB, and router networks.
- DMS.
- DISN.
- Personal communications systems.
- What frequencies are available for the MAGTF in the operations area? What are specific spectrum restrictions?
- What are the general INFOSEC/IA requirements? Who will draft the callout message?
- Who are the potential adversaries? What are their capabilities to conduct offensive EW? Does a joint force plan exist to counter the threat?
- What are the requirements for coalition communications? What are the releasability requirements for coalition operations?
- Who will submit the telecommunications service request and telecommunications service order? Have telecommunications service requests or orders for SCI communications requirements been incorporated?

Subordinate Units

- Where will primary and secondary C2 nodes be located?
- What are their communications requirements? Identify them by function, C2 node/agency, and overall unit priority.
- What are their communications capabilities? Identify by function, C2 node/agency, and overall unit priority.
- What type of communications systems are available—power, mobility, frequency bands,

interoperability, and compatibility with other subordinate components' equipment?

- Who is the unit communications officer (G-6 or S-6) or staff POC for planning and technical management and direction?
- Are there any special communications requirements resulting from the mission and the commander's estimate, intent, and CONOPS?
- Are subordinate and supporting communications plans consistent with the supported commander's communications plan?

Supporting Units

- What is the mission of supporting units or activities? This may include other Services, agencies, and coalition forces.
- What are their communications capabilities?
- What information does the supported MAGTF or unit need from the supporting units or activities—intelligence, weather, imagery, mapping, deployment—and how will it be accessed?

Defense Information System Agency

- Does the operational area have a DISA regional control center or field office?
- Who is the DISA POC?
- What is the DISN infrastructure in the operational area?
- Are sufficient gateways available? What are the interface requirements to access the gateways? Is the equipment available?
- Is the telecommunications service provisioning or national security emergency preparedness authority provided and current?
- What are the anticipated DSCS and commercial satellite requirements?
- Has modeling of space networks been initiated by DISA?

Commercial Networks

- Are commercial networks available for use? Who can approve access to them? Are funds available? Has DISA been contacted to ensure required lead times for normal allocations?
- Satellite.
- Data.
- Voice.
- What special interfaces are required to access the commercial network, and where are the access points?
- What are the types of switches in the commercial network and where are they located? What are their technical parameters?
- What types of systems are providing the backbone transmission network and where are they located?
- What type of power is used—voltage, current, commercial grid, or generator?
- Does the operational area have a cellular network? What are the transmission media, frequency band, and interface requirements? What are the system standards? Is the system available for use?

Chairman of the Joint

Chiefs of Staff Controlled Assets

- What CJCS-controlled assets are available?
- What capabilities are available?
- Will JCSE support be required in the operational area, or will other defense and commercial assets be sufficient?
- Will JCSE support be needed for en route communications?
- Has a support request for CJCS-controlled C2 and communications system assets been submitted?
- What are the JCSE's logistic support and electrical power requirements?
- What are the JCSE airlift considerations, allocations, and priorities?

Other Support

- Is support needed from specialized communications units?
- Who are the POCs and what are the request procedures?
- What are the unit's communications capabilities and limitations?

Planning Activities

General Planning

- What nodes will provide entry into the DISN and where will they be located?
- What transmission media will be used to connect the nodes?
- What types of communications equipment will be located at each node—equipment strings, interoperability of the equipment?
- What are the frequency requirements for each node? How will the frequencies be allotted—joint, multinational, components, the MAGTF, and MSCs? Are there potential frequency conflicts?
- What are the call signs or words for each node?
- What units will provide, install, operate, and maintain the equipment for each node?
- What lift assets are available to deploy these units? When will the units deploy and activate the nodes or network?
- Is the deployment schedule of communications assets consistent with the phases of the plan? Will it permit the provision of communications support when and where needed?
- What is the phased buildup of communications capabilities in the operational area?
- Has communications scheduling information been added to the time-phased force and deployment data and time-phased force deployment list?
- Have the commander and principal staff officers affected been informed of potential communications shortfalls and recommended solutions?

- How will keying material be managed—ordering, generation, storing, distribution, transfer, and destruction? What are the procedures for handling and reporting compromises? Is an EKMS management activity needed in the operations area? What access will allies have to US COMSEC?
- Are network and node diagrams available?
- Have special communications requirements been addressed—maritime prepositioning force, shipboard, SAR, en route communications, and embarkation and debarkation connectivity?
- Have SCI communication requirements been identified and satisfied?
- How will the joint, component, supporting forces, and MAGTF networks interface with nonorganic networks—DISN, commercial, and JCSE?
- When and where will the joint or MAGTF CCCs be established?
- Are the subordinate elements/units and supporting communications plans consistent with the MAGTF communications plan?
- What types of status reports are required and when will they be submitted?

Detailed Planning

Circuit Switches

- Is there a circuit switch network diagram that shows information about the switch and circuit switch network connectivity—switch type, area code, trunk groups, and capacity?
- How does the switch route calls: flood, deterministic, or circuit switch routing task execution plan?
- Where do circuit switches need to be located? How will they be connected?
- What special features or restrictions will be imposed on subscribers? Who will authorize and enforce these restrictions?
- Where are the DSN interfaces? Are precedents authorized? By whom?
- How will subscriber assistance be handled?
- Where is the greatest anticipated traffic load? Is there sufficient capacity to handle it?
- How will traffic metering and network loading be measured, modeled, and managed?
- Who will publish the information systems directory and how will it be distributed?

Data Networking

- What are the anticipated MAGTF or unit bandwidth requirements?
- What are the anticipated MAGTF or unit individual messaging requirements?
- What are the anticipated MAGTF or unit data storage requirements?
- What are the anticipated MAGTF or unit Web requirements?
- What are the anticipated MAGTF or unit collaborative requirements?
- Who are the data network managers?
- Who is the information systems security officer?
- What are the NIPRNET and SIPRNET connectivity requirements?
- Has the G-2 confirmed JWICS connectivity requirements?
- Are there coalition connectivity requirements?
- Will data of various classifications “ride” a secure tactical backbone?
- How will traffic of various classifications be controlled and managed?
- Are MISSI devices needed and are resources available?
- What is the data network architecture?
- What and where are the network identifications and gateways?
- What is the IP addressing scheme?
- What is the quality of service implementation?
- Who will provide IP addresses?

- Will the IP addresses change with command post displacements?
- What are the port settings on the firewalls?
- What is the active directory architecture?
- Is there access to the Global Address Lists of other Services or forces?
- What are the naming conventions for user accounts?
- What are the naming conventions for hardware?
- What are the password management procedures?
- How is the IA vulnerability alert process coordinated and reported?
- How are software updates installed?
- How are antivirus updates installed?
- What are the server security requirements?
- What are the workstation security requirements?
- What are the user security requirements?

Organizational Messaging System

- What are the anticipated MAGTF or unit organizational messaging requirements?
- Have unit plain language addresses been created?
- Have unit forward plain language addresses been created?
- Have unit distinguished names been published in the directory information tree?
- How will special category traffic be handled?
- How will "Personal For" messages be handled?
- Who will be authorized to have access to special traffic?
- How are general administrative messages distributed?
- Who has message releasing authority?
- How are messages released?
- How are Fortezza cards handled?

Transmission Systems

- What STEP sites will be used?
- Has a gateway access request been submitted in accordance with DISA contingency or exercise plans?
- Are the circuit requirements, routing, channelization, and other parameters that were identified in high-level planning valid? Have satellite access requests been submitted? Have frequency requests been approved and published?
- What are the characteristics and connectivity of multiplexers in the network? Are they compatible?
- What are the timing requirements for the network components? How will timing be accomplished?

Technical Management and Direction

Theater, Joint, or MAGTF

Communications Control Centers

- What are the operational procedures for the control centers?
- Where are the joint or MAGTF control centers located?
- How will the control centers be staffed?
- What reports will be required? How often will they be required? When will they be submitted?
- How will network reconfiguration be accomplished?
- Who are the POCs at the subordinate control centers?
- Who will coordinate changes to connectivity with the DISN? With the commercial networks?
- What kind of statistics will be kept? Who will analyze them? What will be done with them?
- How will changes caused by the evolving tactical situation be handled?

- Can the JCCC direct changes within MAGTF networks to optimize C2 and communications systems within the joint operations area?
- Where is the boundary between technical direction and operational direction?
- How will frequency deconfliction be managed? How can potential conflicts be anticipated?
- Who will control frequency spares and authorize their use?
- Who manages the allocated satellite bandwidth used by the geographic joint forces?

Joint Communications Support Element

- Is JCSE support required?
- Who is the JCSE POC?
- How is support requested?
- How will JCSE participate in the technical management process?
- Are there any special reporting requirements for systems provided by the JCSE?

Spectrum Management

- What are the provisions and procedures for frequency planning and use for opposed or unopposed entry operations into an operational area?
- What frequency allotments and assignments are available for the operational area?
- Can the allotted and assigned frequencies support the equipment deployed to the operational area—communications, LANs or WANs, sensors, surveillance radars, GPS [global positioning system], and airspace control radars?
- Will the frequencies work—propagation and topographic analyses?
- What are the enemy capabilities to intercept, radio direction find, jam, or otherwise exploit or degrade MAGTF allotted and assigned

frequencies? Does a joint and MAGTF plan exist to counter the threat?

- Will the JCCC resolve electromagnetic interference issues? Will Joint Spectrum Center support be required to resolve interference issues?
- Who will issue the joint restricted frequency list?
- Are sufficient spare frequencies available?
- What EMCON measures will be applied?
- Will the MAGTF implement an electronic deception plan? Are sufficient frequencies available to support this plan?

Security

- Will cryptographic equipment interoperate?
- What are the keying material requirements?
- Does a key management plan exist?
- How will cryptographic compromises be detected and corrected?
- What INFOSEC measures will be employed on the LANs and WANs in the operational area?
- How will access to the various networks be controlled—electronically and physically?
- Have COMSEC and INFOSEC emergency destruction procedures been established?
- What is the logistic plan for the cryptographic equipment?
- Are equipment and keymat sufficient to support planned and unplanned operations?
- Have cryptographic change times been established and promulgated?
- Have provisions been made for over-the-air rekeying where applicable?
- Is an intertheater COMSEC plan available? Is it needed?
- To what keying materials will we transition and when?
- What is the EW threat?

APPENDIX F

SAMPLE ANNEX K

This section contains a sample of the format of annex K and is followed by the Appendices Content Guide. The content guide offers a further explanation of the material that should be included in each appendix and tab that comprises the annex K report.

CLASSIFICATION

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

ANNEX K TO OPERATIONS ORDER OR PLAN (Number) (Operation
CODEWORD) (U)
COMMUNICATIONS PLAN (U)

(U) **REFERENCES:** List documents required for a complete understanding of the annex, including complementary plans, publications, command and control and communications systems policy, maps, and SOPs. Of particular interest are technical documents, CJCSM 6231 series (manuals on joint tactical communications) and various CJCSI publications, DISA plans, and circulars.

() **TIME ZONE:** Normally, the time zone of the AO. Use Universal Time Coordinated when the plan or order applies to units in different time zones.

1. (U) Situation

- a. (U) General. Describe the general situation, CONOPS, (derived from Annex C [Operations]), and the current status/condition of the communications architecture.
- b. (U) Battlespace. Provide an orientation to the battlespace with respect to communications.

Page number

CLASSIFICATION

CLASSIFICATION

(1) (U) Describe the G-6's/S-6's assessment of the commander's area of interest, influence, and operations, and the relevant operational considerations that pertain to the battlespace, including physical dimensions and locations of key nodes or facilities.

(2) (U) Environmental Conditions. Describe environmental characteristics that may impact communications.

(a) (U) Vegetation impact.

(b) (U) Terrain impact.

(c) (U) Soil composition.

(d) (U) Space weather.

(e) (U) Terrestrial weather.

(f) (U) Manmade terrain.

c. (U) Enemy Forces. Assess, in detail, enemy capabilities to influence, deny, disrupt, or destroy friendly communications, including counter-C2, signals intercept, and computer system entry.

(1) (U) See Annex B (Intelligence) and summarize communications-related threat information. Consider enemy doctrine and historical employment of OPSEC measures, signals interception, deception, jamming, and lethal/nonlethal attacks against communications networks and computer systems. Evaluate enemy COAs and their impact upon friendly communications.

(2) (U) The enemy has the capability to: (list specific enemy capabilities that could potentially threaten friendly communications).

(a) (U) Address ability to employ paramilitary, special operations forces, and civilian personnel to locate and sabotage friendly and civilian communications equipment and systems.

(b) (U) Address ability to conduct meaconing intrusion.

(c) (U) Address potential exploitation of in-country leased circuits and wire systems.

d. (U) Friendly Forces. Describe friendly capabilities, including facilities, resources, and organizations that are not part of the task organization but contribute to the success of the operation and provide communications support (including access to J-6-specific circuits and services) to the MAGTF and its subordinate commands. Include

Page number

CLASSIFICATION

CLASSIFICATION

appropriate interoperability considerations for joint, combined, coalition, and inter-agency operations, as well as international, bilateral agreements that reflect provisioning of communications support. When possible, identify contact information to aid in subsequent coordination.

(1) (U) Higher (grid location). Identify commands that have a bearing on the operation (communications relationships) and explain their purpose. Where appropriate, state mission statements and commander's intent of higher J-6/G-6 commands. For example—

(a) (U) Commander, US XXXXX Command (USXXXCOM); (HQ/CP). Provides communications support to (your unit) to include access to J6-specific circuits and communications services.

(b) (U) Marine Forces XXXXX Command (administrative control [ADCON]); (HQ/CP). Provides COMSEC support, frequency management, and satellite access and service request actions to USXXXCOM.

(c) (U) Commander, Task Force (TF)-XXX (name of actual command) (OPCON); (HQ/CP). Provides CEOI for TF-XX.

(d) (U) Commanding General, X Marine Expeditionary Force (your parent command) (ADCON); (HQ/CP location). Assists with planning and provides support request action coordination with MARFORXXX to USXXXCOM.

(2) (U) Adjacent (grid location). Identify adjacent commands and communications units and agencies and describe any supporting relationships. Where appropriate, state mission statements or relevant tasks of adjacent commanders.

(3) (U) Supporting. Identify any units or organizations that provide support to the command. These units can be supporting establishment-type functions as well as general support or direct support services from tactical commands. Common supporting agencies:

(a) (U) DISA.

1 Provides DSCS space segment, DISN access and extends DSN, DMS access, NIPRNET, SIPRNET, JWICS terminations via STEP and GIG facilities using DISN, leased, or other circuitry as required. Provide contact information.

2 Provides primary routing of all DISN circuitry for DISN entry systems supporting this plan. Provide contact information.

Page number

CLASSIFICATION

CLASSIFICATION

(b) (U) MCNOSC. Provides global network operations and computer network defense of the Marine Corps Enterprise Network, including policy, procedures, and guidance/assistance to deployed forces for the operation of tactical networks, in order to affect information exchange across the GIG. Provide contact information.

(c) (U) MCTSSA. Provides assistance to deployed forces for MAGTF and commander, task force command and control, and communications systems integration and interoperability. Provide contact information.

(4) (U) Attachments and Detachments

(a) (U) See Annex A (Task Organization).

(b) (U) Identify attachments and detachments with respect to communications that are external to the command. For example: C Co, 9th COMM BN attached to United States Marine Corps Forces, Central Command, in order to install, operate, and maintain STEP site access and services. Internal tasks that distribute personnel and equipment are not listed here.

e. (U) Assumptions. State the assumptions that establish essential criteria for development of the annex. For example, availability of mobile or transportable CJCS/Service-controlled assets and security of key facilities outside the combat zone. Address the following:

(1) (U) There will be no change to current frequency allocation and/or current joint CEOI.

(2) (U) No additional DISN services will be available in support of this operation.

(3) (U) No additional communications equipment will be available in time to support this operation.

2. (U) Mission. State clearly and concisely the essential tasks and purposes (who, what, when, where, and why) to be accomplished with respect to communications as it relates to the overall mission contained in the basic order.

3. (U) Execution

a. (U) Commander's Intent. State the G-6's/S-6's intent with respect to communications as it relates to the commander's intent contained in the basic order. Include, if appropriate, a COG and critical vulnerabilities analysis.

b. (U) Concept of Operations. Describe the operation in narrative form to provide a "word picture" of how the communications plan will unfold, emphasizing phasing and

Page number

CLASSIFICATION

CLASSIFICATION

aspects of the operational scheme of maneuver that establish communications requirements and that affect employment options. Tie the phases of the operation to the phases of the communications plan.

c. (U) Tasks. List the tasks assigned to each subordinate unit or tactical grouping, both organic and attached, in separate, numbered subparagraphs. Some tasks may require a specific level of detail or may imply additional tasks not appropriate for a tasking statement in the annex K shell. In those instances, additional requirements should be included elsewhere in the various appendices to the annex. Some tasks may be deemed so critical they may be assigned as missions, and so require a corresponding purpose with the task. Tasks are listed in order of priority of accomplishment and may be listed by phase. Tasks should be sequenced as follows:

- (1) (U) CE (staff sections and associated communications units).
- (2) (U) () GCE (and associated communications units).
- (3) (U) () ACE (and associated communications units).
- (4) (U) () LCE (and associated communications units).

d. (U) CCIR. State the G-6's/S-6's critical information requirements with respect to communications. CCIRs identify information concerning friendly and enemy activities and the battlespace that the G-6/S-6 deems critical to decisionmaking and that could drive changes to the communications mission, CONOPS, or the communications network. CCIRs are subdivided into three categories: PIRs (information about the enemy), FFIRs (information about friendly forces and the environment), and EEFI (information to be protected from the enemy, the disclosure of which could expose friendly vulnerabilities). Examples include:

- (1) (U) Loss of STEP entry/gateway access.
- (2) (U) Loss of a key node or facility.
- (3) (U) Loss of redundant paths that "single thread" a key node and which could lead to node isolation.
- (4) (U) Maintenance readiness of critical low density assets that falls below a pre-designated percentage (e.g., 90%).
- (5) (U) Weather that impacts the operational capability of equipment.
- (6) (U) Indications of enemy jamming activities.
- (7) (U) Indications of enemy network intrusion activities.

Page number

CLASSIFICATION

CLASSIFICATION

- e. (U) Intelligence and Reconnaissance. Describe the concept of support (including specific agreements between the G-6/S-6 and G-2/S-2, relationships, and tasks for support) for communications services for intelligence and reconnaissance operations. Include responsibilities for services provided by organic intelligence assets (such as TROJAN SPIRIT) and services provided by the communications section. Refer to appendix 13 (Special Intelligence Network Plan) of this annex and, if military satellite communications is a requirement, ensure it is addressed in appendix 5 (Radio Network Plan).
- f. (U) Coordinating Instructions. List instructions that are common to two or more units or that are applicable to the force as a whole. Refer to annexes, appendices, or references for coordinating details when appropriate.
- g. (U) Information Management. Refer to annex U (Information Management Plan) for specific information management requirements and C2 systems employment guidance, as well as appendix 8 (Data Network Plan) of this annex for specific communications systems configurations (such as IP assignments, quality of service statements, or virtual private network assignments). This will ensure proper coordination of communications services (bandwidth, switching, and routing configurations) to support the command information management plan.
4. (U) Administration and Logistics
- a. (U) Administration. Include requirements for personnel, administrative records and reports, and other miscellaneous matters significant to operations but not classified according to any of the subjects above. Refer to appendix 1 (Communications Control) of this annex for a list of required reports.
- b. (U) Logistics
- (1) (U) State broad instructions concerning logistic support of the communications mission. Refer to appendix 14 (Communications Support) of this annex for details on items such as power, refueling, and coordinating instructions for logistic procedures.
- (2) (U) Repeat important logistic coordination matters, even if covered in annex D. Include supply and maintenance responsibilities, contractor support, equipment reconstitution, and procurement policies.

Page number

CLASSIFICATION

CLASSIFICATION

5. (U) Command and Signal

a. (U) Command Relationships. Refer to appendix 1 (Communications Control) of this annex for communications command relationships. Refer to annex A (Task Organization) for the basic order for overall command relationships. Describe the relationships of the attachments the command receives as well as the detachments the command provides to other units.

b. (U) Command Posts and Headquarters. List locations of key communications units and facilities (MCCC, SYSCON, TECHCON).

c. (U) Succession to Command. Identify the chain of succession for communications staff officers (G-6/S-6).

d. (U) Signal. Includes instructions or restrictions relating to communications, such as radio restrictions, EMCON, or pyrotechnic signals.

(1) (U) Refer to the automated CEOI for visual command and signal, call signs, call words, frequencies, brevity codes and challenges, and passwords. List pertinent communications POCs.

(2) (U) Identify where electronic copies of the annex K, supporting documentation, and other pertinent communication information can be found.

(3) (U) Refer to SOP if applicable.

Name
Rank and Service
Title

APPENDICES:

1. Communications Control
2. Communications Security (COMSEC)
3. Information Security (INFOSEC)
4. Spectrum (Frequency) Management Plan
5. Radio Network Plan
6. Multiplexing Network Plan
7. Telephone Network Plan
8. Data Network Plan
9. Video Teleconferencing Plan
10. Organizational Messaging Plan
11. Help Desk Procedures
12. Maintenance Procedures

Page number

CLASSIFICATION

CLASSIFICATION

- 13. Special Intelligence Network Plan
- 14. Communications Support
- 15. Operational Risk Management (ORM)

OFFICIAL:

s/

Name

Rank and Service

Title

Page number

CLASSIFICATION

APPENDICES CONTENT GUIDE

Appendix 1: Communications Control

Tab A: Communications Control Diagram

This diagram reflects the communications control that the MCCC has established over the network. It is a quick reference that MCCC/SYSCON/TECHCON watch standers can reference as an aid in reporting significant network-related events and includes the following:

- Unit POCs can be listed on the diagram, or may be included as an exhibit to the tab.
- Include unit names on the diagram.
- Grid coordinates for the MCCC and subordinate SYSCONs may be included.

Tab B: Required Reports

Include a required reports matrix or a simple list with required reports with examples as necessary, to include the following information:

- To what unit/agency reports must be submitted.
- Required time for report submission.
- Transmission media reports are to be submitted via means such as e-mail, telephone, or radio net.

Tab C: Master System Link Designator List

A master system link designator (SLD) list is required to ensure that all links are properly identified, and not used more than once. Consider the following when creating a master SLD:

- The most efficient means to create the SLD list is to use the export tool within the tactical network analysis and planning system (TNAPS).
- A TNAPS can export information to a Microsoft Excel spreadsheet that can be inserted into a Microsoft Word document and placed as a tab within the appendix. This process can also be used to port the SLD to a Web page.
- The SLD list will change over the period of a given exercise or operation and will require continuous update. This can be accomplished efficiently with Web page updates and alerts to subscribers via an e-mail distribution list.
- Links for FRAGOs can be quickly created for an operation using TNAPS, updated within the FRAGO matrix, and ported to the SLD Web page for quick reference.

Tab D: Master Command Communications Service Designator

The process explained on page F-9 for the SLD list also applies to the command communications service designator (CCSD) list.

Appendix 2: Communications Security

This appendix defines the COMSEC plan for the exercise or operation. The communications network planner is responsible for preparing and planning COMSEC requirements (such as keying materials, codes, or equipment) for the communications network, and must work closely with the EKMS manager(s) to accomplish this. For example, the communications network planner will identify the COMSEC keying materials for the MAGTF switched network and the COMSEC and alternate COMSEC parent circuit switches. This appendix will also—

- Define how COMSEC keying material will be distributed throughout the AO.
- Define what unit/agency is responsible for distribution.
- Provide effective and supersession date information for keying materials to be used.
- Provide amplifying guidance and direction for submission of COMSEC incident reports.
- Provide coordinating instructions that might reference what actions are to be taken in event of a compromise.
- Provide POC information for EKMS manager(s).

Tab A: Intent to Use Message

Once the “Intent to Use” message is published, place it in this appendix for easy reference.

Tab B: Communications Security Callout Message

Once the “COMSEC Callout” message is published, place it in this appendix for easy reference.

Tab C: Emergency Action Plan

This is the command’s EKMS emergency action plan. If an SOP exists, reference it here or provide the location of the electronic copy.

Appendix 3: Information Security

This appendix identifies general INFOSEC requirements and procedures. The references should identify the commander’s policies and procedures. The following information (not a complete list) should be outlined in this appendix:

- IA vulnerability alert procedures.

- Types of reports that are to be used. Note: These reports should also be listed in appendix 1: Communications Control, tab B.
- Coordinating instructions which should reference items such as firewall procedures and IA POCs.

Tab A: SIPRNET DSID Diagram

A diagram of the DSID network that identifies SLD/CCSD and IPs used. Exhibits in this tab should list all firewall settings for initial implementation. Specific guidance for how DSIDs are managed should also be included in this appendix.

Tab B: SIPRNET Antivirus Architecture Diagram

A diagram of the antivirus server architecture identifying SLD/CCSD and IPs used.

Tab C: NIPRNET DSID Diagram

Similar to tab A.

Tab D: Information Assurance Vulnerability Alert Process Diagram

This diagram should highlight the IA vulnerability alert process that was outlined previously.

Tab E: Interim Authority to Operate

Once the interim authority to operate package is completed, place it in this appendix for reference.

Tab F: Systems Security Accreditation Authorization

Once the systems security accreditation authorization is published, place it in this appendix for reference.

Tab G: Example End User Agreement

This is a reference that should have been discussed in the appendix. Every Marine that accesses the network must sign one of these agreements.

Appendix 4: Spectrum (Frequency) Management Plan

This appendix defines how spectrum (frequency) management is conducted and, most importantly, how frequencies are requested and deconflicted. Reference to the CEOI and where it can be located will be included. Spectrum management POC information will also be included.

Tab A: Standard Frequency Action Request

Tab B: Master Net List

Appendix 5: Radio Network Plan

The appendix will provide necessary guidance and diagrams required to install, operate, and maintain the radio network, including SCR, MCR, and satellite radio. The satellite access request and gateway access request will be included in this appendix. This will be particularly important information while conducting a relief in place (RIP).

Tab A: Radio Guard Chart

Tab B: HF Radio Network Diagram

Tab C: VHF Radio Network Diagram

Tab D: LOS Radio Network Diagram

Tab E: UHF (LOS) Multichannel TACSAT Radio Network Diagram

Tab F: Gateway Access

Once the gateway access request is published, place it in this appendix for easy reference. This will be particularly useful during a RIP of communications units.

Tab G: SHF (LOS) Multichannel Radio Network Diagram/Gateway Access Authorization

Once the gateway access authorization is released by the STEP site, place it in this appendix for easy reference. This will be particularly useful during a RIP of communications units.

Tab H: UHF SATCOM Radio Network Diagram

Tab I: UHF SATCOM MCR Network Diagram

Tab J: EHF SATCOM MCR Network Diagram

Tab K: EHF SATCOM Orderwire Network Diagram

Tab L: Satellite Access Request (US military)

Tab M: Satellite Access Request (Commercial)

Tab N: Satellite Access Authorization (US military)

Tab O: Satellite Access Authorization (Commercial)

Appendix 6: Multiplexing Network Plan

This appendix will provide necessary guidance and diagrams, and will include any special considerations or restrictions, required to install, operate, and maintain the multiplexing network. Tabs are used to amplify this information.

Tab A: Multiplexing Network Diagram

Tab B: TRITAC Levels One and Two Multiplexing Network Diagram

Tab C: FCC 100 Level One Multiplexing Network Diagram

Tab D: PROMINA Level One Multiplexing Network Diagram

Tab E: Primary Network Timing Diagram

Tab F: Cut Sheet

Appendix 7: Telephone Network Plan

This appendix discusses elements that a network planner should take into account when designing a telephone system. Within the tabs, you will find examples of some of the following topics and other pertinent information.

Tab A: Circuit Switch Diagram

Tab B: Defense Switch Network/Defense Red Switch Network Diagram

Tab C: Dialing Instructions

Tab D: Information Systems Directory Format

Tab E: Generation of Traffic Reports

Tab F: Naming Standard

Tab G: Global Block Numbering Plan

The global block numbering plan (GBNP) is managed by DISA. The GBNP predesignates a range of PRSL to each of the Uniformed Services to avoid conflict in switchboard

identifier codes. Marine Corps Systems Command is the GBNP manager for the Marine Corps designated range, providing a breakdown for each of the four MEFs and MCTSSA.

Tab H: Leased Line Emulation

This feature, commonly referred to as yellow alarm busyout, is available on the primary rate card in the Promina 400/800. When yellow alarm busyout is enabled, it overrides the regular busyout features and all parameters pertaining to regular busyout are no longer displayed in the operator interface of the Promina. When a busyout condition occurs, the digroup will bring down the whole digroup; hence, the emulated leased line, rather than busyout, an individual port, or a group of ports in the digroup, forces the REDCOM to use a secondary route (if available). Yellow alarm busyout is applied in response to the following conditions:

- No bandwidth.
- Primary call path not available.
- Slow response (if enabled).
- Destination Promina failure.
- No echo canceller channel available.
- No compression/decompression channel available.

Tab I: Database Backup

An essential element of maintaining a voice switching network is implementing a backup plan for the database configuration files. Each switchboard has a different method of storing configuration files. This process ensures that current data can be restored in the event of a catastrophic database failure.

Tab J: Incorporating ISDN in a Non-ISDN Network

Tab K: Class of Service/River City

Tab L: Line Route Maps

Tab M: Voice-over Internet Protocol Guidance

Appendix 8: Data Network Plan

This appendix may be very extensive due to increased reliance on more complex data networks. The implementation of directory services, naming standards, and software standards should be discussed. Tabs within the appendix should provide detailed explanation of network diagrams.

Tab A: SIPRNET Routing Diagram

Tab B: SIPRNET Switching Diagram

Tab C: SIPRNET Network Operating System Architecture Diagram

Tab D: SIPRNET Active Directory Planning and Design

Tab E: SIPRNET Individual Messaging Architecture

Tab F: SIPRNET IP Block List

Here, place a list of IPs assigned to units within the architecture. Note: The appendix should highlight how IP management is handled, who is responsible for the assignment, and the procedures for requesting additional IPs.

Tab G: NIPRNET Routing Diagram

Tab H: NIPRNET Switching Diagram

Tab I: NIPRNET Network Operating System Architecture Diagram

Tab J: NIPRNET Active Directory Planning and Design

Tab K: NIPRNET Individual Messaging Architecture

Tab L: SIPRNET IP Address Listing

Appendix 9: Video Teleconferencing Plan

This appendix will provide necessary guidance, special instructions or restrictions, and diagrams required to install, operate, and maintain the VTC network. It will also address particular information pertaining to low bandwidth circuits and how VTC will be implemented on these circuits. Tabs are used to amplify this information.

Tab A: VTC Network Diagram

Tab B: VTC H320 Network Diagram

Tab C: VTC H323 Network Diagram

Tab D: VTC Dialing Instructions

Appendix 10: Organizational Messaging Plan

This plan is often overlooked because of the reliance on individual messaging, but it should not be. It should identify how messages are received and routed to end users as well as how end users/staffs will draft and send their organizational message traffic. Coordinating instructions may specify software to be used, the requirement to submit permissions to release message traffic, and any courier procedures. Handling of Top Secret message traffic should be addressed as well.

Tab A: SIPRNET Organizational Messaging Architecture Diagram

Tab B: NIPRNET Organizational Messaging Architecture Diagram

Tab C: Distinguished Name List

Tab D: Plain Language Addresses List

Appendix 11: Help Desk Procedures

This appendix outlines help-desk support procedures for all types of communications terminal devices and procedures. The fact that most Marines, Sailors, and contractors work with Internet service providers and telephone or cell phone providers while in garrison should become a combat multiplier for the G-6/S-6 in the deployed environment. There is no reason that help desk support in the deployed environment should be any different, or any less responsive. Provide a diagram or flowchart that maps the flow of information. Place this flowchart in a tab. Helpdesk POC should be listed as well. Other information, in tab or other form, may include—

- Procedures for how to establish network users' accounts.
- Procedures for how to modify or delete accounts.
- Procedures for submitting trouble calls.
- Procedures for escalating trouble calls to a higher tier of maintenance/administration.

Tab A: Trouble Ticket Flow Chart Diagram

This tab should explain the trouble ticket work process from initiation of a trouble call, to closing the trouble call with the user's problem fixed.

Appendix 12: Maintenance Procedures

This appendix should outline the procedures for inducting equipment into first echelon maintenance, as well as evacuating equipment to second echelon maintenance and above.

Considering the amount of COTS equipment that is currently used, as well as the contractor support required to repair some critical low density equipment assets within the communications inventory, it is imperative that all users of this equipment are familiar with the proper maintenance procedures. Include maintenance POCs within this appendix.

Tab A: Contracted Logistic Support

Identify equipment that requires this type of support as well as other items such as funding lines, POCs, or Marine Corps Systems Command project managers within this tab. A matrix identifying TAMCN [table of authorized materiel control number]/end item with relevant information is useful.

Tab B: Navy/Marine Corps Intranet Repair Flow Chart

The procedures for repairing Navy/Marine Corps Intranet assets should be identified within this appendix. The flowchart assists as a reference for this difficult process. These procedures and the flowchart ensure that the help desk is aware of the evacuation and repair procedures of these assets.

Appendix 13: Special Intelligence Network Plan

This appendix is a detailed plan of the communications support agreements made between intelligence section communications planners and communications section communications planners. It should expound upon annex K, paragraph 3.e, Intelligence and Reconnaissance.

Tab A: Radio Network Diagram

Similar types of diagrams (symbology, terms, SLD/CCSD) to those used in the Radio Network Plan, appendix 5, apply here; this will ensure standard operations and services provided.

Tab B: Multiplexing Network Diagram

Similar types of diagrams, such as symbology, terms, or SLD/CCSD, to those used in the Multiplexing Network Plan, appendix 6, apply here; this will ensure standard operations and services provided.

Tab C: Telephone Network Diagram

Similar types of diagrams, such as symbology, terms, or SLD/CCSD, to those used in the Telephone Network Plan, appendix 7, apply here; this will ensure standard operations and services provided.

Tab D: Data Network Diagram

Similar types of diagrams, such as symbology, terms, or SLD/CCSD, to those used in the Data Network Plan, appendix 8, apply here; this will ensure standard operations and services provided.

Tab E: VTC Network Diagram

Similar types of diagrams, such as symbology, terms, SLD/CCSD, to those used in the VTC Network Plan, appendix 9, apply here; this will ensure standard operations and services provided.

Appendix 14: Communications Support

This appendix covers the support areas that are required for a communications plan, as well as services that are not always required, but support the plan. For example, it may outline how the power requirements for the command post, xCCC, SYSCON, and TECHCON will be maintained, or how forward command posts will use power. It should also contain diagrams for generators and power cables. In addition, it should outline what agency within H&S (company/battery/battalion) is responsible for power.

Tab A: Power Requirements

Though numerous items may be listed in this tab to include diagrams, concentration should be placed on at least the following items:

- Location of generators.
- Power cable routes.
- Power requirements for the command post/Marine TACC, SYSCON, TECHCON, staff tents/buildings, or maintenance facilities.
- Refueling plan/refueling route.
- Preventive maintenance plan to include power outage procedures and a checklist of what agencies need to be coordinated with for an outage.

Tab B: Special Maintenance Procedures

This tab covers everything that does not properly fit into the maintenance procedures appendix. For example, when video and storage WAN was initially fielded to I MEF as a proof of concept during Operation Iraqi Freedom II, repair parts for the platform were often difficult to obtain. Eventually, a small team of Marines and contractors worked out the supply problems. These procedures would fit well into this tab.

Tab C: Messenger Service

Messenger service during Operation Desert Storm/Desert Shield was used extensively by 5th MEB. During Operation Iraqi Freedom I, the GCE capitalized on this capability, while the ACE did not. This tab is not always required; however, this capability does exist within the GCE, ACE, and LCE. If a messenger plan is established, this appendix should outline the implementation of it. Often messengers travel in teams and leaving what they do to chance can be dangerous and costly in terms of life and equipment. The procedures and details — actions upon completion of the courier's mission, immediate action procedures, or lost communications procedures — need to be thoroughly outlined within this tab.

Appendix 15: Operational Risk Management

The purpose of this appendix is not to teach the operational risk management (ORM) process, but to use the ORM process in support of the various missions and actions the communications community must take in support of an operation. For example, an ORM assessment of the placement of a VHF retransmission team in support of a division forward movement would be critical in identifying the multiple risks and scenarios that a team may face, as well as what actions are required to mitigate those risks. This appendix may list some scenarios for the communicators to consider.

Tab A: ORM Worksheet

An example of a completed communications-related ORM worksheet should be included in this section.

APPENDIX G

INFORMATION SYSTEMS DIRECTORY

SECTION I

An information systems directory (ISD) is one of the most critical documents pertaining to communications planning. It provides information on using a communications system service to the maximum extent possible without assistance from communications personnel. The principal function of this directory is to provide guidelines from which communications officers and telephone systems officers may produce a directory for their commands or organizations. Section II of this appendix is a sample II Marine expeditionary force (MEF) ISD. It supports the design characteristics of the Marine air-ground task force (MAGTF) tactical communications network.

1.1 Security of Information

The ISD for a given organization, even one as large as the MEF, need not be classified if the directory contains information derived from unclassified sources. For example, a listing of organizations with subscriber numbers that are consistent with this appendix and are unchanging from operation to operation need not be classified. An ISD could be used as a source of information for enemy intelligence collection; however, it should be designated as "For Official Use Only" if it contains communications architecture diagrams or if it will be used in an operation outside the continental United States.

1.2 Cover

A cover can specify which organization created the directory, for what community of users the directory is intended, and the effective period for the directory.

1.3 Emergency Numbers

Emergency numbers provide the user rapid access to numbers for certain critical agencies such as the aid station, combat operations center, or force protection platoon. These numbers should also be noted in the organizational listing.

1.4 Index

An index is an optional feature that serves as a table of contents. The size of the directory will determine the need for an index.

1.5 General Instructions

These instructions discuss the differences in the types of telephone equipment that may be used by a unit during an operation. The telephone equipment should include tactical equipment such as the KY-68, TA-1042, Secure Telephone Unit (STU)-III, secure terminal equipment (STE), commercial equipment, and cellular and satellite telephones. Each has its own special operating instructions.

1.6 Operating Instructions

These instructions tell subscribers how to effectively use the telephone network. They should list the unique operating characteristics of each telephone system.

1.7 Dialing Instructions

These instructions will aid the use of different telephone systems found in a MEF-level operation. Instructions should give enough detail to allow people who are unfamiliar with the system to use it effectively. Instructions should not change significantly from unit to unit or from operation to operation, as the equipment characteristics do not change. Instructions do not describe every available subscriber feature of the switching system. This technical information may be found in technical manuals or in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231 series, *Manuals for Employing Joint Tactical Communications*, for the specific equipment.

1.8 Precedence Subscribers

Circuit switched calls within a network are processed according to five levels of precedence. The precedence levels follow in ascending order.

a. Routine

Routine (R) has no precedence over any other call and is handled sequentially as placed by the calling party. There is no preemption of any lines. Routine precedence designation applies to normal official government communications.

b. Priority

Priority (P) has precedence over routine calls. Priority precedence is reserved generally for telephone calls by parties requiring expeditious action or essential information for conducting government operations.

c. Immediate

Immediate (I) has precedence over and preempts routine and priority calls. Immediate precedence is reserved generally for telephone calls pertaining to—

- Situations that gravely affect the security of national and allied forces.
- Reconstitution of forces in a post attack period.
- Intelligence essential to national security.
- Diplomatic negotiations to reduce or limit the threat of war.
- Implementation of Federal Government actions essential to national survival.
- Situations that gravely affect the internal security of the United States.
- Civil defense actions concerning direction of our population and their survival.
- Disasters or events of extensive seriousness having an immediate and detrimental effect on the welfare of the population.
- Vital information having an immediate effect on aircraft, spacecraft, or missile operations.

d. Flash

Flash (F) has precedence over and preempts immediate, priority, and routine calls. Flash precedence is reserved generally for telephone calls pertaining to—

- Command and control of military force essential to defense and retaliation.
- Critical intelligence essential to national survival.
- Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities.
- Dissemination of critical civil alert information essential to national survival.
- Continuity of Federal Government functions essential to national survival.
- Fulfillment of critical US internal security functions essential to national survival.
- Catastrophic events of national or international significance.

e. Flash Override

Flash override (FO) has precedence over and preempts all other types of telephone calls. The application of the flash override capability is available to—

- The President of the United States, Secretary of Defense, and Joint Chiefs of Staff.
- Commanders of unified and specified commands when declaring either defense readiness condition (DEFCON) 1 or defense emergency.
- Commander, United States Northern Command/Commander, North American Aerospace Defense Command when declaring either DEFCON 1 or air defense emergency and other national authorities as the President may authorize.

f. Dialing Precedence Calls

The precedence indicator (P, I, F, or FO) is dialed from the subscriber's telephone terminal keypad, and it is dialed first in any dialing sequence. If no precedence is dialed, the call is processed as routine. The unit communications officer, in accordance with standard operating procedures, determines which telephones will have precedence capability. The precedence capability is programmed into the circuit switch memory. If a subscriber has a precedence capability, any precedence indicator can be chosen in a dialing sequence, up to the level that has been authorized. A subscriber attempting to use precedence levels higher than that authorized will have the call processed at the maximum authorized level. Both loops and trunks are preemptable. A call cannot preempt a loop or trunk in the switch that is handling a call of equal or higher precedence.

1.9 Numbering Plan

The tactical telephone numbering plan is based on a 13-digit numbering scheme and is structured into four parts as illustrated in figure G-1.

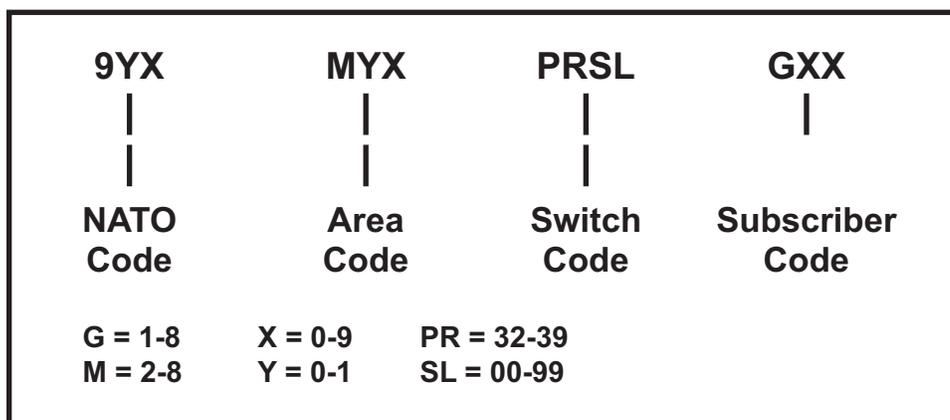


Figure G-1. Tactical Telephone Numbering Plan.

a. NATO Code

The members of North Atlantic Treaty Organization (NATO) agreed to a STANAG [NATO standardization agreement] that established a unique three-digit national identification number (9XY). The national identification code for tactical US forces is 914. Calls to NATO subscribers can be made from most tactically employed circuit switchboards.

b. Area Code

An area code (MYX) is a number that identifies an area or region of switches. Area codes are only assigned during very large military operations in which several Services are

working together in a joint operation. The DISA (Defense Information Systems Agency) Defense Switched Network (DSN) area codes are assigned by geographical areas and function as follows:

- 312 – CONUS voice.
- 314 – Europe voice.
- 315 – Pacific voice.
- 317 – Alaska voice.
- 318 – Central voice.
- 502 – CONUS switched 56/64 VTC/ISDN.
- 504 – Europe switched 56/64 VTC/ISDN.
- 505 – Pacific switched 56/64 VTC/ISDN.
- 507 – Alaska switched 56/64 VTC/ISDN.
- 508 – CONUS switched 56/64 VTC/ISDN.
- 512 – CONUS Low rate data/fax.
- 514 – Europe Low rate data/fax.
- 517 – Alaska Low rate data/fax.
- 515 – Pacific Low rate data/fax.
- 518 – CONUS Low rate data/fax.

(VTC/ISDN = video teleconferencing/integrated services digital network)

(1) Unique Area Codes

If a very large military operation is conducted, each force in a theater might be assigned a unique area code. If a military operation becomes extremely large, the Marine Corps forces have several area codes reserved for their use depending on the geographic area to which they are deployed:

- 204 – MARFORCOM [United States Marine Corps Forces Command].
- 304 – MARFORCENT [United States Marine Corps Forces, Central Command].
- 804 – MARFORPAC [United States Marine Corps Forces, Pacific].
- 408 – MARSOC [United States Marine Corps Forces, Special Operations Command].

(2) Inter-Area Dialing

When calling a subscriber who is serviced by a different area code (MYX), the full 10-digit number must be dialed (MYXPRSLGXX). As with dialing another primary region switch

locator (PRSL), the same 9 or 91 escape codes must be used. The number dialed will be either 9 MYX PRSL GXX or 91 MYX PRSL GXX Switch Code (PRSL).

A switch code is a unique, 4-digit number that identifies one particular circuit switch. The first two digits of the code are the primary region (PR) and the last two digits are the switch locator (SL). The switch code is also called the PRSL. All circuit switches must be assigned a switch code, whether operating independently or as part of a circuit switched network. A 4-digit PRSL switch code within a network is also called a 4/3 numbering plan, since the switch code is four digits and the subscriber number is three digits. The 4/3 numbering plan is preferred in military circuit switched systems since it allows for more circuit switches with fewer subscribers as compared with a commercial switching system which uses a 3/4 numbering plan. A commercial switching system has fewer switches with more subscribers, hence the 3/4 code.

(3) Interswitch Dialing

When calling a subscriber who is serviced by a different circuit switch (PRSL), the full 7-digit number must be dialed (PRSL-GXX). First, however, the circuit switch must be told that the numbers dialed are PRSL numbers and not subscriber numbers by dialing a 1- or 2-digit special “long-distance” or escape code. Some circuit switches require a 9 or a 91 code prior to the 7-digit subscriber number, similar to dialing a “1” for long distance on a telephone at home or in the office. The number dialed will be either 9 PRSL GXX or 91 PRSL GXX.

Primary region codes will be assigned by the higher headquarters J6/G-6, according to the global block numbering plan (GBNP) matrix found in CJCSM 6231.02, *Manual for Employing Joint Tactical Communications – Joint Voice Communications Systems*. Some higher level switches in the military can use a 3/4 numbering plan, which uses a 3-digit switch code (NNX), called a local exchange code, vice a PRSL code. The full subscriber number then takes on the form NNXGXXX subscriber number (GXX).

The subscriber number is a 3-digit number between 100 and 899. Every telephone instrument that is connected to a circuit switch, whether automatic or manual, must be assigned a number. All subscriber numbers are listed together in the ISD, which is published by the unit communications officer prior to an operation. When one user wishes to call another user who is on the same circuit switch, he only needs to dial the subscriber number (GXX).

c. Global Block Numbering Plan

The Marine Corps uses the GBNP to incorporate all of its switches into a joint network. The GBNP identifies all of the Services with a unique, Service-managed block of numbers; simplifies network management into a global network; ensures nonduplication of numbers within an area of responsibility; and identifies databases and subnetworks within the assigned block of numbers. The GBNP associates a block of numbers—PRSL

numbers between 3200–3999—with each major subordinate command and switch type. The major subordinate commands should coordinate with their respective preaffiliation managers to determine their subscriber numbers.

1.10 Local Area Network Instructions

These instructions address how to use the SECRET Internet Protocol Router Network (SIPRNET) and Non-Secure Internet Protocol Router Network (NIPRNET) local area network (LAN) instructions should describe all LAN services available, including e-mail, Internet access, message dissemination, and computer security.

1.11 Information Systems Listing

This listing provides tactical, commercial, DSN, host nation, pager, and cellular telephone numbers for subscribers at every organizational location. It also provides subscriber's SIPRNET and NIPRNET LAN addresses and any operational Web page addresses. The listing should include adjacent major organizations of other Services in a joint operation.

SECTION II. EXAMPLE OF II MEF INFORMATION SYSTEMS DIRECTORY

This section contains a representative information systems directory (ISD) designed according to the principles outlined in the first section of this appendix. The remainder of this appendix is a sample directory and uses II Marine expeditionary force (MEF) as the notional unit. The directory, however, may not accurately reflect the actual composition of the present II MEF, nor does it list all of the potential subscribers to the system. Communications officers should consult with the global block numbering plan (GBNP) and their units' tables of organization and standard operating procedures before preparing a directory to ensure that subscriber numbers are accurate. A legend containing acronyms used in this sample can be found at the end of this appendix.

CLASSIFICATION

II MEF EXERCISE

INFORMATION SYSTEMS DIRECTORY

Effective Date 210800Z October XXXX

EMERGENCY NUMBERS

Operator	000
Combat Operations Center	3420-300
Headquarters Commandant	3420-807
Force Protection Platoon	3420-160

Telephone	
Help Desk	3421-613
LAN	
Help Desk	3420-605

TELEPHONE SECURITY IS EVERYONE’S RESPONSIBILITY. DO NOT DISCUSS CLASSIFIED INFORMATION ON NONSECURE TELEPHONES! OFFICIAL DOD TELEPHONES ARE SUBJECT TO MONITORING AT ALL TIMES FOR COMMUNICATIONS SECURITY PURPOSES.

INDEX

EMERGENCY NUMBERS
GENERAL INSTRUCTIONS.....
OPERATING INSTRUCTIONS.....
DIALING INSTRUCTIONS.....
PRECEDENCE SUBSCRIBERS
NUMBERING PLAN
LAN INSTRUCTIONS.....
II MEF INFORMATION SYSTEMS LISTING.....

Page number

CLASSIFICATION

CLASSIFICATION

General Instructions

The telephone network allows most users to place local and long distance telephone calls without operator assistance. By using the following instructions, telephone service will be quicker and more responsive to your needs. Use the following telephones with digital switching equipment:

Secure Terminal Equipment (STE)

The STE is compatible with analog plain old telephone service (POTS) and integrated services digital network (ISDN) BRI-S/T phone lines. It provides secure voice and data capability with the use of a KOV-14 Fortezza Personal Computer Memory Card International Association card. It is backward compatible with STU-III technology and was designed to replace both STU-III and KY-68 secure telephone instruments. The STE comes with several feature buttons and nonsecure hands free operation. Operating modes and other settings are modified via soft keys. An external 120V power outlet is required to support the display screen and other features.

Standard Desk Telephones

Standard POTS desk telephones are frequently installed for subscribers not requiring secure voice service. Models may vary, but most models provide a standard 12-button keypad and ringer volume control. Other models may provide feature buttons for hook-switch, flash, mute, redial, speed dial, and handset volume control.

TA-1042 Digital Nonsecure Voice Terminal (DNVT)

This is the rugged, green, push-button telephone. The LED [light emitting diode] will blink and a ring will be sounded when the phone receives a call. A knob located on the phone will adjust ringer volume. Ensure that the ear piece is properly reinserted into the body of the phone after the call is completed. DO NOT use the push-to-talk switch on the handset at anytime. This will disrupt your conversation.

KY-68 Digital Secure Voice Terminal (DSVT)

This is the rugged, green, push-button telephone. Once filled, the KY-68 holds the highest classification because of the communications security key loaded inside and must be handled accordingly. After the phone has received its cryptographic fill, it requires no user adjustments other than adjusting the ring volume. ANY OTHER ADJUSTMENTS TO THE REMAINING CONTROLS MAY ZERO OUT THE TELEPHONE, RENDERING IT INOPERATIVE. If this occurs, notify the Telephone Trouble Desk at 411.

Page number

CLASSIFICATION

CLASSIFICATION

SECTEL (Secure Telephone) Multimedia Terminal (MMT) 1500

This is the Motorola 1500 STU-III and can be operated from a garrison telephone or the tactical phone system. The MMT can communicate nonsecurely to any type of phone on the tactical system—the MMT can only be connected to the tactical switch digital line termination unit with the DNVT adapter. The MMT can only go secure with another STU-III. The dialing instructions for the MMT are the same as any tactical instrument on the network unless dialing through an inter-working function.

Page number

CLASSIFICATION

CLASSIFICATION

Operating InstructionsSecure Terminal Equipment

The STE is a desktop telephone communications instrument using pluggable cryptography for digital telecommunications networks. It is designed to use ISDN telephone lines with speeds up to 128 kbps. It is secure voice capable and designed to interoperate with the STU-III secure terminal end device. The STE is capable of performing fax and data services through the means of a built-in RS-232 port.

Plain Old Telephone Service

This service is a desktop telephone communications instrument that uses analog telephone service from the public switched telephone network (PSTN). It transmits the signal over copper, twisted-pair wires and connects homes and businesses by means of a central office. This is referred as a local loop. Central offices are interconnected to establish long-distance connections.

The KY-68 and the TA-1042 may receive and initiate calls with any telephone installed within the tactical automated switch system (TASS). The KY-68 has the following unique operational characteristics:

- Under the handset of the phone is a 3-position pole type plunger that automatically sets itself in the secure mode when the phone is hung up.
- All calls are initiated in the secure mode. The handset is picked up and the number desired is dialed.
- Notifies the caller if the party being called does not have a secure voice telephone line (KY-68). The caller will hear a continuous heartbeat sound in the receiver, and the nonsecure warning will flash. The phone will go to the nonsecure mode when the plunger is pulled up.

Note: The nonsecure warning light will remain on until the call is terminated.

- Automatically resets itself to the secure mode when the phone is hung up.

The DSVTs cannot communicate securely with STU-III telephones. They are not compatible in the secure mode.

Access Through Defense Switched Network (DSN)

The II MEF TASS will have six DSN trunks available through the AN/TTC-42 switchboard. Any DSN use by subscribers will be on a first come first served basis. Precedence subscribers will have the ability to preempt other subscribers when a precedence call is initiated.

Page number

CLASSIFICATION

CLASSIFICATION

Dialing Instructions

Type Call	To Call	Dial Sequence
Inter-country	NATO Routine Precedence	98+9YX+MYX+NNXX-XXX 9P+98+9YX+MYX+NNXX-XXX*
Inter-network	US Area Code Routine Precedence	MYX+NNXX-XXX 9P+MYX+NNXX-XXX*
Intra-network	NNXX Code Routine Precedence	NNXX-XXX 9P+NNXX-XXX*
*P = Precedence Digit = 0 – 4		

The precedence digit (0, 1, 2, 3, or 4) permits a user to dial an authorized precedence level from an appropriately classmarked, 12-button telephone instrument. While it is not necessary to dial or key the precedence access code when dialing routine calls, users must do the following:

- To dial a tactical telephone number from your tactical phone, dial the following:
 - For AN/TTC-42 subscribers, dial 9 and the 7-digit extension (9-XXXX-XXX).
- To dial DSN telephone numbers at Camp Lejeune from your tactical phone, dial the following:
 - For AN/TTC-42 subscribers, dial 5C, wait for tone, and dial 451-XXXX-C (XXXX is the 4-digit DSN number) or dial 000 for the operator.
 - For SB-3865 subscribers, dial 91, wait for the tone, dial 5C, wait for the tone, and dial 451-XXXX-C or dial 000 for the operator.
- To dial a tactical telephone number from a DSN number or to dial a TASS operator from a DSN number, take the following steps:
 - Dial the tactical switch operator at one of the following numbers: 6131 or 6174.
 - Give the operator the 7-digit number (PRSL-XXX) for the subscriber you wish to reach, such as 3469-633.

Page number

CLASSIFICATION

CLASSIFICATION

Precedence Subscribers

The commercial circuit switchboards (AN/TTC-62, AN/TTC-63) are capable of processing five levels of precedence. The precedence levels and associated precedence indicators are—

ROUTINE	(94)
PRIORITY	(93)
IMMEDIATE	(92)
FLASH	(91)
FLASH OVERRIDE	(90)

The maximum precedence level authorized to a particular terminal is assigned by a class-mark. The precedence indicator (93, 92, 91, or 90) is dialed first in any dialing sequence. If no precedence is dialed, the call is processed as routine. Subscribers can initiate calls at a precedence level lower than the maximum authorized. Once a call is established, the originator's precedence level is maintained, regardless of the level authorized to other participating parties. Calls of higher priority are given preference over lower precedence calls. Initiate the call with the assigned precedence, and the call will be completed based on its priority.

Note: When a priority is used, it will disconnect any subscriber who has lower precedence. PLEASE USE THEM WITH DISCRETION.

WARNING

Remember that the telephone network is NOT SECURE. Do not discuss classified material on any telephone UNLESS YOU ARE USING AN STE TELEPHONE IN THE SECURE MODE. Even calls made within the command post are susceptible to interception. Practice good communications security!

Numbering Plan

The primary region (PR) is the primary identification number of subscribers in a geographic area.

Switch locator (SL) assignments are listed for all commands and organizations within II MEF and east coast units. Spare SL numbers are provided at different echelons and for task organization assignments.

Page number

CLASSIFICATION

CLASSIFICATION

The following PR and SL are assigned to II MEF units participating in the MEF exercise:

	PR	SL
II MARINE EXPEDITIONARY FORCE COMMAND ELEMENT	34	20
EIGHTH COMMUNICATIONS BATTALION	34	21
2D MARINE LOGISTICS GROUP	35	77
2D MEDICAL BATTALION	35	80
8TH ENGINEER SUPPORT BATTALION	35	82
2D TSB TRANSPORTATION SUPPORT BATTALION	35	84
8TH MAINTENANCE BATTALION	35	86
2D MARINE AIR WING/MARINE WING COMMUNICATIONS SQUADRON-28 DETACHMENT A	35	27
2D MARINE AIRCRAFT WING/MARINE WING COMMUNICATIONS SQUADRON-28 DETACHMENT B	35	30
2D MARINE AIRCRAFT WING (NEW RIVER)	35	32
2D MARINE AIRCRAFT WING/MARINE WING SUPPORT SQUADRON-274	35	42
2D MARINE AIRCRAFT WING/MARINE WING SUPPORT GROUP-27	35	36
2D MARINE AIRCRAFT WING/MARINE WING SUPPORT SQUADRON-271	35	40
2D MARINE AIRCARFT WING/MARINE AIR SUPPORT SQUADRON-1	35	33
2D MARINE AIRCRAFT WING/MARINE WING SUPPORT SQUADRON-272	35	41
2D MARINE DIVISION	34	69
2D MARINE REGIMENT	34	76
6TH MARINE REGIMENT	34	77
8TH MARINE REGIMENT	34	78
10 MARINE REGIMENT	34	79
2D TANK BATTALION	34	88
2D AMPHIBIOUS ASSAULT BATTALION	34	89
2D LIGHT ARMORED RECONNAISSANCE BATTALION	34	90
2D COMBAT ENGINEER BATTALION	34	91

Page number

CLASSIFICATION

CLASSIFICATION

Local Area Network (LAN) Instructions

***Disclaimer.** The Marine Corps, while recognizing certain commercial products in this directory, does not endorse any of the products listed here. Technology and the marketplace drive the products that are available. The Corps will use the best technology or tool for the job at any given time.*

LAN Overview

The personnel of II MEF will have access to both the Non-Secure Internet Protocol Router Network (NIPRNET) and the SECURE Internet Protocol Router Network (SIPRNET) during this exercise. The NIPRNET and SIPRNET addresses are located on the information systems listing at the end of this directory.

Responsibility for the overall LAN coordination of the exercise will reside with the II MEF assistant chief of staff (AC/S) communications system staff officer (G-6) and the information systems management officer (ISMO) under the cognizance of the II MEF AC/S G-6. The ISMO will be assisted by communications officers and personnel at each of the major subordinate commands. Any LAN questions and problems should be addressed to the LAN help desk at 3420-605.

The II MEF personnel will use a variety of computers loaded with Microsoft WindowsNT® Network and Exchange® software applications during this exercise. WindowsNT® is a multipurpose operating system that integrates a variety of network services. The network services it provides are designed to address requirements in many categories. Windows NT® will be used to connect all of the units within the MEF.

Software Applications

The II MEF computers have been installed with several software application packages, which include Microsoft Outlook® and Internet Explorer®.

Microsoft Outlook® is used for all electronic mail applications, including calendar and scheduling features, and is accessed via the desktop icon.

Microsoft Outlook® is a desktop information management program that helps the user organize and share information on the desktop and communicate with others. It has the ability to manage messages, appointments, contacts, and tasks, as well as track activities, view and open files, and share information with others.

In Outlook®, information is organized in folders. When the user first starts Outlook®, the Inbox folder opens. Use the Inbox to read and send mail messages, or make meeting and task requests.

Page number

CLASSIFICATION

CLASSIFICATION

To create a message, point to **New** on the file menu, and then click **Mail Message**. Enter recipient names in the **To** or **Cc** boxes. Type the subject of the message in the **Subject** box, and then type the message in the text box. When you are ready to send the message, click **Send**.

To go to another part of Outlook® quickly, click a **Shortcut** on the Outlook® Bar to the left of the **Inbox**. For example, click **Calendar** to open your calendar folder. The Folder Banner—the horizontal bar above the information viewer—shows the name of the folder that you have open. To see a complete list of your folders, click the folder name in the Folder Banner.

Outlook® can also be a substitute for Windows Explorer®. To view the files on the hard disk, click **Other** on the Outlook® Bar, and then click **My Computer**, **My Documents**, or **Favorites**.

Outlook® uses views to sort and organize items in a folder. To switch to a different view, click a view in the **Current View** box on the Standard toolbar.

If Microsoft Word® is installed on a computer, use Word® and Outlook® together to create powerful e-mail messages. To turn Word® as your editor on or off, close this message and click **Options** on the **Tools** menu. On the E-mail tab, select or clear **Use Microsoft Word®** as the e-mail editor. With Microsoft Word® as your e-mail editor, you can use features such as autocorrect, spell it, bullets and numbering, document map, and highlighter to create your e-mail messages.

The Internet [Microsoft Internet Explorer®] is used for all Web access and is accessed via the desktop icon. It is a collection of computer networks that connects millions of computers across the United States and around the world. Explorer® enables the user to connect to the Internet to gain access to vast stores of information on these computers. Double click on the Explorer® icon to access the Internet. When a frequently used URL [Uniform Resource Locator] is typed into the address bar, Explorer® will complete the address. In addition, Explorer® can search through incorrectly typed addresses in order to find a match.

Users can search for Web sites using the Explorer® bar. Click on the **Search** button on the toolbar and the Explorer® bar appears in the left side of the browser window. Then click on a link to view that page on the right side of the screen while viewing the list of search documents on the left. It is also possible to browse through favorite sites and history folders, channels, or documents.

Users can find information on the Web in a variety of ways. When the **Search** button is clicked on the toolbar, the Explorer® bar appears to the left of the window. It provides access to a number of search services that offer different kinds of searching capabilities.

Page number

CLASSIFICATION

CLASSIFICATION

To find information quickly, type **GO**, **Find**, or **?**, followed by a word or phrase in the address bar. Explorer® immediately starts a search for the topic. Then, after going to a specific Web page, the user can search for any specific text desired on that page.

LAN Security

The Internet works by sending information from computer to computer until the information reaches its destination. When information is sent from one point to another, every computer in between has an opportunity to look at what's being sent. This access can pose a security problem. Users must understand that classified information must not be sent on unsecured networks. Users should practice good computer security procedures while using the Internet.

II MEF Information Systems Listing (Effective Date: 210800Z October XXXX)

The tactical PRSL numbers are listed below. Communications officers are highly encouraged to check with their unit PAL managers before assigning tactical numbers.

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
II MEF CMD ELEMENT 3420 (TTC-42)				fwd.limef.usmc.mil	fwd.iimef.usmc.smil.mil
CG	3420-106 (DSVT)		751-9475	cg@domain	cg@domain
CELLULAR		(910) 340-8230			
C/S	3420-103 (DSVT)				
HQ CMDT	3420-807 (DNVT)				
SJA	3420-104 (DNVT)				
PAO	3420-105 (DSVT)				
SGT MAJ	3420-109 (DNVT)				
G-1					
AC/S G-1	3420-114 (DSVT)			g1@domain	g1@domain
PERSONNEL OFFICER	3420-110 (DSVT)				
ADJUTANT	3420-112 (DSVT)				
G-2					
AC/S G-2	3420-203 (DSVT)			g2@domain	g2@domain

Page number

CLASSIFICATION

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
G-2 CHIEF	3420-209 (DSVT)				
CIC WATCH OFFICER	3420-225 (DSVT)				
COLLECTIONS OFFICER	3420-211 (DSVT)				
TARGET OFFICER	3420-245 (DSVT)				
RAD BN	3420-201 (DSVT)				
CI	3420-211 (DSVT)				
METOC	3420-240 (DSVT)				
SARC	3420-242 (DSVT)				
RECON OPS CENTER	3420-244 (DSVT)				
G-3					
AC/S G-3	3420-300 (DSVT)			g3@domain	g3@domain
G-3 CHIEF	3420-303 (DSVT)				
COMBAT OPERATIONS CENTER (COC)					
SENIOR WATCH OFFICER	3420-300 (DSVT)				
FUTURE OPS OFFICER	3420-327 (DSVT)				
AIR OPS OFFICER	3420-308 (DSVT)				
CSS OPS OFFICER	3420-405 (DSVT)				
FFCC OFFICER	3420-340 (DSVT)				
FIRES	3420-340 (DSVT)				
TARGETING	3420-319 (DSVT)				
EW PLANS OFFICER	3420-225 (DSVT)				
CIVIL AFFAIRS	3420-105 (DSVT)				
G-4					
AC/S G-4	3420-402 (DSVT)			g4@domain	g4@domain
G-4 CHIEF	3420-402 (DSVT)				

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
G-4 OPERATIONS	3420-403 (DSVT)				
EMBARK	3420-404 (DSVT)				
ENGINEER OFFICER	3420-405 (DSVT)				
MEF SURGEON	3420-430 (DSVT)				
G-5					
AC/S G-5	3420-500 (DVST)			g5@domain	g5@domain
DEP G-5	3420-501 (DSVT)				
G-5 CHIEF	3420-505 (DSVT)				
G-6					
AC/S G-6	3420-600 (DSVT)			g6@domain	g6@domain
G-6 OPS OFFICER	3420-601 (DSVT)				
G-6 OPS CHIEF	3420-602 (DSVT)				
G-6 DATA OFFICER	3420-603 (DSVT)				
G-6 COMM CHIEF	3420-603 (DSVT)				
LAN/WAN TROUBLE DESK	3420-650 (DNVT)				
Miscellaneous					
AID STATION	3420-155 (DNVT)				
FORCE PROTECTION	3420-160 (DNVT)				
8TH COMM BN 3421 (SB-3865)					
CO	3421-806 (DSVT)				
XO	3421-807 (DSVT)				
SGT MAJ	3421-808 (DNVT)				
OPS OFFICER	3421-830 (DSVT)				
OPS CHIEF	3421-931 (DSVT)				
PERSONNEL OFFICER	3421-801 (DNVT)				

Page number

CLASSIFICATION

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
BAS	3421-867 (DNVT)				
BN OOD	3421-802 (DNVT)				
SYSCON	3421-613 (DSVT)			syscon@domain	syscon@domain
TECHCON	3421-623 (DSVT)			techcon@domain	techcon@domain
DATA COM	3421-633 (DSVT)			datacom@domain	datacom@domain
2D MARINE DIVISION 3469 (TTC-42)				fwd.2dmardiv.iimef.usmc.mil	fwd.2dmardiv.iimef.usmc.sml.mil
CG	3469-106 (DSVT)			cg@domain	cg@domain
G-1	3469-114 (DSVT)			g1@domain	g1@domain
G-2	3469-200 (DSVT)			g2@domain	g2@domain
G-3	3469-300 (DSVT)			g2@domain	g2@domain
G-4	3469-400 (DSVT)			g4@domain	g4@domain
CELLULAR		(910)340-8235			
TCO DIAL-IN	3469-675 (DNVT)				
G-6	3469-600 (DSVT)			g6@domain	g6@domain
CELLULAR		(910)340-1014			
DIVISION COMM COMPANY					
CO COMM CO	3469-610 (DSVT)				
TECHCON	3469-113 (DSVT)				
OPS OFFICER	3469-149 (DSVT)				
SYSCON (STU-III)	3469-669 (DSVT)		751-9265		
SIPRNET to MEF	3469-330 (DSVT)				
TSC-93 (GMF)		(910)451-9271			
DASC (STU-III)		(910)451-9272			
LONG LOCAL - MEF	3469-701 (DNVT)				
LONG LOCAL - WING	3469-702 (DNVT)				

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
TTC-42 (SWBD)			751-9470		
2ND MAR REGT 3476 (SB-3865)					
CO	3476-106 (DSVT)				
S-1	3476-114 (DNVT)				
S-2	3476-200 (DSVT)		751-1014		
S-3 (STU-III)	3476-300 (DSVT)		751-5263		
S-4	3476-400 (DNVT)				
S-6	3476-600 (DSVT)				
6TH MAR REGT 3477 (SB-3865)					
CO	3477-675 (DSVT)				
S-1	3477-200 (DNVT)				
S-2	3477-300 (DSVT)				
S-3	3477-662 (DSVT)				
S-4 (FAX)	3477-400 (DNVT)		751-3977		
S-6 (STU-III)	3477-600 (DSVT)		751-2822		
8TH MAR REGT 3478 (SB-3865)					
CO	3478-106 (DSVT)				
S-1	3478-114 (DNVT)				
S-2	3478-200 (DSVT)				
S-3	3478-300 (DSVT)				
S-4	3478-400 (DNVT)				
S-6 (STU-III)	3478-600 (DSVT)		751-2551		
10TH MAR REGT 3479 (SB-3865)					
CO	3479-106 (DSVT)				
S-2	3479-200 (DNVT)				

Page number

CLASSIFICATION

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
S-3	3479-300 (DSVT)				
S-4	3479-400 (DNVT)				
S-6	3479-600 (DSVT)				
2D TANK BN 3488 (SB-3865)					
CO	3486-106 (DSVT)				
S-3	3488-300 (DSVT)				
2D AMPH ASSAULT BN 3489 (SB-3865)					
CO	3489-106 (DSVT)				
S-3	3489-300 (DSVT)				
2D LAR BN 3490 (SB-3865)					
CO	3490-106 (DSVT)				
S-3	3490-300 (DSVT)				
2D COMBAT ENG BN 3491 (SB-3865)					
CO	3491-106 (DSVT)				
S-3	3491-300 (DSVT)				
2D MLG 3577 (TTC-42)				fwd.2dmlg.iimef.usmc.mil	fwd.2dmlg.iimef.usmc.smil.mil
CG (STU-III)	3577-106 (DSVT)			cg@domain	cg@domain
G-1	3577-114 (DSVT)			g1@domain	g1@domain
G-2	3577-200 (DSVT)			g2@domain	g2@domain
G-3	3577-300 (DSVT)			g3@comain	g3@comain
G-4	3577-440 (DSVT)			g4@domain	g4@domain
G-6	3577-606 (DSVT)			g6@domain	g6@domain
H&S BN					
CO	3577-706 (DSVT)				
S-3	3577-703 (DSVT)				

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
S-4	3577-704 (DNVT)				
MLG COMM CO					
CO	3577-610 (DSVT)				
OPSO	3577-149 (DSVT)				
SYSCON	3577-633 (DSVT)				
COMMERCIAL (STU-III)		(910)451-9609			
TECHCON	3577-669 (DSVT)				
SUPPLY	3577-720 (DNVT)				
MAINT	3577-779 (DNVT)				
COMMERCIAL (STU-III)		(910)451-9610			
MD BN 3580 (SB-3865)					
CO	3580-706 (DSVT)				
S-3	3580-703 (DSVT)				
S-4	3580-704 (DNVT)				
S-6	3580-600 (DSVT)				
DENTAL BN	3580-604 (DNVT)				
ENG BN 3582 (SB-3865)					
CO	3582-706 (DSVT)				
S-3	3582-703(DSVT)				
S-4	3582-704 (DNVT)				
S-6	3582-600 (DSVT)				
TSB 3584 (SB-3865)					
CO	3584-706 (DSVT)				
S-3	3584-703 (DSVT)				
S-4	3584-704 (DNVT)				

Page number

CLASSIFICATION

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
S-6	3584-600 (DSVT)				
MT BN 3586 (SB-3865)					
CO	3586-706 (DSVT)				
S-3	3586-703 (DSVT)				
S-4	3586-704 (DNVT)				
S-6	3586-600 (DSVT)				
2D MAW CHERRY POINT 3527 (TTC-42)				fwd.2dmaw.iimef.usmc.mil	fwd.2dmaw.iimef.usmc.smil.mil
CG	3527-106 (DSVT)			cg@domain	cg@domain
G-1	3527-114 (DSVT)			g1@domain	g1@domain
G-2	3527-200 (DSVT)			g2@domain	g2@domain
G-3	3527-300 (DSVT)			g3@domain	g3@domain
G-4	3527-400 (DSVT)			g4@domain	g4@domain
G-6	3527-675 (DSVT)			g6@domain	g6@domain
TACC "DET B" CHERRY POINT					
SYSCON OFFICER	3527-113 (DSVT)				
TECHCON	3527-150 (DSVT)				
TSC-85	3527-185 (DNVT)				
TSC-120	3527-120 (DNVT)				
TSC-96	3527-196 (DNVT)				
TRC-170 (MEF)	3527-170 (DNVT)				
Long Local - MEF	3527-613 (DNVT)				
MWCS 28 CO	3527-106 (DSVT)				
MWCS 28 S-3	3527-103 (DSVT)				
MWCS 28 S-4	3527-104 (DSVT)				
MWCS28 Maint	3527-115 (DNVT)				

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
DET B OFFICE	3527-206 (DNVT)				
DATA COMM	3527-230 (DSVT)				
COMM CENTER	3527-111 (DSVT)				
MSC-63	3527-211 (DNVT)				
MTACS 28					
SAC	3527-333 (DSVT)				
TBMCS SYS ADMIN	3527-380 (DNVT)				
SWO/SAC	3527-334 (DNVT)				
DCN	3527-382 (DSVT)				
ICO	3527-393 (DSVT)				
TACC	3527-381 (DSVT)				
2D MAW BOGUE FIELD DET "A" 3530 (TTC-42)					
SYSCON	3530-113 (DSVT)				
TTC-42 VAN	3530-555 (DNVT)				
TECHCON	3530-150 (DSVT)				
CO	3530-106 (DSVT)				
RADIO	3530-132 (DNVT)				
WIRE	3530-131 (DNVT)				
DATA COMM	3530-129 (DSVT)				
COMM CTR	3530-111 (DSVT)				
MAINT	3530-115 (DNVT)				
MACS-6 ATC SITE					
ATC COMMON	3530-350 (DNVT)				
FACILITY WATCH O	3530-351 (DSVT)				
RADAR SUPERV	3530-352 (DNVT)				

Page number

CLASSIFICATION

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
MACS-6 EW/C SITE					
SAD	3527-330 (DSVT)				
SID	3527-332 (DSVT)				
TECHCON	3527-313 (DSVT)				
SYSCON	3527-310 (DSVT)				
NEW RIVER DET "A" 3532 (SB-3865)					
SYSCON	3532-113 (DSVT)				
SYSCON (SWO)	3532-213 (DSVT)				
TTC-42 VAN	3532-150 (DNVT)				
TECHCON	3532-150 (DSVT)				
CO	3532-106 (DSVT)				
MASS-1 SUBSCRIBERS 3533 (SB-3865)					
SAC	3533-101 (DSVT)				
SYSCON	3533-102 (DSVT)				
SEC WAN	3533-103 (DSVT)				
COMM USER	3533-104 (DNVT)				
MAG-26 NEW RIVER 3535 (SB-3865)					
CO	3535-106 (DSVT)				
S-1	3535-114 (DSVT)				
S-3	3535-300 (DSVT)				
S-4	3535-400 (DSVT)				
S-6	3535-600 (DSVT)				
HMLA-167					
CO	3535-806 (DSVT)				
S-3	3535-330 (DSVT)				

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
MWSG 27 3536 (SB-3865)					
CO	3536-806 (DSVT)				
S-3	3536-803 (DSVT)				
S-6	3536-800 (DSVT)				
S-6 CHIEF	3536-801 (DNVT)				
SYSCON	3536-802 (DSVT)				
TECHCON	3536-833 (DSVT)				
DATA	3536-804 (DSVT)				
WXO	3536-805 (DNVT)				
MWSS 271 3540 (SB-3865)					
CO	3540-506 (DSVT)				
S-3	3540-503 (DSVT)				
S-6	3540-500 (DSVT)				
SYSCON	3540-501 (DNVT)				
TECHCON	3540-502 (DNVT)				
WXO	3540-505 (DNVT)				
MWSS 272 3541 (SB-3865)					
CO	3541-506 (DSVT)				
S-3	3541-503 (DSVT)				
S-6	3541-500 (DSVT)				
SYSCON	3541-501 (DNVT)				
TECHCON	3541-502 (DNVT)				
WXO	3541-505 (DNVT)				

Page number

CLASSIFICATION

CLASSIFICATION

				E-Mail Addresses	
Subscriber	Tactical	Commercial	DSN	NIPRNET Domain:	SIPRNET Domain:
MWSS 274 3542 (SB-3865)					
CO	3542-306 (DSVT)				
S-3	3542-303 (DSVT)				
S-6	3542-300 (DSVT)				
SYSCON	3542-301 (DNVT)				
TECHCON	3542-302 (DNVT)				
WXO	3542-305 (DNVT)				

Legend for appendix G:

AC/S	assistant chief of staff	FFCC	force fires coordination center
AMPH	amphibious	FO	flash over
ATC	air traffic control	G-1	brigade or higher personnel staff officer
BAS	battalion aid station	G-2	brigade or higher intelligence staff officer
BN	battalion	G-3	brigade or higher operations staff officer
CG	commanding general	G-4	brigade or higher logistics staff officer
CI	counterintelligence	G-5	brigade or higher plans staff officer
CIC	combat intelligence center	G-6	brigade or higher communications system staff officer
CJCSM	Chairman of the Joint Chiefs of Staff manual	GBNP	global block numbering plan
CMD	commander	GMF	ground mobile force
CO	commanding officer	H&S	headquarters and service
COMM	communications	HMLA	Marine light/attack helicopter squadron
C/S	chief of staff	HQ CMDT	headquarters commandant
CSS	combat service support	I	immediate
CTR	center	ICO	interface coordination officer
DASC	direct air support center	ISD	information systems directory
DATA COM	data communications	ISDN	integrated services digital network
DCN	data link coordination net	ISMO	information systems management officer
DEFCON	defense readiness condition	kbps	kilobits per second
DEP	deputy	LAN	local area network
DET	detachment	LAR	light armored reconnaissance
DNVT	digital nonsecure voice terminal DSN Defense Switched Network	LED	light emitting diode
DSVT	digital secure voice terminal	MACS	Marine air control squadron
EMBARK	embarkation	MAG	Marine aircraft group
ENG	engineer	MAGTF	Marine air-ground task force
EW	electronic warfare	MAR REGT	Marine regiment
EW/C	early warning/control	MASS	Marine air support squadron
F	flash	MAW	Marine aircraft wing
FAX	facsimile	MD	medical

MEF	Marine expeditionary force	SAD	senior air director
METOC	meteorological and oceanographic	SARC	surveillance and reconnaissance center
MLG	Marine logistics group	SECTEL	secure telephone
MMT	multimedia terminal	SEC WAN	secure wide-area network
MSC	nomenclature for a satellite communications terminal	SGT MAJ	sergeant major
MT	maintenance	SID	surveillance identification director
MTACS	Marine tactical air command squadron	SIPRNET	SECRET Internet Protocol Router Network
MWCS	Marine wing communications squadron	SJA	staff judge advocate
MWSG	Marine wing support group	SL	switch locator
MWSS	Marine wing support squadron	STE	secure terminal equipment
NATO	North Atlantic Treaty Organization	STU	secure telephone unit
NIPRNET	Non-Secure Internet Protocol Router Network	SUPV	supervisor
OOD	officer of the deck	SWBD	switchboard
OPS	operations	SWO	senior watch officer
OPSO	operations officer	SYSCON	systems control
P	priority	TACC	tactical air command center (USMC)
PAO	public affairs officer	TASS	tactical automated switch system
POTS	plain old telephone service	TBMCS	sys admin theater battle management core system administrator
PR	primary region	TCO	tactical combat operations
PRSL	primary region switch locator	TECHCON	technical control
PSTN	public switched telephone network	TRC	tactical combat operations
R	routine	TSB	transportation support battalion
RAD BN	radio battalion	TSC	nomenclature for a satellite communications central
S-1	battalion or regiment manpower staff officer	TTC	nomenclature for an automatic telephone central office
S-2	battalion or regiment intelligence staff officer	USMC	United States Marine Corps
S-3	battalion or regiment operations staff officer	WAN	wide-area network
S-4	battalion of regiment logistics staff officer	WXO	weather officer
S-6	battalion or regiment communications system staff officer	XO	executive officer
SAC	senior air coordinator		

APPENDIX H

EXAMPLE OF A GUARD CHART

UNCLASSIFIED

Copy no. ____ of ____ copies
 I MEF
 GREENTOWN, BLUELAND
 10 March 2008
 AIG

TAB A TO APPENDIX 5 TO ANNEX K TO OPERATION ORDER 0000-00
(OPERATION DESERT PROMISE)
 PHASE I RADIO GUARD CHART (U)

Table H-1. Sample Guard Chart.

LEGEND																								
C-NET CONTROL																								
X-GUARD																								
M-MONITOR																								
A-AS REQUIRED																								
W-WHEN DIRECTED																								
D-DATA																								
S-SATCOM																								
FH-FREQUENCY HOP																								
UHF-HIGH FREQUENCY																								
UH-ULTRA HIGH																								
FREQUENCY																								
MI-MICROWAVE (UHF/SHF)																								
TR-TROPO (SHF)																								
SHF-SATELLITE (SHF)																								
EHF-EXTREMELY HF																								
	CJTF CMD	CJTF TAC	CJTF AIR REQUEST	MEF CMD 1	MEF INTEL 1	MEF GRND RECON 1	MEF TAC 1	MEF CMD 2	MEF TAC 2	MEF INTEL 2	MEF FFC (P)	MEF FFC (S)	MEF CSS (P)	MEF CSS (S)	MEF COMM COORD (P)	MEF COMM COORD (S)	MEF GRND RECON 2 (ALE)	TARIHR	CASEVAC	MEF CONVOY CONTROL 1	MEF CONVOY CONTROL 2	MEF CONVOY CONTROL 2	RETRANS 1	RETRANS 2
BAND	U H	U H	U H	U H	U H	U H	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F	H F
DEVICE	S	S	S	S	S	S/D																		
FREQ HOP NET ID																					1 0 1	1 0 2	1 0 3	
EMISSION	25K9F1E	25K9F1E	25K9F1E	25K9F1E	25K9F1E	25K0G7M	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	3K00J3E	25K0F2E	25K0F2E	25K0F2E	
RESTORATION PRIORITY	IA	2 B	3 B	2 A	8 A	3 C	5 A	4 B	2 C	5 B	9 A	1 C	1 B	1 D	3 A	2 D	6 B	7 A	6 A	6 B	4 C	4 D	4 E	

K-5-A-UNCLASSIFIED

Table H-2. Sample Guard Chart.

LEGEND											
C-NET CONTROL X-GUARD M-MONITOR A-AS REQUIRED W-WHEN DIRECTED D-DATA S-SATCOM FH-FREQUENCY HOPPING UHF-HIGH FREQUENCY UH-ULTRA HIGH FREQUENCY MI-MICROWAVE (UHF/SHF) TR-TROPO (SHF) SHF-SATELLITE (SHF) EHF-Extremely HF	4096K	4096K	1152K	1152K	1152K	1024K	4608K	4608K	4608K	4608K	576K
	STZ01 LANDSTUHL/MEF	STL01 BAHRAIN/MAW	SZL01 MEF/MAW (UAE)	SZL02 MEF/MAW (JASK)	SLP01 MAW (UAE) / DIV	GZP01 MEF/DIV	TZL01 MEF/MAW (UAE)	TZL02 MEF/MAW (JASK)	TZF01 MEF/MLG	TLF01 MAW (JASK) / MLG	MBP01 USS BLUE RIDGE / DIV
BAND	SHF	SHF	SHF	SHF	SHF	EHF	TR	TR	TR	TR	MI
EMISSION	12K5G1D	12K5G1D	10M0F9W	10M0F9W	10M0F9W	1G00F7W	7M00M7D	7M00M7D	7M00M7D	7M00M7D	610KF7W
CRYPTO EQUIPMENT	KIV-19	KIV-19	KIV-19	KIV-19	KIV-19	KIV-19	KIV-19	KIV-19	KIV-19	KIV-19	KG-194A
RESTORATION PRIORITY	1A	2A	4A	5A	6A	7A	1B	2B	3B	4B	3A
UNITS											
LANDSTUHL	C										
BAHRAIN		C									
USS BLUE RIDGE											C
MEF CE	X		C	C		C	C	C	C		
MAW CE		X	X	X	C		X	X		C	
DIV CE					X	X					X
MLG CE									X	X	

I.B. GENERAL
Lieutenant General, USMC
Commanding General

OFFICIAL:
s/
B.A. Colonel
Colonel, USMC
AC/S G-6

GLOSSARY

SECTION I. ACRONYMS AND ABBREVIATIONS

AAW	antiair warfare	COCOM	combatant command (command authority)
ABCS	Army Battle Command System	COG	center of gravity
ACE	aviation combat element	COMM BN	communications battalion
ADCON	administrative control	COMMCON	communications control
AEHF	Advanced Extremely High Frequency	COMPUSEC	computer security
AFSATCOM	Air Force satellite communications	COMSEC	communications security
AMC	air mission commander	CONOPS	concept of operations
AO	area of operations	CONUS	continental United States
AOC	air operations center	COTS	commercial off-the-shelf
AOR	area of responsibility	CS	content staging
ASC(A)	assault support coordinator (airborne)	C/S	chief of staff
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)	CSN	circuit switch network
ATC	air traffic control	CSS	combat service support
C2	command and control	DASC	direct air support center
C2PC	command and control personal computer	DCN	data link coordination net
CATF	commander, amphibious task force	DCTS	Defense Collaboration Tool Suite
CCC	communications control center	DISA	Defense Information Systems Agency
CCDR	combatant commander	DISN	Defense Information Systems Network
CCIR	commander's critical information requirement	DMS	defense message system
CCSD	command communications service designator	DOD	Department of Defense
CE	command element	DODD	DOD directive
CEOI	communications-electronics operating instructions	DRSN	Defense Red Switched Network
CI/D	combat information/detection	DSCS	Defense Satellite Communications System
CIO	chief information officer	DSID	deployed security interdiction device
CJCS	Chairman of the Joint Chiefs of Staff	DSN	Defense Switched Network
CJCSM	Chairman of the Joint Chiefs of Staff manual	EEFI	essential elements of friendly information
CLB	combat logistics battalion	EHF	extremely high frequency
CLF	commander, landing force	EKMS	Electronic Key Management System
CLR	combat logistics regiment	e-mail	electronic mail
CND	computer network defense	EMCON	emission control
COA	course of action	ESG	expeditionary strike group
COC	combat operations center	EW	electronic warfare
			EW/C	early warning/control
			FAC(A)	forward air controller (airborne)
			FAD	fighter air direction

FDC.....	fire direction center	JCCC.....	joint communications control center
FFCC.....	force fires coordination center	JCSE....	joint communications support element
FFIR.....	friendly force information requirement	JDN.....	joint data network
FLTSATCOM....	fleet satellite communications	JFC.....	joint force commander
FRAGO.....	fragmentary order	JIC.....	joint intelligence center
FSCC.....	fire support coordination center	JP.....	joint publication
G-1.....	component manpower and personnel staff officer, brigade or higher staff	JTF.....	joint task force
G-2.....	component intelligence staff officer, brigade or higher staff	JTF-GNO.....	Joint Task Force-Global Network Operations
G-3.....	component operations staff officer, brigade or higher staff	JWICS.....	Joint Worldwide Intelligence Communications System
G-4.....	component logistics staff officer, brigade or higher staff	kW.....	kilowatt
G-5.....	plans officer	LAAD.....	low altitude air defense
G-6.....	component command, control, communications, and computer systems staff officer	LAN.....	local area network
GBNP.....	global block numbering plan	LCE.....	logistics combat element
GBS.....	Global Broadcast System	LFOC.....	landing force operations center
GCCS.....	Global Command and Control System	LOC.....	logistics operations center
GCE.....	ground combat element	LOS.....	line of sight
GHz.....	gigahertz	LPD.....	low probability of detection
GIG.....	Global Information Grid	LPI.....	low probability of intercept
GMF.....	ground mobile force	LTC.....	LAAD team control
H&S.....	headquarters and service	LZCT.....	landing zone control team
HD.....	helicopter direction	MACCS.....	Marine air command and control system
HDC.....	helicopter direction center	MACG.....	Marine air control group
HF.....	high frequency	MAG.....	Marine aircraft group
HQ.....	headquarters	MAGTF.....	Marine air-ground task force
HQMC.....	Headquarters, Marine Corps	MARFOR.....	Marine Corps forces
HR.....	helicopter request	MARFORCOM.....	United States Marine Corps Forces Command
IA.....	information assurance	MARFORPAC.....	United States Marine Corps Forces, Pacific
INFOCON.....	information operations condition	MARFORRES.....	United States Marine Corps Forces Reserve
INFOSEC.....	information security	MARSOC.....	United States Marine Corps Forces, Special Operations Command
INMARSAT....	international maritime satellite	MATCD.....	Marine air traffic control detachment
IP.....	Internet protocol	MAW.....	Marine aircraft wing
IPS.....	Interim Polar System	Mbps.....	megabytes per second
ISD.....	information systems directory	MC.....	multichannel
ISDN.....	integrated services digital network	MCCC.....	Marine Corps Command Center
J-6.....	communications system officer of a joint staff	MCDP.....	Marine Corps doctrinal publication
JC2.....	joint command and control	MCNOSC.....	Marine Corps Network Operations and Security Command
		MCR.....	multichannel radio
		MCS.....	MAGTF communications system

MCTSSA	Marine Corps Tactical Systems Support Activity	RF	radio frequency
MCWP	Marine Corps warfighting publication	RIP	relief in place
MEB	Marine expeditionary brigade	S-2	battalion or regiment intelligence staff officer
MEDEVAC	medical evacuation	S-3	battalion or regiment operations staff officer
MEF	Marine expeditionary force	S-6	communications officer
MEF (Fwd)	Marine expeditionary force (Forward)	SACC	supporting arms coordination center
MEU	Marine expeditionary unit	SAM	surface-to-air missile
MHz	megahertz	SAR	search and rescue
Milstar	military strategic and tactical relay	SARC	surveillance and reconnaissance center
MISSI	Multilevel Information Systems Security Initiative	SATCOM	satellite communications
MLC	Marine logistics command	SBB	switched backbone
MLG	Marine logistics group	SCI	sensitive compartmented information
MNL	Master Net List	SCR	single-channel radio
MSC	major subordinate command	SHF	super high frequency
MSOB	Marine special operations battalion	SINCGARS	single-channel ground and airborne radio system
MUOS	Mobile User Objective System	SIPRNET SECRET	Internet Protocol Router Network
Mux	multiplexer	SLD	system link designator
MWCS	Marine wing communications squadron	SOP	standing operating procedure
NATO	North Atlantic Treaty Organization	SPE	systems planning and engineering
NCS	National Communications System	SPMAGTF	special purpose MAGTF
NETOPS	network operations	STEP	standardized tactical entry point
NGF	naval gunfire	SYSCON	systems control
NIPRNET	Non-Secure Internet Protocol Router Network	Tac	tactical
NOC	network operations center	TAC(A)	tactical air coordinator (airborne)
OCAC	operations control and analysis center	TACC	tactical air command center (Marine TACC); tactical air control center (Navy)
OODA	observe, orient, decide, act	TACLOG	tactical-logistical group
OPCON	operational control	TACP	tactical air control party
OPLAN	operation plan	TACSAT	tactical satellite
OPORD	operation order	TAD	tactical air direction
OPSEC	operations security	TADC	tactical air direction center
ORM	operational risk management	TADIL	tactical digital information link
OSCC	operational systems control center	TAOC	tactical air operations center
OTM	on the move	TAR	tactical air request
PIR	priority intelligence requirement	TATC	tactical air traffic control
POC	point of contact	TBMCS	theater battle management core system
PRSL	primary region switch locator	TECHCON	technical control
PSN	packet switch network	TJTN	theater joint tactical network
		TNAPS	tactical network analysis and planning system

T/O table of organization
TRANSEC transmission security
TRC.....transcoder
TSN..... track supervision net

UAV unmanned aerial vehicle
UFO ultrahigh frequency follow-on
UHF ultrahigh frequency
US United States
USA United States Army
USAF United States Air Force
USN United States Navy
USSOCOM..... United States Special
Operations Command

USSTRATCOM United States
Strategic Command
VHF very high frequency
VPN voice product net
VTC video teleconferencing

WAN..... wide-area network
WGS Wideband Global
Satellite Communications

xCCC major subordinate command
communications control center
XO.....executive officer

SECTION II. DEFINITIONS

application—1. A system or problem to which a computer is applied. Reference is often made to an application as being either of the computational type (arithmetic computations predominate) or of the data processing type (data handling operations predominate). 2. In the intelligence context, the direct extraction and tailoring of information from an existing foundation of intelligence and near real time reporting. It is focused on and meets specific, narrow requirements, normally on demand. (JP 1-02)

architecture—A framework or structure that portrays relationships among all the elements of the subject force, system, or activity. (JP 1-02)

asynchronous—Pertaining to an operation that occurs without a regular or predictable time relationship to a specified event.

asynchronous transfer mode—A method of digitized data transmission based on fixed-length cells. Asynchronous transfer mode can carry multiple types of data—text, voice, imagery, and video—at high speeds. Also called **ATM**.

back lobe—Pertaining to a directional antenna, the radiation occurring in a direction 180 degrees from that of the main axis of radiation.

backbone—The high traffic density connectivity portion of any communications network.

bandwidth—The difference between the limiting frequencies of a continuous frequency band expressed in hertz (cycles per second). The term bandwidth is also loosely used to refer to the rate at which data can be transmitted over a given communications circuit. In the latter usage, bandwidth is usually expressed in either kilobits per second or megabits per second. (JP 1-02)

bomb—A computer program, generally malicious in nature, hidden within or emulating another program and designed to execute at a specific future time or on the occurrence of a specific event.

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combatant command (command authority)—Nontransferable command authority established by title 10 (“Armed Forces”), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called **COCOM**. (JP 1-02)

combat information—Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 1-02)

command—1. The authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel. 2. An order given by a commander; that is, the will of the commander expressed for the purpose of bringing about a particular action. 3. A unit or units, an organization, or an area under the command of one individual. Also called **CMD**. (JP 1-02)

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called **C2**. (JP 1-02)

command and control system—The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned. (JP 1-02)

commonality—A quality that applies to materiel or systems: a. possessing like and interchangeable characteristics enabling each to be utilized, or operated and maintained, by personnel trained on

the others without additional specialized training; b. having interchangeable repair parts and/or components; and c. applying to consumable items interchangeably equivalent without adjustment. (JP 1-02)

common operational picture—A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called **COP**. (JP 1-02)

communicate—To use any means or method to convey information of any kind from one person or place to another. (JP 1-02)

communications security—The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC**. (JP 1-02)

communications system—Communications networks and information services that enable joint and multinational warfighting capabilities. (JP 1-02)

computer network defense—Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called **CND**. (JP 1-02)

computer security—The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called **COMPUSEC**. (JP 1-02)

control—Authority that may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (JP 1-02, part 1 of a 4-part definition)

cryptosecurity—The component of communications security that results from the provision of technically sound cryptosystems and their proper use.

Defense Information Systems Network—Integrated network, centrally managed and configured to provide long-haul information transfer services for all Department of Defense activities. It is an information transfer utility designed to provide dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services. Also called **DISN**. (JP 1-02)

Defense Switched Network—Component of the Defense Communications System that handles Department of Defense voice, data, and video communications. Also called **DSN**. (JP 1-02)

digital backbone—A term loosely applied to the Tri-Service Tactical Communications Program-based circuit switched communications network employed by the Marine Corps. Used synonymously with switched backbone.

digital switch—A switch that performs time-division multiplexed switching of digitized signals. When used with analog inputs analog-to-digital and digital-to-analog conversions are necessary.

digital transmission—The transmission of a digital bit stream that may include digitized voice, data, or both. The transmission signal itself may be either discrete or continuous (analog).

electromagnetic spectrum management—Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (JP 1-02.)

emission security—The component of communications security that results from all measures

taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems.

forward lobe—Pertaining to a directional antenna, the radiation occurring along the main axis of radiation.

frequency management—The requesting, recording, deconfliction of and issuance of authorization to use frequencies (operate electromagnetic spectrum-dependent systems) coupled with monitoring and interference resolution processes.

full duplex—Refers to a mode of transmission in which communication between two terminals takes place in both directions simultaneously.

gateway—In a communications network, a network node that is equipped for interfacing with another network that uses different protocols. The term is loosely applied to a computer or computer software configured to perform the tasks of a gateway.

Global Combat Support System—A strategy that provides information interoperability across combat support functions and between combat support and command and control functions through the Global Command and Control System. Also called **GCSS**. (JP 1-02)

Global Command and Control System—A deployable command and control system supporting forces for joint and multinational operations across the range of military operations with compatible, interoperable, and integrated communications systems. Also called **GCCS**. (JP 1-02.)

half-duplex—Refers to a mode of transmission in which communication between two terminals occurs in either direction, but in only one direction at a time. This is the typical mode of operation for tactical single-channel radios.

host—In a computer network, a computer that provides services to end users. Those services are considered to be hosted on that computer. The term host also refers to the computer on a network that performs network control functions.

information assurance—Measures 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** (JP 1-02)

information environment—The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 1-02)

information operations—The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called **IO**. (JP 1-02)

information superiority—The operational advantage derives from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also **information operations**. (JP 1-02)

information system—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. (JP 1-02)

in-line network encryptor—A cryptographic device that permits the transmission of classified

data on unclassified networks or sensitive compartmented information data on secret networks. A key feature of in-line network encryptors is that they only encrypt the data, not the address information. In-line network encryptors, through software configuration and appropriate keying material, may be used to link multiple local area networks of one classification level by using a data communications network operating at a lower classification level.

Integrated Digital Network Exchange—Devices that provide automated link bandwidth management that allocates available circuits as needed. These devices are used at network nodes to allow for a virtual network with automatic routing and rerouting. Integrated Digital Network Exchange devices are easily upgraded to asynchronous transfer mode capability. Also called **IDNX**.

Internet—The worldwide interconnection of individual computer networks operated by government, industry, academia, and private parties. The Internet was originally developed by the Defense Advanced Research Projects Agency to interconnect laboratories and academic institutions engaged in government-sponsored research.

Internet protocol—A DOD standard protocol designed for use in interconnected systems (Internets) of packet-switched communications networks. The Internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are identified by fixed length addresses (Internet protocol addresses). Also called **IP**.

Internet protocol address—A unique numerical address assigned to each host on an Internet protocol network based on a standard scheme and by a central agency. Used to communicate between hosts on the network.

interoperability—1. The ability to operate in synergy in the execution of assigned tasks. 2. The condition achieved among communications electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02)

joint network operations control center—An element of the J-6 established to support a joint force commander. The joint network operations control center serves as the single control agency for the management and direction of the joint force communications systems. The joint network operations control center may include plans and operations, administration, system control, and frequency management sections. Also called **JNCC**. (JP 1-02)

joint restricted frequency list—A time and geographically-oriented listing of TABOO, PROTECTED, and GUARDED functions, nets, and frequencies. It should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives. Also called **JRFL**. (JP 1-02)

loop—A communication channel from a switching center or an individual message distribution point to the user terminal. In a telephone system, a pair of wires running from a central office to a subscriber's telephone.

MAGTF command and control—An integrating process that provides governance over the command and control community to ensure all objectives are met. It is a strategy to harmonize all aspects of command and control concepts, requirements, training, and doctrine. Also called **MAGTF C2**.

modem—In computer communications, a device used for converting digital signals into, and recovering them from, quasi-analog signals that

are suitable for transmission over analog communications channels.

modulation—The process of varying a characteristic (e.g., frequency, phase, amplitude) of a carrier signal in accordance with an information bearing signal.

multichannel—Pertaining to communications, usually full duplex, on more than one channel simultaneously. Multichannel transmission may be accomplished by time-, frequency-, code-, and phase-division multiplexing, or space diversity. (JP 1-02)

multiplexer—A device that combines (multiplexes) multiple input signals (information channels) into an aggregate signal (common channel) for transmission. (JP 1-02)

National Communications System—The telecommunications system that results from the technical and operational integration of the separate telecommunications systems of the several executive branch departments and agencies having a significant telecommunications capability. Also called **NCS**. (JP 1-02)

National Military Command System—The priority component of the Global Command and Control System designed to support the President, Secretary of Defense, and Joint Chiefs of Staff in the exercise of their responsibilities. Also called **NMCS**. (JP 1-02)

network operations—Activities conducted to operate and defend the Global Information Grid. Also called **NETOPS**. (JP 1-02)

node—1. A location in a mobility system where a movement requirement is originated, processed for onward movement, or terminated. 2. In communications and computer systems, the physical location that provides terminating, switching, and gateway access services to support information exchange. (JP 1-02, parts 1 and 2 of a 3-part definition)

nongovernmental organization—A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging establishment of democratic institutions and civil society. Also called **NGO**. (JP 1-02)

packet switch—A switch that breaks messages into data packets for transmission over a network and reassembles data packets into messages upon receipt.

physical security—2. In communications security, the component that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02, part 2 of a 2-part definition)

protocol—A formal set of specifications governing the format and control of interaction among terminals communicating over a network.

router—A device used to interconnect two or more data communication networks. The router reads the network address of all data packets and forwards to the addressee via the best available communications path.

SECRET Internet Protocol Router Network—The worldwide SECRET-level packet switch network that uses high-speed Internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called **SIPRNET**. (JP 1-02)

Service component command—A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under that command, including the support forces that have been assigned to a combatant command or further assigned to a subordinate unified command or joint task force. (JP 1-02)

standardization—The process by which the Department of Defense achieves the closest practicable cooperation among the Services and Department of Defense agencies for the most efficient use of research, development, and production resources, and agrees to adopt on the broadest possible basis the use of: a. common or compatible operational, administrative, and logistic procedures; b. common or compatible technical procedures and criteria; c. common, compatible, or interchangeable supplies, components, weapons, or equipment; and, d. common or compatible tactical doctrine with corresponding organizational compatibility. (JP 1-02)

synchronous—Pertaining to an operation that occurs with a regular or predictable time relationship to a specified event.

telecommunication—Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. (JP 1-02)

timing—The synchronization of communications signals. Of critical importance for digital communications networks and for secure communications.

transmission security—The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. (JP 1-02)

transponder—1. A receiver-transmitter which will generate a reply signal upon proper interrogation. (JP 1-02) 2. An automatic device that receives, amplifies, and retransmits a signal on a different frequency. 3. An automatic device that transmits a predetermined message in response to a predefined received signal. 4. Device in a communications satellite that receives a signal from a sending earth station and retransmits the signal to one or more receiving earth stations.

Trojan horse—A computer program containing an apparently or actually useful function that also contains hidden functions that allow unauthorized collection, falsification, or destruction of data.

trunk—A trunk is a single circuit between two switching centers or individual message distribution points. This is in contrast to a loop, which is a single circuit between the switching center or message distribution point and the individual subscriber terminal. A trunk group is formed by two or more trunks between the same two points.

virus—A self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

wide-area network—A term loosely applied to any communications network extending over a large geographic area.

worm—An independent computer program designed to self-replicate from computer to computer across computer networks often clogging networks and monopolizing computer system resources as it spreads.

REFERENCES

Department of Defense Publications

DOD Directives (DODDs)

- 5105.19 Defense Information Systems Agency (DISA)
- 8500.1E Information Assurance (IA)

DOD Instruction (DODI)

- 8500.2 Information Assurance (IA) Implementation

Joint Publications

Joint Publications (JPs)

- 1 Doctrine for the Armed Forces of the United States
- 1-02 Department of Defense Dictionary of Military and Associated Terms
- 6-0 Joint Communications System

Chairman of the Joint Chiefs of Staff Manuals (CJCSMs)

- 6231.01C Manual for Employing Joint Tactical Communications – Joint Systems Management
- 6231.02B Manual for Employing Joint Tactical Communications – Joint Voice Communications Systems
- 6231.03B Manual for Employing Joint Tactical Communications – Joint Data Systems
- 6231.04B Manual for Employing Joint Tactical Communications – Joint Transmission Systems
- 6231.05B Manual for Employing Joint Tactical Communications – Joint Communications Security
- 6231.06A Manual for Employing Joint Tactical Communications – Joint Technical Control Procedures and Systems
- 6231.07D Manual for Employing Joint Tactical Communications – Joint Network Management and Control

Chairman of the Joint Chiefs of Staff Instruction (CJCSI)

- 6211.02B Defense Information Systems Network (DISN): Policy, Responsibilities, and Processes

Marine Corps Publications

Marine Corps Doctrinal Publication (MCDP)

- 6 Command and Control

Marine Corps Warfighting Publications (MCWPs)

- 3-40.1 Marine Air-Ground Task Force Command and Control
- 3-40.8 Componency

Navy Publications

Naval Doctrine Publication (NDP)

6 Naval Command and Control

Secretary of the Navy Instruction (SECNAVINST)

5510.30B Department of the Navy Personnel Security Program

Miscellaneous Publications

A Cooperative Strategy for 21st Century Seapower, US Navy, US Marine Corps, US Coast Guard. October, 2007.

Clinger-Cohen Act, United States Code, Title 40, sec. 5142 (1996).

Coram, Robert. 2002. *Boyd: The Fighter Pilot Who Changed the Art of War*. New York: Little, Brown and Company.

Defense Information Systems Agency (DISA) Contingency Plan 10-95.

JCSE C4I Planning Guide. Joint Communications Support Element. March, 2005.

Joint Integrating Concept. *Command and Control*. September, 2005.

Joint Integrating Concept. *Net-Centric Operational Environment*. October, 2005.

Joint Functional Concept. *FORCEnet: A Functional Concept for the 21st Century*. February, 2005.

Marine Corps Strategy 21

Marine Requirements Oversight Council Decision Memoranda 29-2005.

Marine Requirements Oversight Council Decision Memoranda 39-2004.

Secretary of Defense. FY2006. Forces for United Commands Memorandum.

Secretary of the Navy. M-5510.30 Department of the Navy Personnel Security Program.

United States Department of Defense. Office of Force Transformation. *Network Centric Operations Conceptual Framework*, Version 1. 2003.

United States Department of Defense. *2006 Quadrennial Defense Review Report*. Downloaded from www.defenselink.mil/qdr/.