MCIP 3-40.02

Marine Corps Cyberspace Operations

US Marine Corps

DISTRIBUTION STATEMENT B: Distribution authorized to US Government agencies only; for official use only

PCN 146 000020 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 on-line Marine Corps Publications Electronic Library:

http://www.marines.mil/News/Publications/ELECTRONICLIBRARY.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: If this publication is not an electronic only distribution, a printed copy 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 United States Marine Corps Doctrine web 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, D.C. 20350-3000

6 October 2014

FOREWORD

Marine Corps Interim Publication (MCIP) 3-40.02, *Marine Corps Cyberspace Operations*, elaborates on Marine Corps-specific information and procedures addressed in Joint Publication 3-12, *Cyberspace Operations*, dated 5 February 2013 (SECRET). Providing an introduction to cyberspace, MCIP 3-40.02 discusses how the Marine Corps is currently organized to conduct cyberspace operations, planning considerations, and emerging changes that will affect our cyberspace operations capability and capacity.

The Marine Corps depends on cyberspace to enable the successful execution of warfighting functions across the range of military operations and in the fulfillment of business practices. In order to maintain freedom of action within cyberspace, the Marine Corps must develop and maintain robust capabilities to operate and defend the Marine Corps information enterprise. Additionally, the Marine Corps requires the capability to utilize cyberspace operations in concert with other lines of operation to identify, understand, disrupt, attack, and defeat a wide range of adversaries.

This interim publication is a first effort to indoctrinate the force on cyberspace operations. The target audience is Marine air-ground task force commanders, their staffs, and other personnel involved in cyberspace operations. As that audience gains experience incorporating cyberspace into operational design and execution, doctrine will be further refined and developed.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

K. J. GLUECK, JR.
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

PUBLICATION CONTROL NUMBER: 146 000020 00

This Page Intentionally Left Blank

TABLE OF CONTENTS

Chapter 1. Overview

Chapter 2. Organization

Chapter 3. Planning

CHAPTER 1
OVERVIEW

Nearly every aspect of modern life depends on information technology to some extent. Not many decades ago, computers were highly specialized advanced technology devices that were very expensive, difficult to operate, and largely unfamiliar to the general public. However, in recent years, computer processors have simultaneously become smaller, cheaper, more energy efficient, and much more powerful. Likewise, telecommunications infrastructure was largely oriented on transporting voice communication via wires and cables. Today, telecommunications technology can transmit vast amounts of data among multiple global locations at nearly the speed of light. Likewise, secondary storage devices, such as hard disks and solid state drives, have become more capable and more affordable. Software applications have also become more powerful and more user-friendly.

While information technology continues to play a large role in the activities of governments, infrastructure providers, industry, and academia, it has also proliferated among consumers around the world in the form of products and services. Key products and services include personal computers, tablets, smartphones, embedded processors in automobiles and appliances, wired and wireless broadband, Internet-based services, and the software that enables all of them.

This same technology influences core functions within the Marine Corps and the joint force:

- Enables the personnel center to more promptly and accurately execute administrative actions.
- Enhances the intelligence section's capabilities within the intelligence cycle. Such capabilities are used to inform commanders' decisionmaking processes.
- Provides the operations staff with tools to conduct planning to effectively integrate the actions of all elements of the Marine air-ground task force (MAGTF) and/or joint task force.
- Enhances logisticians' ability to track the status of supplies at remote outposts and to develop and execute plans to resupply them in an efficient manner.
- Provides commanders with text-based, voice, and video communication tools to facilitate the exercise of command and control.

Just as the financial, communications, transportation, utilities, and other sectors have become dependent on the availability of information technology services, so have many core functions performed by elements of the Marine Corps, such as headquarters, supporting establishment, and operating forces. However, along with the benefits of information technology come vulnerabilities. Marine Corps systems are at risk to adversary attempts to deny, disrupt, degrade, exploit, or destroy these systems or the data therein via lethal/nonlethal means. Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations*, states:

> *The Marine Corps derives its agility from its expeditionary mindset, flexible structure, and . . . Marines can adapt quickly across an extraordinary range of military operations with the organizational design and training to transition seamlessly between these operations, providing the necessary capability to operate effectively.*

Marines have long excelled in the domains of air, land, and sea. Now, and into the foreseeable future, Marines will increasingly be called upon to excel at operating in cyberspace.

Fundamentals of Cyberspace

Cyberspace is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations are the employment of cyberspace capabilities to achieve objectives in or through cyberspace. Cyberspace can be viewed as consisting of three layers: physical network, logical network, and cyber-persona. See figure 1-1. Targeting in cyberspace operations presents a challenge to identify, coordinate, and deconflict activities occurring across those layers.

Physical Network Layer

The physical network layer is the medium in which the data travels. It includes wired (e.g., land and undersea cable) and wireless (e.g., radio, radio-relay, cellular, satellite) transmission means. It is the first point of reference for determining jurisdiction and application of authorities. It is also the primary layer for geospatial intelligence, which can also contribute data useful for targeting in cyberspace.

Logical Network Layer

The logical network layer constitutes an abstraction of the physical network layer, depicting how nodes in the physical dimension of the information environment logically relate to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical dimension of the information environment is lost.

Cyber-Persona Layer

The cyber-persona layer is the digital representation of individual or group online identities. It holds important implications for Marine forces in terms of positive target identification and affiliation and activity attribution. Cyber-personas can be complex, with elements in many virtual locations, and not necessarily linked to a single physical location or form; therefore, Marines require significant intelligence collection and analysis capabilities to gain sufficient insight and situational awareness of a cyber-persona to enable effective targeting and generation of the Marine commander's desired effects.

Fundamentals of Cyberspace Operations

The fundamentals of cyberspace operations consist of understanding the various threats in cyberspace and their impact across its three lines of operation (LOOs) within the context of the Marine Corps.

Lines of Operation

The three LOOs within cyberspace are Department of Defense information networks (DODIN) operations, defensive cyberspace operations (DCO), and offensive cyberspace operations (OCO).

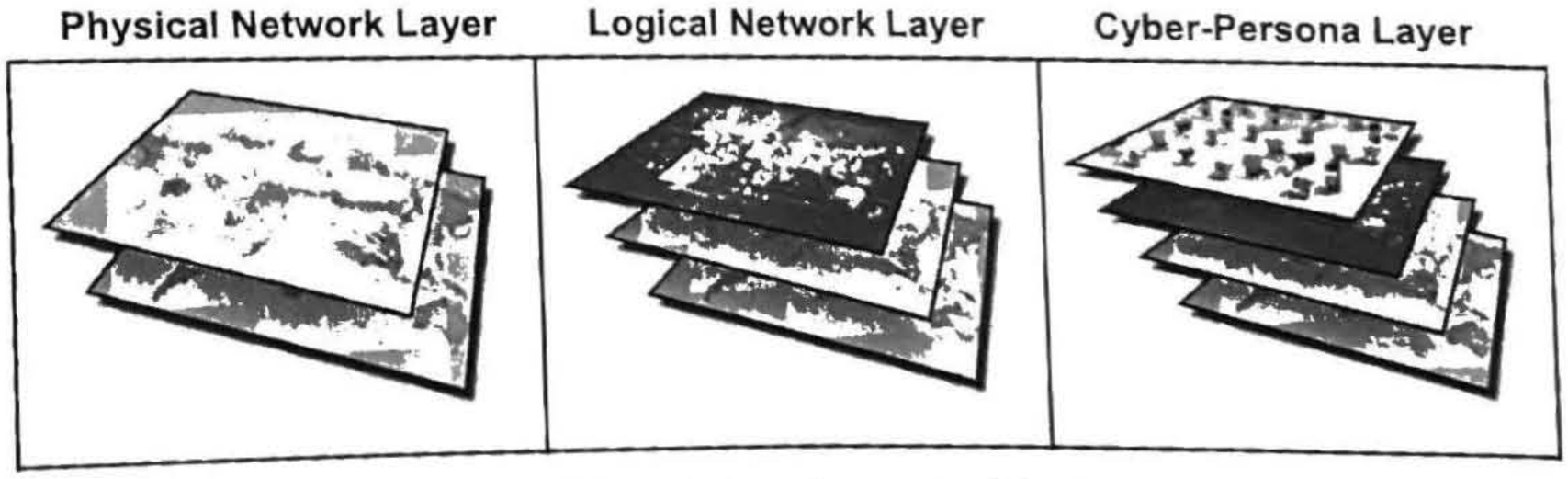

Figure 1-1. The Three Layers of Cyberspace.

The DODIN operations are actions taken to design, build, configure, secure, operate, maintain, and sustain Department of Defense (DOD) communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and nonrepudiation. Defensive cyberspace operations can be passive and active and are intended to preserve the ability to use friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Offensive cyberspace operations are intended to project power by the application of force in or through cyberspace.

Threats and Actors in Cyberspace

Actors

A growing range of state or nonstate actors may develop or acquire the capability to conduct both physical and virtual attacks against information technology infrastructure. Unlike actors in the physical domains, actors in cyberspace can acquire significant capabilities in a short amount of time with a small amount of capital. Acquisition of an OCO capability by state or nonstate actors in order to conduct operations against friendly critical infrastructure could represent a significant threat to information dependencies and communication flows of friendly forces.

Foreign Nations

A growing array of nation-states is targeting information infrastructures for reconnaissance, surveillance, exploitation, and potential disruption or destruction. Such infrastructures include the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Criminal Groups

Cyberspace intrusions by criminal groups who attack information systems for monetary and informational gain are increasing. Criminals' toolkits are evolving rapidly to use new technologies that increase the sophistication of attacks. Often, such groups may offer their toolkits and software robot networks, also known as botnets (networks of infected computers of unwitting victims that perform automated tasks to achieve the goals of the cyber criminals), for rent to the highest bidder, thereby increasing the threat capacity of less advanced actors.

Hackers

Hackers may infiltrate networks for the thrill of the challenge or for bragging rights in the hacker community. Whereas remote hacking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and toolkits from the Internet and launch them against victim sites. Thus, attack tools have become simultaneously more sophisticated and easier to use.

Hacktivism

Hacktivism refers to politically motivated attacks on publicly available assets. Groups and individuals may overload e-mail or Web servers through denial-of-service attacks or may hack into Web sites to send a political message.

Insiders

Insiders have been perpetrators of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because they often have enough access to systems to cause damage or steal data. The insider threat may include military, DOD civilian, and contractor personnel.

Terrorists

Terrorists may seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security; cause mass casualties; weaken the economy; and damage public morale and confidence. However, terrorist adversaries of the United States have typically been less developed in their computer network capabilities than state adversaries have been. Terrorists may now focus on traditional attack methods, but growing cyberspace

threats should be anticipated as a more technically competent generation enters the ranks.

Targets

Every target has distinct intrinsic or acquired characteristics. These characteristics form the basis for target detection, location, identification, target value within the adversary target system, and classification for future surveillance, analysis, strike, and assessment. While this is true from an offensive point of view, Marine planners and cyberspace operations personnel must recognize those potential adversaries will view *friendly* assets in cyberspace similarly—as potential targets. Therefore, the same types of defensive principles Marines employ in the physical domains, such as active security and defense in depth, must be employed in cyberspace. Additional information on cyberspace targets, at the SECRET level, can be found in Joint Publication (JP) 3-12, *Cyberspace Operations*; JP 3-60, *Joint Targeting*; and *Department of Defense Strategy for Operating in Cyberspace*.

Marine Corps Perspective

The Marine Corps must be prepared, through organic and nonorganic means, to operate and defend information technology resources and generate effects in cyberspace in support of assigned missions. Commanders at all levels must be aware of the opportunities and threats inherent in depending on cyberspace, both for friendly and adversary operations in cyberspace. Freedom of action in cyberspace facilitates freedom of action in the physical domains of air, sea, land, and space. Similarly, an inability to freely act in cyberspace would severely limit Marine forces' ability to operate in the operational environment. For example, imagine the level of difficulty involved in commanding, controlling, and supporting a widely dispersed MAGTF without the benefit of computers, telephones, and data networks. Conversely, imagine the opportunities afforded the MAGTF commander when a technologically advanced adversary is denied access to critical information technology-dependent systems.

It is not envisioned that every Marine in the MAGTF will be capable of conducting full spectrum cyberspace operations (DODIN operations, DCO, and OCO). However, Marines at every level must recognize that the information technology systems on which they depend are potential points of entry for adversaries. Cyberspace affords adversaries the potential to achieve an asymmetric advantage; hence, dependence on cyberspace is deemed a weakness that adversaries seek to take advantage of for relatively little cost and at minimal physical risk.

As the Marine Corps' involvement in cyberspace operations increases and as new operational imperatives exceed the scope of Service and joint doctrine, feedback will be crucial to ensure that doctrine is updated and operational knowledge diffused.

National/Joint Concepts and Policy

There are national and joint concepts and policies that outline strategic initiatives, national interests, priorities, and challenges regarding the role of the nation, DOD, and joint forces in cyberspace. It is imperative that the Marine Corps and its leaders understand their roles in cyberspace operations in the broader context of national and joint concepts and policies.

Presidential Policy Directive 20

The Presidential Policy Directive 20, *U.S. Cyber Operations Policy*, issued in October 2012, addresses cyberspace operations of the military and federal agencies. The directive establishes a strict set of guidelines for dealing with cyberspace threats and makes a distinction between offensive and defensive cyberspace operations.

Department of Defense Strategy for Operating in Cyberspace

The *Department of Defense Strategy for Operating in Cyberspace*, issued in July 2011, establishes strategic initiatives that provide a roadmap for the DOD to operate effectively in cyberspace, defend national interests, and achieve national security objectives. The strategy focuses on a number of central aspects of the cyberspace threat, including external threat actors, insider threats, supply chain vulnerabilities, and threats to DOD's operational ability. The DOD must address vulnerabilities and the concerted efforts of both state and nonstate actors to gain unauthorized access to its networks and system. There are five strategic initiatives associated with this document:

- Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of its potential in military, intelligence, and business operations.
- Employ new defense operating concepts, including active cyberspace defense, to protect DOD networks and systems.
- Partner closely with other US government departments and agencies and the private sector to enable a whole-of-government strategy and a nationally integrated approach to cybersecurity.
- Build robust relationships with US allies and international partners to enable information sharing and strengthen collective cybersecurity.
- Leverage the nation's ingenuity by recruiting and retaining an exceptional cyberspace workforce and enabling rapid technology innovation.

Joint Concept for Cyberspace

(FOUO) The *Joint Concept for Cyberspace* was approved 21 August 2012 and identifies high-level operational effects and broad military capabilities for achieving cyberspace superiority. Cyberspace superiority is securing friendly freedom of action within cyberspace while denying the same to the adversary. Although extremely difficult for any actor in cyberspace to monopolize cyberspace superiority, it is realized and achieved through a concerted effort with the right balance and integration of advanced technology and cyberspace capabilities; a responsive and streamlined command and control structure; clear guidance, policies, and legal framework; and a trained and mission-ready workforce. The *Joint Concept for Cyberspace* proposes the need for centralized control and decentralized execution as one of several possible command and control structures for cyberspace operations and effects. Such a construct enables joint force commanders to satisfy mission objectives and requirements supporting the performance of synchronized joint force operations in and through cyberspace. The *Joint Concept for Cyberspace* also identifies the need to fully integrate cyberspace with joint functions and operations to assist warfighters in meeting the full range of national challenge identified in the *Capstone Concept for Joint Operations*.

This Page Intentionally Left Blank

CHAPTER 2
ORGANIZATION

Command, Authorities, and Organizations

Cyberspace operations are organized across a wide variety of commands and organizations, each of which employs the organic and nonorganic cyberspace capabilities at their disposal in accordance with their respective authorities. Each command and organization is organized in hierarchy, authority, and scope of responsibility to ensure the most effective use of its capabilities within cyberspace in relation to its higher, adjacent, and subordinate commands and organizations.

The following subparagraphs outline the missions, roles, and responsibilities of key organizations at the national and joint levels.

Commander, United States Strategic Command

(FOUO) The Commander, United States Strategic Command (USSTRATCOM) has responsibility to direct DODIN operations and defense through the subunified command United States Cyber Command (USCYBERCOM). In missions assigned by the Unified Command Plan, the Commander, USSTRATCOM:

- Plans, synchronizes, advocates, and employs capabilities to meet the United States strategic deterrence; space operations; cyberspace operations, global strike, and missile defense; intelligence, surveillance, and reconnaissance (ISR); and combating weapons of mass destruction.
- Provides planning and cyberspace support to coalition forces in theater.

Commander, United States Cyber Command

The Commander, USCYBERCOM, in support of the Commander, USSTRATCOM, has the following duties:

- Directs DODIN operations and defense.
- Plans against designated cyberspace threats.
- Coordinates with other combatant commanders and government agencies for effects that cross areas of responsibility.
- Plans operational preparation of the environment (OPE) and executes or synchronizes OPE in coordination with the geographic combatant commands (CCMDs).
- Provides military representation to US national agencies, US commercial entities, and international agencies for matters related to cyberspace, as directed.
- Executes cyberspace operations, as directed.

Service Components to the United States Cyber Command

The Marine Corps Service component to USCYBERCOM is United States Marine Corps Forces, Cyber Command (MARFORCYBER). The Marine Corps Network Operations and Security Center (MCNOSC) and Company L, Marine Cryptologic Support Battalion is under the operational control of MARFORCYBER.

The Commander, MARFORCYBER advises Commander, USCYBERCOM on the proper employment and support of Marine Corps forces; coordinates deployment, employment,

and redeployment planning and execution of assigned/attached forces; and conducts full-spectrum cyberspace operations. Such operations include DODIN operations, DCO, and, when directed, OCO. Those operations support the MAGTF, joint, and combined forces in order to enable freedom of action throughout the operational environment and deny the same to adversarial forces.

The MCNOSC is located in Quantico, Virginia. It directs global network operations and defense of the Marine Corps Enterprise Network (MCEN) and provides technical leadership to support seamless information exchange in support of Marine and Joint Forces operating worldwide. It is the operational, organizational, and technical construct for operating and defending the MCEN. It provides continuous, secure, global communications and operational sustainment and defense of the MCEN for Marine forces worldwide. Operationally, the MCNOSC functions as the network operations—also called NetOps—enterprise lead responsible for all cross-regional information technology issues.

Company L plans and, when directed, conducts OCO in support of Service, joint, and combined cyberspace requirements. When directed, it also provides support to DCO.

Like the Marine Corps, each military Service has a Service component to USCYBERCOM. These include Fleet Cyber Command, Army Cyber Command, and Air Forces Cyber. Each Service component commander to USCYBERCOM is responsible for advising Commander, USCYBERCOM with regard to the employment of its forces relative to cyberspace.

Cyberspace Support Element

Cyberspace support elements are organized from USCYBERCOM forces and deployed to CCMDs for full integration with their staffs. Cyberspace support element resources are provided by USCYBERCOM and are drawn from a pool of trained individuals, both at USCYBERCOM and the Service components. Such support provides the CCMDs with joint cyberspace operations planners and other subject matter experts on cyberspace operations. These personnel facilitate development of cyberspace requirements and coordinate, integrate, and deconflict cyberspace operations into the command's planning process.

Marine Corps Roles and Responsibilities

Cyberspace operations roles span the entire Marine Corps from the headquarters and supporting establishment to the operating forces and their unit-level organizations. Each organization's role either directly or indirectly supports the ability of the Marine Corps to perform cyberspace operations across the three LOOs, while continually re-evaluating and reshaping its capabilities to retain freedom of action within cyberspace.

Headquarters and Supporting Establishment

The supporting establishment consists of 16 major bases, training activities, formal schools, Marine Corps Recruiting Command, Marine Corps Combat Development Command, Marine Corps Systems Command, and Headquarters Marine Corps. The supporting establishment's contributions are vital to the overall cyberspace readiness of the Marine Corps. This support is necessary to effectively deploy and implement modern information technology in support of the MAGTF, both in garrison and when deployed.

Deputy Commandant, Plans, Policies and Operations

The Deputy Commandant, Plans, Policies and Operations serves as the Marine Corps advocate for cyberspace operations. He provides expert advice to the Commandant of the Marine Corps to develop the Marine Corps position on cyberspace operations issues and represent those positions and enabling capabilities that support the Marine Corps operating forces and the supporting establishment.

Director, Command, Control, Communications, and Computers Department

The Director, Command, Control, Communications, and Computers Department plans, directs, and coordinates all staff activities relating to such functions. He supports the Commandant of the Marine Corps in his role as a member of the Joint Chiefs of Staff. As the chief information officer of the Marine Corps, the director provides oversight of Marine Corps information technology infrastructure, cybersecurity, governance, and policy. He also represents the Marine Corps at DOD, joint, and Department of the Navy information technology forums. As the authorizing official, he oversees, implements, and directs the formal security accreditation process, ensuring all information systems operate within acceptable levels of risk. He also serves as the lead for Marine Corps information technology portfolios and establishes Marine Corps information technology portfolio management policy, processes, guidance, and oversight.

Director of Intelligence

The Director of intelligence (DIRINT) is responsible for policy, plans, programming, budgets, and staff supervision of intelligence and supporting activities within the Marine Corps. The DIRINT has Service staff responsibility to ensure there is a single synchronized strategy for the development of the Marine Corps ISR enterprise to support the intelligence needs of Marine commanders throughout the operational environment. The DIRINT also manages the Marine Corps' sensitive compartmented information (SCI) computer network, in close coordination with the director, Command, Control, Communications, and Computers, to ensure that the enterprise-level management of SCI networks is comparable to that of the general service networks. This relationship between the two directors recognizes that special measures are required for the protection/handling of foreign intelligence, counterintelligence, or other need-to-know information. Accordingly, implementation of these measures must be tailored to comply with separate and coordinated Director of National Intelligence directives and intelligence community policies. Systems that combine SCI and general service capabilities will be under the authority of the director Command, Control, Communications, and Computers with the exception of specific SCI security activities.

Deputy Commandant, Combat Development and Integration

The Deputy Commandant, Combat Development and Integration is responsible for the integration and execution for all Marine Corps warfighting development activities associated with cyberspace. Specifically, the Command and Control/Cyber and Electronic Warfare Integration Division coordinates with the operating forces, supporting establishment, and mission partners. Together they identify, prioritize, and integrate command and control, expeditionary cyberspace, and electronic warfare capability solutions across the pillars of DOTMLPF [doctrine, organization, training, materiel, leadership and education, personnel, facilities], policy, warfighting functions, and joint requirements.

Deputy Commandant, Installations and Logistics

The Deputy Commandant, Installations and Logistics shapes logistic plans and policies to sustain excellence in warfighting. The focus of effort is to increase MAGTF lethality by providing superior support through modernizing logistic processes, implementing proven technology and best practices, developing standards of performance, and fully integrating the supporting establishment as the "fifth element" of the MAGTF.

Marine Corps Installation Command. The Marine Corps Installation Command (MCICOM) exercises command and control of Marine Corps installations via regional commanders to provide oversight, direction, and coordination of installation services and to optimize support to the operating forces, tenants, and activities. For installations under the command and control of the

commanding general of Marine Corps Training and Education Command, MCICOM only provides installation support.

MAGTF Information Technology Support Centers. Seven of the eight MAGTF information technology support centers (MITSCs) are under the operational control (OPCON) of MCICOM. The MITSCs execute NetOps functions for the eight subregions in support of the Regional Network Operations and Security Centers (RNOSCs) by providing information technology services to Marine expeditionary forces (MEFs) in garrison and Marine Corps supporting establishment elements within its area of responsibility. The eight subregions supported by the MITSCs are:

- Headquarters, Marine Corps.
- The national capital region.
- East, supporting the US mid-Atlantic region.
- West, supporting the US Pacific region.
- United States Marine Corps Reserves.
- Mid Pacific (Hawaii).
- West Pacific.
- Europe.

Unlike the other MITSCs, MITSC Europe is not under the OPCON of MCICOM; rather, it has a unique command relationship with United States Marine Corps Forces, Europe due to lack of a Marine Corps installation in Europe. The MITSCs are the support centers for the bases, posts, and stations within their region, providing information technology support and enforcing established information technology policies.

Marine Corps Intelligence Activity

The Marine Corps Intelligence Activity provides tailored intelligence and services to the Marine Corps, other Services, and the intelligence community based on expeditionary mission profiles in littoral areas. It supports the development of Service doctrine, force structure, training and education, and acquisition. Reachback analysis and production capabilities provided by MCIA should be leveraged by Marines planning and conducting operations throughout the operational environment.

The DIRINT, Headquarters, Marine Corps, is responsible for implementing and managing Marine Corps SCI architecture in accordance with intelligence community directives and references. The Marine Corps SCI Executive Office administers and operates the Marine Corps SCI enterprise by providing policy implementation, governance, technical support, and assistance in establishing and sustaining Marine Corps SCI networks. The SCI Executive Office provides enterprise management, network operations, network security, information assurance, and asset management across the Marine Corps in accordance with relevant directives and guidance from the Office of the Director of National Intelligence, Defense Intelligence Agency, and National Security Agency.

Marine Cryptologic Support Battalion

Marine Cryptologic Support Battalion is under the OPCON of the Director, National Security Agency/Chief, Central Security Service via the DIRINT in his role as the Marine Corps Service Cryptologic Component Chief. This battalion trains, employs, and deploys Marines to conduct signals intelligence (SIGINT), information assurance, and national-tactical integration activities that satisfy National Security Agency/Central Security Service, MAGTF, and joint force intelligence requirements.

Marine Corps Operating Forces

Staff Capabilities

Marine Corps forces are assigned to CCMDs. Staffs advise combatant commanders on the proper employment and support of Marine Corps forces, conduct deployment/redeployment planning and execution of assigned/attached Marine Corps forces, and accomplish other operational missions as assigned. Marine Corps forces are the

bridge between the CCMDs and deployed/employed MAGTFs. With the exception of MARFORCYBER, few Marine Corps forces have robust organic cyberspace planning capabilities. Some have none; however, the Marine Corps forces can and should leverage cyberspace planning support from their CCMD's Joint Cyberspace Center and the cyberspace support elements, which are in direct support of the Joint Cyberspace Center. Additionally, Marine Corps forces should leverage cyberspace planning capabilities resident in their assigned MAGTFs and the MEFs, which have primary and secondary planning support responsibilities to their respective Marine Corps forces.

The MAGTFs have long been staffed, trained, and equipped to plan and conduct certain aspects of cyberspace operations, such as NetOps and DCO. At this writing, additional structure is being phased into the operating forces (fiscal years 2013–2016) to help enable MAGTFs to integrate all three LOOs of cyberspace operations into broader MAGTF operations. This involves not just em-ploying organic capabilities, but also planning for, requesting, and integrating externally available capabilities.

Regional Network Operations and Security Centers

The four RNOSCs support the four regions that collectively form the backbone of all DODIN operations for the Marine Corps:

- United States Marine Corps Forces, Pacific.
- United States Marine Corps Forces Reserve.
- United States Marine Corps Forces Command.
- National capital region.

The RNOSCs encompass a total of eight subregions called MITSCs, described earlier in this chapter. The RNOSCs provide policy and regional oversight, the tasking and reporting framework, decision support, and recommendations to their respective MITSCs. The RNOSCs are provided guidance and operational direction by the MCNOSC. The RNOSCs are responsible to implement the direction and then report back to the MCNOSC.

Cyberspace Operations Within the Marine Expeditionary Force

The MEF is the principal Marine Corps warfighting organization for larger crises or contingencies. While the MEF command elements have limited resources to perform specific DODIN functions, the preponderance of cyberspace operations capabilities reside in organizations subordinate to the command element. Within the MEF, the communication battalion, major subordinate commands, the radio battalion, and the intelligence battalion conduct cyberspace operations.

Communication Battalion

The communication battalion is the senior MAGTF organization that conducts cyberspace operations; that is, DODIN operations and DCO. The communication battalion deploys as a task-organized unit or deploys task-organized detachments in support of MAGTF command elements. The communication battalion is equipped to serve as the hub for linking MAGTF networks to the DODIN and leading the extensive coordination required for DCO. Subordinate units execute the same kinds of activities, with backbone connectivity provided by the communication battalion. Specific communication battalion actions include:

- Installing, operating, and maintaining the transmission systems that enable cyberspace operations.
- Installing, operating, and maintaining the digital backbone that routes network traffic to the appropriate nodes.
- Installing, operating, and maintaining the local area networks/wide area networks for the MEF command element.
- Leading changes to the network directed by higher headquarters.
- Installing, operating, and maintaining boundary defense devices in support of DCO.

Additional information on the communication battalion can be found in Marine Corps Warfighting Publication (MCWP) 3-40.3, *Communications and Information Systems*.

Major Subordinate Commands (Unit Level Defensive Cyberspace Operations and Department of Defense Information Networks Operations)

The division, air wing, and logistic group each have communications units that conduct DODIN operations and DCO at their levels of command. Division and logistic groups each have communications companies, while the air wing has a communications squadron. The specific actions they execute are comparable to the communication battalion. Additional information on MAGTF communications units can be found in MCWP 3-40.3.

Radio Battalion

(FOUO) Each MEF has an organic radio battalion. Radio battalions are task-organized to support any size MAGTF. The mission of radio battalion is to provide SIGINT, ground electronic warfare, limited cyberspace operations, and special intelligence communications support to the MAGTF and joint force commander, as directed. Specifically, radio battalion support to the MAGTF includes the following:

- Briefs the MAGTF commander and his staff on the capabilities and limitations of SIGINT and, when directed, limited OCO support.
- Provides access to special intelligence networks to facilitate reachback/coordination with higher headquarters for cyberspace operations.
- Provides SIGINT support to cyberspace operations (DODIN operations, DCO, and OCO).
- Researches the availability of organic and externally available resources to meet the MAGTF commander's requirements.
- Identifies and collects on networks of interest to satisfy mission requirements.
- Conducts analysis to refine the collection effort and validate follow-on targeting and exploitation.
- Produces Digital Network Intelligence Reports.
- Manages cyberspace ISR collection assets.
- Supports all-source intelligence fusion operations.
- Coordinates with appropriate agencies for the deconfliction of activities in cyberspace.
- Conducts operations in and through cyberspace to affect designated targets in accordance with the supported commander's intent.
- Plans and conducts ground electronic warfare to generate effects in cyberspace.
- Provides technical information to support mission planning.
- Applies legal consideration to OCO, as required.
- Supports the development of measures of effectiveness (MOEs) and/or battle damage assessment criteria.

Additional information on the radio battalion can be found in MCWP 2-22, *Signals Intelligence*.

Intelligence Battalion

(FOUO) The intelligence battalion plans, directs, collects, produces, and disseminates intelligence and provides counterintelligence support to the MEF, major subordinate commands, subordinate MAGTFs, and other commands, as directed. The following are among its responsibilities:

- Install required communications and networking gear to support the Joint Worldwide Intelligence Communications System (JWICS) connectivity to the MEF command element and the intelligence battalion.
- Operates JWICS at the MEF and intelligence battalion in support of garrison requirements.
- When deployed, supports operations and exercises with communications terminals in order to establish general service and SCI connectivity.

Authorities

Authority for actions undertaken by the Armed Forces of the United States is derived from the US Constitution and Federal law. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace. Key statutory authorities that apply to the Marine Corps include United States Code, Title 10, *Armed Forces*, and Title 50, *War and National Defense*.

Legal Considerations

Marines and the entire joint force must conduct cyberspace operations consistent with US domestic law, applicable international law, and relevant US government and DOD policies. The legal framework applicable to conduct cyberspace operations depends on the nature of the activities to be conducted, such as offensive or defensive military operations. Before conducting cyberspace operations, commanders, planners, and operators must understand the relevant legal framework so as to comply with laws and policies.

Application of the Law of War

The law of war is defined as that part of international law that regulates the conduct of armed hostilities. It encompasses all international law for the conduct of hostilities binding on the United States or its individual citizens, including treaties and international agreements to which the United States is a party and applicable customary international law. The law of war rests on the fundamental principles of military necessity, unnecessary suffering, proportionality, and distinction (discrimination), which will apply to the conduct of cyberspace operations. For more information on the law of war, see JP 1-04, *Legal Support to Military Operations*, and Chairman of the Joint Chiefs of Staff Instruction 5810.01D, *Implementation of the DOD Law of War Program*.

Lawful Military Attacks

Attacks will be directed only at military targets. Only a military target is a lawful object of direct attack. By their nature, location, purpose, or use, military targets are those objects whose total or partial destruction, capture, or neutralization offer a direct and concrete military advantage.

This Page Intentionally Left Blank

CHAPTER 3
PLANNING

Planning Cyberspace Operations

(FOUO) Cyberspace operations share many similarities with operations in the physical domains; moreover, it has unique tactical command and control, planning, and resource considerations, such as a significant need for reachback support. The integration of cyberspace operations must be within the construct of the Marine Corps Planning Process (MCPP). That is, the commander and staff must be made aware of cyberspace operations principles, capabilities, limitations, and planning considerations. Cyberspace considerations must be integrated into all six steps of the MCPP, taking into account the complexities added by the authority considerations not traditionally associated with operational planning. Likewise, outputs of the MCPP must reflect considerations and planned activities for cyberspace operations.

Considerations

(FOUO) Given the three LOOs that make up cyberspace operations—DODIN operations, DCO, and OCO—the following are examples of appendices and tabs that will reflect cyberspace operations:

- Information operations.
- Priority intelligence requirements.
- SIGINT.
- Human intelligence.
- Counterintelligence.
- Targeting intelligence.
- Information operations intelligence integration.
- National intelligence support team.
- Intelligence estimate.
- Intelligence products.
- Intelligence collection plan.
- Intelligence operations.
- Electronic warfare.
- Cyberspace operations (formerly known as computer network operations).
- Rules of engagement (ROE).
- Targeting.
- Information systems security.
- Communications planning.
- Space operations.
- Integrated joint special technical operations.

(FOUO) When the MCPP is initiated, whether informally in response to indications and warnings or more formally when an order or directive is received, the cyberspace operations planner should be aware of what information is required during each step. Whether conducting contingency or crisis action planning, the input to the MCPP is the same. There are planning directives and strategic or operational guidance that will support the initiation of the process, along with ongoing intelligence preparation of the battlespace (IPB). Included in IPB are attempts to determine the adversary's possible courses of action (COAs) and those cyberspace ISR efforts to gather and analyze intelligence information about target and adversary systems. The planning coordination and support process should begin as early as possible with the commander submitting a request for support message to the supported joint force commander. Early submission allows sufficient time for resource prioritization. The request message must include as much intelligence detail from the G-2/S-2 as possible. The level of detail in the information request will have a significant bearing on how the request fares in the requirements review process. The more detailed the request input, the more readily

coordination and deconfliction with interagency organizations can occur. Robust intelligence details will also greatly assist staff elements in the performance of their support missions.

Cyberspace Operations Planner

The cyberspace operations planner is responsible for planning across all LOOs and integrating organic and externally available cyberspace operations capabilities in support of the commander's objectives, scheme of maneuver, and end state. Cyberspace operations planners ensure the effective integration of cyberspace capabilities to accomplish mission support activities, which include coordinating activities to counter the adversary's use of cyberspace and to enable friendly freedom of action in cyberspace. These activities support planning for operations in a degraded environment and consolidating operational requirements for cyberspace capabilities in support of the commander's single-battle concept. Cyberspace operations planners develop viable options to enable effective shaping of the situation and response to contingencies. To ensure successful integration and synchronization of cyberspace operations with all other elements of multinational, joint, interagency, and Marine Corps operations, cyberspace operations planners are involved in all stages of the Joint Operation Planning Process and/or MCPP, as appropriate.

In order to increase the MAGTF's capacity to plan and conduct cyberspace operations, additional personnel possessing technical cyberspace operations skills began arriving at all Marine expeditionary force and unit staffs in 2013. Through 2016, these new billets will continue to be filled at the Marine expeditionary forces, battalions, and units. The structure consists of the 8834, 0689, and 2611 MOSs.

The officers assigned to the technical information operations officer/cyberspace operations planner (MOS 8834) billets will each hold a Master's degree in information warfare systems engineering from the Naval Postgraduate School and will be familiar with the MCPP. These officers serve as the MAGTF's functional and technical planners for cyberspace operations. The cyberspace operations planner is capable of providing support for planning and mission execution through expert knowledge of joint cyberspace components, processes, capabilities, authorities, and partner operations. They maintain situational awareness of ongoing and planned cyberspace operations by coordinating with the G-2/S-2, G-3/S-3, and G-6/S-6 subject matter experts to ensure operations align with the commander's objectives.

Cyberspace security/defensive cyberspace technical planner (MOS 0689) Marines assist in ensuring the data availability, integrity, authentication, confidentiality, nonrepudiation, and mission assurance of Marine Corps information systems. Defensive cyberspace technical planners coordinate closely with the intelligence staff to incorporate focused/proactive defensive measures based upon the latest tipping and queuing from cyberspace intelligence. They advise and assist in the planning and identification of cyberspace defense requirements associated with MAGTF operational requirements, operational risk management, and mitigation processes with respect to cyberspace vulnerabilities and threats. The primary focus of this Marine will be on DODIN operations and DCO efforts.

Cryptologic digital network operator/analyst/offensive cyberspace technical planner (MOS 2611) Marines are involved in all facets of planning and coordinating OCO. Offensive cyberspace technical planners coordinate closely with the intelligence staff to ensure that intelligence requirements reflect targets and threats in cyberspace. They also assist in coordinating support from external OCO organizations/units. These Marines provide technical advice regarding the applicability of available OCO capabilities to the mission at hand, coordinate with appropriate agencies to deconflict activities in cyberspace, conduct or assist in conducting planning for electronic warfare to generate effects in cyberspace, and support the development of MOEs and/or battle damage assessment criteria.

Cyberspace operations planners must be engaged in the following activities:

- Identify threats, risks, and opportunities in cyberspace that may affect operational planning.
- Ensure cyberspace operations are adequately addressed in relevant operation plans and contingency plans.
- (FOUO) Maintain situational awareness of current operations.
- Obtain current cyberspace intelligence, including cyberspace ISR or cyberspace OPE status for potential OCO.
- Review intelligence and create requests for intelligence and intelligence requirements to fill intelligence gaps.
- Review all sources for cyberspace information, including other government agencies, to identify possible cyberspace intelligence conflicts or collaboration opportunities.
- Include current cyberspace situational assessments in meetings with the commander and staff (e.g., during staff meetings, working groups, and intelligence updates).
- Use these engagements as foundation building opportunities for future cyberspace operations.
- Maintain situational awareness of updated cyberspace topographies of enemy computer networks, high-value individuals and high-value targets, and functions of identified centers of gravity through reachback capabilities.
- Investigate cyberspace communities of interest and database resources, to include information on previous cyberspace operations for effective methods and lessons learned.

Depending on the planner's current level of clearance and access, additional access and/or accounts may be required to review all resources listed or referenced in this document, including the following:

- Intelligence.
- OCO target lists.
- Local intelligence officer.
- Local G-3 current operations.
- Lethal/nonlethal weapon systems.
- Cyberspace threat intelligence acquired by the Central Intelligence Agency.
- USSTRATCOM Strategic Knowledge Integration Web.
- Integrated Strategic Planning Analysis Network.
- National Security Agency/Central Security Service Threat Operations Center.
- USCYBERCOM, including countering the adversary's use of the Internet portal, library files, and available intelligence—
  - Review USCYBERCOM's cyberspace capabilities registry for existing cyberspace tools. Contact USCYBERCOM for permission to access this registry via JWICS. The cyberspace capabilities registry is the centralized Web-based resource for the cyberspace community where developers, operators, and planners may obtain information about cyberspace tools.
  - Consult the supporting Joint Cyberspace Center to identify a suitable cyberspace tool or to document requirements.
  - Review current combat ready cyberspace strike packages and determine compatibility with the developing situation. Intelligence, accesses, staff judge advocate review, capability readiness, and deconfliction status should all be complete. Determine which packages require additional refinement, development, coordination, or accesses.

The USCYBERCOM, combatant commands, or local Joint Cyberspace Center will have the status of OCO strike packages and engage in the following activities:

- (FOUO) Integrate with planning and targeting process.
- Participate in information operations working group (IOWG), joint planning group, operational planning team, and special technical operations working group, as required.

- Use these forums as a conduit to establish working relationships with other lethal/nonlethal planners and related subject matter experts.
- Review available local standing operating procedures, paying particular attention to how they will affect DODIN operations, DCO, and OCO planning.
- (FOUO) Review restricted and no-strike target lists. Sources could include the local and affected command, agencies, USCYBERCOM, and other entities.
- (FOUO) Review standing ROE, supplemental measures, and multinational ROEs, as required.

Cyberspace Operations and the Marine Corps Planning Process

The following subparagraphs discuss the six MCPP steps in terms of the tasks, input, and output required by cyberspace operations planners.

Problem Framing

Since freedom of action in cyberspace facilitates freedom of action throughout the operational environment, planners must incorporate both offensive and defensive aspects of cyberspace operations into their approach. During problem framing, the cyberspace operations planner develops the cyberspace operations portion of the problem framing brief. In support of this effort, cyberspace operations information requirements are developed and tasks are defined. Cyberspace operations objectives are determined and evaluated in terms of scope, levels and duration of effects, collateral damage (friendly and enemy), reversibility, planning and execution timelines, and access required. Cyberspace ISR support for this type of information is included in the SIGINT support plan generated by the staff for fusion and coordination. As part of this step, cyberspace policies and ROE are evaluated as potential limitations, cyberspace high value targets are considered as critical factors, and cyberspace information needs are folded into the commander's critical information requirements (CCIRs), as applicable.

Cyberspace operations planner tasks directed by the G-3/S-3—

- Conduct initial assessment of the mission across the three LOOs.
- Analyze commander's mission objectives and guidance.
- Determine initial cyberspace ISR, DCO, and OCO requirements.
- Analyze how to integrate cyberspace ISR, DCO, and OCO into mission objectives.
- Coordinate with G-2/S-2 for cyberspace ISR support.
- Coordinate with G-6/S-6 for DCO support.
- Coordinate with a special technical operations officer for the review and approval process (RAP).
- Coordinate tasks with IOWG.
- Define and analyze the information environment and threat.
- Determine DCO planning factors to ensure system and network availability is achieved through visibility and control over the system and network resources.
- Scope OCO tasks (consider desired effects, duration, reversibility, collateral damage, and target accessibility).
- Assist G-2/S-2 in developing related cyberspace operations information needs.
- Identify organic cyberspace capabilities and vulnerabilities.
- Identify specified, implied, and essential cyberspace operations tasks.
- Identify friendly cyberspace operations centers of gravity and critical vulnerabilities.
- Identify adversary cyberspace operations centers of gravity and critical vulnerabilities.

Cyberspace operations planner input—

- Cyberspace operations input to initial staff estimate.
- Higher headquarters center of gravity analysis.
- Higher headquarters cyberspace OPE and information operations-related intelligence products.

Cyberspace operations planner output—

- Convene the cyberspace operations cell.
- Review higher headquarters orders and guidance.
- Submit initial requests for intelligence.
- Develop a cyberspace operations mission statement.
- Identify facts, assumptions, constraints, and restraints.
- Develop information requirements.
- Identify initial cyberspace operations shortfalls and risks.
- Recommend initial CCIRs related to cyberspace operations.
- Input cyberspace operations to the IOWG.
- Submit recommended commander's cyberspace operations planning guidance.

Course of Action Development

During this step, the cyberspace operations planner develops the cyberspace operations concepts in support of COAs that use objectives and tasks developed during problem framing to determining possible MOEs. A DCO analysis is conducted to determine metrics for information assurance requirements that protect and defend information and information systems, protect and defend information and networks, and identify critical infrastructure protection requirements.

Additionally, the cyberspace operations target development, validation, and nomination process occurs during this step and helps drive the identification of desired OCO effects. Additionally, the cyberspace operations planner may include recommendations for cyberspace capabilities to be used, such that they may be analyzed for measures of performance (MOPs) and possible interference or attribution issues in cyberspace.

For cyberspace operations actions that fall under special technical operations, an evaluation request message, also known as an EReqM, is sent as part of the integrated joint special technical operations process. The cyberspace operations planner will assist in developing input to the OCO RAP. The RAP package will consist of the concept of operations (CONOPS), legal reviews, intelligence and technical gains versus losses, political and military assessment, operational security, and a detailed description of the operation.

Cyberspace operations planner tasks—

- Assist in evaluation request message and Cyberspace Effects Request Form development to identify desired OCO effects.
- Review the evaluation request messages received from supporting components.
- Plan integration of OCO with other information-related capabilities (IRCs) and the overall mission plan.
- Assist in developing cyberspace operations concept of support.
- Review standing operating procedures, standing ROE, and supplemental measures and multinational ROE, as required.

Cyberspace operations planner input—

- Center of gravity products.
- Problem framing products.
- Cyberspace operations-related commander's planning guidance.
- Cyberspace OPE and combined information overlay.

Cyberspace operations planner output—

- Cyberspace operations concept of support.
- Cyberspace operations tasks and MOE.
- Cyberspace operations target development, validation, and nomination.
- Cyberspace operations input to the information operations synchronization matrix.
- Cyberspace operations CONOPS.
- Narrative/sketch.
- Required supplemental ROE for cyberspace operations.
- Desired DCO objectives identified.

- Defense of information and information systems, their availability, integrity, authentication, confidentiality, and nonrepudiation.
- Incorporation of protection, detection, and reaction capabilities.
- Defense of information and networks from disruption, denial, degradation, or destruction.
- Prevention, remediation, or mitigation of the risks resulting from critical infrastructure vulnerabilities.
- OCO effects.
- Development of an evaluation request message input.
- Review of evaluation request message.
- Cyberspace operations input to combatant commander RAP.
- Legal reviews: traditional law of war, international law, and effect of domestic and foreign law.
- Intelligence gain versus loss.
- Impact of OCO on intelligence collection activities.
- Refined CCIRs with cyberspace operations input.
- Additional cyberspace operations-related shortfalls.
- Updated cyberspace operations input to staff estimate.

Course of Action Wargaming

Cyberspace operations are incorporated into the COA analyses. Refinements are made to all aspects of the cyberspace operations plan, including (but not limited to) targets, synchronization, branches and sequels, decision points, MOEs, MOPs, objectives, and tasks. Using a synchronization matrix helps the staff visually synchronize the COA across time and space in relation to the adversary's possible COAs. The wargame and synchronization matrix efforts are particularly useful in identifying cross-component support resource requirements. These efforts result in mature cyberspace operations inputs to the staff estimate. The difference for cyberspace operations planning is the emphasis on characteristics of the weapons used; there is far greater concern about interference with other cyberspace operations and attribution of the weapons.

(FOUO) Cyberspace operations planner tasks—

- Employ technical tools in the cyberspace and information environments to enhance situational awareness.
- In conjunction with G-2, wargame cyberspace operations concept of support against how the enemy will employ its information systems, assets, and cyber-enabled weapons (when applicable).

Cyberspace operations planner input—

- Commander's cyberspace operations guidance for the wargame.
- Cyberspace operations input to information operations concept of support.
- Cyberspace operations target nominations.

Cyberspace operations planner output—

- Refined cyberspace operations concept of support.
- Refined cyberspace operations tasks and MOE.
- Refined cyberspace operations targets.
- Refined cyberspace operations-related risks.
- Refined cyberspace operations-related decision points.
- Updated cyberspace operations input to information operations staff estimates.

Course of Action Comparison and Decision

The cyberspace operations planners assigned to support the commander will identify the advantages and disadvantages of the cyberspace operations CONOPS for each COA. They should also examine each cyberspace COA for deconfliction of their proposed actions with national, combatant command (command authority), and other pertinent efforts. Once deconfliction is accomplished, the cyberspace operations planners will assist in updating the staff estimate.

Cyberspace operations planner tasks—

- Analyze and evaluate cyberspace operations support to each COA.
- Identify the best COA to recommend to the commander with supporting rationale.

Cyberspace operations planner input—

- Cyberspace operations input to information operations concept of support.
- Commander's cyberspace operations related guidance for COAs.

Cyberspace operations planner output—

- Advantages and disadvantages of cyberspace operations concept of support identified.
- Updated cyberspace operations input to information operations staff estimate.
- Recommended COA to G-3/S-3.
- Submit cyberspace operations inputs to COA approval brief.

Orders Development

Cyberspace operations planners prepare the cyberspace operations appendices and tabs to be inserted into annex C of the commander's operation plan. Those products are appendix 3, Tab F (OCO), and Tab G (DCO). Cyberspace ISR is included in Annex B (Intelligence) of the commander's operation plan.

Cyberspace operations planner tasks—

- Assist in cyberspace operations mission CONOPS development. Consider command and control authorities, request for forces, equipment, and intelligence gain/loss.
- Prepare cyberspace operations appendixes and tabs: Tab F (OCO) and Tab G (DCO).
- Assist in preparation of Annex S (Special Technical Operations), if applicable.

The cyberspace operations planner input is the commander's approved COA with the corresponding cyberspace operations concept.

Cyberspace operations planner output—

- Cyberspace operations inputs to such documents as the operation plans and OPORD.
- Staff coordination.
- Backbriefs from subordinate cyberspace operations cells and rehearsals.
- Synchronization of cyberspace operations.
- Considerations across the range of military operations.
- Assessment of cyberspace operations.
- MOEs.
- MOPs.

Transition

Transition, the sixth step of MCPP, is universal. There are no unique cyberspace operations planner tasks, input, or output.

Integrating Cyberspace Operations into MAGTF Operations

In order to be of greatest value to Marine Corps forces and MAGTF commanders, cyberspace operations must be integrated with operations throughout the operational environment. Cyberspace operations should be planned, coordinated, conducted, and assessed in concert with operations in the operational environment in the context of specific missions and commander's intent.

Cyberspace Operations and Targeting

(FOUO) Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. Integrating cyberspace operations into the process is the same as integrating any other capability the MAGTF commander and staff have available.

(FOUO) Time is a major consideration for planning and integrating cyberspace operations into the targeting process. Much like most conventional lethal capabilities the MAGTF commander employs, cyberspace operations will also be time

constrained. However, the planning horizon for employing some cyberspace operations capabilities is considerably greater than for most conventional capabilities.

(FOUO) It is paramount that targets are identified early in the planning process. During the initial phases of the MCPP, the G-3/S-3 and G-2/S-2 must ensure that possible targets are identified to allow for the development of those targets and the time required for the approval process.

(FOUO) In June 2010, United States Strategic Command's Joint Test and Evaluation [Activity] published *Joint Non-Kinetic Effects Integration Tactics, Techniques, and Procedures (TTP)*. It provides an excellent foundation for planners integrating nonlethal effects. These tactics, techniques, and procedures are intended to complement, not replace, existing Service and joint doctrine.

Targeting Process

(FOUO) The targeting process supports the commander's decisions. It helps the targeting team decide which targets must be acquired and attacked to support achievement of the commander's objectives. It helps in the decision of which attack option(s) to use to engage the targets. Options can be lethal or nonlethal and organic or supporting. Given the range of military operations to which Marines are assigned and the present security environment impacting US national interests, Marine commanders can expect to operate in situations in which lethal options are extremely limited. Therefore, MAGTF commanders and their staffs must be skilled at applying the targeting process to use nonlethal options, such as cyberspace operations and electronic warfare. Due to the long lead times often associated with cyberspace ISR, IPB and OCO planning, approval, and execution, commanders must ensure that contingency planning considers cyberspace options and execution timelines.

(FOUO) The targeting process is detailed in MCWP 3-43.3, *Marine Air-Ground Task Force Fires*. The functional steps in the targeting process are decide, detect, deliver, and assess.

(FOUO) Decide. Identifying "potential" targets will allow organic and supporting assets to begin the process of cyberspace ISR and IPB. Early identification of potential targets will allow the approval process to begin prior to mission planning and the decide phase of the targeting process.

(FOUO) Detect. Maintaining situational awareness and identifying potential targets within an area of responsibility allow the organic and supporting assets to detect and develop those targets early in the process. Conventional capabilities *typically* require less detailed technical detection than cyberspace capabilities do.

(FOUO) Deliver. Several driving factors in the delivery of fires and generation of effects, whether cyberspace or conventional, are the ability to support commander's scheme of maneuver, the integration with other fires/effects to create a combined arms effect, and effective MOE and MOP.

(FOUO) Assess. Assessment is a process that measures progress of the MAGTF toward mission accomplishment.

Categories of Offensive Cyberspace Operations Effects

(FOUO) The OCO planning process is dependent on the availability of and access to OCO tools. This will drive the development of MOPs and MOEs based on the tools' performance characteristics. There are five categories of OCO effects: deny, degrade, disrupt, destroy, and manipulate.

(FOUO) Deny. To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources.

(FOUO) Degrade. To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified.

(FOUO) Disrupt. To completely but temporarily deny (a function of time) access to or operation of

a target for a period represented as a function of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent.

(FOUO) Destroy. To permanently, completely, and irreparably deny (time and amount are both maximized) access to or operation of a target.

(FOUO) Manipulate. To control or change information, information systems, and/or networks in a manner that supports the commander's objectives, including deception, decoying, conditioning, spoofing, and falsification. Manipulation uses an adversary's information resources for friendly purposes.

Cyberspace Effects Request Form

(FOUO) The MAGTF commander must request and coordinate OCO support via higher headquarters. The Cyberspace Effects Request Form is the mechanism by which tactical commanders request cyberspace effects on a target. This format contains the baseline information end users must provide to facilitate the planners' requests for cyberspace fires to support tactical operations. A Cyberspace Effects Request Form must be submitted whether the capability desired to be employed is organic or supporting. A detailed description and example(s) of Cyberspace Effects Request Forms are located in MCRP 3-16.6A, *Multi-Service Tactics, Techniques, and Procedures (MTTP) for the Joint Application of Firepower (JFIRE)*. Additionally, the description in the reference provided also describes the approval chain.

Assessment of Cyberspace Operations

(FOUO) The focus is on measuring progress toward the end state and delivering relevant reliable feedback into the planning process to adjust operations during execution. Assessment involves deliberately comparing forecasted outcomes with actual events to determine the overall effectiveness of force employment.

(FOUO) Cyberspace planners adjust their MOPs and MOEs during COA development, analysis and wargaming, comparison, approval, and plans/orders development. Planners must stay actively engaged because the plan changes and must be adjusted during every step of the MCPP (and during execution) since MOPs and MOEs will change in the plan. Any change has the potential to affect the criteria of relevance, measurability, responsiveness, and proper resourcing.

(FOUO) Measures of Effectiveness. The MOEs assess changes in system behavior, capability, or the operational environment. They measure the attainment of an end state, achievement of an objective, or generation of an effect. When expressed quantitatively, MOEs generally reflect a trend or show progress toward a measurable threshold. The MOEs enable cyberspace operations planners to maintain updated cyberspace topographies of enemy computer networks, engineering, programming, high-value targets, and functions of identified centers of gravity.

(FOUO) In order for any MOE to be valid, it must have the following characteristics:

- Relevant to the intended effects and objectives.
- Measurable from a baseline that demonstrates movement toward (or away) from the effects and objectives.
- Responsive enough to enable a commander to make timely follow-on decisions or verify expectations of mission accomplishment along with assessments of projected and unexpected secondary and tertiary effects.
- Supported by sensors and reporting systems. Without proper commitment of resources, it would be nearly impossible to obtain an accurate, responsive assessment of the action results.

(FOUO) Measures of Performance. The MOPs are criteria for measuring task performance or accomplishment. They are generally quantitative and are used in most aspects of combat assessment, which typically seeks specific, quantitative data or a direct observation of an

event to determine accomplishment of tactical tasks. In cyberspace operations, an appropriate MOP might pertain to the ability to obtain a required access or implant a particular exploit or defense. Analysis of data collected on MOE/MOP will allow the planners to make a determination on the success of the cyberspace operations across all three LOOs (DODIN operations, DCO, OCO). For example, the cyberspace operations planner can assess effects on a target and any reattack recommendations if needed, as well as assess the reliability and resilience of the network. Inherent latencies often exist between OCO actions and effects; hence, indications of first, second, and third order effects may vary greatly in time (from hours to years).

(FOUO) A detailed description of cyberspace targeting and OCO tactics, techniques, and procedures can be found in *Joint Non-Kinetic Effects Integration Tactics, Techniques, and Procedures*. Additional information can be found in JP 3-60 and JP 3-12.

Cyberspace Information Requirements

(FOUO) Information requirements are general or specific subjects upon which there is a need for the collection of information or the production of intelligence. During problem framing, the MAGTF staff identifies gaps in what is known about the adversary, the operational environment, and friendly forces. Information requirements can be general or specific and require an answer to facilitate mission success. The two broad categories of information requirements are friendly force and adversary/operational environment requirements.

Friendly Information

(FOUO) Information gaps related to friendly forces are answered by the relevant organizations within or in support of the MAGTF. The exact number of vehicles or aircraft available to support a particular COA could be an example of a question that needs to be answered prior to mission execution. The availability of communications/data networks to support a COA would be an example of an information requirement to which cyberspace planners may need to respond.

Intelligence Requirements

(FOUO) Information gaps related to the adversary or the operational environment are referred to as intelligence requirements. The G-2/S-2 is responsible for coordinating collection assets to support the collection, analysis, and production of intelligence to answer intelligence requirements. Cyberspace-related intelligence requirements may require long lead times to coordinate with theater-/national-level collection assets. It is, therefore, important that the planning staff, specifically the G-6/S-6 and SIGINT/electronic warfare organizations, collaborate and identify intelligence requirements early in the planning process. The current nodal construct of an adversary's data network or the specific technical details of a proposed target are examples of cyberspace-related intelligence requirements. For additional information on information/intelligence requirements, see MCWP 2-2, *MAGTF Intelligence Collections*, and MCWP 2-1, *Intelligence Operations*.

Cyberspace and Information Operations

(FOUO) Information operations is the integrated employment, during military operations, of IRCs in concert with other LOOs to influence, disrupt, corrupt, or usurp the decisionmaking of adversary and potential adversaries while protecting that of friendly forces. The IRCs are tools, techniques, or activities employed across all dimensions of the information environment that can be used to create effects and operationally desirable conditions. Therefore, cyberspace operations capabilities, offensive or defensive, are IRCs that may be employed to support information operations objectives. For example, cyberspace can be used as a medium to support military information support operations or military deception.

Cyberspace and Electronic Warfare

(FOUO) The existence of the virtual layer of cyberspace is largely dependent on the physical existence of the electromagnetic spectrum (EMS). In terms of tactical military operations, electronic warfare and cyberspace operations can and, to the extent possible, should be mutually supporting. Even in cases in which they are not used synergistically, they must be deconflicted with each other and with other EMS-dependent activities. The overarching goal of electronic warfare is to enable commanders to gain and maintain freedom of action across the physical domains and the information environment (which includes cyberspace), through control of the EMS. Control of the EMS is achieved by the effective management and coordination of friendly EMS-dependent systems, such as communications and ISR, while countering and exploiting adversary systems.

(FOUO) Electronic warfare, which includes electronic warfare support, electronic attack, and electronic protection, are all the military activities conducted within the EMS to influence the operational environment in support of the commander's objectives. In practical terms, electromagnetic spectrum operations (EMSO) merge electronic warfare with spectrum management and closely coordinates the efforts of EMS-reliant disciplines, particularly SIGINT, cyberspace operations, space operations, and information operations. Electromagnetic spectrum operations do not replace electronic warfare and spectrum management; instead, EMSO align the two disciplines most responsible for transmissions across the EMS. Additionally, EMSO support management of EMS collections and the requirement to accurately characterize the electromagnetic operational environment. It supports integration with cyberspace operations as well as space and information operations and encourages operational synchronization between mission-essential, EMS-reliant disciplines in support of commander's objectives.

(FOUO) Technological advances continually redefine how operations within cyberspace and the EMS converge. Payloads, techniques, and tactics are rapidly created and rendered obsolete, while the processes by which these capabilities are planned, requested, approved, and employed evolve at a much slower pace. To maintain operational tempo and leverage combined arms to the greatest extent, the Marine Corps employs the MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC). The CEWCC concept originates from the traditional Electronic Warfare Coordination Cell but with additional capability for planning, requesting, and/or coordinating organic and external support for cyberspace operations. The CEWCC is the principal means for the commander to plan, coordinate, synchronize, and deconflict operations in and through the EMS and cyberspace, and assess their potential impacts on the electromagnetic operational environment and cyberspace, respectively. By leveraging the staff section's expertise and relationships in an integrated planning process, the CEWCC can enhance collaborative decision support and feedback, reduce apparent cyberspace/EMS technical complexity, and enhance nonorganic capabilities and reachback support.

This Page Intentionally Left Blank

CHAPTER 4
EMERGING CAPABILITIES

New organizations and network architecture efforts have been established within DOD to address the challenge of cyberspace operations. Emerging capabilities that will significantly increase the Marine Corps' capacity to conduct cyberspace operations include Cyber Mission Force, MAGTF Cyberspace and Electronic Warfare Coordination Cell, and the Joint Information Environment.

Cyber Mission Force

(FOUO) On 11 December 2012, the Deputy Secretary of Defense's Management Action Group approved the cyberspace force presentation model with implementation that began in 2013. This model builds upon existing cyberspace forces, such as Service computer network defense service providers and network operations and security centers. It establishes the DOD cyberspace mission force, which contains national mission teams (NMTs), combat mission teams, combat support team, and cyber protection teams. The Marine Corps, through MARFORCYBER, has been tasked to provide 13 teams: 1 NMT, 3 combat mission teams, 1 combat support team, and 8 cyber protection teams by fiscal year 2016.

National Mission Team

(FOUO) An NMT is a USCYBERCOM force constituted and designated by Commander, USCYBERCOM. The NMT is supported by the National Security Agency/Central Security Service. It consists of dedicated offensive and defensive operators, analysts, planners, targeteers/fires planners and leadership to conduct planned operations to meet mission needs for a specific problem set and to rapidly evaluate, decide, and take action in response to unexpected and dynamic situations in cyberspace. The NMTs are reinforced by intelligence support teams, which provide additional capacity in the form of analysis, linguistics, reporting, capability tool development, and targeting. These teams are prepared to defend the nation in response to a foreign hostile action or imminent threats in cyberspace.

Combat Mission Team

(FOUO) The combat mission team provides combatant command support and, when authorized, assists the delivery of cyberspace effects against combatant command prioritized targets.

Combat Support Team

(FOUO) The combat support team will support the combat mission team to provide additional levels of analysis and fusion of all-source intelligence, planning, capability development, and, when directed, conduct of OCO.

Cyber Protection Team

(FOUO) The cyber protection team focuses on protecting the Department of Defense information networks and, when authorized and directed, may support other US government networks and the Nation's critical infrastructure. A cyber protection team consists of personnel organized under a leadership element with subelements task-organized around mission requirements. Each member is trained to execute DCO to sustain cyberspace superiority against nation state and asymmetric threats within cyberspace.

MAGTF Cyberspace and Electronic Warfare Coordination Cell

The CEWCC coordinates the integrated planning, execution, and assessment of cyberspace and EMS actions across the MAGTF's operational environment to increase operational tempo and achieve military advantage. To perform this primary function, the CEWCC is placed within the MAGTF at the commander's discretion, but should be established within the command element S-3/G-3 in order to ensure it can support all phases of the commander's scheme of maneuver with EMSO and cyberspace operations. Such operations can be complex, technical, highly classified, and may have global consequences. Wherever the CEWCC exists, it is responsible for coordinating across principal staff sections (e.g., G-2/S-2, G-3/S-3, G-6/S-6), major subordinate commands, major subordinate elements working groups, boards, bureaus, and higher headquarters to enhance the integration of cyberspace and EMS-dependent capabilities applicable to all warfighting functions and MAGTF objectives.

During planning, the CEWCC supports the development of the MAGTF's scheme of maneuver, concept of fires support, and appropriate detailed plans and annexes. During mission execution, the CEWCC supports coordinated actions in cyberspace and the EMS by providing enhanced collaborative decision support and visualization tools to MAGTF staff sections and those organizations responsible for planning and employing various cyberspace- and EMS-dependent capabilities. The CEWCC concept is consistent with emerging joint doctrine for EMSO and performs the function of the traditional electronic warfare coordination cell, but with additional planning and coordination considerations for relevant cyberspace operations and EMS management functions performed by the G-2/S-2 and G-6/S-6.

In this capacity, CEWCC planners will often support these staff sections, as well as the information operations working group, the radio battalion detachment, and unmanned aerial system planners. Summarizing the aforementioned actions, the CEWCC performs the following basic organizational tasks to enhance MAGTF mission accomplishment:

- Enhance collaborative decision support and feedback.
- Reduce apparent cyberspace/EMS technical complexity.
- Enhance nonorganic capabilities and reachback support.

Joint Information Environment

In November of 2011, the Commander, USCYBERCOM briefed the Joint Chiefs of Staff on the risk associated with the inability to "see" the entire DOD network in order to protect and defend it and made recommendations to consolidate information technology infrastructure to improve effectiveness. In response, the Joint Chiefs of Staff directed the J-6 and USCYBERCOM to work with the DOD chief information officer to develop a joint information environment. The overarching concept of the Joint Information Environment was to develop and engineer a network architecture with enduring flexibility to support existing and future capabilities identified by components and other future department programs. The objective is to provide a secure joint information environment, consisting of shared information technology infrastructure, enterprise services, and single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security, and realize information technology efficiencies. The joint information environment will be operated and managed per the *Unified Command Plan* using enforceable standards, specifications, and common tactics, techniques, and procedures.

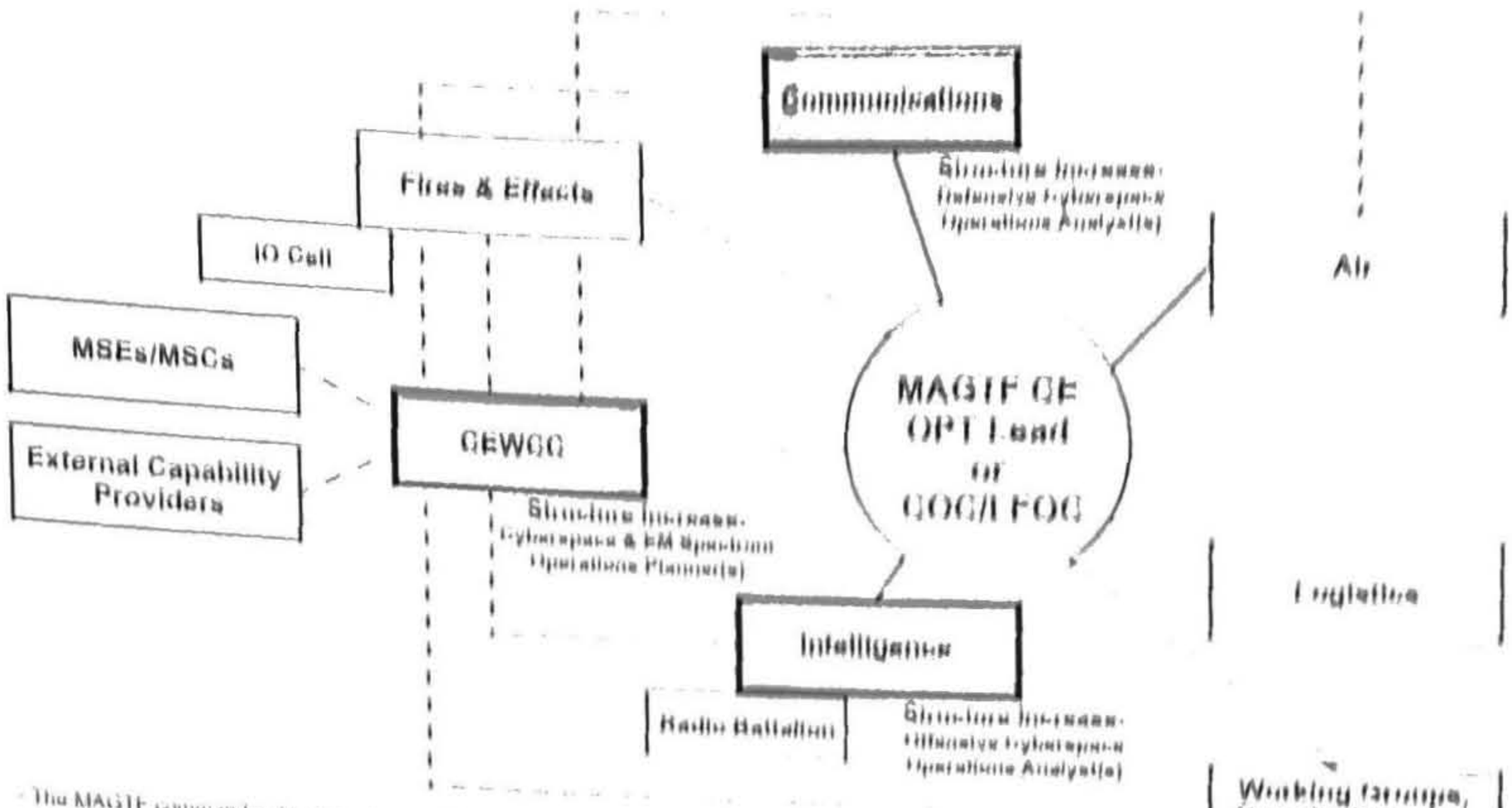

Figure 4-1. Cyberspace and Electronic Warfare Coordination Cell Coordination Diagram.

This Page Intentionally Left Blank

GLOSSARY

SECTION I. ACRONYMS

CCDR . . . . . combatant commander
CCIR . . . . . commander's critical information requirement
CCMD . . . . . combatant command
CEWCC . . . . . Cyberspace and Electronic Warfare Coordination Cell
COA . . . . . course of action
CONOPS . . . . . concept of operations

DCO . . . . . defensive cyberspace operations
DIRINT . . . . . director of intelligence (USMC)
DOD . . . . . Department of Defense
DODIN . . . . . Department of Defense information networks

EMS . . . . . electromagnetic spectrum
EMSO . . . . . electromagnetic spectrum operations

FOUO . . . . . for official use only

G-2 . . . . . assistant chief of staff, intelligence
G-3 . . . . . assistant chief of staff, operations
G-6 . . . . . assistant chief of staff, communications system

IOWG . . . . . information operations working group
IPB . . . . . intelligence preparation of the battlespace
IR . . . . . intelligence requirement
IRC . . . . . information-related capability
ISR . . . . . intelligence, surveillance, and reconnaissance

J-6 . . . . . communications system directorate of a joint staff; command, control, communications, and computer systems staff section
JP . . . . . joint publication
JWICS . . . . . Joint Worldwide Intelligence Communications System

LOO . . . . . line of operation

MAGTF . . . . . Marine air-ground task force
MARFORCYBER . . . . . United States Marine Corps Forces, Cyber Command
MCEN . . . . . Marine Corps enterprise network
MCICOM . . . . . Marine Corps Installation Command
MCNOSC . . . . . Marine Corps Network Operations and Security Center
MCPP . . . . . Marine Corps Planning Process
MCWP . . . . . Marine Corps warfighting publication
MEF . . . . . Marine expeditionary force
MEU . . . . . Marine expeditionary unit
MITSC . . . . . Marine Air-Ground Task Force Information Technology Support Center
MOE . . . . . measure of effectiveness
MOP . . . . . measure of performance
MOS . . . . . military occupational specialty

NMT . . . . . national mission team

OCO . . . . . offensive cyberspace operations
OPCON . . . . . operational control
OPE . . . . . operational preparation of the environment

RAP . . . . . review and approval process
RNOSC . . . . . Regional Network Operations and Security Center
ROE . . . . . rules of engagement

S-2 . . . . . intelligence officer
S-3 . . . . . operations officer
S-6 . . . . . communications system officer
SCI . . . . . sensitive compartmented information
SIGINT . . . . . signals intelligence

TFSMS . . . . . Total Force Structure Management System

USCYBERCOM . . . . . United States Cyber Command
USSTRATCOM . . . . . United States Strategic Command

SECTION II. TERMS AND DEFINITIONS

electromagnetic spectrum operations—The totality of military activities conducted within the EMS to influence the operational environment in support of the commander's objectives. Also called **EMSO**.

electronic attack—A division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 1-02)

electronic protection—A division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

electronic warfare support—A division of electronic warfare involving actions tasked by, or under direct control of operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 1-02)

information environment—The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

operational environment—A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 1-02)

operational preparation of the environment—The conduct of activities in likely or potential areas of operations to prepare and shape the operational environment. Also called **OPE**. (JP 1-02)

target—1. An entity or object that performs a function for the adversary considered for possible engagement or other action. (JP 1-02, part 1 of a 4-part definition)

REFERENCES AND RELATED PUBLICATIONS

Federal Publications

Presidential Policy Directive (PPD) 20, U.S. Cyber Operations Policy
United States Code, Title 10, Armed Forces
United States Code, Title 50, War and National Defense

Department of Defense Directive (DODD)

8500.1 Information Assurance

Chairman of the Joint Chiefs of Staff Publications

Chairman of the Joint Chiefs of Staff Manuals (CJCSMs)
3122.07_ IJSTO Supplement to Joint Operation Planning and Execution System (JOPES) Volume I (Planning, Policies, and Procedures)
3122.08_ IJSTO Supplement to Joint Operational Planning and Execution System (Volume II) Planning Formats and Guidance
3139.01_ Review and Approval Process for Cyberspace Operations (U)
3150.07_ Joint Reporting Structure for Cyberspace Operations Status
3213.02_ Joint Staff Focal Point Program
6510.01_ Cyber Incident Handling Program

Chairman of the Joint Chiefs of Staff Instructions (CJCSIs)
5810.01D Implementation of the DOD Law of War Program
6510.01D Information Assurance (IA) and Computer Network Defense (CND)

Joint Publications (JPs)

1-02 Department of Defense Dictionary of Military and Associated Terms
1-04 Legal Support to Military Operations
2-01.3 Joint Intelligence Preparation of the Operational Environment
3-0 Joint Operations
3-12 Cyberspace Operations
3-13 Information Operations
3-13.1 Electronic Warfare
3-60 Joint Targeting
6-0 Joint Communications System

Marine Corps Publications

Marine Corps Doctrinal Publication (MCDP)
1-0 Marine Corps Operations

Marine Corps Warfighting Publications (MCWPs)
3-40.3 Communications and Information Systems
3-43.3 Marine Air-Ground Task Force Fires
2-1 Intelligence Operations
2-2 MAGTF Intelligence Collection
2-22 Signals Intelligence
5-1 Marine Corps Planning Process

Marine Corps Reference Publications (MCRPs)
3-16C Tactics, Techniques and Procedures for Fire Support for the Combined Arms Commander
3-16.6A Multi-Service Tactics, Techniques, and Procedures (MTTP) for the Joint Application of Firepower (JFIRE)

Marine Corps Orders (MCOs)
3100.4 Cyberspace Operations
5230.21 Information Technology Portfolio Management
5239.2A Marine Corps Cybersecurity Program (MCCSP)

Miscellaneous
Marine Corps Regional NETOPS Tasking and Reporting Structure, 30 July 2012
United States Marine Forces Cyberspace Command Campaign Plan (FY 12-15)
MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept

Miscellaneous

Capstone Concept for Joint Operations
Department of Defense Strategy for Operating in Cyberspace
Execute Order to Implement Cyberspace Operations Command and Control (C2) Framework, 21 June 2013
Joint Concept for Cyberspace (USSTRATCOM)
Unified Command Plan
United States Strategic Command's Joint Test and Evaluation [Activity] published Joint Non-Kinetic Effects Integration Tactics, Techniques, and Procedures (TTP)

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu