FM 3-12

CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

APRIL 2017

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited

HEADQUARTERS, DEPARTMENT OF THE ARMY

SUPERCESSION STATEMENT: This publication supersedes FM 3-38, dated 12 February 2014.

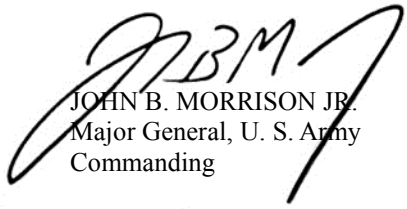
FOREWORD

Over the past decade of conflict, the U.S. Army has deployed the most capable communications systems in its history. U.S. forces dominated cyberspace and the electromagnetic spectrum (EMS) in Afghanistan and Iraq against enemies and adversaries lacking the technical capabilities to challenge our superiority in cyberspace. However, regional peers have since demonstrated impressive capabilities in a hybrid operational environment that threaten the Army's dominance in cyberspace and the EMS.

The Department of Defense information network-Army (DODIN-A) is an essential warfighting platform foundational to the success of all unified land operations. Effectively operating, securing, and defending this network and associated data is essential to the success of commanders at all echelons. We must anticipate that future enemies and adversaries will persistently attempt to infiltrate, exploit, and degrade access to our networks and data. A commander who loses the ability to access mission command systems, or whose operational data is compromised, risks the loss of lives and critical resources, or mission failure. In the future, as adversary and enemy capabilities grow, our ability to dominate cyberspace and the EMS will become more complex and critical to mission success.

Incorporating cyberspace electromagnetic activities (CEMA) throughout all phases of an operation is key to obtaining and maintaining freedom of maneuver in cyberspace and the EMS while denying the same to enemies and adversaries. CEMA synchronizes capabilities across domains and warfighting functions and maximizes complementary effects in and through cyberspace and the EMS. Intelligence, signal, information operations (IO), cyberspace, space, and fires operations are critical to planning, synchronizing, and executing cyberspace and electronic warfare (EW) operations. CEMA optimizes cyberspace and EW effects when integrated throughout Army operations.

FM 3-12 defines and describes the tactics to address future challenges while providing an overview of cyberspace and EW operations, planning, integration, and synchronization through CEMA. It describes how CEMA supports operations and the accomplishment of commander's objectives, and identifies the units that conduct these operations. Due to the rapidly evolving cyberspace domain, the Cyber COE will review and update FM 3-12 and supporting publications on a frequent basis in order to keep pace with a continuously evolving cyberspace domain.



JOHN B. MORRISON JR.
Major General, U. S. Army
Commanding

This page intentionally left blank.

Field Manual
No. 3-12

Headquarters
Department of the Army
Washington, DC, 11 April 2017

CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

Contents

This publication supersedes FM 3-38, dated 12 February 2014.

Figures

Tables

Preface

FM 3-12 provides tactics and procedures for the coordination and integration of Army cyberspace and electronic warfare operations to support unified land operations and joint operations. FM 3-12 explains Army cyberspace and electronic warfare operations fundamentals, terms, and definitions. This publication provides overarching guidance to commanders and staffs on Army cyberspace and electronic warfare operations at all echelons.

The principal audience for FM 3-12 is all members of the profession of arms. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and in some cases host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate according to the law of war and the rules of engagement. (See FM 27-10.)

FM 3-12 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which FM 3-12 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Terms and definitions for which FM 3-12 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

FM 3-12 applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent of FM 3-12 is the United States Army Cyber Center of Excellence. The preparing agency is the Cyber Center of Excellence Doctrine Division, United States Army Cyber Center of Excellence. Send comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-ID (FM 3-12), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735; by E-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil.

Introduction

FM 3-12 provides overarching doctrinal guidance and direction to the Army for conducting cyberspace and electronic warfare (EW) operations using cyberspace electromagnetic activities (CEMA) in unified land operations. FM 3-12 defines and provides an understanding of Army cyberspace operations, EW, title authorities, roles, relationships, responsibilities, and capabilities to support Army and joint operations. It expands upon the methods by which Army forces approach the defense of Army networks and data and addresses the opportunities commanders have to integrate tailored cyberspace and EW capabilities across the range of military operations.

FM 3-12 nests with and supports joint cyberspace and EW operations doctrine and ADRP 3-0, Operations, and provides the doctrinal context to address the relationship among ADRP 5-0, The Operations Process, and cyberspace and EW operations. To understand the fundamentals of integrating and synchronizing cyberspace and EW operations, ADP 2-0, ADRP 2-0, ADP 3-0, ADRP 3-0, ADP 5-0, ADRP 5-0, ADP 6-0, ADRP 6-0, ATP 2-01.3, FM 3-13, and FM 6-0 must first be read. CEMA, by planning, integrating, and synchronizing cyberspace and EW operations, integrates functions and capabilities across warfighting functions, defends the network, and provides critical capabilities for commanders at all levels during unified land operations. Cyberspace and EW operations affect, and are affected by, all of the warfighting functions.

This FM provides detail on tactics and procedures for Army cyberspace and EW operations. This FM supersedes FM 3-38, dated February 2014. FM 3-12 is the proponent for Army cyberspace and EW operations. This FM includes the fundamentals and guiding principles for cyberspace operations, EW, and CEMA in one publication. It provides a cohesive and coherent description of how they support and enable operations as well as other mission tasks and functions at each echelon. This FM sets the basis for the subordinate Army techniques publications.

Cyberspace and EW operations are integrated into operations using already established joint and Army processes such as the intelligence process, targeting, and the military decision-making process (MDMP). This FM explains the fundamental ideas of Army cyberspace and EW operations. This includes the staff responsibilities, contributions to the MDMP, targeting in cyberspace and the EMS, the reliance on intelligence and operational preparation of the environment (OPE) in cyberspace.

This FM describes the cyberspace operations, missions, actions, EW, the electromagnetic spectrum (EMS), and the interrelation of these activities among each other and all Army operations. The description includes CEMA as the planning, integrating and synchronizing activity for echelons corps and below.

Chapter 1 provides an understanding of cyberspace, cyberspace operations, missions, actions, and effects. It describes cyberspace and situational understanding and awareness, threats, risks, vulnerabilities and its relationship with the information and operational environment. The chapter describes the layers and characteristics of cyberspace and identifies the legal authorities that apply to cyberspace and cyberspace operations. Chapter 1 includes the fundamental information of EW and spectrum management functions as they relate to cyberspace and EW operations.

Chapter 2 provides information on operations and missions that use cyberspace for more than daily business. Information operations, intelligence, space operations, and targeting may affect cyberspace, the EMS, cyberspace operations, and EW operations. Commanders and staffs integrate and synchronize cyberspace and EW operations with these during all phases of operations.

Chapter 3 describes Army CEMA and mission command, the commanders' role, cyberspace and EW operations with the warfighting functions, and the commanders' resources that have effects on, in, and through cyberspace and the EMS. This chapter discusses how cyberspace and EW operations planning factors into the operations process. This includes planning, preparing, executing, assessing, and targeting. The discussion of the operational environment is combined with the MDMP followed by an overview of preparation requirements, execution tactics, and how to assess cyberspace and EW operations.

Appendix A discusses cyberspace operations and the various unified action partners.

Appendix B highlights the location of cyberspace operations information in operations orders and appendix 12 to Annex C. This appendix includes an example of Appendix 12 to Annex C with a description of the types of information included in this appendix and various sections.

Appendix C includes procedures for processing cyberspace effects requests at echelons corps and below, echelons above corps, and the cyber effects request format (CERF) fields and information. A blank copy of the CERF and an explanation of the fields are part of the procedures.

Appendix D includes the electronic attack request format (EARF) fields and information. A blank copy of the EARF and 5-line briefing with an explanation of the fields are part of the procedures.

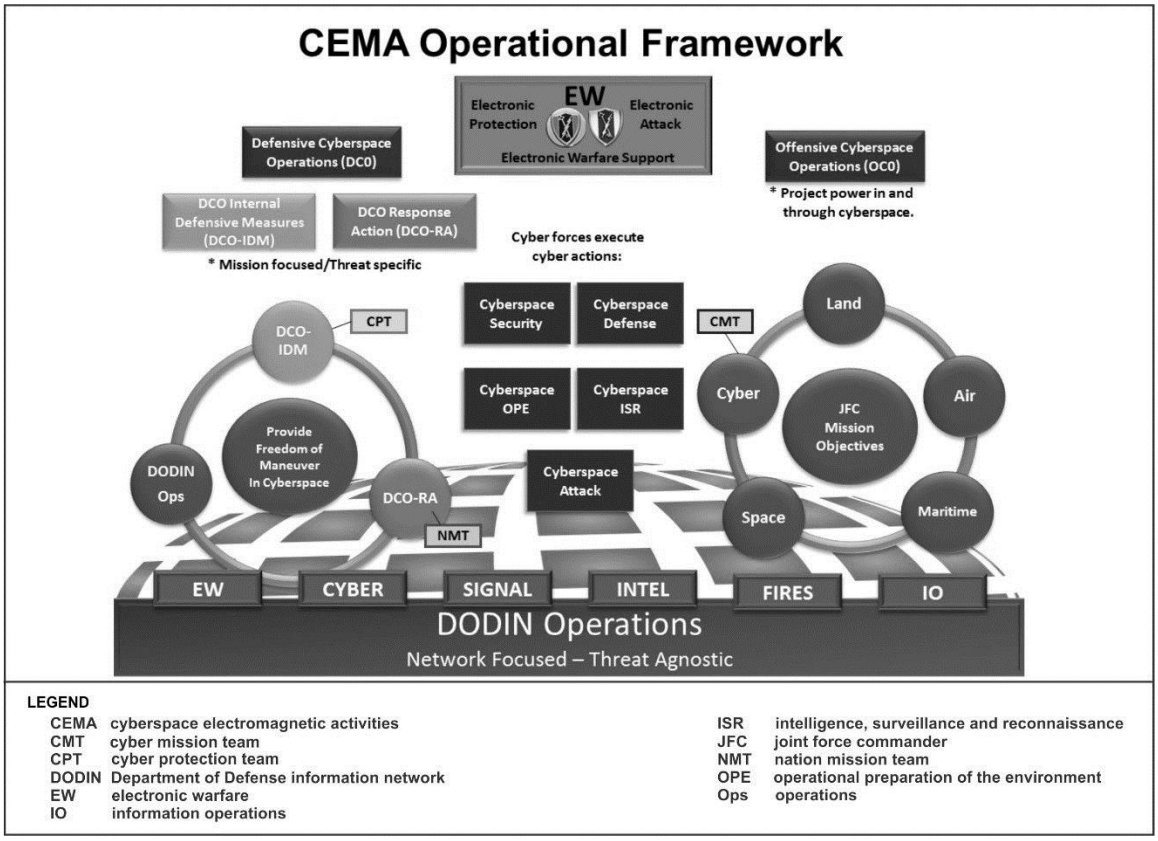


Figure Introduction-1. Cyberspace electromagnetic activities operational framework

Chapter 1

Cyberspace and Electronic Warfare Operations Fundamentals

This chapter introduces cyberspace and electronic warfare operations. Section one is an overview of cyberspace and the electromagnetic spectrum. Section two delivers a foundation for understanding cyberspace and environments. Section three describes electronic warfare operations.

1-1. Superiority in cyberspace and the electromagnetic spectrum (EMS) provides a decisive advantage to commanders at all levels in modern combat. The Army's ability to exploit cyberspace and EW capabilities will prove critical to the success of unified land operations. As cyberspace and EW operations develop similar and complementary capabilities, the Army must plan, integrate, and synchronize these operations with unified land operations.

1-2. Employing cyberspace and EW capabilities under a single planning, integration, and synchronization methodology increases the operational commander's ability to understand the environment, project power, and synchronize multiple operations using the same domain and environment. Synchronizing offensive and defensive activities allows a faster response to enemy and adversary actions. The EMS is the common denominator for both cyberspace and EW operations, and also impacts every operation in the Army.

1-3. The distinctions between cyberspace and EW capabilities allow for each to operate separately and support operations distinctly. However, this also necessitates synchronizing efforts to avoid unintended interference. Any operational requirement specific to electronic transfer of information through the wired portion of cyberspace must use a cyberspace capability for affect. If the portion of cyberspace uses only the EMS as a transport method, then it is an EW capability that can affect it. Any operational requirement to affect an EMS capability not connected to cyberspace must use an EW capability.

1-4. The Department of Defense information network-Army (DODIN-A) is the Army's critical warfighting platform, which enables mission command, precision fires, intelligence, logistics, and tele-medicine, and supports all operations. (See paragraph 1-25 for additional information on DODIN-A.) Access to the DODIN-A allows commanders to project combat power, conduct support operations, and achieve joint and Army force commander objectives. Securing and operating this expansive network is one of the most complex and important operations the Army currently undertakes. A single vulnerability within this network can place units and operations at risk, potentially resulting in mission failure. Understanding how to operationalize cyberspace and the EMS is a fundamental staff proficiency and commander's priority.

1-5. Superiority in cyberspace and the EMS to support Army operations results from effectively synchronizing Department of Defense information network (DODIN) operations, offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), electronic attack, electronic protection, electronic warfare support, and spectrum management operations (SMO). *Cyberspace electromagnetic activities* is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0). Through CEMA, the Army plans, integrates, and synchronizes these missions, supports and enables the mission command system, and provides an interrelated capability for information and intelligence operations.

1-6. Cyberspace and the EMS will likely grow increasingly congested, contested, and critical to successful unified land operations. Success will be measured by the ability to execute operations freely in cyberspace and the EMS, while controlling the ability of others to operate in the domain.

1-7. Rapid developments in cyberspace and the EMS will challenge any assumptions of the Army's advantage in this domain. While it cannot defend against every kind of intrusion, the Army must take steps to identify, prioritize, and defend its most important networks and data. Commanders and cyberspace

operations experts must also adapt quickly and effectively to enemy and adversary presence inside cyberspace systems.

1-8. Protecting the DODIN and friendly EMS includes controlling communication signatures in the EMS. There is a correlation to activities in cyberspace and those in the EMS. Current communications systems transfer data in the EMS as one of the transport methods, leaving signatures of activities. Identifying, attributing, and affecting the activity (in or through cyberspace or the EMS) can have detrimental effects on the operations of the entity attempting to communicate. Commanders stand to gain an advantage over an enemy or adversary by maintaining superiority in cyberspace and the EMS, whereas the reverse can threaten friendly systems if the proper security, defense, and protection measures are not in place.

SECTION I – OVERVIEW OF CYBERSPACE AND THE ELECTROMAGNETIC SPECTRUM

1-9. Section 1 is an overview of cyberspace including the cyberspace domain, operations, missions, and actions, covering effects in cyberspace and the difference between joint and Army effects terminology. This section includes information about the EMS and SMO.

THE CYBERSPACE DOMAIN

1-10. *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 (JP 3-12[R]). The Army performs cyberspace operations and supporting activities within this domain as part of joint and Army operations. Friendly, enemy, adversary, and host nation networks, communications systems, computers, cellular phone systems, social media Web sites, and technical infrastructures are all part of cyberspace. *Cyberspace operations* are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). The interrelated cyberspace missions are DODIN operations, DCO, and OCO. A cyberspace capability is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (See JP 3-12[R] for more information.) Figure 1-1 on page 1-3 is a visual representation of cyberspace and use of the EMS in an operational environment.

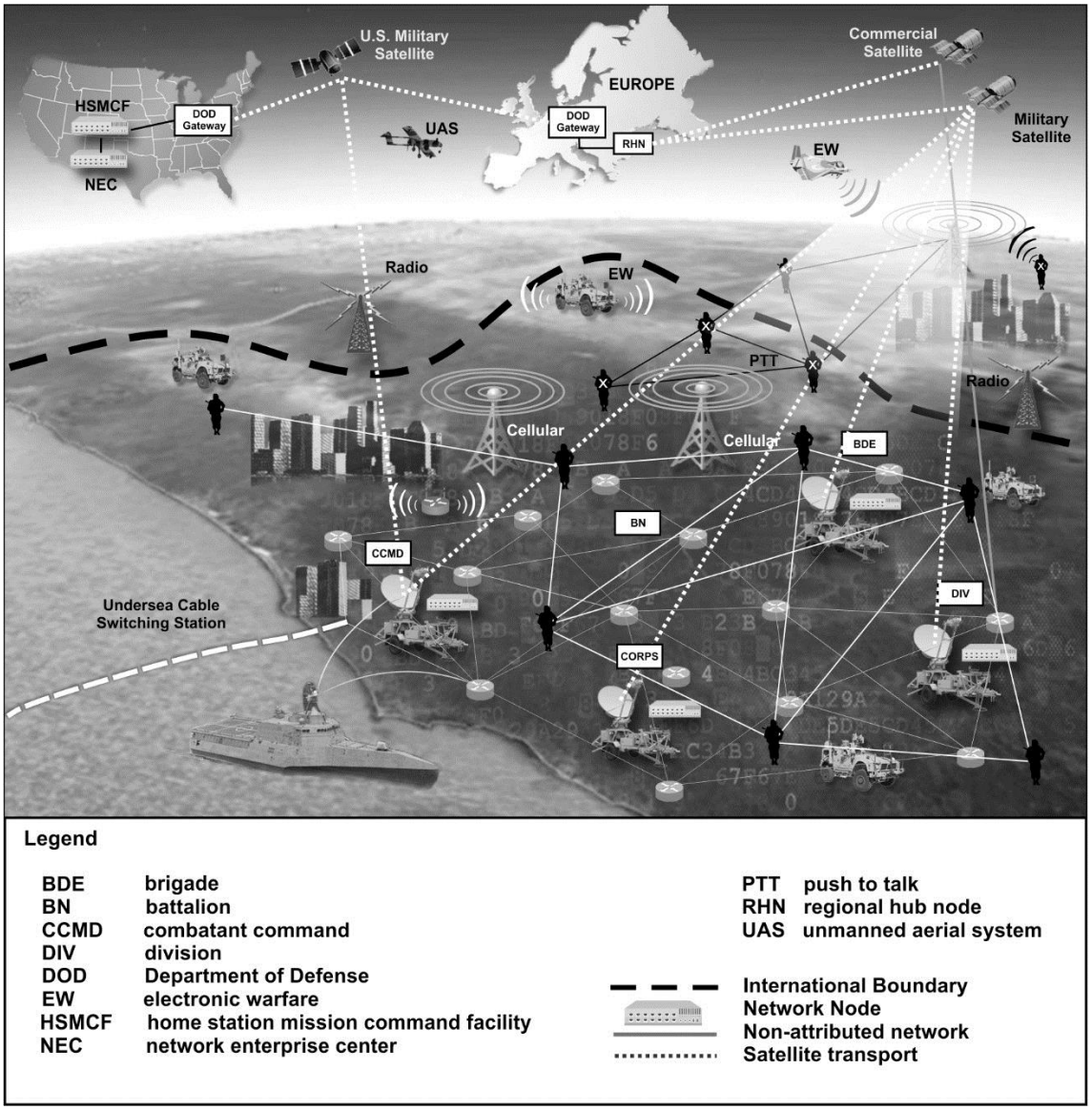


Figure 1-1. Visualization of cyberspace and the electromagnetic spectrum in an operational environment

1-11. Cyberspace and the EMS are essential for Army operations and are inherently joint, inter-organizational, multinational, and commercial. All Army operations, missions, activities, and functions use cyberspace. *Cyberspace superiority* is the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an enemy or adversary (JP 3-12[R]). Cyberspace superiority enables, supports, provides, and facilitates warfighting capabilities that affect, support, and enable every warfighting function and daily activity.

Note. For clarity, the Army reserves the use of the term 'cyber' for the naming convention of commands and organizations. For the Army, the full term 'cyberspace' is correct to explain the domain, activities, effects, actions and when referring to capabilities in the cyberspace domain. The Army uses Department of Defense (DOD) established terms that may not follow this principle.

1-12. Although cyberspace coexists with the other domains, it is a separate domain. Cyberspace pervades the land, air, maritime, and space domains through the EMS and wired networks. Cyberspace enables integration across physical domains by moving data along transmission paths through links and nodes in cyberspace and the EMS. The man-made aspects of cyberspace, coupled with continual advances in technologies, contribute to a continuous obligation to manage risk and protect portions of cyberspace. (For more information on the EMS and its management, see section two.)

1-13. Cyberspace enables and enhances the ability of commanders to perform mission command. The DODIN is the DOD's portion of cyberspace and is distinct in that it provides the medium for communication among the forces within other operational domains. The *Department of Defense information network* is the set of information capabilities, and associated processes to collect, process, store, disseminate, and manage information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems (JP 6-0). The DODIN includes all DOD information technologies broadly grouped as DOD information systems, platform information technology, information technology services, and information technology products.

1-14. The Army uses the cyberspace domain every day to communicate, store data, plan missions, and perform tasks. In today's dynamic operational environment, the exercise of mission command depends on freedom of maneuver within the cyberspace domain.

OPERATIONS AND THE CYBERSPACE DOMAIN

1-15. Army operations depend on cyberspace for synchronizing, storing, coordinating, and protecting information. Commanders rely on cyberspace to exercise mission command. In the 2014 Army's Strategic Planning guidance, the Secretary of the Army and Army Chief of Staff jointly stated:

> *"Similar to other domains, Army leaders and organizations must be capable of employing capabilities in cyberspace, but not to the point of dependency should those capabilities be negated. This convergence between land and cyberspace has created dependencies and vulnerabilities for the Army's ability to exercise mission command through the Army network. The Army will prioritize the defense of its network and key systems against increasingly sophisticated and evolving threats in order to retain freedom of maneuver and exploit its advantages. As the Army addresses these challenges, it will build cyberspace capabilities that are integrated within a [j]oint construct, but also include integration with Army units down to the tactical edge. Finally, when authorized, the Army must be prepared to plan and conduct cyberspace operations in support of national, joint, and Service requirements."*

1-16. Freedom of maneuver in cyberspace enables mission command and freedom of maneuver in the other domains. By enabling mission command and the freedom of maneuver, Army operations support the joint force commander (JFC) objectives. (See figure 1-2 on page 1-5.)

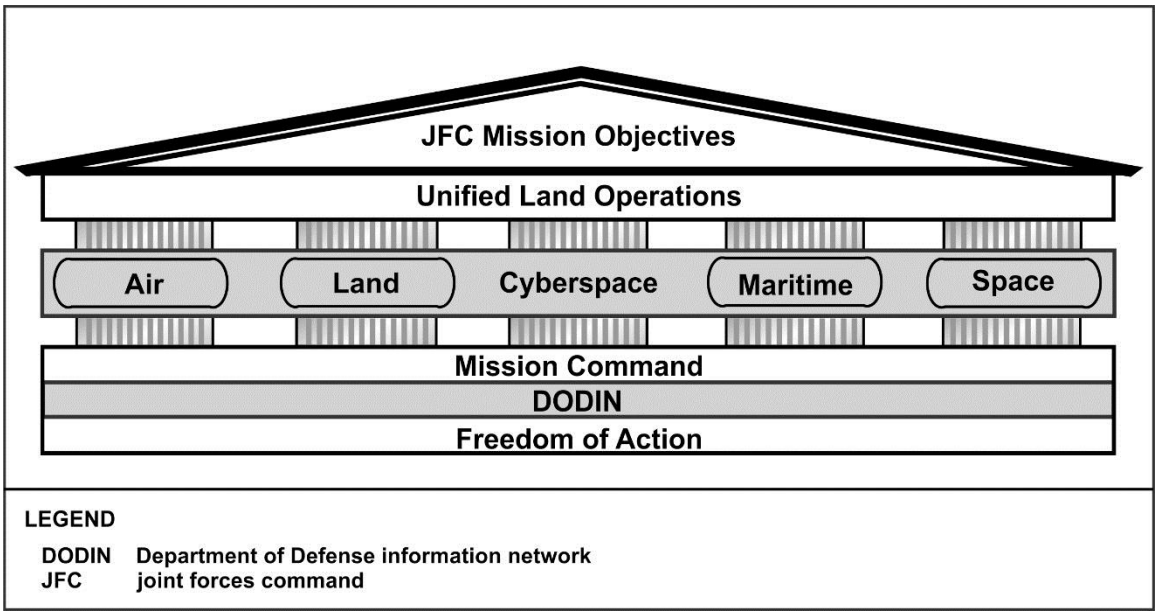


Figure 1-2. Freedom of maneuver to support joint force commander objectives

JOINT OPERATIONS AND THE CYBERSPACE DOMAIN

1-17. The DODIN supports the end-to-end communications systems for joint command and control of military operations and the joint communications use of the cyberspace domain. The DODIN represents the DOD portion of cyberspace and includes joint and Service data communications as well as interfaces to non-DOD and multinational users.

1-18. Joint cyberspace operations support and enable operations for joint and Service specific organizations. Joint commanders and staffs conduct operations in and through cyberspace to assure U.S. and allied forces freedom of maneuver in all domains to include cyberspace while denying enemies and adversaries the same. Joint commanders use existing theater communications systems that provide theater-wide voice, data, and message connectivity between all components and elements to coordinate activities. Combatant commands establish and manage the theater systems and receive additional capabilities based on operational need.

ARMY OPERATIONS AND THE CYBERSPACE DOMAIN

1-19. Army cyberspace operations range from defensive to offensive. These operations establish and maintain secure communications, detect and deter threats in cyberspace to the DODIN, analyze incidents when they occur, react to incidents, and then recover and adapt while supporting Army and joint forces from strategic to tactical levels while simultaneously denying adversaries effective use of cyberspace and the EMS. The Army contribution to the DODIN is the technical network that encompasses the Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide. Army cyberspace operations provide support to, and receive support from, joint cyberspace operations. The close coordination and mutual support with joint cyberspace operations provides Army commanders and staffs enhanced capabilities for operations.

1-20. The Army plans, integrates, and synchronizes cyberspace operations through CEMA as a continual and unified effort. The continuous planning, integration, and synchronization of cyberspace and EW operations, enabled by SMO, can produce singular, reinforcing, and complementary effects. Though the employment of cyberspace operations and EW differ because cyberspace operates on wired networks, both operate using the EMS.

CYBERSPACE MISSIONS AND ACTIONS

1-21. Cyberspace missions and actions are interrelated; synchronizing and supporting efforts among the cyberspace missions is imperative to maintaining freedom of maneuver in cyberspace. Supporting the cyberspace missions are the cyberspace actions: cyberspace defense; cyberspace intelligence, surveillance, and reconnaissance (ISR); cyberspace OPE; cyberspace attack; and cyberspace security. Cyberspace actions support DODIN operations, DCO, OCO, or any combination thereof. Executing cyberspace actions at any echelon is dependent on authority, capability, and coordination. The actions are interrelated and a cyberspace mission may require more than one action to achieve mission success.

1-22. Army forces can execute cyberspace missions and actions under the proper authority. Since DODIN operations and some DCO tasks may overlap, Army forces may conduct multiple cyberspace missions or actions as part of their daily duties and responsibilities. Situational requirements may dictate the transition from cyberspace security to DCO internal defensive measures (DCO-IDM). Figure 1-3 shows the relationship of the cyberspace missions and cyberspace actions both external and internal to the DODIN and the owned, leased, shared partner portions of cyberspace. EW can affect the cyberspace capabilities that use the EMS.

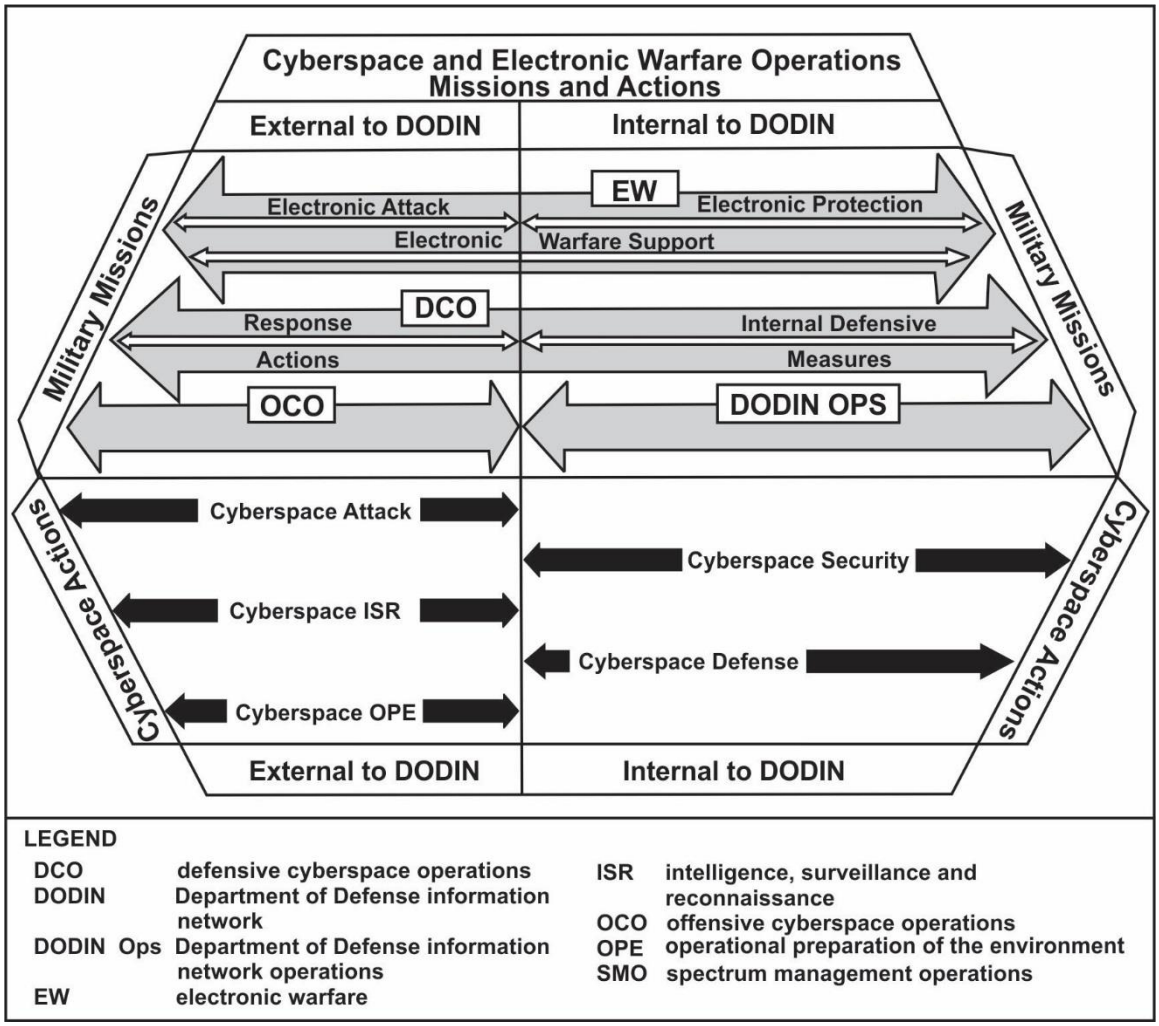


Figure 1-3. Cyberspace and electronic warfare operations - missions and actions

1-23. Use of the DODIN relies upon DODIN operations, DCO, and at times on OCO for freedom of maneuver to employ a network capability. Cyberspace security and DCO protect and defend Army networks, thereby maintaining communications and mission command. Current intrusion information may lead to future defensive cyberspace operations response action (DCO-RA) or OCO missions. DCO and OCO

depends on the DODIN for planning, synchronization, and integration of missions. EW may also support and enable cyberspace operations through electronic attack (EA), electronic protection (EP), and electronic warfare support (ES).

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

1-24. The DODIN includes DOD information technology which cyberspace operations forces must secure and protect to ensure mission assurance for DOD components. The DODIN supports the synchronization and integration of all warfighting functions. Army forces use the DODIN to collaborate internally and externally, move and manage information, transmit and receive orders, and maintain situational awareness.

1-25. The DODIN-A is an Army operated enclave of the DODIN which encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide. The DODIN-A enables mission command and facilitates all warfighting and business functions. The DODIN-A seamlessly supports deployed forces and operations at bases, posts, camps, stations, and other locations worldwide including at the strategic, operational, and tactical levels.

1-26. The DODIN-A enables access to the right information at the right place and time for commanders, staffs, Soldiers, civilians, and joint, inter-organizational, and multinational elements. The DODIN-A allows access while at home station or a temporary duty location; through post, camp, or station networks; and through deployed tactical networks. These segments allow operating and generating forces to access centralized resources from any location during all operational phases. Network support is available at the home post, camp, or station, throughout deployment and on redeployment to home station. The network support may be organic depending on the organization and forces aligned to that organization.

1-27. *Department of Defense information network operations* are operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information network (JP 3-12[R]). DODIN operations are threat agnostic and network specific to provide users and systems at all levels with end-to-end network and information system availability, information protection, and prompt information delivery. DODIN operations allow commanders to effectively communicate, collaborate, share, manage, and disseminate information using automated information systems. The Army conducts distributed DODIN operations within the DODIN-A, from the global level to the tactical edge. DODIN operations personnel design, build, configure, secure, operate, maintain, and sustain global, theater, and tactical portions of the DODIN-A. DODIN operations provide assured and timely network-enabled services to support DOD warfighting, intelligence, and business missions across strategic, operational, and tactical boundaries. DODIN operations provide system and network availability, information protection through defensive tools and procedures, and information delivery. (See FM 6-02 for additional information on DODIN operations.)

DEFENSIVE CYBERSPACE OPERATIONS

1-28. *Defensive cyberspace operations* are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems (JP 3-12[R]). DCO are threat-specific and mission prioritized to retain the ability to use the DODIN. The Army uses a defense-in-depth concept, incorporating a layered approach to defend the network.

1-29. The two types of DCO are DCO-RA and DCO-IDM. Both are threat-specific and defend the DODIN, but the similarity ends with that purpose. DCO-RA is more aligned with OCO in execution, authorities, and techniques supporting the mission. DCO-IDM include mission assurance actions.

1-30. DCO respond to unauthorized activity, alerts, and threat information against the DODIN, and leverages intelligence, counterintelligence, law enforcement, and other military capabilities as required. DCO include outmaneuvering adversaries taking or about to take offensive actions against defended networks, or responding to internal and external cyberspace threats. DCO also include actively hunting for advanced internal threats that evade routine security measures. DCO consist of those actions designed to protect friendly cyberspace from enemy and adversary actions.

1-31. DCO may be a response to attacks, exploitations, intrusions, or effects of malware on the DODIN or other assets that the DOD is directed to defend. Most DCO occur within the defended network. DOD DCO missions are accomplished using a layered, adaptive, defense-in-depth approach, with mutually supporting elements of digital and physical protection. A key characteristic of DOD DCO activities is active cyberspace defense.

1-32. DCO activity may lead to follow on activities such as additional cybersecurity measures, information collection, or development of OCO targets. Reporting unauthorized network activity and anomalies increases the data available to identify trends and to take appropriate defensive measures. The personnel confirming the unauthorized activity report the details for intelligence and forensic purposes.

Defensive Cyberspace Operations Internal Defensive Measures

1-33. DCO-IDM occur within the DODIN. DCO-IDM may involve reconnaissance measures within the DODIN to locate internal threats and may respond to unauthorized activity, alerts, and threat information. Internal threat cueing may come from cybersecurity tools employed on the network. DCO-IDM focus to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks to ensure sufficient cyberspace access for JFC forces.

1-34. Army forces employ various DCO-IDM to protect and defend the DODIN. Army units plan, integrate, and synchronize DCO-IDM to create and achieve actions by friendly forces against the enemy to support the commander's objectives as part of the operations process.

Defensive Cyberspace Operations Response Action

1-35. *Defensive cyberspace operations response action* is defined as deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend DOD cyberspace capabilities or other designated systems (JP 3-12[R]). Provocation that leads to employing DCO-RA includes indicators from the various sensors and capabilities that detect and identify indications of an imminent or ongoing cyberspace attacks. If approved, specially trained cyber mission forces employ actions to protect and defend friendly force cyberspace. Some adversary actions can trigger DCO-RA necessary to defend networks by creating effects outside of the DODIN, when authorized. Some of the specially trained personnel are Army forces operating as part of a joint force.

1-36. DCO-RA requires the same type of information collection support as OCO for threat information. DCO-RA may involve using nondestructive countermeasures that identify the source of the threat to the DODIN-A, and then use nonintrusive techniques to stop or mitigate that threat. Joint forces may provide DCO-RA support to Army commanders at corps and below.

Note. Countermeasures require deconfliction with other departments and agencies to the maximum extent practicable according to the Trilateral Memorandum of Agreement among the DOD, the Department of Justice, and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities, 9 May 2007.

OFFENSIVE CYBERSPACE OPERATIONS

1-37. *Offensive cyberspace operations* are cyberspace operations intended to project power by the application of force in or through cyberspace (JP 3-12[R]). The Army provides forces trained to perform OCO across the range of military operations in and through cyberspace providing effects outside of the DODIN. Army forces conducting OCO do so under the authority of CCMDs and United States Cyber Command (USCYBERCOM).

1-38. Forces conducting OCO missions deconflict, coordinate, and synchronize OCO with other cyberspace operations, cyberspace activities, and other operations. Joint forces may provide OCO support to corps and below Army commanders in response to requests using the CERF. OCO focus on targeting objectives in or through cyberspace and related portions of the EMS. Army units plan, integrate, and synchronize OCO to create and achieve effects to support the commander’s objectives as part of the operations process. OCO targets may require extended planning time, extended approval time, synchronization and deconfliction. The

CERF provides detailed information on requested effects. (For more information on CERF procedures, see Appendix C.)

CYBERSPACE ACTIONS

1-39. The cyberspace missions require the employment of various actions to create specific effects in cyberspace. (See figure 1-4.) The cyberspace actions are cyberspace defense, cyberspace ISR, cyberspace OPE, cyberspace attack, and cyberspace security. To plan for, authorize, and assess these actions, it is important to understand the differences between the actions and their specific purposes. (For more information on the cyberspace actions see JP 3-12[R].)

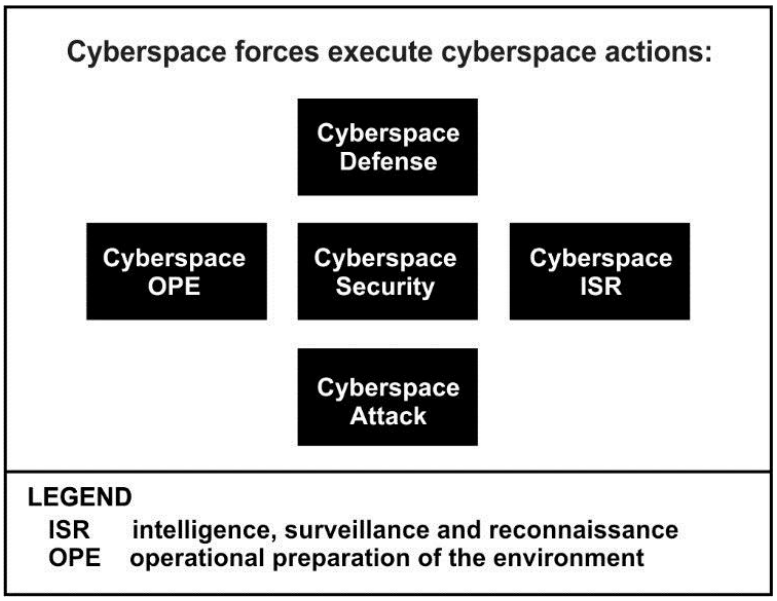


Figure 1-4. Cyberspace actions

Cyberspace Defense

1-40. Cyberspace defense are actions normally taken within the DOD cyberspace for securing, operating, and defending the DODIN against specific threats. The purpose of cyberspace defense includes actions to protect, detect, characterize, counter, and mitigate threats. Such defensive actions are usually created by the JFC or Service that owns or operates the network, except in cases where these defensive actions would affect the operations of networks outside the responsibility of the respective JFC or Service.

Cyberspace Intelligence, Surveillance & Reconnaissance

1-41. Cyberspace ISR is an intelligence action conducted by the JFC authorized by an execute order or conducted by attached signals intelligence (SIGINT) units under temporary delegated SIGINT operational tasking authority. Cyberspace ISR includes activities in cyberspace conducted to gather intelligence required to support future OCO or DCO. These activities support planning and execution of current and future cyberspace operations. Cyberspace ISR focuses on tactical and operational intelligence and on mapping enemy and adversary cyberspace to support military planning. Cyberspace ISR requires appropriate deconfliction and authorization. Cyberspace forces are trained and certified to a common standard with the intelligence community. Cyberspace ISR is conducted pursuant to military authorities and must be coordinated and deconflicted with other United States Government departments and agencies. Army units conducting cyberspace ISR operate as part of a joint force or specially trained service retained forces supporting specific cyberspace operations missions.

Cyberspace Operational Preparation of the Environment

1-42. Cyberspace OPE consists of the non-intelligence enabling activities for the purpose of planning and preparing for ensuing military operations. Cyberspace OPE requires forces trained to a standard that prevents compromise of related intelligence collection operations. OPE in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted with other United States Government departments and agencies.

Cyberspace Attack

1-43. *Cyberspace attack* is a cyberspace action that creates various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial, that is hidden or that manifests in the physical domains (JP 3-12[R]). The purpose of cyberspace attack is the projection of power to provide an advantage in cyberspace or the physical domains for friendly forces. For example, a cyberspace attack may target information residing on, or in transit between, computers or mobile devices to deny enemy or hostile actors the ability to use resources. Cyberspace attack may be for offense or defense operations in cyberspace.

Cyberspace Security

1-44. Cyberspace security actions are those taken within a protected network to prevent unauthorized access to, an exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cyberspace security is not specific to an enemy or adversary. Cyberspace security actions protect the networks and systems through all phases of network planning and implementation. Cyberspace security activities include vulnerability assessment and analysis, vulnerability management, incident handling, continuous monitoring, and detection and restoration capabilities to shield and preserve information and information systems.

EFFECTS OUTSIDE OF THE DEPARTMENT OF DEFENSE INFORMATION NETWORK AND CYBERSPACE

1-45. Effects delivered in and through cyberspace manifest in cyberspace or in one or more of the other domains. The Army requests effects in cyberspace after planning and targeting activities. The effects may be delivered by or through an OCO or DCO-RA mission. The effects support Army operations and JFC objectives. Cyber mission forces conducting cyberspace actions deliver effects in and through cyberspace. EW capabilities can be a conduit to deliver effects in and through cyberspace. Joint organizations express the effects in cyberspace in different terms than expressed in the traditional Army targeting methodology. Army targeting efforts result in requirements using Army terms similar in meaning to joint cyberspace terms. However, the difference in terms requires that any requests from echelons corps and below to joint organizations use the joint terms for effects in cyberspace.

1-46. Joint cyberspace operations doctrine describes cyberspace actions. Cyberspace actions at the joint level require creating various direct denial effects in cyberspace (degradation, disruption, or destruction). Joint cyberspace operations doctrine also explains that manipulation leads to denial (hidden or manifesting) in any domain.

1-47. These specific actions are—

- 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 enemy or adversary use of resources.
- 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.
- Disrupt. To completely but temporarily deny (a function of time) access to, or operation of, a target for a period 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.

- Destroy. To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.
- Manipulate. To control or change the enemy or adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.

1-48. Army commanders request effects using the terms deny, degrade, disrupt, destroy, and manipulate. The Army considers these as separate effects rather than a subset of deny. These terms are common for targeting guidance or to describe effects for information operations (IO). These are desired effects that support operations and are achievable using cyberspace capabilities. Army planners will utilize these terms to describe and plan for cyberspace and electronic warfare effects. The most common effects associated with cyberspace operations are deny, degrade, disrupt, destroy, and manipulate. (For more effects or information on effects see ATP 3-60.)

- *Denial operations* are actions to hinder or deny the enemy the use of space, personnel, supplies, or facilities (FM 3-90-1). An example of deny is to use EW capabilities to jam specific frequencies using an EW capability for a predetermined amount of time, or to block a router communication port using cyberspace capability for some predetermined amount of time; however, the duration of denial will depend on the enemy's ability to reconstitute.
- Degrade is to use nonlethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems and information collections efforts or means. An example of degrade is slowing the cyberspace connection speed affecting the ability to effectively communicate or pass data in a timely manner.
- Disrupt is a tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt the enemy's timetable, or cause enemy forces to commit prematurely or attack in a piecemeal fashion. An obstacle effect that focuses fires planning and obstacle efforts to cause the enemy force to break up its formation and tempo, interrupt its timetable, commit breaching assets prematurely, and attack in a piecemeal effort (FM 3-90-1). An example of disrupt is interrupting the connection to cyberspace, either wired or wireless, affecting the ability to communicate or pass data.
- *Destroy* is tactical mission task that physically renders an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt (FM 3-90-1). Destroy is applying lethal combat power on an enemy capability so that it can no longer perform any function. The enemy cannot restore it to a usable condition without being completely rebuilt. An example of destroy using cyberspace capabilities is causing a system to lose all of its operating information or causing it to overheat to a point it is no longer usable. (See ADRP 3-0 for more information on destroy.)
- *Manipulate* is to control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives. The Army uses the same description as the joint cyberspace action for this effect.
- Deceive is when military leaders attempt to mislead threat decision makers by manipulating their understanding of reality. An example of deceive is modifying a message causing the enemy or adversary to assemble in a location not originally designated by their own chain of command. More information on deceive is found in FM 3-90-1 and ATP 3-60.

1-49. Effects in and through cyberspace may have the same consequences as other types of traditional effects. Effects during operations include lethal and non-lethal actions and may be direct or indirect. Direct effects are first order consequences and indirect effects are second, third, or higher order consequences. Similar characteristics of direct and indirect effects in cyberspace can be cumulative or cascading if desired. These effects are planned and controlled in order to meet the commander's objectives. Cumulative refers to compounding effects and cascading refers to influencing other systems with a rippling effect. The desired effects in cyberspace can support operations as another means to shape the operational environment to provide an advantage. (For more information on cascading and cumulative effects see JP 3-60.)

SECTION II – UNDERSTANDING CYBERSPACE AND ENVIRONMENTS

1-50. Understanding the cyberspace domain begins with understanding the EMS, the information environment, the layers of cyberspace, and the characteristics of cyberspace. Understanding the integration of cyberspace operations begins with comprehending cyberspace as a part of the operational environment and the impact on operational and mission variables: threats, risks, and authorities.

CYBERSPACE AND THE ELECTROMAGNETIC SPECTRUM

1-51. Cyberspace wireless capabilities use the EMS for a transport medium to form links in the DODIN. The *electromagnetic spectrum* is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (JP 3-13.1). The Army manages its use of the EMS through SMO. *Spectrum management operations* are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02). Electromagnetic spectrum operations (EMSO) include SMO and EW (see section three for information on EW). SMO are the management functions of EMSO managing the man-made access to the EMS.

1-52. Conducting SMO supports and enables the execution of cyberspace and EW operations. The objective is to ensure access to the EMS to support Army operations. Synchronizing efforts between cyberspace and EW operations, and other users of the spectrum, allow unifying and complementary efforts and minimizes conflicting effects within the spectrum. (See figure 1-5.) (For more information on SMO see FM 6-02 and ATP 6-02.70.)

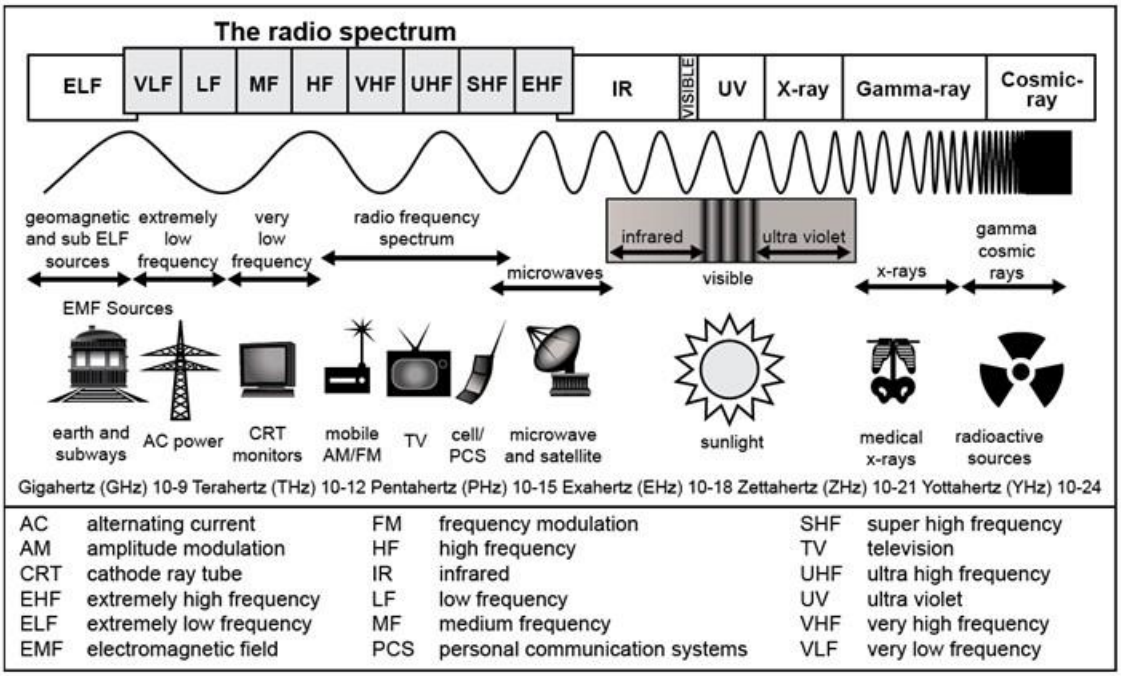


Figure 1-5. The electromagnetic spectrum

CYBERSPACE AND THE INFORMATION ENVIRONMENT

1-53. The Army conducts cyberspace and EW operations in the information environment. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). The ease of access to technical networks facilitates information sharing and enhances the social aspect of the information environment. The dimensions of the information environment

are physical, informational, and cognitive. IO, whether inside or outside of cyberspace, can affect friendly, neutral, and threat operations within cyberspace. (For more information on the information environment see JP 3-13.)

PHYSICAL DIMENSION

1-54. The physical dimension consists of the physical portions of the environment. The tangible elements of cyberspace and access to the EMS are part of the physical dimension of the information environment. The tangible network elements include communications networks, information systems, and network infrastructures. This dimension is where network platforms reside along with the infrastructures that enable them. EW platforms also reside in this dimension.

INFORMATIONAL DIMENSION

1-55. The informational dimension consists of the information itself. Cyberspace and EW operations support collecting, processing, storing, disseminating, and displaying text, images, or data in this dimension. The informational dimension enables the linkage between the physical and cognitive dimensions. This dimension links to cyberspace and the EMS due to the volume of information resident on and traversing information technology infrastructures. The physical dimension of cyberspace and EW operations allows access to and control of the information and data to those in the cognitive dimension. This dimension includes data at rest or in transit.

COGNITIVE DIMENSION

1-56. The *cognitive dimension* encompasses the minds of those who transmit, receive, and respond to or act on information (JP 3-13). The cognitive dimension in cyberspace represents individuals, groups, or organizations. Cyberspace links the data and ideas of those who transmit, receive, respond or act on, or add new information. This dimension represents the individuals that utilize cyberspace.

CYBERSPACE LAYERS

1-57. *Cyberspace* can be described in terms of three layers: physical network, logical network, and cyber-persona (JP 3-12[R]). Commanders and staffs leverage the layers of cyberspace to build, gain, and maintain situational understanding and create operational opportunities.

PHYSICAL NETWORK LAYER

1-58. The physical network layer of cyberspace is comprised of the geographic component and is part of the physical dimension. The geographic component is the location in land, air, maritime, or space where elements of the network reside. The physical network layer is comprised of the hardware, system software, and infrastructure (wired, wireless, cable links, EMS links, satellite, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, switches, servers, and computers). The physical network layer uses logical constructs as the primary method of security and integrity.

LOGICAL NETWORK LAYER

1-59. The logical network layer consists of the components of the network related to one another in a way abstracted from the physical network. For instance, nodes in the physical layer may logically relate to one another to form entities in cyberspace not tied to a specific node, path, or individual. Web sites hosted on servers in multiple physical locations where content can be accessed through a single uniform resource locator or web address provide an example. This may also include the logical programming to look for the best communications route, which is not the shortest physical route, to provide the information requested.

CYBER-PERSONA LAYER

1-60. The cyber-persona layer is a digital representation of an individual or entity identity in cyberspace. This layer consists of the people who actually use the network and therefore have one or more identities that

can be identified, attributed, and acted upon. These identities may include e-mail addresses, social networking identities, other web forum identities, computer internet protocol addresses, and mobile device numbers. One individual may have multiple cyber-personas through internet services at work and personal e-mail addresses, web forum, chat room, and social networking site identities; which may vary in the degree to which they are factually accurate. The authenticity of a cyber-persona is a concern especially with the ability of a threat force to hide their identity.

1-61. Conversely, a single cyber-persona can have multiple users — for example, a username and password for an administrative account multiple people access. As a result cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form. Consequently, attributing responsibility and targeting in cyberspace requires significant intelligence and technical knowledge. Understanding the complexity of the cyber-persona allows leaders and commanders to make more informed decisions. Figure 1-6 shows an individual person with multiple cyber-personas and the relationship with the other layers.

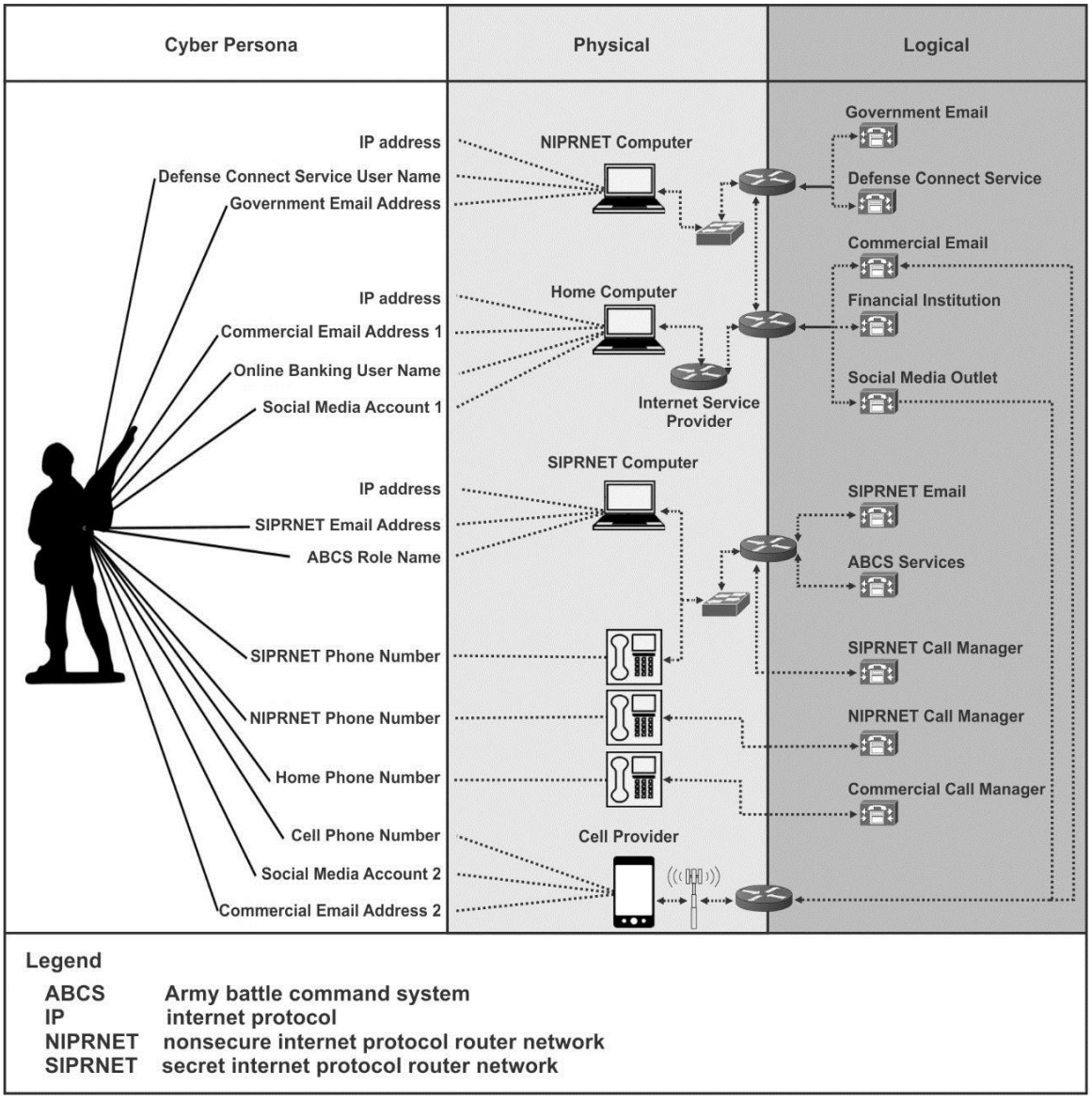


Figure 1-6. Cyber-persona relationship to the physical and logical layers

THE CHARACTERISTICS OF CYBERSPACE

1-62. To better understand cyberspace, examine the physical information technology networks. For instance, cyberspace is interconnected computer communications networks (logical layer) that make information globally available through wired and wireless connections at high rates of speed using the physical layer, which is then accessed by individuals using the cyber-persona layer. The internet pervades societies and enables global communication and information flow. Cyberspace characteristics include—

- Networked.
- Socially enabling.
- Technical.
- Interdependent and interrelated.
- Vulnerable.

NETWORKED

1-63. Cyberspace is an extensive and complex global network of wired and wireless links connecting nodes that permeate every domain. The core of these networks are technological infrastructures consisting of several distinct enclaves connected into a single logical network that enables data transport. Identifying these infrastructures and their operations is accomplished by analyzing the layers of cyberspace, the dimensions of the information environment, the variables of the operational environment, and the other technical aspects of wired and wireless networks. The networks can cross geographic and political boundaries connecting individuals, organizations, and systems around the world.

SOCIALLY ENABLING

1-64. Cyberspace allows interactivity among individuals, groups, organizations, and nation-states. Computer systems and technical networks make it possible to create, store, process, manipulate, and quickly transport data and information for a select or very broad audience. Users can apply data and information to exert influence, accomplish tasks, and make decisions. Text messaging, e-mail, e-commerce, social media, and other forms of interpersonal communication are possible because of cyberspace.

TECHNICAL

1-65. Advancements in technology increase the complexity of hardware and software system components and devices. Cyberspace consists of numerous elements requiring personnel with specific technical skills. For example, the development of encryption and encoding require personnel trained to perform specialized functions that comply with protocols and other industry standards. The technical network infrastructure and logical layer is complex, but accessing and utilizing cyberspace is relatively simple. The advanced use of the EMS is a fundamental part of cyberspace.

INTERDEPENDENT AND INTERRELATED

1-66. Operations within the other four domains are dependent on cyberspace. Commanders achieve situational understanding of the operational environment and the interdependent and interrelated nature of the cyberspace domain through intelligence preparation of the battlefield (IPB) and information requirements. The dependence of information and data distribution, timeliness, and quantity directly relate to the network infrastructure capabilities and limitations. IPB can help identify capabilities and vulnerabilities of the enemy's and adversary's cyberspace infrastructure, including electronic links to automated weapons systems, communications systems, and other critical nodes supporting the threat network. Unique to the cyberspace domain is the ability of combatants and non-combatants to move information across the domain quickly.

VULNERABLE

1-67. Cyberspace is vulnerable for several reasons including ease of access, network and software complexity, lack of security consideration in network design and software development, and inappropriate

user activity. Access to cyberspace by an individual or group with a networked device is easy, and an individual with a single device may be able to disable an entire network. Vulnerabilities in the systems that operate in cyberspace contribute to a continuous obligation to manage risk and protect portions of cyberspace. Understanding the vulnerabilities of DODIN may lead to changes of the operational design. Vulnerabilities found on enemy or adversary systems may cause changes to those portions of cyberspace as well. Effects generated in cyberspace can have global impact across the physical domains.

CYBERSPACE AS A COMPONENT OF THE OPERATIONAL ENVIRONMENT

1-68. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Cyberspace, operational variables, mission variables, and the dimensions of the information environment share a complex relationship within an operational environment. Staffs perform tasks and missions in and through cyberspace to support the warfighting functions. Cyberspace supports, enables, and integrates operations for warfighting functions in the operational environment within all the domains.

1-69. While cyberspace enables communications capabilities, it also creates critical vulnerabilities for adversaries and enemies to attack or exploit. The complexity, low entry cost, widely available resources, minimally required technological investment, and ease of anonymity in cyberspace enables enemies and adversaries to inflict serious harm. The expanded availability of commercial off-the-shelf technology provides adversaries with increasingly flexible and affordable technology to adapt to military purposes. Low barriers to use cyberspace significantly decrease the traditional capability gap between the United States and adversaries, allowing them to field sophisticated cyberspace capabilities.

1-70. DODIN operations enables Army operations. DODIN operations, DCO, EW, and intelligence facilitate freedom of maneuver in cyberspace. Freedom of maneuver allows the integration of the warfighting functions across all domains. Army operations, enabled and supported by the DODIN, support the JFC's objectives.

SITUATIONAL UNDERSTANDING AND AWARENESS OF CYBERSPACE

1-71. *Situational understanding* is the product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables to facilitate decision making (ADP 5-0). Operational variables enable a comprehensive understanding of a given operational environment, while mission variables enable a more focused understanding of a given area of operations. The continuous application of these analytical frameworks enables the commander and staff to analyze cyberspace from various perspectives throughout the operations process. (See FM 6-0 for additional information on operational and mission variables.)

1-72. Situational understanding of cyberspace is gained and maintained by identifying, characterizing, and monitoring certain types of enemy, adversary, and friendly activity in designated cyberspace and the EMS. Situational understanding of cyberspace involves—

- Developing, disseminating, and maintaining relevant information enabling the commander and staff to achieve situational understanding of friendly, enemy, and adversary utilization of cyberspace, including the cyberspace related use of the EMS.
- Determining, validating, and mitigating network intrusions or other unauthorized activities within friendly force networks, particularly the Army's contribution.
- Information collection efforts to support cyberspace operations to produce and disseminate a common operational picture and to answer the commander's critical information requirements (see FM 3-55 for additional information). Continuous tracking, monitoring and assessment of friendly force activity inside and outside of the DODIN including collaboration with higher headquarters and their development of joint cyberspace situational awareness (see JP 3-12[R] for additional information).
- Identifying and applying authorities, other legal considerations, intelligence gain or loss, and associated risks that each serve to inform decision making.

- Direct coordination with host nations to develop and monitor the status of critical infrastructure and key resources.

1-73. It is important to ensure commanders and staff understand how cyberspace enables their operations. Cyberspace includes physical and logical networks and cyber-personas. The networks include nodes linked together by transmission paths. A link is the connection between nodes. A node is broadly defined as an element of a system that represents a person, place, or physical thing (see JP 3-0). A technical definition describes a node as a physical location that provides terminating, switching, or gateway access services to support information exchange (see JP 6-0). Nodes, along with the transmission paths that link them together, contain in-transit and resident data available for access and use by individuals, groups, and organizations. Combining a network diagram with other situational information enhances the understanding of the operational environment because of the inclusion of cyberspace specific information.

1-74. Some nodes in cyberspace, especially commercial systems, are used by various entities, including friendly, neutral, and enemy or adversary. Figure 1-7 displays friendly, threat, and neutral (or non-attributed) networks in an operational area. Network nodes, links, and communications link types provide additional information to form a better picture of the operational environment. Included is the threat network overlay depicting network nodes used by enemies and adversaries. The graphic includes nodes located at known unit, adversary and host nation locations as elements of physical infrastructure, and transmission paths as wired or wireless links (through the EMS). Friendly units aid in situational understanding by identifying their location relative to the enemy, adversary, and host nation nodes. Combining the operational view with the network diagram aids in identifying key terrain in cyberspace.

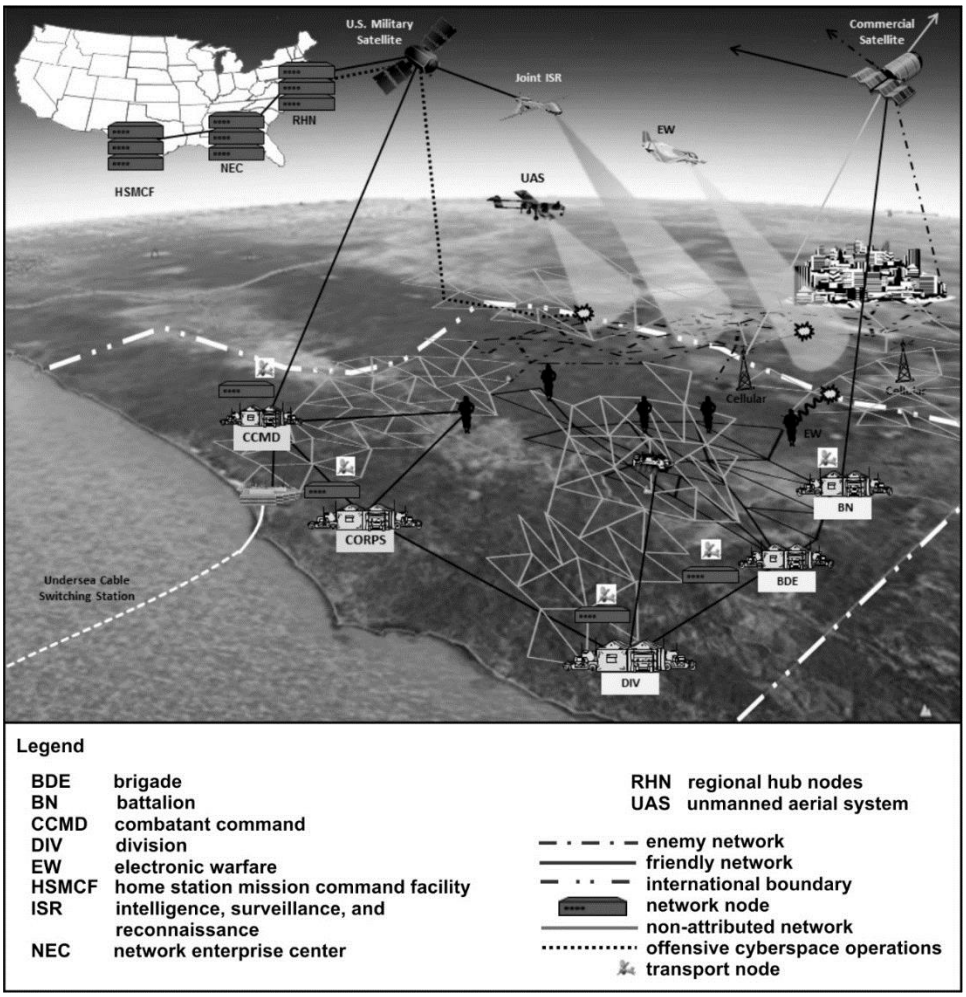


Figure 1-7. Operational area with network topology information

1-75. In the context of traditional land operations, *key terrain* is any locality, or area, the seizure or retention of which affords a marked advantage to either combatant (JP 2-01.3). However, cyberspace operations uses the concept of key terrain as a model to identify key aspects of the cyberspace domain. Identified key terrain in cyberspace is subject to actions the controlling combatant (whether friendly, enemy, or adversary) deems advantageous such as defending, exploiting, and attacking. References to key terrain correspond to nodes, links, processes, or assets in cyberspace, whether part of the physical, logical, or cyber-persona layer. The marked advantage of key terrain in cyberspace may be for intelligence, to support network connectivity, a priority for defense, or to enable a key function or capability.

CYBERSPACE AND THE OPERATIONAL VARIABLES

1-76. Commanders and staffs continually analyze and describe the operational environment in terms of eight interrelated operational variables: political, military, economic, social, information, infrastructure, physical environment, and time. Each variable applied to an analysis of designated cyberspace can enable a more comprehensive understanding of the operational environment. The analysis describes the planning, preparation, execution, and assessment activities for both the wired and EMS portions cyberspace operations. (See FM 6-0 for more information on operational variables.) The following are operational variable example questions specific to networks and nodes—

- **Political**. What networks and nodes require the most emphasis on security and defense to enable the functioning of the government?
- **Military**. Where are networks and nodes utilized by enemy and adversary actors to enable their activities?
- **Economic**. What networks and nodes require the most emphasis on security and defense to enable commerce and other economic-related activities?
- **Social**. What network nodes enable communication with the host nation population for the purpose of providing information or protecting them from potential negative effects caused by military operations in cyberspace?
- **Information**. What is the nature of the data transiting cyberspace that influences or otherwise affects military operations?
- **Infrastructure**. What networks and nodes enable critical infrastructure and key resource capabilities and supporting supervisory control and data acquisition systems?
- **Physical Environment**. How are wireless networks affected by the electromagnetic environment which includes terrain and weather?
- **Time**. What are the optimal times to create effects to support the overarching mission?

CYBERSPACE AND THE MISSION VARIABLES

1-77. The analysis of mission variables specific to cyberspace operations enables Army forces to integrate and synchronize cyberspace capabilities to support Army operations. Mission variables describe characteristics of the area of operations. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations. (See ADRP 5-0 and FM 6-0 for more information on mission variables.) For cyberspace operations, mission variables provide an integrating framework upon which critical questions can be asked and answered throughout the operations process. The questions may be specific to either the wired portion of cyberspace, the EMS, or both. The following is a list of the mission variables example questions—

- **Mission**. Where can we integrate elements of cyberspace operations to support the unit mission? What essential tasks could be addressed by the creation of one or more effects by cyberspace operations?
- **Enemy**. How can we leverage information collection efforts regarding threat intentions, capabilities, composition, and disposition in cyberspace? What enemy vulnerabilities can be exploited by cyberspace capabilities?
- **Terrain and weather**. What are the opportunities and risks associated with the employment of cyberspace operations capabilities when terrain and weather may cause adverse impacts on supporting information technology infrastructures?

- **Troops and support available**. What resources are available (internal and external) to integrate, synchronize, and execute cyberspace operations? What is the process to request, receive, and integrate these resources?
- **Time available**. How can we synchronize OCO and related desired effects with the scheme of maneuver within the time available for planning and execution?
- **Civil considerations**. How can we employ cyberspace operations without negative impacts on noncombatants?

RISK IN CYBERSPACE

1-78. Risk is inherent in all military operations. When commanders accept risk they create opportunities to seize, retain, and exploit the initiative and achieve decisive results. The willingness to incur risk is often the key to exposing enemy and adversary weaknesses considered beyond friendly reach (ADRP 3-0). Commanders assess and mitigate risk continuously throughout the operations process. Many of the risks to the DODIN and the Army's contribution to cyberspace come from enemies, adversaries, and insiders. Some threats are well equipped and well trained while some are novices using readily available and relatively inexpensive equipment and software. Army users of the DODIN are trained on cybersecurity, focusing on safe use of information technology and to recognize how threats operate to help mitigate risks.

1-79. Risk management is the Army's primary decision-making process for identifying hazards and controlling risks. Using this process, operational effectiveness and the probability of mission accomplishment increases. This provides a way of identifying hazards, assessing them, and managing the associated risk. The process applies to all types of operations, tasks, and activities including cyberspace operations. The factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations provide a standardized methodology for addressing both threat and hazard based risk. Risks associated with cyberspace operations fall into four major categories—

- Operational risks.
- Technical risks.
- Policy risks.
- Operations security risks.

***Note*.** See ATP 5-19 for more on risk management.

OPERATIONAL RISKS

1-80. Operational risks pertain to consequences that cyberspace threats pose to mission effectiveness. Operational consequences are the measure of cyberspace attack effectiveness. Cyberspace intrusions or attacks can compromise technical networks, systems, and data; which can result in operational consequences such as injury or death of personnel, damage to or loss of equipment or property, degradation of capabilities, mission degradation, or even mission failure. Exfiltration of data from Army networks by the enemy can undermine the element of surprise and result in an ambush. Enemy or adversary forces may conduct cyberspace and EMS attacks to exposed friendly networks and capabilities, compromising future cyberspace attacks and cyberspace exploitation missions.

TECHNICAL RISKS

1-81. Technical risks are exploitable weaknesses in Army networks and systems. Nearly every technical system within the Army is networked, creating shared vulnerabilities. These potentially vulnerable networked systems and components directly impact the Army's ability to project military power and support the mission. DCO and cybersecurity measures mitigate risks and defend against the threats from taking advantage of the technical vulnerabilities. Robust systems engineering, supply chain risk management, security, counterintelligence, intelligence, hardware and software assurance, and information systems security engineering disciplines enable the Army to manage technical risk to system integrity and trust. Friendly forces examine the technical risks when conducting cyberspace attacks to avoid making friendly networks vulnerable to enemy cyberspace counterattacks. The Army uses a defense-in-depth approach, utilizing

software; such as anti-virus and anti-malware programs, monitoring hardware and software, network sensors, intrusion prevention, and physical security to mitigate technical risks. These are effective when all elements are implemented and updated regularly.

POLICY RISKS

1-82. Policy risk pertains to authorities, legal guidance, and international law. Policies address cyberspace boundaries, authorities, and responsibilities. Commanders and decision makers must perform risk assessments and consider known probable cascading and collateral effects due to overlapping interests between military, civil, government, private, and corporate activities on shared networks in cyberspace. Policies, the United States Code (USC), Uniform Code of Military Justice, regulations, publications, operation orders, and standard operating procedures all constitute a body of governance for making decisions about activities in cyberspace.

1-83. Risk occurs where policy fails to address operational necessity. For example, due to policy concerns, an execution order or applicable rules of engagement may limit cyberspace operations to only those operations that result in no or low levels of collateral effects. A collateral effects analysis to meet policy limits is distinct from the proportionality and necessity analysis required by the law of war. Even if a proposed cyberspace operation is permissible after a collateral effects analysis, the proposed cyberspace operation must determine a legitimate military objective also be permissible under the law of war.

1-84. Policy risk applies to risk management under civil or legal considerations. An OCO mission requested by an Army unit may pose risk to host nation civilians and noncombatants in an operational environment where a standing objective is to minimize collateral damage. During the course of a mission, it may be in the Army's best interest for host nation populations to be able to perform day-to-day activities. Interruptions of civil networks may present hazards to Army networks and pose dangers to Army forces because of social impacts that lead to riots, criminal activity, and the emergence of insurgent opportunists seeking to exploit civil unrest.

OPERATIONS SECURITY RISKS

1-85. Cyberspace provides a venue for operations security risks. The Army depends on security programs and cybersecurity training to mitigate the operations security risks. Commanders emphasize and establish operations security programs to mitigate the risks. Operations security measures include actions and information on the DODIN and non-DODIN information systems and networks. All personnel are responsible for protecting sensitive and critical information. (See AR 530-1 for information about operations security.)

Note. See AR 530-1 for information about operations security.

THREATS IN CYBERSPACE

1-86. The Army faces multiple, simultaneous, and continuous threats in cyberspace. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm the United States forces, United States national interests, or the homeland (ADRP 3-0). Threats include state and non-state actors, criminals, insider threats, and the unwitting individuals who intend no malice. These diverse threats have disparate agendas, alliances, and range of capabilities. Enemies and adversaries employ regular and irregular forces and use an ever-changing variety of conventional and unconventional tactics. Risks from insiders may be malicious or cause damage unintentionally. Insider risks include non-compliance of policies and regulations, causing vulnerabilities on the network. Table 1-1 on page 1-21 lists sample threat capabilities with examples of methods, indicators, and first order effects.

Table 1-1. Sample cyberspace and electronic warfare threat capabilities

Capability	*Methods*	*Indicators*	*First-order effects*
Denial of service attack	Overwhelming a web service, server, or other network node with traffic to consume resources preventing legitimate traffic	Abnormal network performance, inability to navigate web and access sites, uncontrolled spam, and system reboots	Degraded network capabilities ranging from limited operational planning to total denial of use
Network penetration	Man-in-the-middle attacks, phishing, poisoning, stolen certificates, and exploiting unencrypted messages and homepages with poor security features	Unfamiliar e-mails, official looking addresses requiring urgent reply, internet protocol packets replaced, non-legitimate pages with the look of legitimate sites, directed moves from site to site, requests to upgrade and validate information, and unknown links	Uncontrolled access to networks, manipulation of networks leading to degraded or compromised capabilities that deny situational awareness or theft of data
Emplaced malware (virus, worms spyware, and rootkits)	Phishing, spear-phishing, pharming, insider threat introduction, open-source automation services, victim activated through drive-by downloads and victim emplaced data storage devices	Pop-ups, erroneous error reports, planted removable storage media, unknown e-mail attachments, changed passwords without user knowledge, automatic downloads, unknown apps, and degraded network	Spyware and malware on affected systems allow electronic reconnaissance, manipulation, and degrading system performance
Disrupt or deny information systems in the EMS	Prevent friendly antennas from receiving data transmitted in the EMS by using military or commercially available high-powered lasers, high powered microwaves, and repurposed or re-engineered communications systems	Symptoms may not be evident if passive; may manifest as transmission interference, software or hardware malfunctions, or the inability to transmit data	Degraded or complete denial of service in ability to control the EMS denying situational awareness and degrading operational planning

AUTHORITIES

1-87. The United States Constitution establishes the authority of the President as Commander in Chief of the Armed Forces and gives authority for Congress to fund and regulate the Armed Forces. The President, as Commander in Chief commands the missions of the Armed Forces and, according to the laws passed by Congress, administers the Armed Forces.

1-88. Army Commanders conduct cyberspace operations and EW when directed by the orders of the President of the United States, the Secretary of Defense, and Combatant Commanders designated to conduct operations on behalf of the President. These orders are issued under the President's authority from Article II, United States Constitution, in consideration of the Bill of Rights, other executive orders, presidential policy, DOD and DA regulations, U.S. Treaty obligations, and other laws (including funding appropriations) passed by Congress.

1-89. Within this legal framework, Army forces conduct cyberspace and EW operations as authorized through Execute Orders (EXORDs); Operations Orders; Rules of Engagement; and the policies directed by the Secretary of Defense and the Combatant Commanders.

1-90. Army forces conduct cyberspace operations and EW as part of the joint force. Army forces may conduct OCO, DCO, and EW with Army force organic or joint requested effects to support the joint commander's intent. (See JP 3-12(R), Cyberspace Operations and JP 3-13.1, Electronic Warfare for more information.) United States Strategic Command has overall responsibility for directing DODIN operations and defense, which has been delegated to the Commander, U.S. Cyber Command for execution. U.S. Army Cyber Command (ARCYBER) and Second Army conduct DODIN operations and DCO within Army networks, and when directed, within other DOD and non-DOD networks.

1-91. Army forces conduct operations directed by the President while adhering to appropriations, authorizations, and statutes of the USC by Congress. These statutes cover wide areas of law including domestic security, the regulation of the Armed Forces, Federal crimes, the National Guard, information technology acquisition and service, electromagnetic spectrum management, and intelligence.

1-92. Domestic Security, USC Title 6. Establishes responsibilities for information analysis and infrastructure protection, chief information officers, and cybersecurity oversight. USC Title 6 responsibilities include comprehensive assessments of key resources, critical infrastructure vulnerabilities, and identifying priorities for protective and supportive measures regarding threats. (For more information, see U.S. Code Title 6.)

1-93. The Armed Forces, USC Title 10, Enables the Army to organize, train, equip, and provide land, cyberspace operations, and EW units and headquarters. USC Title 10 authorities and restrictions provide context and foundation for how the Secretary of Defense directs military cyberspace operations, EW, and military intelligence operations.

1-94. Crimes and Criminal Procedure, USC Title 18. Army forces conduct cyberspace operations and EW in compliance with Federal law and takes measures to ensure operations respect the rights of persons against unlawful searches and seizures pursuant to the 4th Amendment. Coordination with the Army Criminal Investigation Division ensures appropriate investigation of criminal activity on the DODIN under Title 18 authorities. USC Title 18 includes those crimes conducted in cyberspace.

1-95. The National Guard, USC Title 32. National Guard units are state military units which are equipped and trained pursuant to Federal statutory authorization. The National Guard, may conduct missions for their state, but paid for by the Federal government under USC Title 32, if the Secretary of Defense determines the mission is in the interests of the DOD.

1-96. Information Technology Acquisition, USC Title 40, Ch. 113, is applicable to the Army and all Federal agencies. USC Title 40 establishes the responsibilities of the agency heads and agency chief information officers and guidance for acquisition of information technology.

1-97. USC Title 44, Public Printing and Documents, establishes responsibilities of agency heads for statutory requirements and authority for ensuring information security and information resource management. This includes information security in cyberspace.

1-98. Telecommunications, USC Title 47, prescribes the statutory requirements and authority for access to, and use of, the EMS within the United States and Possessions to Federal agencies. The chief information officer/assistant chief of staff, signal (G-6), as outlined in AR 5-12, implements national, international, DOD, joint, host nation, and Headquarters, Department of the Army spectrum management policies and guidance throughout the Army. In this capacity, the chief information officer/G-6 ensures compliance with 47 USC as well as other applicable Federal, DOD, and military department EMS governance and policy to minimize radio frequency interference at DOD and Service test ranges and installations for activities such as GPS testing and EA clearances for training, testing, and evaluating.

1-99. War and National Defense, USC Title 50, provides authorities concerning the conduct of both military and intelligence activities of the U.S. Government. Intelligence activities conducted by the U.S. Government must be properly authorized, conform to the U.S. Constitution, and be conducted under presidential authority. Executive Order 12333, establishes the framework and organization of the intelligence community as directed by the President of the United States. For example, the order directs the NSA as the lead for signals

intelligence. DOD policy documents, including DoD Manual 5240.01, "DoD Intelligence Activities," establish DOD policy for the conduct of intelligence operations.

1-100. The Army strictly limits and controls collection of information on U.S. persons and collection in the United States. AR 381-10 identifies the types, means, and limitations concerning collection retention and dissemination of information in the United States and on U.S. persons. This regulation applies to cyberspace within the boundaries of the United States and U.S. persons abroad. Table 1-2 on page 1-24 provides more information on authorities in cyberspace.

Table 1-2. United States Code-based authorities

United States Code (USC)	*Title*	*Key Focus*	*Principal Organization*	*Role in Cyberspace*
Title 6	Domestic Security	Homeland Security	Department of Homeland Security	Security of U.S. government portion of cyberspace
Title 10	Armed Forces	National Defense	Department of Defense	Man, train, and equip, U.S. forces to conduct military operations in cyberspace
Title 18	Crimes and Criminal Procedures	Federal Offenses	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace
Title 32	National Guard	National defense and DSCA training and operations in the U.S.	Army National Guard, Air National Guard	Domestic consequence management when in a Title 32 status
Title 40	Public Buildings, Property, and Works	Chief Information Officer roles and responsibilities	All federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies
Title 44	Public Printing and Documents	All federal agencies	All federal departments and agencies	Information security and information resource management
Title 47	Telecom-munications	All federal agencies	All federal departments and agencies	Use of the electromagnetic spectrum
Title 50	War and National Defense	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure U.S. interests by conducting military and foreign intelligence operations in cyberspace

SECTION III – ELECTRONIC WARFARE OPERATIONS

1-101. This section includes fundamental information about EW including EA, EP, ES, and considerations for employment.

ELECTROMAGNETIC SPECTRUM OPERATIONS

1-102. EMSO are comprised of EW and SMO. The importance of the EMS and its relationship to the operational capabilities of the Army is the focus of EMSO. EMSO include all activities in military operations to successfully control the EMS. Figure 1-8 illustrates EMSO and how they relate to SMO and EW.

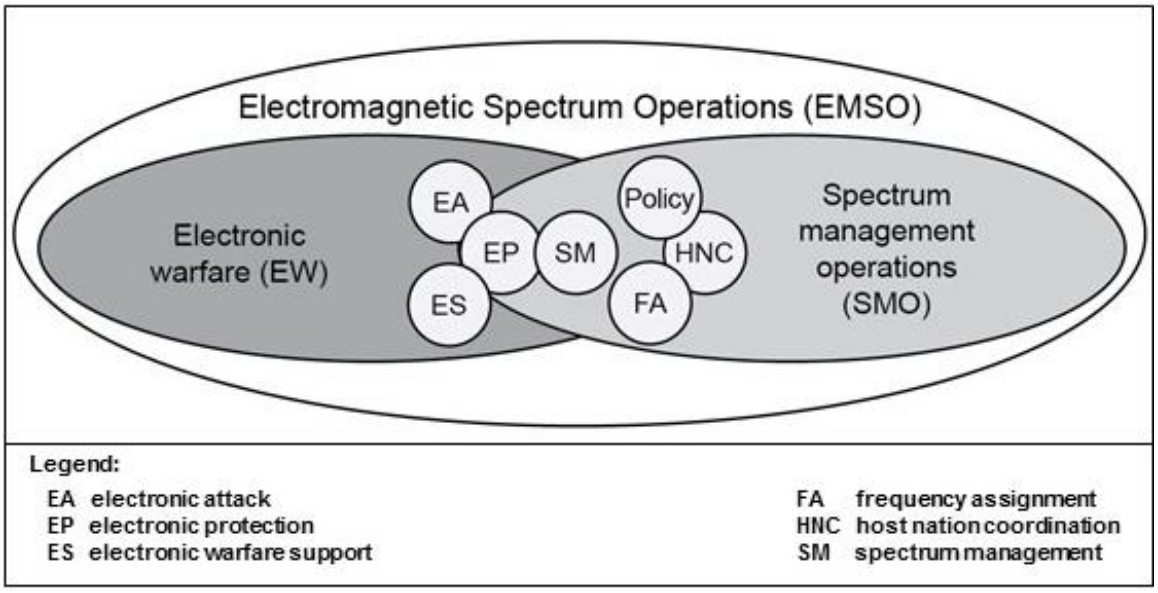


Figure 1-8. Electromagnetic spectrum operations

ELECTRONIC WARFARE

1-103. *Electronic warfare* refers to military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). EW capabilities enable Army forces to create conditions and effects in the EMS to support the commander's intent and concept of operations. EW includes EA, EP, and ES and includes activities such as electromagnetic jamming, electromagnetic hardening, and signal detection, respectively. EW affects, supports, enables, protects, and collects on capabilities operating within the EMS, including cyberspace capabilities. (See figure 1-9 on page 1-26.) With proper integration and deconfliction, EW can create reinforcing and complementary effects by affecting devices that operate in and through wired and wireless networks. Throughout this document, the term EW operations refers to planning, preparing, execution, and continuous assessment of the electronic warfare activities of an operation. The term EMSO indicates the addition of those operationally related spectrum management operations activities.

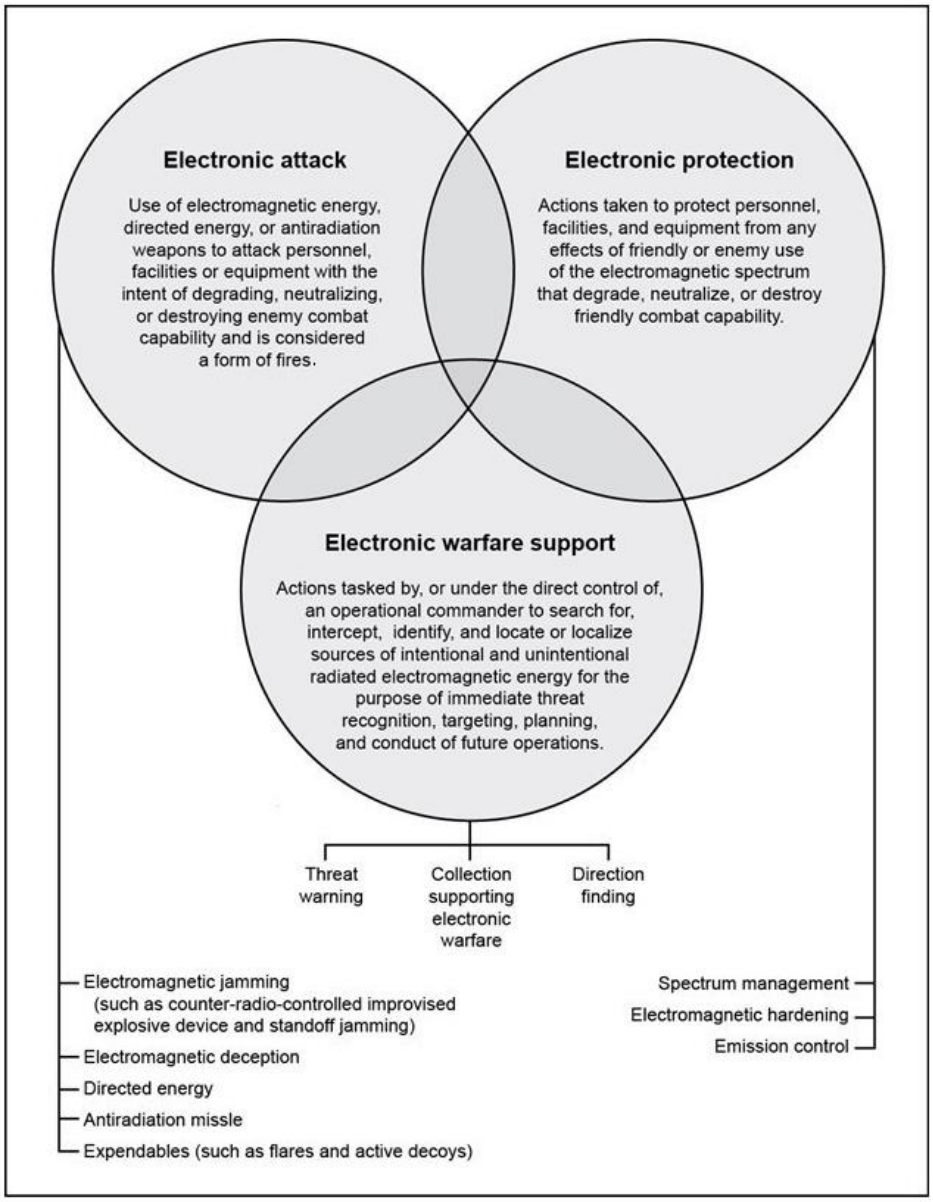


Figure 1-9. Electronic warfare missions

ELECTRONIC ATTACK

1-104. EA involves the use of electromagnetic energy, directed energy, or anti-radiation 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. EA includes—

- Actions taken to prevent or reduce an enemy's effective use of the EMS.
- Employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism.
- Offensive and defensive activities, including countermeasures.

1-105. EA includes using weapons that primarily use electromagnetic or directed energy for destruction. These can include lasers, radio frequency weapons, and particle beams. *Directed energy* is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or

atomic or subatomic particles (JP 3-13.1). In EW, most directed-energy applications fit into the category of EA. A directed-energy weapon uses electromagnetic energy to damage or destroy an enemy's equipment, facilities, and/or personnel. In addition to destructive effects, directed-energy weapon systems support area denial and crowd control.

1-106. Army operations use offensive and defensive tasks for EA. Examples of offensive EA include—

- Jamming electronic command and control or enemy radar systems.
- Using anti-radiation missiles to suppress enemy air defenses (anti-radiation weapons use radiated energy emitted from a target as the mechanism for guidance onto the target).
- Using electronic deception to provide false information to enemy ISR systems.
- Using directed-energy weapons to deny, disrupt, or destroy equipment or capabilities.

1-107. Defensive EA uses the EMS to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as the use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasures, and counter radio-controlled improvised explosive device systems.

ELECTRONIC ATTACK ACTIONS

1-108. Actions related to EA are either offensive or defensive. Though they are similar actions and capabilities, they differ in purpose. Defensive EA protects friendly personnel and equipment or platforms. Offensive EA denies, disrupts, or destroys enemy capability. EA actions include—

- Countermeasures.
- Electromagnetic deception.
- Electromagnetic intrusion.
- Electromagnetic jamming.
- Electronic probing.
- Electromagnetic pulse.

Countermeasures

1-109. *Countermeasures* are that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity (JP 3-13.1). They can be deployed preemptively or reactively. Devices and techniques used for EW countermeasures include electro-optical-infrared countermeasures and radio frequency countermeasures.

1-110. *Electro-optical-infrared countermeasures* consist of a device or technique employing electro-optical-infrared materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems (JP 3-13.1). Electro-optical-infrared countermeasures may use laser jammers, obscurants, aerosols, signature suppressants, decoys, pyrotechnics, pyrophorics, high-energy lasers, or directed infrared energy countermeasures.

1-111. *Radio frequency countermeasures* are any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision-guided weapons and sensor systems (JP 3-13.1). Radio frequency countermeasures can be active or passive. Expendable jammers used by aircraft to defend against precision guided surface-to-air missile systems are an example of radio frequency countermeasures.

Electromagnetic Deception

1-112. Electromagnetic deception is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy’s combat capability. Types of electromagnetic deception include manipulative, simulative, and imitative. Manipulative involves actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces. Simulative involves actions to simulate

friendly, notional, or actual capabilities to mislead hostile forces. Imitative introduces electromagnetic energy into enemy systems that imitates enemy emissions.

Electromagnetic Intrusion

1-113. *Electromagnetic intrusion* is the intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion (JP 3-13.1). Electromagnetic intrusion is often conducted by inserting false information. This information may consist of voice instructions, false targets, coordinates for fire missions, or rebroadcasting prerecorded data transmissions.

Electromagnetic Jamming

1-114. *Electromagnetic jamming* is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability (JP 3-13.1). Examples of targets subject to jamming include radios, radars, navigational aids, satellites, and electro-optics.

Electronic Probing

1-115. *Electronic probing* is intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems (JP 3-13.1). This activity is coordinated through joint or interagency channels and supported by Army forces.

Electromagnetic Pulse

1-116. *Electromagnetic pulse* is the electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges (JP 3-13.1). An electromagnetic pulse induces high currents and voltages in the target system, damaging electrical equipment or disrupting its function. An indirect effect of an electromagnetic pulse can be electrical fires caused by the heating of electrical components.

ELECTRONIC PROTECTION

1-117. EP involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the EMS that degrade, neutralize, or destroy friendly combat capability. For example, EP includes actions taken to ensure friendly use of the EMS, such as frequency agility in a radio or variable pulse repetition frequency in radar. Commanders should avoid confusing EP with self-protection. Both defensive EA and EP protect personnel, facilities, capabilities, and equipment. However, EP protects from the effects of EA (friendly and enemy) and electromagnetic interference, while defensive EA primarily protects against lethal attacks by denying enemy use of the EMS to guide or trigger weapons.

1-118. During operations, EP includes, but is not limited to, the application of training and procedures for countering enemy EA. Army commanders and forces understand the threat and vulnerability of friendly electronic equipment to enemy EA and take appropriate actions to safeguard friendly combat capability from an exploitation and attack. EP measures minimize the enemy's ability to conduct ES and EA operations successfully against friendly forces. To protect friendly combat capabilities, units—

- Regularly brief friendly force personnel on the EW threat.
- Safeguard electronic system capabilities during exercises and pre-deployment training.
- Coordinate and deconflict EMS usage.
- Limit the EMS signatures to reduce adversary ability to locate nodes.
- Provide training during routine home station planning and training activities on appropriate EP active and passive measures under normal conditions, conditions of threat EA, or otherwise degraded networks and systems.
- Take appropriate actions to minimize the vulnerability of friendly receivers to enemy jamming (such as reduced power, brevity of transmissions, and directional antennas).

- Ensure redundancy in systems is maintained and personnel are well-versed in switching between systems.

1-119. EP also includes spectrum management. A spectrum manager works for the assistant chief of staff, signal G-6 (S-6) and for the cyberspace planner in the CEMA Section. The spectrum manager is key in the coordination and deconfliction of spectrum resources allocated to the force. Spectrum managers or their direct representatives participate in the planning for EW operations.

1-120. The development and acquisition of communications and EMS dependent systems includes EP requirements to clarify performance parameters. Army forces design their equipment to limit inherent vulnerabilities. If EA vulnerabilities are detected, then units must review these programs. (See DODI 4650.01 for information on the certification of spectrum support and electromagnetic compatibility.)

ELECTRONIC PROTECTION ACTIONS

1-121. There are several actions related to EP. They include—

- Electromagnetic compatibility.
- Electromagnetic hardening.
- Electronic masking.
- EMS management.
- Emission control.
- Wartime reserve modes.

Electromagnetic Compatibility

1-122. *Electromagnetic compatibility* is the ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response (JP 3-13.1). It involves the application of sound EMS management; system, equipment, and device design configuration that ensures interference-free operation. It also involves clear concepts and doctrines that maximize operational effectiveness.

Electromagnetic Hardening

1-123. *Electromagnetic hardening* consists of action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (JP 3-13.1). Electromagnetic hardening is accomplished by using a comprehensive shielding of sensitive components and by using non-electrical channels for the transfer of data and power.

Electromagnetic Spectrum Management

1-124. *Electromagnetic spectrum management* is planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures (JP 6-01). The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.

Electronic Masking

1-125. Another task of electronic protection is electronic masking. *Electronic masking* is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/SIGINT without significantly degrading the operation of friendly systems (JP 3-13.1).

Emission Control

1-126. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability

to execute a military deception plan (JP 3-13.1). Emission control prevents the enemy from detecting, identifying, and locating friendly forces. It is also used to minimize electromagnetic interference among friendly systems.

Wartime Reserve Modes

1-127. *Wartime reserve modes* are characteristics and operating procedures of sensors, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance (JP 3-13.1). Wartime reserve modes are deliberately held in reserve for wartime or emergency use and seldom employed outside of conflict.

ELECTRONIC WARFARE SUPPORT

1-128. ES involves actions tasked by, or under direct control of, an 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 ES enables U.S. forces to identify the electromagnetic vulnerability of an enemy's or adversary's electronic equipment and systems. Friendly forces take advantage of these vulnerabilities through EW operations.

1-129. ES systems are a source of information for immediate decisions involving EA, EP, avoidance, targeting, and other tactical employment of forces. ES systems collect data and produce information to—

- Corroborate other sources of information or intelligence.
- Conduct or direct EA operations.
- Create or update EW databases.
- Initiate self-protection measures.
- Support EP efforts.
- Support information related capabilities.
- Target enemy or adversary systems.

1-130. ES and SIGINT missions may use the same or similar resources. The two differ in the intent, the purpose for the task, the detected information's intended use, the degree of analytical effort expended, the detail of information provided, and the timelines required. ES missions respond to the immediate requirements of a tactical commander or to develop information to support future cyberspace or EW operations. (See ADRP 2-0 and FM 2-0 for more information on SIGINT.)

ELECTRONIC WARFARE SUPPORT ACTIONS

1-131. There are several actions related to ES. They include—

- Electronic intelligence.
- Electronic reconnaissance.
- Electronics security.

Electronic Intelligence

1-132. *Electronic intelligence* is technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources (JP 3-13.1). Electronic intelligence is a subcomponent of SIGINT. Examples of noncommunications electromagnetic radiations include radars, surface-to-air missile systems, and aircraft.

Electronic Reconnaissance

1-133. *Electronic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-13.1). Electronic reconnaissance is used to update and maintain the threat characteristics information. The threat electronic characteristics information is used in the planning and integrating processes.

Electronics Security

1-134. *Electronics security* is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar (JP 3-13.1). Examples of electronics security are EMS mitigation and network protection.

Note. See JP 3-13.1 and ATP 3-36 for additional information on EW capabilities, tasks, and techniques.

ELECTROMAGNETIC INTERFERENCE

1-135. *Electromagnetic interference* is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment (JP 3-13.1). It can be induced intentionally, as in some forms of EW, or unintentionally, because of spurious emissions and responses, intermodulation products, and other similar products.

ELECTRONIC WARFARE REPROGRAMMING

1-136. *Electronic warfare reprogramming* is the deliberate alteration or modification of electronic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment (JP 3-13.1). These changes may be the result of deliberate actions on the part of friendly, enemy, adversary, third parties, or they may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of EW reprogramming is to maintain or enhance the effectiveness of EW and target sensing system equipment. Electronic warfare reprogramming includes changes to self-defense systems, offensive weapons systems, ES, and intelligence collection systems. Joint and multinational coordination of Service reprogramming efforts ensures friendly forces consistently identify, process, and implement reprogramming requirements. (For more information on EW reprogramming, see ATP 3-13.10.)

EMPLOYMENT CONSIDERATIONS

1-137. EW has specific ground-based, airborne, and functional (EA, EP, or ES) employment considerations. The electronic warfare officer (EWO) ensures EW-related employment considerations are properly articulated early in the operations process. Each capability employed has certain advantages and disadvantages which are considered during the course of action development in the MDMP before selecting the best course of action. The staff plans for these before executing EW operations.

GROUND-BASED ELECTRONIC WARFARE CONSIDERATIONS

1-138. Ground-based EW capabilities support the commander's scheme of maneuver. Ground-based EW equipment can be employed by a dismounted Soldier or on highly mobile platforms. Due to the short-range nature of tactical signals direction finding, EA assets are normally located in the forward areas of the battlefield, with or near forward units.

1-139. Ground-based EW capabilities have certain advantages. They provide direct support to maneuver units (for example, through counter-radio-controlled improvised explosive device and communications or sensor jamming). Ground-based EW capabilities support continuous operations and respond quickly to EW requirements of the ground commander. To maximize the effectiveness of ground-based EW capabilities, maneuver units must understand the associated EMS signature and protect EW assets from enemy ground and aviation threats. EW equipment should be as survivable and mobile as the force it supports. Maneuver units must logistically support the EW assets, and supported commanders must clearly identify EW requirements.

1-140. Ground-based EW capabilities have certain limitations. They are vulnerable to enemy attack and can be masked by terrain. They are vulnerable to enemy geolocation, electromagnetic deceptive measures, and EP actions. In addition, they have distance or propagation limitations against enemy electronic systems.

AIRBORNE ELECTRONIC WARFARE CONSIDERATIONS

1-141. While ground-based and airborne EW planning and execution are similar, they significantly differ in their EW employment time. Airborne EW operations are performed at much higher speeds and generally have a shorter duration than ground-based operations. The timing of airborne EW support requires detailed planning.

1-142. Airborne EW requires the following—

- A clear understanding of the supported commander's EW objectives.
- Detailed planning and integration.
- Ground support facilities.
- Liaisons between the aircrews of the aircraft providing the EW support and the aircrews or ground forces being supported.
- Protection from enemy aircraft and air defense systems.

1-143. Airborne EW capabilities have certain advantages. They can provide direct support to other tactical aviation missions such as suppression of enemy air defenses, destruction of enemy air defenses, and employment of high-speed anti-radiation missiles. They can provide extended range over ground-based assets. Airborne EW capabilities can provide greater mobility and flexibility than ground-based assets. In addition, they can support ground-based units in beyond line-of-sight operations.

1-144. The various airborne EW assets have different capabilities. The limitations associated with airborne EW capabilities are—

- Time-on-station.
- Vulnerability to enemy EP actions.
- Electromagnetic deception techniques.
- Geolocation by enemy and adversary forces.
- Limited assets (support from nonorganic EW platforms need to be requested).

ELECTRONIC ATTACK CONSIDERATIONS

1-145. EA includes both offensive and defensive activities. These activities differ in their purpose. Defensive EA protects friendly personnel and equipment or platforms. Offensive EA denies, disrupts, or destroys enemy or adversary capability. Considerations for planning or employing EA include—

- Integration with the scheme of maneuver and other effects.
- Persistency of effect.
- Intelligence collection.
- Friendly communications.
- EMS signatures allowing enemy and adversary geolocation, and targeting by threats.
- Non-hostile local EMS use.
- Hostile intelligence collection.

1-146. The EWO; the assistant chief of staff, intelligence (G-2/S-2); the assistant chief of staff, operations G-3 (S-3); G-6 (S-6); the spectrum manager; and the IO officer coordinate closely to avoid friendly communications interference that can occur when using EW systems on the battlefield. Coordination ensures that EA systems frequencies are properly deconflicted with friendly communications and intelligence collection systems or that ground maneuver and friendly information tasks are modified accordingly.

1-147. The number of information systems, EW systems, and sensors operating simultaneously on the battlefield makes deconfliction with communications systems a challenge. The EWO, the G-2 (S-2), the G-6 (S-6), and the spectrum manager plan and rehearse deconfliction procedures to quickly adjust their use of EW or communications systems.

1-148. EA operations depend on EW support and intelligence, especially SIGINT to provide targeting information and battle damage assessment. However, not all intelligence collection is focused on supporting EW. If not properly coordinated with the G-2 (S-2) staff, EA operations may impact intelligence collection significantly deterring the ability to answer information requirements. In situations where a known conflict between the intelligence collection effort and the use of EA exists, the EW working group brings the problem to the G-3 (S-3) for resolution.

1-149. EA supports unified land operations. Integrating EA with the scheme of maneuver is critical to ensure units fully exploit the effects delivered against enemy or adversary forces. The limited duration of these effects require close coordination and synchronization between EW assets and forces and the supported maneuver forces.

1-150. Other operations rely on the EMS. For example, a given set of frequencies may be used for IO to broadcast messages or cyberspace operations for wireless communications. In both examples, the use of EA could unintentionally interfere with such operations if not properly coordinated. To ensure EA does not negatively impact planned operations, the EWO coordinates between fires, DODIN operations, and other functional or integrating sections, as required.

1-151. EA can adversely affect local media, communications systems, and infrastructure. Planners should consider unintended consequences of EW operations and deconflict these operations with the various functional or integrating cells. For example, friendly jamming could potentially deny the functioning of essential services such as ambulance or fire fighters to a local population. EWOs routinely synchronize EA with the other functional or integrating cells responsible for the information tasks. In this way, they ensure that EA efforts do not cause fratricide or unacceptable collateral damage to their intended effects.

1-152. The potential for hostile intelligence collection also affects EA. An enemy or adversary can detect friendly EW capabilities and thus gain intelligence on friendly force intentions. For example, the frequencies Army forces jam could indicate where they believe the enemy's capabilities lie. The EWO and the G-2 (S-2) develop an understanding of the enemy's collection capability. Along with the red team (if available), they determine what the enemy might gain from friendly force use of EA. A *red team* is an organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of enemies, adversaries, and others (JP 2-0).

1-153. The primary effects of jamming only persist when the jammer is within range of the target and emitting. Secondary and tertiary effects of jamming are evident in the actions of the enemy or adversary following the EA mission.

ELECTRONIC PROTECTION CONSIDERATIONS

1-154. EP is achieved through physical security, communications security measures, system technical capabilities (such as frequency hopping and shielding of electronics), spectrum management, and emission control procedures. The EW working group must consider the following key functions when planning for EP operations—

- Vulnerability analysis and assessment.
- EP measures and how they affect friendly capabilities.

Vulnerability Analysis and Assessment

1-155. Vulnerability analysis and assessment is the basis for formulating EP plans. The Defense Information Systems Agency conducts vulnerability analysis and assessment, focusing on automated information systems.

Electronic Protection Measures Affects

1-156. EP includes any measure taken to protect the force from hostile EA. EP measures can also limit friendly capabilities or operations. For example, denying frequency usage to counter-radio-controlled improvised-explosive-device EW systems on a given frequency to preserve it for a critical friendly information system could leave friendly forces vulnerable to certain radio-controlled improvised explosive

devices. The EWO and the G-6 (S-6) carefully consider these second-order effects when advising the G-3 (S-3) regarding EP measures.

ELECTRONIC WARFARE SUPPORT CONSIDERATIONS

1-157. Whether an asset is performing a SIGINT or EW support mission depends on mission purpose and intent. Operational commanders task assets to conduct EW support for the purpose of immediate threat recognition, targeting, future plans, and other tactical actions. The EWO coordinates with the G-2 (S-2) to ensure EW support needed for planned EW operations is identified and submitted to the G-3 (S-3) for commander approval. In cases where EA actions may conflict with the G-2 (S-2) intelligence collection efforts, the G-3 (S-3) or commander decides which has priority. The EWO and the G-2 (S-2) develop a structured process within each echelon for conducting this intelligence gain-loss calculus during mission rehearsal, exercises, and pre-deployment preparation, providing the commander with the intelligence and operational gain-loss considerations in order to enable a decision on which activity to prioritize.

ELECTRONIC WARFARE REPROGRAMMING CONSIDERATIONS

1-158. EW reprogramming refers to modifying friendly EW or target sensing systems in response to validated changes in enemy equipment and tactics or the electromagnetic environment. Each Service or organization is responsible for its respective EW reprogramming support programs. During joint operations, swift identification and reprogramming efforts are critical in a rapidly evolving hostile situation. The key consideration for EW reprogramming is joint coordination. (For more information on EW reprogramming, see ATP 3-13.10.)

SPECTRUM MANAGEMENT

1-159. Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage use of the electromagnetic spectrum and enables cyberspace, signal and EW operations. Spectrum management includes frequency management, host nation coordination, and joint spectrum interference resolution. Spectrum management enables spectrum-dependent capabilities and systems to function as designed without causing or suffering unacceptable electromagnetic interference. Spectrum management provides the framework to utilize the electromagnetic spectrum in the most effective and efficient manner through policy and procedure.

SPECTRUM MANAGEMENT OPERATIONS FUNCTIONS

1-160. SMO are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. The SMO functional area is ultimately responsible for coordinating EMS access among civil, joint, and multinational partners throughout the operational environment. The conduct of SMO enables the commander's effective use of the EMS. The spectrum manager at the tactical level of command is the commander's principal advisor on all spectrum related matters.

1-161. The conduct of SMO enables and supports the execution of cyberspace operations and EW. SMO are critical to spectrum dependent devices such as air defense radars, navigation, sensors, EMS using munitions, manned and unmanned systems of all types (ground and air, radar, sensor), and all other systems that use the EMS. The overall objectives of SMO are to enable these systems to perform their functions in the intended environment without causing or suffering unacceptable electromagnetic interference.

1-162. SMO are normally performed by trained spectrum managers from the battalion through Army component level. SMO are largely hierarchal processes. SMO requirements are requested from lower echelons, but EMS resources are allocated from higher echelons.

1-163. Understanding the SMO process in planning, managing, and employing EMS resources is a critical enabler for cyberspace and EW operations. SMO provides the resources necessary for the implementation of the wireless portion of net-centric warfare (see ATP 6-02.70).

ELECTRONIC WARFARE COORDINATION

1-164. The spectrum manager should be an integral part of all EW planning. The SMO assists in the planning of EW operations by providing expertise on waveform propagation, signal, and radio frequency theory for the best employment of friendly communication systems to support the commander's objectives. The advent of common user "jammers" has made this awareness and planning critical for the spectrum manager. In addition to jammers, commanders and staffs must consider non-lethal weapons that use electromagnetic radiation. Coordination for EW will normally occur in the CEMA section. It may occur in the EW cell if it is operating under a joint construct or operating at a special echelon.

1-165. Although in some respects the functions of the EWO and the spectrum manager appear similar, they differ in that the spectrum manager is concerned with the proper operation of friendly spectrum dependent devices, while the EWO is the expert on threat EW capabilities and their effects on operations and works to protect the EMS for friendly forces while denying the enemy use of the EMS.

FREQUENCY INTERFERENCE RESOLUTION

1-166. Interference is the radiation, emission, or indication of electromagnetic energy (either intentionally or unintentionally) causing degradation, disruption, or complete obstruction of the designated function of the electronic equipment affected. The reporting end user is responsible for assisting the spectrum manager in tracking, evaluating, and resolving interference. Interference resolution is performed by the spectrum manager at the echelon receiving the interference. The spectrum manager is the final authority for interference resolution. For interference affecting satellite communications, the Commander, Joint Functional Component Command for Space is the supported commander and final authority of satellite communications interference. (For more information on satellite communications interference, see Strategic Instruction 714-04.)

1-167. Interference may come from signal devices (such as unintentional friendly and unfriendly radios and radars) and from non-signal devices (such as welders or vehicle engines). The skill level of systems operators and maintenance personnel can mean the difference between a minor inconvenience and complete system disablement.

1-168. When experiencing harmful interference, the operator should be able to discern whether the interference is coming from natural phenomena or man-made sources. If natural phenomena is the cause, the operator should try to work through the interference. An alternate frequency may be assigned if the interference persists. If the operator suspects man-made interference, ensure an internal equipment check is conducted to exclude equipment malfunctions. Improper alignment, degraded components, antenna disorientation, or poor maintenance is usually the cause of interference. After the operator has ruled out internal causes, a check with other friendly units in the area may reveal incompatibilities between operations.

1-169. If a compromise cannot be worked out between the units, the case is referred to the spectrum manager at the next higher echelon. The spectrum manager will conduct an analysis of the database, a site survey (if possible), and coordinate with other units in the vicinity to identify the cause of the interference. If the spectrum manager is unable to isolate the cause of the interference, the spectrum manager will submit a report to the next spectrum management level for resolution. For interference affecting satellite communications, a joint spectrum interference resolution report will be generated according to CJCSM 3320.02 D.

This page intentionally left blank.

Chapter 2

Relationships with Cyberspace and the Electromagnetic Spectrum

This chapter provides information on operations and missions that use cyberspace and the electromagnetic spectrum. These operations and actions may affect cyberspace, the electromagnetic spectrum, cyberspace operations, and electronic warfare operations. Commanders and staffs integrate and synchronize cyberspace operations with these during all phases of operations.

INTERDEPENDENCIES

2-1. Cyberspace and EW operations are conducted to support Army operations and missions. This support provides methods for other operations such as signal, IO, intelligence, and space to enable or utilize cyberspace and EW operations to execute their core missions. The associated staff elements are more directly involved in planning or facilitating cyberspace capabilities than other staff functions. The results of actions from these operations affect all aspects of operations to include mission command and freedom of maneuver in cyberspace, and use of the EMS.

2-2. Commanders and staffs consider how other operations affect or utilize cyberspace and the EMS. Actions in cyberspace and the EMS may impact other operations, functions, missions, and tasks as well. The broad impact of cyberspace and EW operations must be considered when planning and conducting operations.

INFORMATION OPERATIONS

2-3. Information operations is the integrated employment, during military operations, of information-related capabilities (IRC) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of enemies and adversaries while protecting our own (JP 3-13). IO synchronizes IRCs, in concert with operations, to create effects in and through the information environment inclusive of cyberspace. IRC advance the commander's intent and concept of operations; seize, retain, and exploit the initiative in the information environment; and consolidate gains in the information environment, to achieve a decisive information advantage over the threat. Because cyberspace is fully part of the information environment, cyberspace operations are inherently IRCs. As such, the IO element and IO working group include cyberspace operations in the IRC synchronization process. A key responsibility of the IO working group is to help the IO element and, in turn, the commander and staff to understand that portion of cyberspace affecting operations, how the threat is attempting to gain advantage in it, and how to prevent the threat from gaining an advantage in it.

2-4. Commanders must understand the information environment and determine how the threat operates in that environment. Understanding begins with analyzing the threat's use of the information environment and IRC to gain an advantage. It continues with threat vulnerabilities friendly forces can exploit or must defend against with IRC. IO provides commanders an implementation strategy and integrative framework for employing IRC. Integrating cyberspace capabilities generates synergistic information environment effects. When employed as part of an information operation that includes multiple IRC, cyberspace operations can provide commanders an alternative solution to challenging operational problem sets. An integrated operation may include the use of cyberspace and the EMS to deliver IO products, observe enemy or adversary actions and reactions, or to deliver cyberspace or EW effects. IRC can provide commanders additional ways and means to—

- Degrade, disrupt, or destroy threat capabilities that inform or influence decision making.

- Degrade, disrupt, or destroy threat capabilities that command and control maneuver, fires, intelligence, communications, and information warfare capabilities employed against friendly forces.
- Deny, delay, or limit threat capabilities employed to gain situational awareness of friendly unit capabilities, status, intent, and exploitable vulnerabilities.
- Deny, delay, or limit threat capabilities that track, monitor, and report on friendly unit activities, status, and disposition.
- Degrade, disrupt, counter, or destroy threat capabilities that target and attack friendly mission command and related decision support systems.
- Degrade, disrupt, counter, or destroy threat capabilities that distribute, publish, or broadcast information designed to persuade targeted foreign audiences or human networks to oppose friendly operations.
- Degrade, disrupt, or destroy threat capabilities that distribute, publish, or broadcast information designed to target friendly military and civilian audiences or human networks in an effort to influence morale and affect support for friendly operations.
- Degrade, disrupt, or destroy threat capabilities that monitor and protect critical threat networks and information pathways, as well as information in transit or at rest.
- Enable military deception directed against threat decision making, intelligence and information gathering, communications and dissemination, and command and control capabilities.
- Enable friendly operations security to protect critical information and operationally vital details.
- Enable friendly influence activities such as military information support operations to improve or sustain positive relations with foreign audiences in and around the operational area and to degrade threat influence over the same.
- Enable friendly influence activities, such as military information support operations, to target threat military and civilian audiences or human networks in an effort to affect morale and support for threat operations and activities within the operational area.
- Protect friendly information, technical networks, and decision-making capabilities from an exploitation by enemy and adversary information warfare assets.

***Note*.** See FM 3-13 for more about information operations.

INTELLIGENCE

2-5. Intelligence supports cyberspace operations through the application of the intelligence process, IPB, and information collection. Intelligence at all echelons supports DODIN operations, DCO, and OCO planning and assists with defining measures of performance and measures of effectiveness. The intelligence process leverages all sources of information and expertise, including the intelligence community and non-intelligence entities to provide situational awareness to the commander and staff. Information gathered provides insight into enemy activities, capabilities, motivations, and objectives and enables the planning, preparation for, and execution of cyberspace and EW operations. Cyberspace planners need to leverage intelligence reach, analysis, reporting, and production capabilities provided by the intelligence warfighting function. This will enable cyberspace planners supporting operations throughout the operational environment. Intelligence assets coordinate with cyberspace planners, the G-6 (S-6), or the CEMA working group to use cyberspace capabilities for—

- Enabling collection assets.
- Linking intelligence capabilities.
- Providing near real time analysis.
- Providing information capabilities.
- Information collection.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

2-6. To define the cyberspace and EMS portions of the operational environment using IPB, the staff considers how the adversary or enemy utilizes cyberspace and the EMS to achieve their objectives. Identifying the area of interest includes considering state and non-state actors with capability, access, and motivation to affect friendly operations. In the context of cyberspace and the EMS, the operational environment includes network topology overlays that graphically depict how information flows and resides within the operational area and how the network transports data in and out of the area of interest.

2-7. Weather (terrestrial and space) affects cyberspace, EW, and signal operations. In assessing environmental effects on cyberspace, the staff considers key terrain in cyberspace in relation to the physical locations in the area of interest and the area of operations.

2-8. Intelligence analysts, with support from other staff elements, evaluate enemy and adversary use of cyberspace and the EMS. This includes evaluating aspects such as—

- Adversary or enemy use of cyberspace and the EMS.
- Reliance on networked capabilities.
- Sophistication of cyberspace attack capabilities.
- Cyberspace defense capabilities.
- EW capabilities.
- Motivation to conduct cyberspace operations against friendly forces.
- Network vulnerabilities.
- Ability to synchronize cyberspace operations with other operations.
- Social media.

2-9. When assessing the enemy or adversary courses of action, the intelligence staff considers how the enemy or adversary will include cyberspace and EW in its operations. The commander and staff should consider threat courses of action in cyberspace when planning friendly operations. (See ATP 2-01.3 for more information about IPB.)

INFORMATION COLLECTION

2-10. Requirements drive the intelligence process and information collection. At echelons corps and below, intelligence collection capabilities focus on the land domain. The analysis of intelligence derived from all intelligence disciplines across all echelons including theater and national collection assets provides insight about enemy cyberspace and EW operations. Leveraging the information collection requirements process may support aspects of cyberspace and EW operations. Both the CEMA section and the G-6 (S-6) coordinate intelligence requirements with the G-2 (S-2) to ensure the necessary intelligence is available to plan, conduct, and assess cyberspace and EW operations.

Note: See FM 3-55 for more material on information collection.

SPACE OPERATIONS

2-11. The relationship between the space and cyberspace domains is unique. Space operations depend on the EMS for the transport of information and the control of space assets. Space operations provide specific capability of transport through the space domain for long haul and limited access communications. Space provides a key global connectivity capability for cyberspace operations. Conversely, cyberspace operations provide a capability to execute space operations. This interrelationship is an important consideration across cyberspace operations, and particularly when conducting targeting in cyberspace.

2-12. Many cyberspace operations occur in and through the space domain via the EMS, resulting in an interdependent relationship between space and cyberspace. Space operations and the capabilities, limitations, and vulnerabilities of space-based systems affect support to cyberspace operations and the Army operations.

2-13. Space and cyberspace operations complement each other, but also have mutually exclusive mission sets and processes. Space provides and supports global access to cyberspace operations through satellite

communications. While satellite communications provides links as part of the DODIN, the nature of satellite operations makes them significantly different from other terrestrial or air-based communications systems. Similarly, space relies on cyberspace and the EMS for command and control of satellite systems and associated ground nodes. The Army relies on space-based capabilities that provide satellite communications, joint ISR, missile warning, environmental monitoring, positioning navigation and timing, and space control. Space-based systems, and the capabilities they support, enable the ability to plan, communicate, navigate, maneuver, and maintain battlefield situational awareness.

2-14. Space is a joint and multinational domain that supports operations in each domain and is congested, contested, and competitive. Space is congested due to the number of objects within key orbital areas, and the number is increasing. Space is increasingly contested due to the employment of capabilities denying free access to space. Finally, space is competitive, with greater numbers of nations and commercial entities operating larger numbers of much smaller and more capable satellites than before. Friendly, neutral, enemy, and adversary communications may occur on the same satellite. Managing this congested, contested, and competitive space environment allows access to space and enables global cyberspace operations.

2-15. The space domain consists of three segments: space, ground, and control. The segments interoperate to provide space-based capabilities and control. Control of the space domain is interdependent with cyberspace operations. Examples of integrated space and cyberspace components are—

- DODIN operations with network transport and information services relate to space-based communications systems to provide the long haul network transport and a direct connection to the tactical portion of the network in a complex, beyond line-of-sight environment.
- DCO support defensive space control planning and execution to protect and defend the DOD cyberspace capabilities and designated systems.

2-16. Coordinating cyberspace, EW, and space operations enables commanders and staffs at each level to synchronize and integrate capabilities and effects. Space-based capabilities enable distributed and global cyberspace operations. Cyberspace and space-based capabilities provide responsive and timely support from the highest echelons down to the tactical level commander. Coordinating with EW operations is necessary to ensure availability of the EMS and to prevent spectrum conflicts.

TARGETING

2-17. Targeting is the means by which commanders and staffs pair targets with effects in and through cyberspace or the EMS. Through the MDMP, the staff identifies the high value targets and high pay-off targets, and through the CEMA working group identifies targets that may qualify for targeting using effects from cyberspace or EW operations. The common operational picture, DCO, cyberspace security information, information collection efforts, and the desired operational outcomes also guide targeting efforts. Army forces plan and execute (with proper authorities) effects on, in, and through cyberspace and the EMS using available capabilities. Units synchronize effects with the next higher command. (See chapter 3 for more information on applying targeting principles.)

Chapter 3

Cyberspace Electromagnetic Activities within Operations

This chapter describes Army cyberspace electromagnetic activities within operations including fundamentals of cyberspace electromagnetic activities; the commander's role; planning, integrating and synchronizing cyberspace electromagnetic activities with the warfighting functions; and the commander's resources that have effects on, in, and through cyberspace and the electromagnetic spectrum. This chapter discusses the contribution of cyberspace operations planning factors into the operations process to include planning, preparing, executing, and assessing with a section on targeting. The discussion of the operational environment is combined with the military decision-making process followed by an overview of preparation requirements, execution tactics, and assessments for cyberspace operations.

FUNDAMENTALS

3-1. Commanders and their staffs conduct CEMA to plan, integrate, and synchronize cyberspace and EW operations as a unified effort to project power in and through cyberspace and the EMS. Executing cyberspace and EW operations enables the Army to secure and defend friendly force networks, and to protect personnel, facilities, and equipment. SMO enables CEMA by ensuring access and deconfliction for the Army's use of the EMS. Planning, integration, and synchronization of the interrelated actions support the overall mission.

3-2. Conducting cyberspace operations and EW operations independently may detract from their efficient employment. If uncoordinated, these activities may result in conflicts and mutual interference internally with other entities that use the EMS. Conflicts and interference may result in the inability to communicate, loss of intelligence, or the degradation of EP systems capabilities.

CONSIDERATIONS

3-3. Only forces with proper legal and command authority can create offensive effects, including DCO-RA, in cyberspace or the EMS. Commanders have the authority to secure and defend their portion of the DODIN-A. All echelons can plan cyberspace and EW operations. Echelons that do not have organic capabilities or authorities for cyberspace or EW operations may integrate supporting effects from forces with those with capabilities to support operations. The approval authority to execute the cyberspace and EW operations is described in the operations orders.

3-4. Commanders when authorized, employ cyberspace and EW operations to shape the environment and support offensive and defensive operations. Information collection and intelligence production efforts may provide information leading the commander and staff to identify targets eligible for effects through cyberspace or the EMS. OCO effects may require proximity to a target for implementation, depending on the asset used to deliver the effects. If commanders determine there is a requirement for OCO, the staff determines whether the capability and authority reside within the unit through the normal targeting process. The staff uses the CERF to request for OCO if the capability does not exist in the unit or supporting forces.

3-5. The defense-in-depth approach to the DODIN integrates defense actions at all echelons. Global and regional efforts establish baseline security and defense of the DODIN. Commanders at echelons corps to brigade are responsible for defending their portion of the network. Personnel from corps to brigade echelons also defend their portion of the network within their capabilities. Units may coordinate for external support as required if the capability to defend the network does not exist in the unit. Support may be provided remotely or on-site. Defense-in-depth allows for network-wide situational awareness, trend analysis, and focused security and defense efforts.

3-6. Collaboration of cyberspace operations occurs within a secure environment. At the appropriate level, access to a sensitive compartmented information facility (SCIF) or temporary SCIF is required for planning, synchronization, and the assembly of the staff members for truly effective collaboration. The corps, division, and brigade must have access to a SCIF or temporary SCIF space for the purpose of cyberspace operations collaboration in the command posts.

3-7. All automated information systems in the Army are part of cyberspace. The actions taken to expand, reduce, defend, and use the DODIN directly affect mission command and warfighting functions. During the exercise of mission command, commanders consider effects to cyberspace and their impact on operations. The freedom of maneuver in cyberspace directly impacts the commander's ability to synchronize warfighting functions. The commander can attain and maintain freedom of maneuver to support freedom of maneuver across all domains through organic and nonorganic capabilities on, in, and through cyberspace and the EMS.

3-8. All warfighting functions use the DODIN as the primary collaboration medium for mission command synchronization. The DODIN supports and enables each of the warfighting functions, tasks, and missions that contribute to the overall operation. Providing access to, securing, and defending the network enables enhanced capabilities for the commander and staff. The individual warfighting functions use the DODIN for daily activities and require access to local and distant services.

COMMANDER'S ROLE

3-9. Commanders exercise mission command to synchronize the warfighting functions (ADRP 6-0). They are able to understand, visualize, describe, direct, lead, and assess courses of action. Commanders must consider cyberspace and EW operations at all times, whether in a tactical environment or in home station. Commanders leverage cyberspace and EW operations as part of combined arms operations to achieve objectives in the natural domains, cyberspace, and the EMS through lethal and nonlethal means.

3-10. Commanders should—

- Include cyberspace and EW operations within the operations process.
- Continually enforce cybersecurity standards and configuration management.
- Understand cyberspace and EW effects, capabilities, constraints, and limitations, including second and third order effects.
- Understand the legal and operational authorities to affect threat portions of cyberspace or EMS.
- Understand the implications of cyberspace and EW operations on the mission and scheme of maneuver.
- Understand how the selected course of action affects the prioritization of resources to their portion of the DODIN.
- Leverage effects in and through cyberspace and the EMS to support the concept of operations.
- Develop and provide intent and guidance for actions and effects inside and outside of the DODIN (examples are conduct cyberspace security, conduct EMS deconfliction, and create effects in and through cyberspace and the EMS).
- Identify critical mission or tasks by phase to enable identification of key terrain in cyberspace.
- Ensure cyberspace operations and EW are integrated into all processes (including operations, intelligence, and targeting).
- Ensure active collaboration across the staff, subordinate units, higher headquarters, and unified action partners to enable shared understanding of cyberspace and the EMS.
- Consider legal implications along with operational authorities and the opportunities and risks they present for operations in cyberspace and the EMS.
- Approve high-priority target lists, target nominations, collection priorities, and risk mitigation measures for operation in cyberspace and the EMS.
- Create massed effects by synchronizing cyberspace operations with lethal and nonlethal actions to support the concept of operations.
- Anticipate and account for related second- and third-order effects in cyberspace and the EMS.

ENABLING RESOURCES

3-11. Echelons corps to brigade have the resources available to execute CEMA. The available resources enable operating in cyberspace and the EMS and affecting enemy and adversary cyberspace and use of the EMS to provide freedom of maneuver. The staff sections and nonorganic support provide the mission support for operations at echelons corps and below.

3-12. All commanders from echelons corps to brigade have organic assets to plan DODIN operations, OCO, DCO, and EW operations. Organic resources at echelons corps and below include, but are not limited to, the EWO (cyberspace planner), the G-2 (S-2) section, the G-6 (S-6) section, signal company, spectrum manager, and other EW personnel. Together, they provide and secure the network at their level to enable synchronization of the warfighting functions and the ability to communicate with other units and echelons. Some commanders have the organic assets to prepare, execute and assess EW operations.

3-13. Nonorganic assets enhance the organic capabilities by providing additional personnel and equipment to meet mission requirements. Expeditionary signal, joint EW capabilities, cyberspace mission forces, and national agencies provide additional assets based on operational requirements and requires coordination to ensure the appropriate equipment and personnel are provided. Units can request support for nonorganic capabilities to provide effects on, in, and through cyberspace and the EMS.

3-14. Critical enablers that support the Army's defense-in-depth include the Army Cyber Operations and Integration Center and the regional cyber centers. The Army Cyber Operations and Integration Center is an operational element of the ARCYBER headquarters and is the top-level control center for all Army cyberspace activities. It provides situational awareness and DODIN operations reporting for the DODIN-A. The center coordinates with the regional cyber centers and provides operational and technical support as required.

3-15. The regional cyber center is the single point of contact for operational status, service provisioning, incident response, and all Army network services in its assigned theater. It coordinates directly with tactical units to provide DODIN-A services, support to DODIN operations, and when required DCO to enable mission command and the warfighting functions.

RESPONSIBILITIES AT CORPS AND BELOW

3-16. Army forces at echelons corps and below plan, integrate, and synchronize all aspects of cyberspace and EW operations. Commanders and staffs synchronize cyberspace and EW operations with all warfighting functions to create complementary and reinforcing effects. The commanders and staff elements execute CEMA to support the commanders' objectives. Executing CEMA provides an advantage to maintain freedom of maneuver in cyberspace and the EMS. Coordinating and synchronizing the efforts of staff elements ensures available information is concentrated to make an appropriate decision based on impacts to current operations and the commanders' objectives.

Staff Responsibilities

3-17. Support to cyberspace operations and EMS control is provided internally as the staff execute CEMA and collaborates to plan, coordinate, integrate, prepare for, and conduct (as required) cyberspace operations. After CEMA collaboration, the staff can—

- Advise the commander on the capabilities, limitations, and effects of cyberspace and EW specific to the unit mission, cyberspace threat, commander's intent and concept of operations, legal authority, and rules of engagement.
- Develop and provide OCO courses of action to support the scheme of maneuver, facilitate OCO missions as directed, and coordinate and integrate DCO-RA with DCO and DODIN operations, as required.
- Ensure integration and synchronization of cyberspace and EW operations into the schemes of maneuver and fires.
- Collect, process, store, display, disseminate, and protect information relevant to cyberspace operations.

- Coordinate and collaborate across the warfighting functions and with external entities (staff counterparts at higher and lower echelons, adjacent units, and the intelligence community) to facilitate and employ cyberspace operations.

Corps to Brigade-Level Cyberspace Electromagnetic Activities

3-18. These tactical echelons employ organic and coordinate for nonorganic capabilities, outside and inside of the DODIN, to accomplish various DODIN operations, DCO, OCO, and EW functions and tasks to support Army operations. DCO-IDM capabilities reside at these echelons, and the staff coordinates and synchronizes for nonorganic DCO-IDM support. (See FM 3-94 for additional information regarding the corps to brigade roles and responsibilities.) The staff may integrate nonorganic cyberspace and EW forces as authorized and required.

Cyberspace Electromagnetic Activities Outside of the Department of Defense Information Network

3-19. The corps and below commanders and staffs plan, integrate, and synchronize for cyberspace and EW operations outside of the DODIN. These echelons only execute actions outside the DODIN with the proper authority. The key staff members involved in these activities include the G-2 (S-2), G-3 (S-3), EWO, and fire support coordinator. The following list of activities is not all-inclusive. The corps and below commander and staff—

- Plan, request, and synchronize effects in cyberspace and the EMS supporting freedom of maneuver.
- Coordinate with higher headquarters staff to integrate and synchronize information collection efforts to support cyberspace and EW operations.
- Synchronize cyberspace and EW effects requests with organic targeting capabilities.
- Prepare and submit effect requests using the CERF or electronic attack request format (EARF).
- Develop, maintain, and disseminate a common operational picture of designated cyberspace and EMS to enable situational understanding.
- Prepare for cyberspace and EW operations by conducting information collection activities, technical rehearsals, and pre-operation checks and inspections.
- Conduct SMO for the headquarters and subordinate units within the area of operations.

Cyberspace Electromagnetic Activities Inside of the Department of Defense Information Network

3-20. The corps and below commanders and staffs plan, prepare, and synchronize for cyberspace and EW operations occurring primarily inside of the DODIN. The key staff members involved in these activities include the G-2 (S-2), G-3 (S-3), G-6 (S-6) (supported by the corps network operations and service center and corps signal company), and EWO. The following list of activities is not all-inclusive. The corps and below commander and staff—

- Plan, coordinate, prepare for, and conduct DODIN operations and DCO-IDM.
- Oversee and direct the planning, operations, and coordination of network transport, information services, and SMO.
- Establish the unit's portion of the DODIN and provide operational and technical support to subordinate elements.
- Design, build, configure, secure, operate, maintain, and sustain the network.
- Provide DODIN operations and management facilities including a network command element, cyberspace security, and communications security account.
- Establish and implement procedures for relevant information and information systems to develop and disseminate the common operational picture.
- Coordinate with the regional cyber center for matters concerning event and incident management, networthiness violations, DODIN operations tools, and cyberspace security tools.
- Plan, coordinate, integrate, prepare for, and conduct EW operations.
- Conduct SMO for the headquarters and subordinate units within the area of operations.

- Perform fault, configuration, accounting, performance, and security management of network system components and services to ensure systems and software applications meet the commander's operational requirements.
- Receive and integrate cyber protection teams and other enablers as directed by higher headquarters to support brigade DCO.
- Prepare and submit effect requests using the CERF, as required.
- Oversee and direct the planning, operations, and coordination of matters concerning DODIN operations, network transport, information services, and SMO for the corps and below headquarters and assigned units.
- Establish communications systems in area of operations and recommend DODIN operations priorities to support the commander's priorities.

3-21. Each of the staff elements has specific responsibilities that contribute to CEMA. The nucleus of CEMA are a coordination of actions, functions, and tasks with cyberspace and EMS implications. Operations which require targeting, defending the unit's portion of the DODIN, and integrating new equipment are examples of activities specific staff elements execute and coordinate with other staff elements as part of CEMA. (See figure 3-1 on page 3-6.)

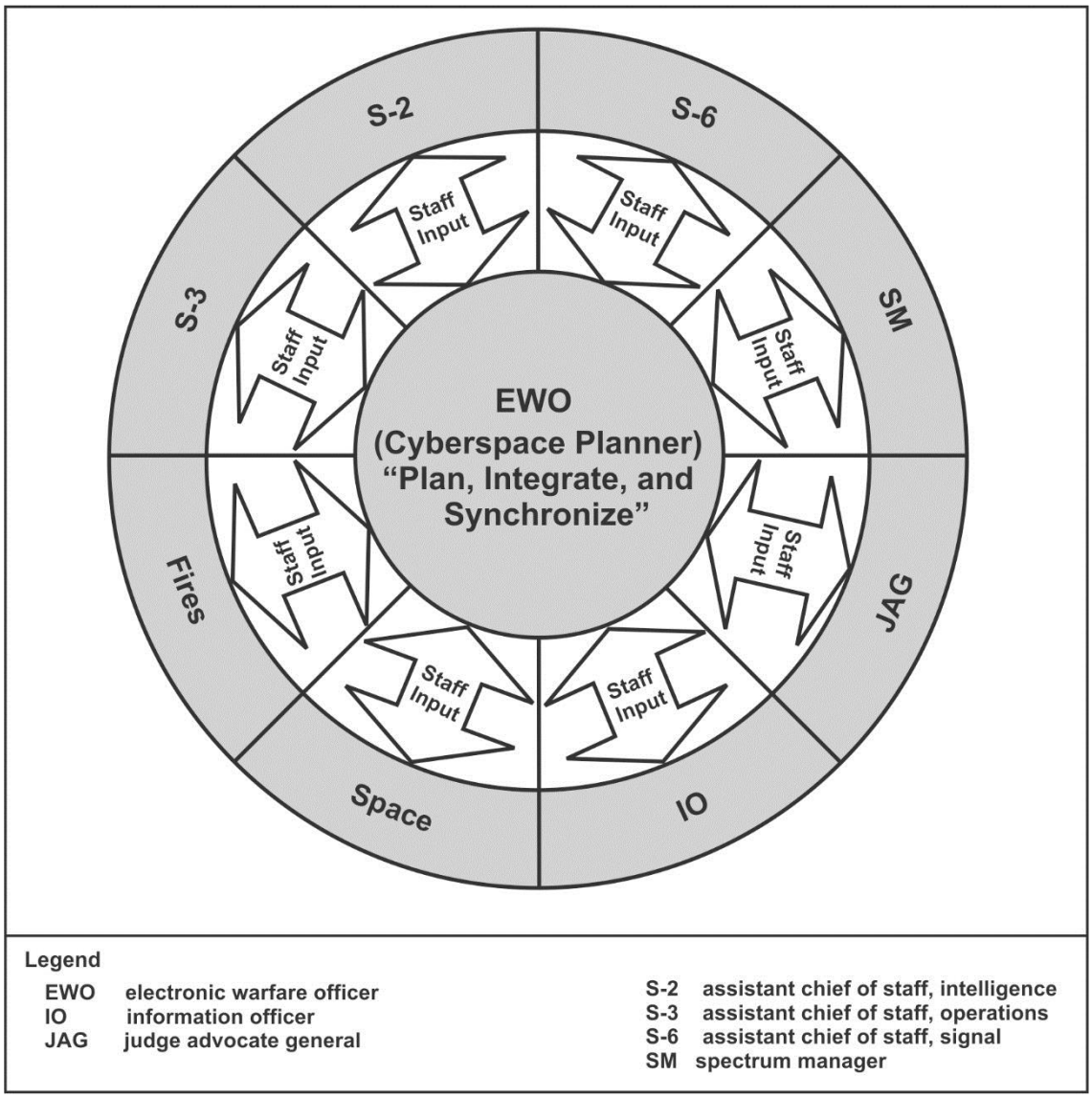


Figure 3-1. Cyberspace electromagnetic activities coordination and synchronization

Cyberspace Electromagnetic Activities Section

3-22. The CEMA section of the G-3 (S-3) from brigade to corps coordinates and synchronizes cyberspace and EW operations for effective collaboration across staff elements. This section includes the EWO (who has additional responsibility as the cyberspace planner), the spectrum manager, the EW technician, and EW noncommissioned officers. The CEMA section is key to the collaboration of cyberspace and EW operations. The cyberspace planner understands the operations and missions of the unit and the commander's intent. The CEMA section participates in the planning and targeting process, and leads the CEMA working group to support the MDMP. The cyberspace planner requests for effects provided by non-organic resources.

Electronic Warfare Officer (Cyberspace Planner)

3-23. The EWO serves as the commander's designated staff officer for the planning, integration, synchronization, and assessment of cyberspace and EW operations. The EWO collaborates with other members of the staff to integrate cyberspace and EW operations into the commander's concept of operations. As the cyberspace planner, the EWO is responsible for understanding policies relating to cyberspace, EW,

and SMO to provide accurate information to the commander for proper planning, coordination, and synchronization of cyberspace operations, EW, and SMO. Cyberspace planners (EWO)—

- Integrate, coordinate, and synchronize effects in cyberspace and the EMS.
- In coordination with the appropriate legal support, advises the commander on effects in cyberspace (including associated rules of engagement, impacts, and constraints).
- Develop and maintain the consolidated cyberspace target synchronization matrix and place on the units' target synchronization matrix.
- Nominate OCO and EW targets for approval from the fire support coordinator and commander.
- Receive, vet, and process OCO and EW targets from subordinate units.
- Develop and prioritize effects in cyberspace and the EMS.
- Develop and prioritize targets with the fire support coordinator.
- Monitor and continually assess measures of performance and measures of effectiveness of cyberspace and EW operations.
- Coordinate targeting and assessment collection with higher, adjacent, and subordinate organizations or units.
- Advise the commander and staff on plan modifications, based on the assessment.
- Advise the commander on how cyberspace and EW effects can impact the operational environment.
- Receive and integrate cyberspace operations team(s) and capabilities.
- Coordinate for OCO support on approved targets.
- Provide recommendations on commander's critical information requirements.
- Prepare and process the CERF and the EARF.
- Participate in other cells and working groups, as required, to ensure integration of cyberspace and EW operations.
- Deconflict EW operations with the spectrum manager.
- Coordinate the CEMA working group to plan and synchronize cyberspace and EW operations.
- Assist the G-2 (S-2) during IPB, as required.
- Provide information requirements to support planning, integration, and synchronization of cyberspace and EW operations.
- Serve as the Jam Control Authority (JCA) for EW operations as directed by the commander.
- Assist in the mission command of cyberspace operations as directed by the commander.

Electronic Warfare Personnel

3-24. The EWO, EW technician, or EW noncommissioned officer plans, coordinates, and supports EW as part of CEMA. EW personnel—

- Plan, coordinate, and assess EA, EP, and ES requirements.
- Support the G-2 (S-2) during IPB.
- Provide information collection requirements to the G-2 (S-2) to support the assessment, planning, preparation, and execution of EW.
- Support the fire support coordinator to ensure the integration of EA with all other effects.
- Provide tactical targeting information derived from EW support to the fire support coordinator.
- Prioritize EW effects and targets with the fire support coordinator.
- Plan and coordinate EW operations across functional and integrating cells.
- Deconflict EW operations with the spectrum manager.
- Maintain a current assessment of available EW resources.
- Participate in cells and working groups (as required) to ensure EW integration.
- Serve as EW subject matter expert on existing EW rules of engagement.
- When designated, serve as the EW jamming control authority.

- Prepare, submit for approval, and supervise the issuing and implementation of the EW portion of orders.
- Synchronize EW operations with the G-2 (S-2) to prevent conflicts with information collection activities.

Cyberspace Electromagnetic Activities Section Spectrum Manager

3-25. The CEMA section spectrum manager's role is to plan and synchronize EP; integrate and synchronize operational spectrum considerations across cyberspace and EW operations; and collaborate with the G-6 (S-6) spectrum manager on EW issues affecting SMO. (See ATP 3-36 for more information on spectrum management operations.) In support of CEMA the spectrum managers—

- Lead, develop, and synchronize the EW-EP plan by assessing EA effects on friendly force emitters.
- Mitigate harmful impact of EA on friendly forces through coordination with higher and subordinate units.
- Synchronize with intelligence on the EA effects to support intelligence gain and loss considerations.
- Synchronize cyberspace operations to protect radio frequency enabled transport layers.
- Coordinate to support protecting radio frequency enabled IO.
- Collaborate with staff, subordinate, and senior organizations to identify unit emitters for inclusion on the joint restricted frequency list.
- Perform EW related documentation and investigation of prohibitive electromagnetic interference to support the G-6 (S-6) led joint spectrum interference resolution program.
- Participate in the CEMA working group to deconflict EMS requirements.
- Provide advice and assistance in the planning and execution of spectrum portions of cyberspace and EW operations.

Assistant Chief of Staff, G-6 (S-6), Signal

3-26. The G-6 (S-6) staff conducts information management and facilitates knowledge management at theater and below levels. In collaboration with the joint force and multinational forces (as appropriate), the G-6 (S-6) staff directly or indirectly supports cyberspace operations by conducting DODIN operations. (For more information on DODIN operations and responsibilities, see FM 6-02.) The G-6 (S-6) is the primary staff representative responsible for SMO. The G-6 (S-6) staff—

- Assists the commander by establishing a tactical information network at theater levels and below to enable mission command.
- Conducts DODIN operation processes and network defense activities.
- Assists in the development of the cyberspace threat characteristics specific to enemy and adversary activities and related capabilities within friendly networks, and then advises on cyberspace operations courses of action.
- Conducts DCO-IDM risk assessments based on enemy or adversary tactics, techniques, and procedures; to identify vulnerabilities to key infrastructure that may require protection measures that exceed unit capabilities.
- Provides information on friendly cyberspace for situational awareness.
- Participates in the CEMA working group to deconflict friendly EMS requirements, support operations with communications requirements, provide DODIN operational picture for planning purposes, and provide subject matter expert information on wired and wireless networks.
- Coordinates for intelligence support to defense of the network.
- Ensures network is configured and monitored based on threat reports.
- Ensures defense-in-depth by effectively employing cybersecurity tools to provide network security status visibility to higher unit network operations security centers, supporting regional cyber centers, and the Army Cyber Operations and Integration Center.

- Coordinates with the supporting regional cyber center to ensure cybersecurity policy compliance; internet protocol address advertisement, identity, and access management; reporting requirements; and incident response procedures.
- Requests satellite and gateway access through the regional satellite communications support center.
- Coordinates with regional hub node to establish network connectivity and services.

Spectrum Manager

3-27. The spectrum manager coordinates EMS use for a wide variety of communications and electronic resources. The spectrum manager—

- Issues the signal operating instructions.
- Provides spectrum resources to the organization.
- Coordinates for spectrum usage with higher echelon G-6 (S-6), applicable host-nation, and international agencies as necessary.
- Coordinates the preparation of the joint restricted frequency list and issuance of emissions control guidance.
- Coordinates frequency allotment, assignment, and use.
- Coordinates electromagnetic deception plans and operations in which assigned communications resources participate.
- Coordinates measures to mitigate electromagnetic interference or natural phenomena.
- Coordinates with higher echelon spectrum managers for electromagnetic interference resolution that cannot be resolved internally.
- Assists the EWO in issuing guidance to the unit (including subordinate elements) regarding deconfliction and resolution of interference problems between EW systems and other friendly systems.
- Participates in the CEMA working group to deconflict friendly EMS requirements with planned EW, cyberspace operations, and information collection.

Assistant Chief of Staff, G-2 (S-2), Intelligence

3-28. The G-2 (S-2) provides intelligence to support CEMA. The intelligence staff facilitates understanding the enemy, terrain (including weather), and civil considerations. The G-2 (S-2) staff provides direct or indirect support to cyberspace and EW operations through information collection, support to situational understanding, and support to targeting and information capabilities. The G-2 (S-2)—

- Provides all-source intelligence support to CEMA.
- Coordinates with the intelligence community to help establish attribution for associated threat-initiated cyberspace, EA, or exploitation activities.
- Requests intelligence support and collaborates with the intelligence community for intelligence support to cyberspace and EW operations.
- Assists the commander and staff by providing information and intelligence on enemy and adversary cyberspace and EW threat characteristics. This facilitates situational understanding and supports decision making.
- Submits information requests to fill gaps identified during the MDMP.
- Ensures the information collection plan supports the target acquisition and combat assessment for targets.
- Collects, processes, stores, displays, and disseminates cyberspace and EW operations relevant information throughout the operations process and through the use of the mission command system.
- Contributes EP input for the joint restricted frequency list.
- Participates in the CEMA working group to intelligence support to planned cyberspace and EW operations.
- Develops cyberspace and EMS aspects of IPB.

- Coordinates for all source intelligence support to cyberspace and EW operations.

Information Operations Officer

3-29. The information operations officer (or assigned IO representative) integrates designated IRC and other capabilities a commander may use for IO, including coordinating for IO capabilities using cyberspace and the EMS. This staff officer is the primary advisor to the commander on ways to shape operational activity in and through the information environment and cyberspace that will degrade enemy or adversary decision making and protect our own. When integrating CEMA, the IO staff officer—

- Continually assesses IO implemented in and through cyberspace and the EMS and makes necessary adjustments.
- Identifies information capabilities and infrastructures in the area of operations that will impact the conduct of cyberspace and EW operations.
- Nominates and coordinates targets to the CEMA working group to integrate and deconflict effects with other information-related capability effects.
- Provides requirements for the information collection plan to enhance understanding and visualization of cyberspace aspects of the information environment within the operational area.
- Participates in the CEMA working group to coordinate IO requirements with planned cyberspace and EW operations.
- Coordinates cyberspace and EW operations support to IO.

Fire Support

3-30. Fire cells plan, coordinate, integrate, synchronize, and deconflict fire support, current and future, for the command including Army, joint, interorganizational, and multinational partners, as appropriate. Through targeting, CEMA are integrated and synchronized by the EWO. For CEMA, the fire support personnel—

- Review target nominations for inclusion to and verify addition on the joint integrated prioritized target list.
- Lead the targeting working group and participate in the targeting board.
- Provide input to the information collection plan and designate targets in coordination with the analysis and control element.
- Participate in the CEMA working group to deconflict targeting and fires requirements with cyberspace and EW operations.
- Ensure the synchronization of cyberspace and EW effects through the fires synchronization matrix.

Staff Judge Advocate

3-31. The staff judge advocate and staff advises the commander and the CEMA working group with respect to operational law and cyberspace actions, particularly if cyberspace operations may affect noncombatants. The staff judge advocate—

- Ensures cyberspace and EW actions comply with applicable policies and laws.
- Reviews potential cyberspace and EW operations according to relevant legal frameworks and authorities granted at national and regional command levels.
- Participates in the CEMA working group to provide legal advice on cyberspace and EW operations, as required.

Cyberspace Electromagnetic Activities Working Group

3-32. The CEMA working group is accountable for integrating cyberspace and EW operations and related actions into the concept of operations. CEMA working groups do not add additional structure to an existing organization. The CEMA working group is led by the EWO to analyze, coordinate, and provide recommendations for a particular purpose, event, or function. Deletions or modifications to the CEMA working group staff are based on requirements. See figure 3-2 on page 3-11 for an outline of the functions of the CEMA working group. The CEMA working group augments the function of the staff executing CEMA.

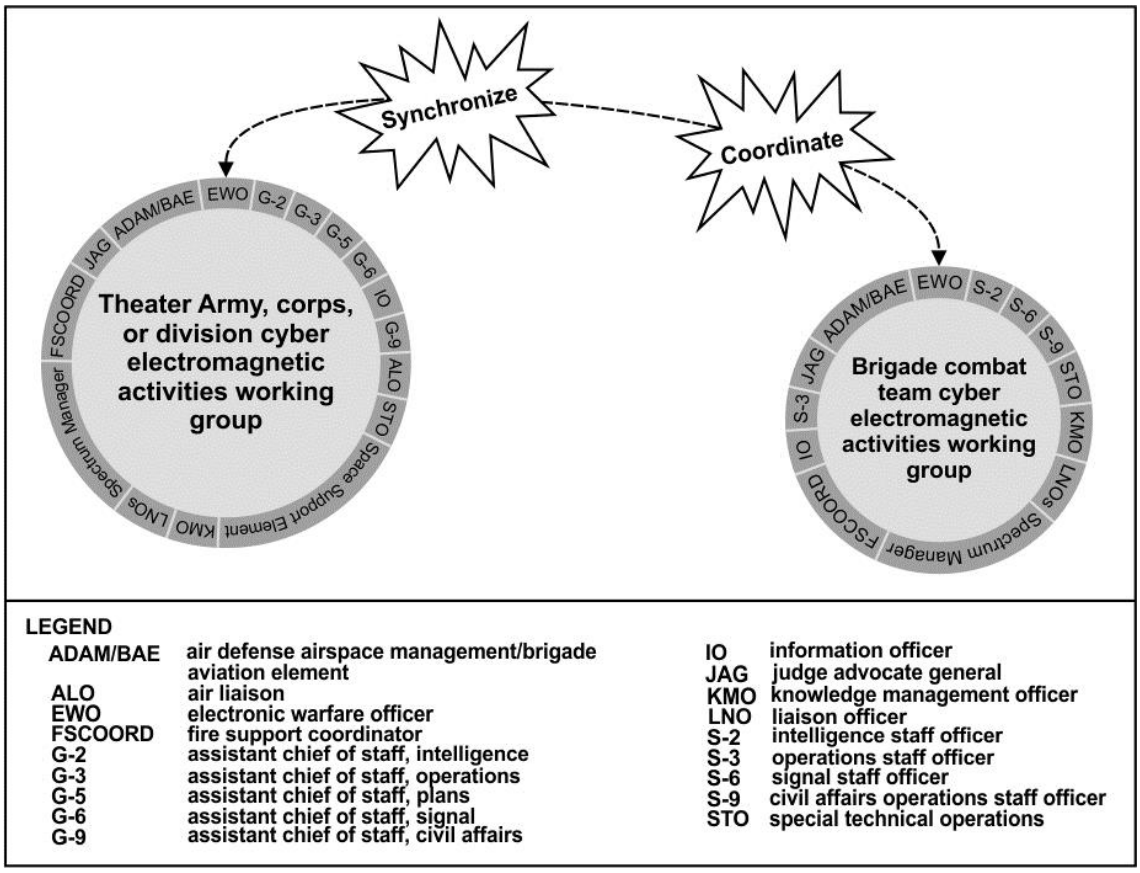


Figure 3-2. Cyberspace electromagnetic activities working group organization

ROLES IN THE CYBERSPACE ELECTROMAGNETIC ACTIVITIES WORKING GROUP

3-33. The CEMA working group is responsible for coordinating horizontally and vertically to support unified land operations and will primarily deconflict detection and delivery assets through the planning and targeting processes. Staff representation within the CEMA working group may include the G-2 (S-2), G-3 (S-3), G-6 (S-6), assistant chief of staff, civil affairs operations G-9 (S-9), fire support coordinator, IO officer, space support element, legal advisor, and a joint terminal attack controller when assigned. (See table 3-1 on page 3-12.) Deletions or modifications to the CEMA working group staff are based on requirements for certain capabilities and assets. When scheduled, the CEMA working group is a critical planning event integrated into the staff's battle rhythm.

Table 3-1. Tasks of the cyberspace electromagnetic activities working group

CEMA Working Group Participants	CEMA Working Group Functions
Division and above Airspace Management /brigade aviation element ALO EWO G-2 G-3 G-5 G-6 G-9 IO Officer FSCOORD JAG KMO LNOs Spectrum manager Space support element STO	• Plan, integrate, and synchronize cyberspace and EW operations to support operations or command requirements. • Plan and nominate targets within cyberspace and the EMS to achieve effects that support the commander's intent. • Develop and integrate cyberspace and EW operations actions into operations plans and operational concepts. • Develop information to support planning (joint restricted frequency list, spectrum management, and deconfliction). • Develop and promulgate CEMA policies and support higher-level policies. • Identify and coordinate intelligence support requirements for CEMA. • Maintain current assessment of resources available to the commander for cyberspace and EW operations. • Prioritize effects and targets for functions and capabilities within cyberspace and the EMS. • Predict effects of friendly and enemy cyberspace and EW operations. • Plan and submit measures of performance and effectiveness information requirements to intelligence section. • Identify the measures of effectiveness for cyberspace and EW operations. • Coordinate spectrum management and radio frequency deconfliction with G-6 and J-6. • Plan, assess, and implement friendly electronic security measures. • Ensure cyberspace and EW operations actions comply with applicable policy and laws. • Identify civilian and commercial cyberspace and EW operations related capacity and infrastructure within the area of operations.
Brigade ADAM/BAE ALO EWO FSCOORD JAG KMO S-2 S-3 S-6 S-9 IO Officer LNOs Spectrum manager	• Develop and integrate cyberspace and EW actions into operation plans and exercises. • Support CEMA policies. • Plan, prepare, execute, and assess cyberspace and EW operations. • Integrate intelligence preparation of the battlefield into the operations process. • Identify and coordinate intelligence support requirements for BCT and subordinate units' cyberspace and EW operations. • Assess offensive and defensive requirements for cyberspace and EW operations. • Maintain current assessment of cyberspace and EW resources available to the unit. • Nominate and submit approved targets within cyberspace to division. • Prioritize BCT targets within cyberspace and the EMS. • Plan, coordinate, and assess friendly CEMA. • Implement friendly electronic and network security measures (for example, electromagnetic spectrum mitigation and network protection). • Ensure cyberspace and EW operations actions comply with applicable policy and laws. • Identify civilian and commercial cyberspace and EMS-related capacity and infrastructure within the area of operations.

ADAM/BAE air defense airspace management/brigade aviation element operations
ALO air liaison officer
BCT brigade combat team
CEMA cyberspace electromagnetic activities staff
EMS electromagnetic spectrum
EW electronic warfare
EWO electronic warfare officer
FSCOORD fire support coordinator
G-2 assistant chief of staff, intelligence
G-3 assistant chief of staff, operations
G-5 assistant chief of staff, plans
G-6 assistant chief of staff, signal
G-9 assistant chief of staff, civil affairs
IO information operations
JAG judge advocate general
J-6 communications directorate of a joint
KMO knowledge management officer
LNO liaison officer
NCO noncommissioned officer
STO special technical operations
S-2 intelligence staff officer
S-3 operations staff officer
S-6 signal staff officer
S-9 civil affairs officer

Battalion

3-35. Battalions rely on their brigade for core services, network accessibility, and network defense. The battalion S-6 performs the planning and operations associated with the main and tactical command posts,

including establishing connectivity with adjacent, subordinate, and higher elements. Currently, battalions do not have organic capabilities to plan and integrate all aspects of cyberspace operations. Battalions do have capabilities to support cybersecurity policies and request for information regarding cyberspace and the EMS.

Company

3-36. Companies rely on their battalion for network service, access, and network defense. The company performs the planning and operations associated with the command post, including establishing connectivity with adjacent, subordinate, and higher elements. Commanders at this echelon are responsible for applicable cybersecurity measures.

PLANNING AND CYBERSPACE ELECTROMAGNETIC ACTIVITIES

3-37. The commander and staff include the cyberspace planner during the MDMP for operations. The cyberspace planner is the subject matter expert to create effects in cyberspace and the EMS, with considerations from the CEMA section. Involving the cyberspace planner early in development of the commander's vision and planning allows for synchronization and integration with missions, functions, and tasks. A consideration of cyberspace operations is the lead time required for effects support. Early involvement, inclusion in operations orders preparation, and effects approval early in the process enhance the possibility of effects in cyberspace and the EMS supporting an operation. The two primary methodologies commanders and staffs use for planning cyberspace and EW operations are the Army design methodology and the MDMP.

3-38. *Planning* is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Planning is one of the four major activities of mission command that occurs during operations process (plan, prepare, execute, and assess). Commanders apply the art of command and the science of control to ensure cyberspace and EW operations support the concept of operations.

3-39. The full scope of planning for cyberspace and EW operations is not addressed by the Army design methodology or the MDMP. These methodologies will allow Army forces to determine where and when effects in cyberspace and EW can be integrated to support the concept of operations. Army forces plan, prepare, execute, and assess cyberspace and EW operations in collaboration with the joint staff and other joint, interorganizational, and multinational partners as required. Whether cyberspace and EW operations are planned and directed from higher headquarters or requested from tactical units, timely staff actions and commander's involvement coupled with continued situational awareness of cyberspace and the EMS are critical for mission success.

3-40. Army commanders and staffs will likely coordinate or interact with joint forces to facilitate cyberspace operations. For this reason, commanders and staffs must have an awareness of joint planning systems and processes that facilitate cyberspace operations. Some of these processes and systems include the—

- Joint Operations Planning Process (see JP 5-0).
- Adaptive Planning and Execution System (see JP 5-0).
- Review and Approval Process Cyberspace Operations (see CJCS Manual 3139.01 and appendixes A and C).

ARMY DESIGN METHODOLOGY INCLUDING CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

3-41. The *Army design methodology* is a methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them (ADP 5-0). Given the unique and complex nature of cyberspace, commanders and staffs benefit from implementing the Army design methodology to guide more detailed planning during the MDMP. This entails framing an operational environment, framing a problem, and developing an operational approach to solve the problem. (See ATP 5-0.1 for additional information on the Army design methodology.)

3-42. Framing an operational environment involves critical and creative thinking by a group to build models that represent the current conditions of the operational environment (current state) and models that represent

what the operational environment should resemble at the conclusion of an operation (desired end state). A planning team designated by the commander will define, analyze, and synthesize characteristics of the operational and mission variables and develop desired future end states. Cyberspace should be considered within this framing effort for opportunities as they envision desired end states.

3-43. Framing a problem involves understanding and isolating the root causes of conflict discussed and depicted in the operational environment frame. Actors may represent obstacles for commanders as they seek to achieve desired end states. Creating and employing cyberspace capabilities shapes conditions in the operational environment supporting the commander's objectives.

THE MILITARY DECISION-MAKING PROCESS WITH CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

3-44. Cyberspace and EW operations planning is integrated into MDMP, an iterative planning methodology to understand the situation and mission, develop a course of action (COA), and produce an operation plan or order (ADP 5-0). The commander and staff integrate cyberspace and EW operations throughout the MDMP. They ensure courses of action are supported by the scheme of cyberspace operations and meet requirements for suitability, feasibility, and acceptability. Staff members responsible for planning and integrating cyberspace operations participate in the MDMP events and CEMA working groups.

3-45. The MDMP consists of the following seven steps—

- Step 1: Receipt of mission.
- Step 2: Mission analysis.
- Step 3: COA development.
- Step 4: COA analysis.
- Step 5: COA comparison.
- Step 6: COA approval.
- Step 7: Orders production, dissemination, and transition.

Receipt of Mission

3-46. Commanders initiate the MDMP upon receipt or in anticipation of a mission. Staff members responsible for planning and integrating cyberspace and EW operations initiate coordination with higher headquarters staff counterparts to obtain information on current and future cyberspace and EW operations, running estimates, and other cyberspace and EW operations planning products. Table 3-2 on page 3-15 explains cyberspace and EW operations planning inputs, actions, and outputs for step 1.

Table 3-2. The military decision-making process, step 1: receipt of mission

Key inputs	Process	Key outputs
Higher headquarters plan or order Planning products from higher headquarters including the cyberspace effects running estimate	Begin updating the cyberspace effects and electronic warfare running estimates Gather the tools to prepare for mission analysis specific to cyberspace operations Provide cyberspace and electronic warfare operations input for formulation of the commander's initial guidance and the initial warning order	Updated cyberspace effects and electronic warfare running estimate

Mission Analysis

3-47. Commanders and staffs perform mission analysis to better understand the situation and problem, identify what the command must accomplish, when and where it must be done, and why (the purpose of the operation). Staff members responsible for planning and integrating cyberspace and EW operations gather, analyze, and synthesize information on current conditions of the operational environment with an emphasis on cyberspace, the EMS, and the information environment.

3-48. The Army design methodology may have been performed before the MDMP, scheduled to occur in parallel with the MDMP, or it may not be fulfilled at all. Army design products, if and when available, should be reviewed by the commander and staff to enhance situational understanding and for integration into the MDMP.

3-49. *Intelligence preparation of the battlefield* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3). (See ATP 2-01.3 for additional information on the IPB.) Intelligence support to cyberspace and EW operations begins with the IPB and continues throughout the operations process. Staff members responsible for planning cyberspace operations will coordinate with the intelligence staff to identify enemy and adversary capabilities and their use of cyberspace and the EMS to assist in the development of models, situation templates, event templates, high-value targets, named areas of interest, and other outputs from the intelligence process, which include enemy and adversary cyberspace information. Table 3-3 on page 3-16 describes cyberspace operations planning inputs, actions, and outputs for step 2.

Table 3-3. The military decision-making process, step 2: mission analysis

Key inputs	Process	Key outputs
Commander's initial guidance Army design methodology product Higher headquarters' plans, orders, or knowledge products	Analyze inputs and develop information requirements Participate in the intelligence preparation of the battlefield process Identify and develop high-value targets Identify vulnerabilities of friendly, enemy, adversary, and neutral actors Determine cyberspace and electronic warfare operations specified, implied, and essential tasks Determine cyberspace operations limitations and constraints Identify cyberspace critical facts and assumptions Identify and nominate cyberspace related commander's critical information requirements Identify and nominate cyberspace critical information Provide input to the combined information overlay Provide input for the development of the mission analysis brief and warning order Participate in the mission analysis brief	List of cyberspace information requirements Intelligence preparation of the battlefield products to support cyberspace and electronic warfare operations Most likely and most dangerous enemy courses of action List of cyberspace operations specific and implied tasks List of cyberspace limitations and constraints List of cyberspace assumptions Updated cyberspace operations running estimate

Course of Action Development

3-50. COA development generates options for subsequent analysis and comparison that satisfy the commander's intent and planning guidance. Staff members responsible for planning and integrating cyberspace operations apply knowledge gained from the mission analysis step to help with overall COA development. During COA development, staff members responsible for planning cyberspace and EW operations develop an initial scheme of cyberspace and EW operations consisting of cyberspace support tasks. The scheme of cyberspace and EW operations describes how the commander intends to use cyberspace operations to support the concept of operations with an emphasis on the scheme of maneuver. Table 3-4 on page 3-17 lists cyberspace and EW operations planning inputs, actions, and outputs for step 3.

Table 3-4. The military decision-making process, step 3: course of action development

Key inputs	Process	Key outputs
Initial commander's planning guidance, mission, and intent Initial commander's critical information requirements Updated intelligence preparation of the battlefield products Updated cyberspace effects and electronic warfare running estimates Higher headquarters' plans, orders, or knowledge products	Develop information requirements for the information collection plan Integrate and synchronize cyberspace operations into the scheme of maneuver and concept of operations Analyze high-value targets and develop a list of tentative high-payoff targets Provide cyberspace input for the combined information overlay Develop initial scheme of cyberspace and electronic warfare operations Provide cyberspace operations and electronic warfare input for the development of the course of action development brief Begin development of cyber effects request format Begin development of electronic attack request format Submit cyber effects request format (if sufficient guidance on COAs exist)	Updated cyberspace operations and electronic warfare information requirements Cyberspace operations initial input for high-payoff target list and target folders Draft scheme of cyberspace operations including objectives and effects Updated cyberspace operations running estimate

3-51. Upon completion of COA development, many outputs from the mission analysis should be updated such as the cyberspace and EW operations-related input for the commander's critical information requirements and essential elements of friendly information. The staff updates the portions of the operations orders, including annexes and appendixes that contain cyberspace and EW operations information. (See Appendix B for an example of operations orders.)

Course of Action Analysis

3-52. COA analysis enables commanders and staffs to identify difficulties or coordination problems as well as probable consequences of planned actions for each COA under consideration. Staff members responsible for planning and integrating cyberspace and EW operations use the draft products from COA development to participate in COA analysis. During COA analysis, they refine their scheme of cyberspace and EW operations, ensuring that it nests with the scheme of maneuver.

3-53. Upon completion of COA analysis, operational planning continues with drafting and submitting the CERF and then updating these requests when the COA is later refined. Development and submission of the CERF is one method by which Army forces request, coordinate, and integrate effects to support cyberspace and EW operations. The CERF contains baseline information for coordinating and integrating effects in cyberspace and EW. Table 3-5 on page 3-18 describes cyberspace and EW operations planning inputs, actions, and outputs for step 4.

Table 3-5. The military decision-making process, step 4: course of action analysis

Key inputs	Process	Key outputs
Revised commanders planning guidance Cyberspace operations and electronic warfare initial requirements for high-payoff target list and supporting target folders Draft scheme of cyberspace operations Updated cyberspace effects and electronic warfare running estimates Higher headquarters' plans, orders, or knowledge products Feedback from submitted cyber effects request formats	Provide cyberspace operations and input and participate in the war-game briefing as required Develop cyber effects request format Develop input for electronic attack request format Continue development of scheme of cyberspace operations Provide cyberspace operations and electronic warfare input for the development of the decision support matrix and decision support template Provide refined cyberspace operations and electronic warfare input to the combined information overlay	Refined cyberspace and electronic warfare input to commander's critical information requirements Refined cyberspace operations and electronic warfare input to the high-payoff targets list Refined scheme of cyberspace operations Updated cyberspace effects and electronic warfare running estimate

Course of Action Comparison

3-54. COA comparison is an objective process to evaluate each COA independently and against set evaluation criteria approved by the commander and staff. Staff members responsible for cyberspace and EW operations may not be directly involved in this process, but will provide recommendations for consideration during the process. Upon completion of the COA comparison, output products and the base operation order, become final draft. Table 3-6 on page 3-19 lists cyberspace and EW operations planning inputs, actions, and outputs for step 5.

Table 3-6. The military decision-making process, step 5: course of action comparison

Key inputs	Process	Key outputs
War-game results Refined cyberspace operations and electronic warfare input to commander's critical information requirements Refined cyberspace operations and electronic warfare input to the high-payoff target list Refined scheme of cyberspace operations Updated cyberspace effects and electronic warfare running estimate Higher headquarters' plans, orders, or knowledge products Feedback from submitted cyber effects request formats	Conduct an analysis of advantages and disadvantages for each course of action Provide cyberspace operations input to the decision matrix tool as required Provide cyberspace operations input for the risk assessment (collateral effects evaluations) Develop recommendation for the most supportable course of action from a cyberspace operations perspective Provide cyberspace and electronic warfare operations input for the development of the course of action decision brief as required	Recommended course of action Updated cyberspace effects running estimate

Course of Action Approval

3-55. During COA approval the commander selects the COA to best accomplish the mission. The best COA must first be ethical, and then the most effective and efficient possible. The commander will issue final planning guidance including refined commander's intent, commander's critical information requirements, and any additional guidance on priorities for the warfighting functions. Table 3-7 on page 3-20 describes cyberspace and EW operations planning inputs, actions, and outputs for step 6.

Table 3-7. The military decision-making process, step 6: course of action approval

Key inputs	Process	Key outputs
Updated cyberspace effects running estimate including refined products for each course of action Evaluated courses of action Recommended course of action Higher headquarters' plans, orders, or knowledge products Feedback from submitted cyber effects request formats	Receive and respond to final planning guidance from the commander Assess implications and take actions to revise operation order products Finalize and submit cyber effects request formats Finalize and submit input for electronic attack request format Finalize scheme of cyberspace operations	Commander approved course of action Final draft Tab A (Offensive Cyberspace Operations) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final draft Tab B (Defensive Cyberspace Operations) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final draft Tab C (Electronic Attack) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final draft Tab D (Electronic Protect) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final draft Tab E (Electronic Warfare Support) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final draft cyberspace operations input to Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal) Final draft cyberspace operations input to Appendix 2 (DODIN Operations) to Annex H (Signal) Final cyberspace operations input to Annex B (Intelligence) and Annex L (Information Collection) Nominated targets in cyberspace and the EMS Updated intelligence preparation of the battlefield products to support cyberspace and electronic warfare operations

Orders Production, Dissemination, and Transition

3-56. The final step of the MDMP is orders production, dissemination, and transition. All planning products are finalized including the cyberspace and EW operations running estimate and CERF. As time permits, the staff may conduct a more detailed war game of the selected COA. Outputs are internally reconciled and

approved by the commander. Table 3-8 details cyberspace and EW operations planning inputs, actions, and outputs for step 7.

Table 3-8. The military decision-making process, step 7: orders production, dissemination, and transition

Key inputs	Process	Key outputs
Commander-approved course of action and any modifications Final draft operations order products Higher headquarters' plans, orders, or knowledge products Feedback from submitted cyber effects request formats	Participate in the staff plans and orders reconciliation as required Participate in the staff plans and orders crosswalk as required Provide final input to the risk assessment specific to cyberspace operations Finalize and submit cyber effects request formats Finalize and submit input for evaluation request messages as required Produce operations order products Participate in the operations order brief and confirmation brief as required	Final Tab A (Offensive Cyberspace Operations) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final Tab B (Defensive Cyberspace Operations) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final Tab C (Electronic Attack) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final Tab D (Electronic Protect) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final Tab E (Electronic Warfare Support) to Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) Final cyberspace operations input to Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal) Final cyberspace operations input to Appendix 2 (DODIN Operations) to Annex H (Signal) Final cyberspace operations input to Annex B (Intelligence) and Annex L (Information Collection)

CYBER EFFECTS REQUEST FORMAT AND TARGETING ACTIVITIES

3-57. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting is an integrating and iterative process that occurs throughout the major activities of the operations process. The functions of decide, detect, deliver, and assess define the targeting process and occur simultaneously and sequentially during the operations process. Targeting activities for cyberspace and EW operations which involve the employment of cyberspace and EW effects closely follow standard targeting processes.

3-58. Targets identified through the operations process appear on the integrated target list. Organic cyberspace and EW capabilities, with the proper authority, may fulfill the desired effect on the target. Time

and synchronization issues may affect the decision to use organic assets as well as the legal and operational authorities. The capability to affect targets may require proximity of capabilities and operational reach access.

3-59. If the unit's organic capabilities or authorities do not fulfill the targeting requirements to support the commander's intent, they request support from the next higher echelon. As requests pass from echelon to echelon, each unit processes the target packet or request to use organic capabilities and authorities to support the subordinate unit's requirement. The requirement elevates until it reaches an echelon that can support the requirement with the appropriate capabilities and authority, or the request for targeting is denied. Fulfilling cyberspace and EW effects requests on targets may not be possible due to prioritization, timing, capabilities, authorization, or conflict with other cyberspace and EW capability requirements.

3-60. Identifying targets early in the planning process is key to approval and synchronization. Integrating the targets into the normal targeting process identifies if the organic capabilities can achieve the desired effects. Due to their impact, some cyberspace and EW effects delivery capabilities (such as EA) require synchronization and coordination across the entire staff. Some effects may prohibit friendly use of cyberspace and EW, knowingly or inadvertently, and the situational awareness of the cyberspace and EW operation will enable the staff in taking the appropriate remediation actions and decisions.

3-61. OCO and EW targets not available for effects through Army means may continue to joint echelons for processing. The targets may require additional joint force cyberspace or EW assets to support the Army commander mission. This could result in the corps and below targets being included on the joint integrated prioritized target list. In addition, targets developed with the initial intention to employ cyberspace and EW effects may be struck with lethal fires or engaged through other non-lethal means.

3-62. In table 3-9 on page 3-23, targets are described as systems with components and subcomponents that enable the determination of aimpoints for designated friendly force capabilities. An *aimpoint* is a point associated with a target and assigned for a specific weapon impact (JP 3-60). To develop targets suitable for effects created by a cyberspace attack requires a concerted staff effort focused on IPB, cyber-enabled intelligence, the targeting process, and cyberspace information collection. Ultimately, decisions to employ cyberspace attack capabilities alone or with other capabilities will be determined by commanders, with the assistance of their staffs, throughout the operations process.

Table 3-9. Examples of simultaneous and complimentary effects

Target Description	Target System Components	System Subcomponent Aimpoint	Desired Effects by Various Army Capabilities
Integrated air defense forces	Early warning radars	Supporting network	Destroy (primary equipment) Disrupt (cueing flow) Degrade (sensor integrity) Deceive (operators and leadership)
	Support facilities	Public switched telephone network	Destroy (supporting nodes) Disrupt (command and control systems) Deny (secondary battery access)
Enemy safe haven	Virtual locations	Host server	Destroy (supporting nodes) Exploit (data and information) Degrade (content) Disrupt (data flow) Deceive (through false bonafides)
	Key personnel (for example, leaders, facilitators, and enablers)	Smartphone	Disrupt (command and control systems) Deny (access) Deceive (through false persona)

DECIDE

3-63. Decide is the first step in the targeting process. It begins with the MDMP. It does not end when the plan is completed; the decide function continues throughout the operation. Using the outputs from the planning process, commanders and staffs determine where and when effects in designated cyberspace should be created to support the concept of operations. Targeting has an initial focus on enemy and adversary networks.

3-64. Due to the nature of cyberspace operations, commanders should allow as much planning time as possible when requesting effects through cyberspace. Army commanders are encouraged to consider cyberspace and EW effects during the targeting process.

3-65. The characteristics of cyberspace and the EMS provide enemies and adversaries with considerable measures of anonymity. Information collection is critical for identifying potential enemies or adversaries in cyberspace. Designating targets that reside within cyberspace and the EMS depends heavily on the information collection effort. Each designated target is assigned to the most appropriate means to achieve the desired effect, which may include lethal fires.

3-66. An important part of this step in the targeting process is identifying potential adverse impacts and mitigating them. This requires coordination and synchronization on the part of the staff executing CEMA. Any action in cyberspace and the EMS, either offensive or defensive, must be coordinated and balanced with potential degradation inflicted on friendly systems. The SMO enabling component to CEMA are leveraged to ensure that EA does not cause unwanted interference on friendly systems or degrade friendly networks.

3-67. During the decide step, the staff develops information regarding cyberspace and EW targets by asking—

- What targets should be affected?
- When and where are the targets likely to be identified, accessed, or otherwise engaged to create desired effects?

- How long will the targets remain accessible?
- What are the related information collection requirements essential to the targeting effort; and how and when must the information be collected, processed, and disseminated?
- When, where, how, why, and in what priority should the targets be affected?
- What are the measures of performance and measures of effectiveness?
- What or who will obtain assessment or other information required for determining the success or failure of each engagement of target nodes? Who must receive and process that information, how rapidly, and in what format?

DETECT

3-68. Detect is the next critical function in targeting. The information collection plan is a critical component of the detect function. Information requirements in cyberspace are considered throughout the intelligence process and the G-2 (S-2) serves a key role in developing and managing the information collection plan specific to cyberspace.

3-69. The detailed analysis of cyberspace provides information as network topology, configuration, and enemy and adversary actions. During this step units gather the information needed to gain access, pair a capability, and develop the necessary intelligence to vet and validate nominated targets. After analysis, it may be possible to determine enemy intentions, when combined with other information. Situational understanding of the EMS is attained through situational data as geospatial location, signal strength, system type, and frequency of target to focus effects on the intended target.

3-70. The detect function includes tasks in and through specific portions of cyberspace or the EMS to locate, track, and validate targets or follow on action by friendly forces. Target development, vetting, and validation are implemented in parallel with the information collection plan.

DELIVER

3-71. The CEMA section, through the targeting process, ensures the full coordination, integration, deconfliction, and employment of cyberspace and EW effects according to the commander's scheme of maneuver. Close coordination between collection assets and delivery assets is critical during the engagement to avoid unintended effects and enable the assessment phase.

3-72. Attack guidance for target is initiated because of the detection function and executed as planned. Close coordination is required between those engaged in detecting targets and those engaged in delivering effects upon targets. Integration and synchronization is vitally important during the deliver step.

ASSESS

3-73. Assessment occurs throughout the operations process. Targeting in cyberspace is continually refined and adjusted between the commander and staff during the operation. Assessment in cyberspace provides information on the effectiveness of decide and detect functions and whether the targets need reengaging. Although assessment is discussed as a final step in the operations process, it also informs and guides the other activities of the operations process. Assessment involves deliberately comparing forecasted outcomes with actual events to determine the overall effectiveness of force employment. Measures of performance and measures of effectiveness are key activities during assessment.

Note. Commanders should be aware that full assessment of effects in cyberspace may be more complex due to the nature of cyberspace operations.

3-74. Effects produced in cyberspace are not always physically visible or apparent. In certain cases, intelligence processing, exploitation, and dissemination may provide the raw data. This data is converted into information that then supports the execution of CEMA. In some cases, intelligence is available for immediate use by tactical forces. Intelligence is the primary contributor to the assessment of effects on enemies and adversaries and their reactions to counter these effects. Intelligence allows for the adjustment of the targeting process. (For more information on intelligence, see ADRP 2-0, FM 2-0, and ATP 2-01.3.)

3-75. Commanders and staffs continually assess operations by using measures of performance and measures of effectiveness. A measure of performance is a criterion used to assess friendly actions tied to measuring task accomplishment. A measure of effectiveness is a criterion used to assess changes in system or enemy behavior, capability, or operational environment. A measure of effectiveness is an identifiable and measureable event or action which tells the commander that the action taken had the desired effect. The action was effective.

3-76. Measures of performance help answer the following questions—

- Was the action taken?
- Were the tasks completed to standard?

3-77. Examples of measures of performance may include the following—

- Were DCO-IDM conducted in response to detected intrusions? What types, on what networks, and how many times per day?
- Was the adversary contained and cleared to or from the designated location (DCO-IDM)?
- Did the sensors get put in place to monitor traffic (screening operations)?
- Did the sensors cover the suspected adversary entry points into the network?

3-78. Assessment of effectiveness may occur external to the requesting organization. The effectiveness of a requested effect may not be realized by the requester. A *measure of effectiveness* is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (JP 3-0). Measures of effectiveness help measure changes in conditions, both positive and negative.

3-79. Measures of effectiveness help answer the following—

- Was the purpose accomplished?
- Measures the why in the mission statement.

3-80. Examples of measures of effectiveness may include the following—

- Were there any valid intrusions on critical networks?
- Did OCO have the intended effect?
- Did the target change behavior?

This page intentionally left blank.

Appendix A

Integration with Unified Action Partners

Army forces conduct operations as part of a joint, interdependent force. In addition, they routinely work with multinational forces and interagency, intergovernmental, and nongovernmental partners as part of unified action. As such, Army commanders must work with unified action partners throughout the operations process. This chapter discusses how commanders and staffs integrate cyberspace electromagnetic activities with unified action partners.

JOINT OPERATIONS CONSIDERATIONS

A-1. Army operations that involve the use of cyberspace and the EMS can have joint implications. Each Service component has cyberspace operations, EMS requirements, and EW capabilities that contribute to an integrated whole, synchronized by a joint force headquarters. The CEMA section ensures that cyberspace and EW operations align with joint IO, cyberspace operations, EW, SMO, and doctrine.

A-2. Army units may work as subordinate elements of a joint task force or form the core headquarters of a joint task force. The Army uses its CEMA section to integrate cyberspace and EW operations into the joint operations planning process. The integration of these capabilities into operations occurs at the IO working group, at the joint spectrum management element in the communications directorate of a joint staff for SMO, and for EW that may occur at the joint EW cell in the joint force headquarters. When transitioning to become a part of a joint task force, an Army unit has the option of maintaining the CEMA section separately from the joint EW cell, integrating the element into the higher CEMA section, or converting to a joint organization model.

A-3. The theater campaign plan guides the planning of CEMA. The Army contributes an integrated CEMA plan to support joint operations. (For more information on joint IO, see JP 3-13. For more information on joint SMO, see JP 6-01.)

INTERAGENCY AND INTERGOVERNMENTAL CONSIDERATIONS

A-4. Army commanders must consider the unique capabilities, structures, and priorities of interagency and intergovernmental partners in the execution of CEMA. Successful execution of missions with partners requires a shared understanding and common objective for the operation.

A-5. Interagency and intergovernmental partners often have command relationships, lines of authority, and planning processes that can vary greatly from the Army. This will generally require liaison elements to be in place before operations, as it will likely be too late and ineffective to establish these elements after-the-fact. Partners often manage tasks through committees, steering groups, and interagency working groups organized along functional lines. The commander is responsible for developing interagency and intergovernmental coordination requirements and will likely require a robust liaison element similar to that required for multinational operations.

A-6. Interagency and intergovernmental partners sometimes have policies that differ or are more restrictive than the Army's policies. These differences manifest in legal authorities, roles, responsibilities, procedures, and decision-making processes. The commander must ensure that the interagency and intergovernmental planners clearly understand military capabilities, requirements, operational limitations, liaisons, and legal considerations. Staffs integrating these partners into operations must understand the nature of these relationships and types of support that partners can provide. Commanders will likely need to achieve consensus in the absence of a formal command structure to accomplish mission objectives with these organizations.

MULTINATIONAL CONSIDERATIONS

A-7. Army units executing CEMA within multinational operations require a robust liaison effort. Effective liaison mitigates complications caused by differences in policy and facilitates system integration and information sharing.

A-8. Differences in national standards and laws pertaining to sovereignty in cyberspace and the EMS may affect the willingness or the legality of a country's participation in CEMA. Some partners may refuse to participate, while others will enable or undertake their own operations separate from the Army commander's mission.

A-9. Connectivity is essential when multi-national forces function in mutual support during combat operations. Connectivity issues may be compounded by interoperability issues. Hardware and software incompatibilities and disparities in standards, information security, and information assurance policy may cause gaps in security or capability that require additional effort to fix. This will likely slow down the collection, dissemination, and sharing of information among partners. Commanders and staffs should anticipate connectivity incompatibilities and disparities before entering a multinational operation.

A-10. Intelligence and information sharing with allies and multinational partners is important during multinational operations. Special attention and awareness is important when sharing information due to specific and varying classification sharing policies. When synchronizing cyberspace and EW operations with multinational partners, Army units must ensure adherence to foreign disclosure and cybersecurity procedures. Security restrictions may prevent full disclosure of some cyberspace and electromagnetic capabilities or planning, which may severely limit synchronization efforts. Effective synchronization requires access to systems and information at the lowest appropriate security classification level. Commanders are responsible for establishing procedures for foreign disclosure of intelligence information. (See AR 380-10 for more information on foreign disclosure.)

NONGOVERNMENTAL ORGANIZATIONS CONSIDERATIONS

A-11. Commanders ensure adherence to cybersecurity procedures when conducting cyberspace operations with nongovernmental organizations. Planning with nongovernmental organizations may be necessary for foreign humanitarian assistance, peace operations, and civil military operations. Incorporation of these organizations into an operation requires the commander to balance the need of the nongovernmental organization for information with operation security. Many nongovernmental organizations may be hesitant to become associated with the military to prevent compromising their status as independent entities. Many seek to maintain this status to prevent losing their freedom of movement or to keep their members from being at risk in hostile environments. Strategic level planning for inclusion of nongovernmental organizations into civil affairs operations will likely need to coordinate cyberspace operations.

HOST NATION CONSIDERATIONS

A-12. Each nation has sovereignty over its EMS and cyberspace components within its geographic area. The use of a nation's cyberspace and the EMS require coordination and negotiation through formal approvals and certifications. Host nation coordination with regard to the use of the EMS is a function of SMO. Coordinating spectrum use is based largely on the potential for electromagnetic interference with local receivers. This coordination ensures initial spectrum availability and supportability for operations and establishes cyberspace availability, such as bandwidth allocation. Additionally, coordination seeks to develop an interoperable cyberspace defense capability. Considerations for coordination must be given to adjacent countries, particularly if forces stage, train, or operate within these countries. Likewise, compatibility of protective measures, such as countermeasures systems, is essential to avoid system fratricide that degrades protection for all.

INSTALLATION CONSIDERATIONS

A-13. Cyberspace and EW operations systems are complex and constantly evolving. Warfighter readiness and the ability to fight upon arrival are crucial for a fully capable, ready force. Commanders and system

operators must be proficient at using the cyberspace and EW tools, systems, and processes necessary to execute CEMA.

A-14. Executing CEMA in a garrison environment presents unique challenges for several reasons. First, staffs may not be co-located physically, and this requires them to use telephonic or virtual collaboration and coordination. Second, the limitations on cyberspace and EW operations will be constrained due to laws, policies, and regulations. Third, specific mission sets for different installations (testing, training, and maintenance) may require special considerations. Lastly, operational relationships with garrison organizations such as the Network Enterprise Center need to be firmly established.

PRIVATE INDUSTRY CONSIDERATIONS

A-15. Private industry plays a significant role in cyberspace and the EMS. The Army relies on its connectivity with its defense industrial base partners and the private industry for many of its non-warfighting day-to-day functions for support and sustainment. Examples include electronic databases and interfaces for medical services, accounting and finance services, personnel records, equipment maintenance, and logistics functions. Global transport and logistics require data exchange between military and private networks. The Army relies on shipping companies, transportation grid providers, and suppliers as a part of the global transportation system.

A-16. The security and reliability of private industry networks directly affects DOD operations. These networks are not administered by DOD personnel, but they are essential to effective Army operations. Responsibility for these networks falls on the network owners.

A-17. Private industry has proven to be the primary catalyst for advancements in information technology. This has resulted in the DOD becoming increasingly reliant on commercial off-the-shelf technology. Many of these products are developed by, manufactured by, or have components produced by foreign countries. These manufacturers, vendors, service providers, and developers can be influenced by adversaries or unwittingly used by them to provide counterfeit products or products that have built-in vulnerabilities. The DD Form 1494 (Application for Equipment Frequency Allocation) process determines compatibility and interoperability of commercial off-the-shelf systems that use the EMS to support national needs. Risk assessments and procedures should be followed to ensure proper supply chain management and the acquisition of software and hardware does not adversely affect the security of the DODIN.

A-18. The DODIN resides on commercial networks as undersea cables, fiber optic networks, telecommunication services, satellite and microwave antennas from local telephone companies, and leased channels from satellites. Many of these commercial networks are under foreign ownership, control, and influence. This makes the conduct of cyberspace and EW operations vulnerable to access denial, service interruption, communications interception and monitoring, infiltration, and data compromise. Army commanders pursue risk mitigation through adherence to operations security, cybersecurity policies, inspection of vendor supplied equipment, encryption, and promotion of user and commander education.

This page intentionally left blank.

Appendix B

Cyberspace in Operations Orders

Appendix B highlights the location of cyberspace operations information in operations orders and Appendix 12 to Annex C.

OPERATIONS ORDERS AND CYBERSPACE ELECTROMAGNETIC ACTIVITIES

B-1. Operations Orders, fragmentary orders, and warning orders include cyberspace operations information. The information is throughout the orders in different attachments found in Annex C and Annex H. The sections in the base operations orders and fragmentary orders with cyberspace operations information are paragraph 3, c; 3, g; and paragraph 5, c. Warning orders have cyberspace operations information in paragraph 5, c.

B-2. Annexes to the operations order also have cyberspace operations information. All annexes in paragraph 5, Command and Signal, have a subsection to describe the communications plan among the issuing force and interagency organizations including the primary and alternate means of communications. The subsection includes operations security requirements and indicates to refer to Annex H (Signal) as required. Tabs C, D, and E of Annex C contain operations information necessary for close coordination with cyberspace operations. The assistant chief of staff, plans (G-5) or the G-3 (S-3) writes Annex C and the G-6 (S-6) writes Annex H. The attachments to the base orders containing detailed information on cyberspace operations include—

- ANNEX C–OPERATIONS (G-5 OR G-3 [S-3]).
  - Appendix 12–Cyberspace Electromagnetic Activities (Electronic Warfare Officer).
  - Tab A–Offensive Cyberspace Operations.
  - Tab B–Defensive Cyberspace Operations (RA & IDM).
  - Tab C–Electronic Attack.
  - Tab D–Electronic Protection.
  - Tab E–Electronic Warfare Support.
- ANNEX H–SIGNAL (G-6 [S-6]).
  - Appendix 1–Defensive Cyberspace Operations.
  - Appendix 2–DODIN Operations.
  - Appendix 3–Voice, Video, and Data Network Diagrams.
  - Appendix 4–Satellite Communications.
  - Appendix 5–Foreign Data Exchanges.
  - Appendix 6–Spectrum Management Operations.
  - Appendix 7–Information Services.

Note. See FM 6-0 for more information on operations orders, fragmentary orders, and warning orders.

APPENDIX 12 (CYBERSPACE ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPERATIONS PLANS AND ORDERS

B-3. Commanders and staffs use Appendix 12 to Annex C to operations plans and orders to describe the cyberspace and EW operations support in a base plan or order. The EWO is the staff officer responsible for this appendix. This Appendix 12 is a guide, and it should not limit the information contained in an actual Appendix 12 based on this recommended context. Appendix 12 should be specific to the operation plan and order being conducted, and therefore content of actual Appendix 12 will vary greatly.

B-4. This appendix describes CEMA and objectives. Complex cyberspace and EW support may require a schematic to show integration and synchronization requirements and task relationships. This includes a discussion of the overall cyberspace and EW concept of operations, required support, and specific details in element subparagraphs and attachments. This appendix contains the information needed to synchronize timing relationships of each of the elements related to cyberspace and EW operations. This appendix also includes related constraints, if appropriate. Figures B-1 to B-5 describe the sections of Appendix 12 to Annex C of the operations order.

[CLASSIFICATION]

Place the classification at the top and bottom of every page of the OPLAN or OPORD. Place the classification marking at the front of each paragraph and subparagraph in parentheses. See AR 380-5 for classification and release marking instructions.

Copy ## of ## copies
Issuing headquarters
Place of issue
Date-time group of signature
Message reference number

Include the full heading if attachment is distributed separately from the base order or higher-level attachment.

APPENDIX 12 (CYBERSPACE ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarter] [(classification of title)]

(U) **References:** *Add any specific references to cyberspace electromagnetic activities, if needed.*

1. (U) Situation. *Include information affecting cyberspace and electronic warfare (EW) operations that paragraph 1 of Annex C (Operations) does not cover or that needs expansion.*

a. (U) Area of Interest. *Include information affecting cyberspace and the electromagnetic spectrum (EMS); cyberspace may expand the area of local interest to a worldwide interest.*

b. (U) Area of Operations. *Include information affecting cyberspace and the EMS; cyberspace may expand the area of operations outside the physical maneuver space.*

c. (U) Enemy Forces. *List known and templated locations and cyberspace and EW unit activities for one echelon above and two echelons below the order. Identify the vulnerabilities of enemy information systems and cyberspace and EW systems. List enemy cyberspace and EW operations that will impact friendly operations. State probable enemy courses of action and employment of enemy cyberspace and EW assets. See Annex B (Intelligence) as required.*

d. (U) Friendly Forces. *Outline the higher headquarters' cyberspace electromagnetic activities (CEMA) plan. List plan designation, location and outline of higher, adjacent, and other cyberspace and EW operations assets that support or impact the issuing headquarters or require coordination and additional support. Identify friendly cyberspace and EW operations assets and resources that affect the subordinate commander. Identify friendly forces cyberspace and EMS vulnerabilities. Identify friendly foreign forces with which subordinate commanders may operate. Identify potential conflicts within the EMS, especially for joint or multinational operations. Deconflict and prioritize spectrum distribution.*

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. *Identify and describe other organizations in the area of operations that may impact cyberspace and EW operations or implementation of cyberspace and EW operations specific equipment and tactics. See Annex V (Interagency) as required.*

[page number]
[CLASSIFICATION]

Figure B-1. Appendix 12-cyberspace electromagnetic activities

[CLASSIFICATION]

f. (U) Third Party. *Identify and describe other organizations, both local and external to the area of operations that have the ability to influence cyberspace and EW operations or the implementation of cyberspace and EW operations specific equipment and tactics. This category includes criminal and non-state sponsored rogue elements.*

g. (U) Civil Considerations. *Describe the aspects of the civil situation that impact cyberspace and EW operations. See Tab C (Civil Considerations) to Appendix 1 (Intelligence Estimate) to Annex B (Intelligence) and Annex K (Civil Affairs Operations) as required.*

h. (U) Attachments and Detachments. *List units attached or detached only as necessary to clarify task organization. List any cyberspace and EW operations assets attached or detached, and resources available from higher headquarters. See Annex A (Task Organization) as required.*

i. (U) Assumptions. *List any CEMA specific assumptions.*

2. (U) **Mission**. *State the commander's mission and describe cyberspace and EW operations to support the base plan or order.*

3. (U) Execution.

a. Scheme of Cyberspace Electromagnetic Activities. *Describe how cyberspace and EW operations support the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how cyberspace and EW effects will degrade, disrupt, deny, and deceive the enemy. State the defensive and offensive cyberspace and EW measures. Identify target sets and effects, by priority. Describe the general concept for the integration of cyberspace and EW operations. List the staff sections, elements, and working groups responsible for aspects of CEMA. Include the cyberspace and EW collection methods for information developed in staff section, elements, and working groups outside the CEMA section and working group. Describe the plan for the integration of unified action and nongovernmental partners and organizations. See Annex C (Operations) as required. This section is designed to provide insight and understanding of the components of cyberspace and EW and how these activities are integrated across the operational plan. It is recommended that this appendix include an understanding of technical requirements.*

This appendix concentrates on the integration requirements for cyberspace and EW operations and references appropriate annexes and appendixes as needed to reduce duplication.

(1) (U) Organization for Combat. Provide direction for the proper organization for combat, including the unit designation, nomenclature, and tactical task.

(2) (U) Miscellaneous. Provide any other information necessary for planning not already mentioned.

b. (U) Scheme of Cyberspace Operations. *Describe how cyberspace operations support the commander's intent and concept of operations. Describe the general concept for the implementation of planned cyberspace operations measures. Describe the process to integrate unified action partners and nongovernmental organizations into operations, including cyberspace requirements and constraints. Identify risks associated with cyberspace operations. Include collateral damage, discovery, attribution, fratricide (to U.S. or allied or multinational networks or information), and possible conflicts. Describe actions that will prevent enemy and adversary action(s) to critically degrade the unified command's ability to effectively conduct military operations in its area of operations. Identify countermeasures and the responsible agency. List the warnings, and how they will be monitored. State how the cyberspace operations tasks will destroy, degrade, disrupt, and deny enemy computer networks. Identify and prioritize target sets and effect(s) in cyberspace. If appropriate, state how cyberspace operations support the accomplishment of the operation. Identify plans to detect or assign attribution of enemy and adversary actions in the physical domains and cyberspace. Ensure subordinate units are conducting*

[page number]
[CLASSIFICATION]

Figure B-1. Appendix 12-cyberspace electromagnetic activities (continued)

[CLASSIFICATION]

defensive cyberspace operations (DCO). Synchronize the CEMA section with the IO officer. Pass requests for offensive cyberspace operations (OCO) to higher headquarters for approval and implementation. Describe how DOD information network operations support the commander's intent and concept of operations. Synchronize DODIN operations with the G-6 (S-6). *Prioritize the allocation of applications utilizing cyberspace. Ensure the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Considerations should be made for degraded network operations. (Reference appropriate annexes and appendixes as needed to reduce duplication).*

(1) (U) DODIN Operations. *Describe how information operations are coordinated, synchronized, and support operations integrated with the G-6 (S-6) to design, build, configure, secure, operate, maintain, and sustain networks. See Annex H (Signal) as required*.

(2) (U) Defensive Cyberspace Operations. *Describe how DCO are conducted, coordinated, integrated, synchronized, and support operations to defend the DODIN-A and preserve the ability to utilize friendly cyberspace capabilities.*

(3) (U) Offensive Cyberspace Operations. *Describe how OCO are coordinated, integrated, synchronized, and support operations to achieve real time awareness and direct dynamic actions and response actions. Include target identification and operational pattern information, exploit and attack functions, and maintain intelligence information. Describe the authorities required to conduct OCO.*

c. (U) Scheme of Electronic Warfare. *Describe how EW supports the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how the EW tasks will degrade, disrupt, deny, and deceive the enemy. Describe the process to integrate and coordinate unified action partner EW capabilities which support the commander's intent and concept of operations. State the electronic attack, electronic protection, and electronic warfare support measures and plan for integration. Identify target sets and effects, by priority, for EW operations.*

Synchronize with IO officer. See the following attachments as required: Tab C, D, E (Electronic Warfare) to Appendix 12 (Cyberspace Electromagnetic Activities); Appendix 15 (Information Operations of Annex C).

(1) (U) Electronic Attack. *Describe how offensive EW activities are coordinated, integrated, synchronized, and support operations. See Tab C (Electronic Attack) to Appendix 12 (Cyberspace Electromagnetic Activities)*.

(2) (U) Electronic Protection. *Describe how defensive EW activities are coordinated, synchronized, and support operations. See Tab D (Electronic Protection) to Appendix 12 (Cyberspace Electromagnetic Activities)*.

(3) (U) Electronic Warfare Support. *Describe how EW support activities are coordinated, synchronized, and support operations. See Tab E (Electronic Warfare Support) to Appendix 12 (Cyberspace Electromagnetic Activities)*.

d. (U) Scheme of Spectrum Management Operations. *Describe how spectrum management operations (SMO) support the commander's intent and concept of operations. Outline the effects the commander wants to achieve while prioritizing SMO tasks. List the objectives and primary tasks to achieve those objectives. State the spectrum management, frequency assignment, host nation coordination, and policy implementation plan. Describe the plan for the integration of unified action partners' SMO capabilities. See Annex H (Signal) as required.*

e. (U) Tasks to Subordinate Units. *List cyberspace and EW operations tasks assigned to each subordinate unit not contained in the base order.*

[page number]
[CLASSIFICATION]

Figure B-1. Appendix 12-cyberspace electromagnetic activities (continued)

[CLASSIFICATION]

f. (U) Coordinating Instructions. *List cyberspace and EW operations instructions applicable to two or more subordinate units not covered in the base order. Identify and highlight any cyberspace and EW operations specific rules of engagement, risk reduction control measures, environmental considerations, coordination requirements between units, and commander's critical information requirements and critical information that pertain to CEMA.*

4. (U) Sustainment. *Identify priorities of sustainment for cyberspace and EW operations key tasks and specify additional instructions as required. See Annex F (Sustainment) as required.*

a. (U) Logistics. *Use subparagraphs to identify priorities and specific instruction for logistics pertaining to cyberspace and EW operations. See Appendix 1 (Logistics) to Annex F (Sustainment) and Annex P (Host Nation Support) as required.*

b. (U) Personnel. *Use subparagraphs to identify priorities and specific instruction for human resources support pertaining to cyberspace and EW operations. See Appendix 2 (Personnel Services Support) to Annex F (Sustainment) as required.*

c. (U) Health System Support. *See Appendix 3 (Army Health System Support) to Annex F (Sustainment) as required.*

5. (U) Command and Signal.

a. (U) Command.

(1) (U) Location of Commander. *State the location of key cyberspace and EW operations leaders.*

(2) (U) Liaison Requirements. *State the cyberspace and EW operations liaison requirements not covered in the unit's SOPs.*

b. (U) Control.

(1) (U) Command Posts. *Describe the employment of cyberspace and EW operations specific command posts (CPs), including the location of each CP and its time of opening and closing.*

(2) (U) Reports. *List cyberspace and EW operations specific reports not covered in SOPs. See Annex R (Reports) as required.*

c. (U) Signal. *Address any cyberspace and EW operations specific communications requirements. See Annex H (Signal) as required.*

ACKNOWLEDGE: *Include only if attachment is distributed separately from the base order.*

[Commander's last name]
[Commander's rank]

The commander or authorized representative signs the original copy of the attachment. If the representative signs the original, add the phrase "For the Commander." The signed copy is the historical copy and remains in the headquarters' files.

OFFICIAL:

[Authenticator's name]
[Authenticator's position]

[page number]
[CLASSIFICATION]

Figure B-1. Appendix 12-cyberspace electromagnetic activities (continued)

[CLASSIFICATION]

Use only if the commander does not sign the original attachment. If the commander signs the original, no further authentication is required. If the commander does not sign, the signature of the preparing staff officer requires authentication and only the last name and rank of the commander appear in the signature block.

ATTACHMENTS: *List lower level attachment (tabs and exhibits). If a particular attachment is not used, place "not used" beside the attachment number. Unit standard operating procedures will dictate attachment development and format. Common attachments include the following:*

APPENDIX 12 (CYBERSPACE ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPERATION PLAN/ORDER [number] [(code name)]-[issuing headquarter] [(classification of title)]

ATTACHMENT : List lower-level attachment (tabs and exhibits)
Tab A - Offensive Cyberspace Operations
Tab B - Defensive Cyberspace Operations - Response Actions
Tab C - Electronic Attack
Tab D - Electronic Protection
Tab E - Electronic Warfare Support

DISTRIBUTION: *Show only if distributed separately from the base order or higher-level attachments.*

[page number]
[CLASSIFICATION]

Figure B-1. Appendix 12-cyberspace electromagnetic activities (continued)

This page intentionally left blank.

Appendix C

Cyber Effects Request Format

Appendix C includes the procedures for approving cyberspace effects at echelons corps and below, echelons above corps, and the cyber effects request format fields and information.

REQUESTING CYBERSPACE EFFECTS

C-1. The CERF is the format forces use to request effects in and through cyberspace. Effects in cyberspace can support operations in any domain. Execution orders provide authorization to execute cyberspace effects. Support in response to CERFs may be from joint cyberspace forces such as the combat mission teams, from other joint or service capabilities, or from service retained cyberspace forces.

EFFECTS APPROVAL AT ECHELONS CORPS AND BELOW

C-2. During the operations process at echelons corps and below, the commander and staff identify the effects desired in and through cyberspace to support operations against specific targets. If the requesting and higher echelons determine that a current capability is insufficient, the commander and staff approves and processes the CERF. This happens at each echelon until the CERF reaches a joint headquarters and the approval process varies slightly depending on the hierarchy. The CERF approval process at echelons corps and below follows the below steps—

- Identify targets of cyberspace effects.
- Verify if organic capabilities can create desired effects.
- Approve target for cyberspace effects.
- Forward to next higher Army echelon for deconfliction and synchronization.
- Verify if other organic capabilities can create desired effects, if organic cyberspace capabilities do not exist.
- If current capabilities fulfill requirement, synchronize operations.
- If current capabilities do not fulfill requirement, approve target for cyberspace effects.
- Forward to next higher Army echelon for approval until CERF enters joint process.
- Synchronize operation with cyberspace effect (if possible).

EFFECTS APPROVAL AT ECHELONS ABOVE CORPS

C-3. Cyberspace operations provide a means by which Army forces can achieve periods or instances of cyberspace superiority to create effects to support the commander's objectives. The employment of cyberspace capabilities tailored to create specific effects is planned, prepared, and executed using existing processes and procedures. However, there are additional processes and procedures that account for the unique nature of cyberspace and the conduct of cyberspace operations to support unified land operations. Commander and staffs at all echelons apply additional measures for determining where, when, and how to use cyberspace effects.

C-4. Commanders and staffs at each echelon will coordinate and collaborate regardless of whether the cyberspace operation is directed from higher headquarters or requested from subordinate units. The Army intelligence process informed by the joint intelligence process provides the necessary analysis and products from which targets are vetted and validated and aimpoints are derived. As a result of the Army IPB informed by the joint intelligence preparation of the operational environment, network topologies are developed for enemy, adversary, and host nation technical networks.

C-5. Targets determined during the planning process are described broadly as physical and logical entities in cyberspace consisting of one or more networked devices used by enemy and adversary actors. These targets may be established as named area of interests and targeted area of interests as appropriate. Additionally, an analysis of friendly force networks will inform the development of critical information and provide a basis for establishing key terrain in cyberspace. Key terrain in the defense are those physical and logical entities in friendly force technical networks of such extraordinary importance that any disruption in their operation would have debilitating effects upon accomplishment of the mission.

C-6. As part of CEMA, the staff will perform a key role in target network node analysis. As effects are determined for target and critical network nodes, the staff will prepare, submit, and track the CERF. This request will elevate above the corps echelon and integrate into the joint targeting cycle for follow on processing and approval. The joint task force, combatant command, and USCYBERCOM staff play a key role in processing the CERF and coordinating follow on cyberspace capabilities. Figure C-1 depicts the standard routing of the CERF.

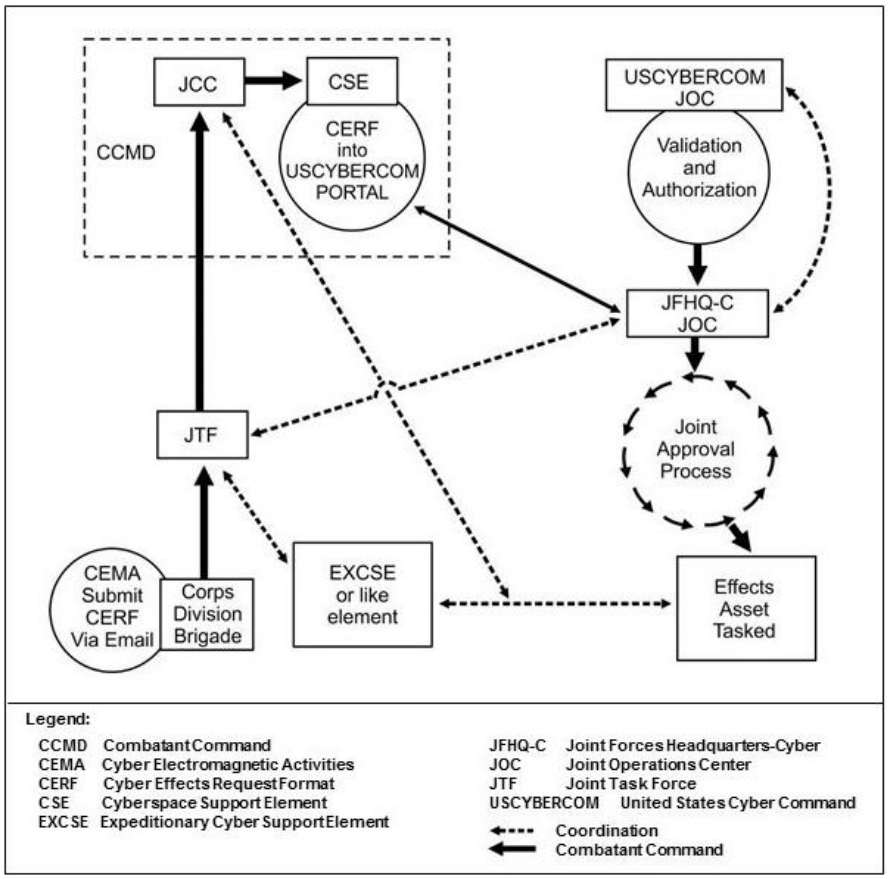


Figure C-1. Cyber effects request format routing for cyberspace operations

C-7. Joint forces receive cyberspace effects requests from different organizations. Cyberspace effects requests from Army forces at echelons corps and below process through a joint headquarters. Requests from joint task force receive guidance from the expeditionary cyber support element. Request from a combatant commander receives support from the cyber support element. The CERF is input into the USCYBERCOM portal for processing. All cyberspace effects support approved operations. Joint Forces Headquarters-Cyber coordinates with USCYBERCOM for approval and synchronization cyberspace effects missions and operations. USCYBERCOM sends approved cyberspace effect mission to the appropriate Joint Forces Headquarters-Cyber for execution. The Joint Forces Headquarters-Cyber synchronizes execution with the cyberspace or expeditionary cyberspace element as appropriate to support the echelon corps and below mission. The CERF at echelons above corps follows the below steps:

- The joint task force receives the CERF.

- Coordinates with the expeditionary cyberspace support element.
- Approves CERF and send to combatant command.
- Approves CERF.
- Inputs CERF into USCYBERCOM portal.
- USCYBERCOM approves CERF.
- Cyberspace effects target added to joint integrated prioritized target list.
- USCYBERCOM sends cyberspace effects mission to appropriate Joint Forces Headquarters-Cyber.
- Joint Forces Headquarters-Cyber synchronizes with cyberspace support element or expeditionary cyberspace element.
- Expeditionary cyberspace support element or cyberspace support element synchronizes with joint headquarters.

CYBER EFFECTS REQUEST FORMAT PREPARATION

C-8. Although the requesting unit may not have the specific target network topology information it should provide current target information. The approval process for cyberspace effects may take longer than other targeting capabilities. Figure C-2 on page C-4 shows an example the format and instructions required to complete the CERF. The requesting unit will complete all sections except the USCYBERCOM operations directorate of a joint staff (J-3) portion of the CERF as described below.

Format 26. Cyber Effects Request Format (CERF)		
SECTION 1 REQUESTING UNIT INFORMATION		
SUPPORTED MAJOR COMMAND:	DATE:	TIME SENT:
REQUESTED UNIT:	BY:	
POINT OF CONTACT::	CLASSIFICATION (Unclassified Until Filled in)	
	USCYBERCOM J3 USE ONLY:	
SUPPORTED OPLAN/COMPLAN/ORDER:	RECEIVED BY JOC	
	DATE:	TIME:
SUPPORTED MISSION STATEMENT:	NAME/RANK:	
SUPPORTED COMMANDER'S INTENT:	CERF TRACKING NUMBER:	
	ASSIGNED TO:	
SUPPORTED COMMANDER'S ENDSTATE	STAFF SECTION:	
SUPPORTED CONCEPT OF OPERATION:	DATE:	
	TIME:	
SUPPORTED OBJECTIVE (STRAP/OP/TACT):	POC:	
SUPPORTED TACTICAL OBJECTIVE/TASK	REMARKS:	
SECTION 3 - COMPUTER NETWORK OPERATIONS (CNO) SPECIFIC INFORMAITON		
TYPE OF TARGET: SCHEDULED ON-CALL	TARGET PRIORITY: EMERGENCY PRIORITY ROUTINE	
TARGET NAME:	TARGET LOCATOR	
TARGET DESCRIPTION:	DESIRED EFFECT:	
TARGET FUNCTION:	TARGET SIGNIFICANCE:	
TARGET DETAILS: Include any relevant device information such as type; operating system version and patch level, software, number of users, activity, friendly actors in the area of operations, surrounding/adjacent/parallel devices, etc.		
CONCEPT OF CYBER OPERATION: Include Task, Purpose, Method and Endstate. Also specify intelligence collection plan for battle damage assessment (BOA), to include allocated resources, measures of performance (MOPs), measure of effectiveness (MREs), and Measures of Effectiveness indicators (MOEs).		
TARGET EXPECTATION STATEMENT:		
REMARKS: If any of the following information is available, please provide 1.) Time on target/Duration of Effect 2.) No Earlier Than/No Later Than Need Time 3.) Trigger Event, or Conditions for Execution 4.) Persistence Requirement (ie., effect must persist through a restart of the target, trigger event)) 5.) Command and Control Requirement (ie., effect must be able to be turned on/off remotely) 6.) Self-Destruct / Auto Delete Requirement (ie., effect must stop itself if C2 is lost after X amount of time) 7.) Level of Attribution Requirement (ie., unattributable to CONUS or USG, misattributed, attributed to USG, etc) 8.) Level Desectability allowed (ie., should not be detected by (a) administrator, (b) user © forensic analyst, etc) 9.) Level Co-optability allowed (ie., low, medium, high) 10.) Remote Monitoring Requirement (ie., effect should be able to be monitored by (a) operator, (b) JOC, etc) 11.) Infrastucture Requirement (ie., effect should be launched from (a) National Security Agency (NSA) Tailored Access Operations (TAO) (b) naval vessel, etc) 12.) Reversability Requirement (ie., effect should be reversible/not reversibility)		

Figure C-2. Cyber effects request format

CYBER EFFECTS REQUEST FORMAT SECTION 1 REQUESTING UNIT INFORMATION

C-9. Section 1 of the CERF requests the following unit information—

- Supported Major Command. Enter the major command authorized to validate and prioritize the CERF. For Army units at corps level and below this entry will commonly include the geographic or functional combatant command.
- Date. Enter the date the completed CERF(s) are submitted to higher headquarters.
- Time Sent. Enter the time the CERF is submitted to higher headquarters.
- Requesting Unit. Enter the name of the unit originating the requirement for the creation of effect(s) or conduct of specific activities.

- By. Enter the rank, last, and first name of the unit point of contact that time stamped and processed the CERF.
- Point of Contact. Enter the rank, last, and first name of the unit point of contact from the requesting unit. Also, enter phone number and e-mail.
- Classification. Enter the overall classification of the document. Ensure classification markings are applied to each section and supporting documentation.

CYBER EFFECTS REQUEST FORMAT SECTION 2 SUPPORTED OPERATION INFORMATION

C-10. Section 2 of the CERF requests the following supported operation information—

- Supported OPLAN/CONPLAN/Order. Describe key information within the plan that the requested effect(s) will support.
- Supported Mission Statement. Describe the unit's essential task(s) and purpose that the requested effect(s) will support.
- Supported Commander's Intent. Describe key information within the commander's intent that the requested effect(s) will support.
- Supported Commander's End State. Describe key information within the commander's end state that the requested effect(s) will support.
- Supported Concept of Operations. Describe key information within the concept of operations that the requested effect(s) will support.
- Supported Objective (strategic, operational, and tactical). Describe the supported objective(s) that the requested effect(s) will directly support.
- Supported Tactical Objective/Task. Describe the tactical objectives and tasks that the requested effect(s) will directly or indirectly support.

C-11. The remaining portion of Section 2 is completed by the USCYBERCOM J3.

CYBER EFFECTS REQUEST FORMAT SECTION 3 COMPUTER NETWORK OPERATIONS

C-12. Section 3 of the CERF requests the following computer network operations and specific information—

- Type of Target.
  - Indicate "scheduled" if specific dates, times, and or supporting conditions are known.
  - Indicate "on-call" if trigger events or supporting conditions are known.
- Target Priority.
  - Indicate "emergency" if target requires immediate action. Indicate "priority" if target requires a degree of urgency.
  - Indicate "routine" if target does not require immediate action or a degree of urgency beyond standard processing.
- Target Name. Enter name of target as codified in the Modernized Integrated Database.
- Target Location.
  - Provide target location according to CJCSI 3370.01, Enclosure D.
  - Disregard if the request is for specific activities to support DODIN operations or DCO.
- Target Description.
  - Provide target(s) description according to CJCSI 3370.01, Enclosure D.
  - Provide description of network node(s) wherein specific activities are to support DODIN operations or DCO.
- Desired Effect.
  - Enter deny, degrade, disrupt, destroy, or manipulate for OCO.
  - Provide timing as "less than 96 hours", "96 hours to 90 days", or "greater than 90 days".
- Target Function. Enter target(s) primary function and additional functions if known.
- Target Significance. Describe why the target(s) is important to the enemy's or adversary's target system(s) and/or value in addition to its functions and expectations.

- Target Details. Describe additional information about the target(s) if known. This information should include any relevant device information such as type; number of users; activity; friendly actors in the area of operations; and surrounding/adjacent/parallel devices.
- Concept of Cyberspace Operations.
  - Describe how the requested effect(s) would contribute to the commander's objectives and overall concept of operations.
  - Include task, purpose, method, and end state.
  - Describe the intelligence collection plan and specific assessment plan if known.
  - Provide reference to key directives and orders.
- Target Expectation Statement. According to CJCSI 3370.01, Enclosure D, describe how the requested effect(s) will impact the target system(s). This description must address the following questions.
  - How will the target system be affected if the target's function is neutralized, delayed, disrupted, or degraded? (Two examples are operational impact and psychological impact.)
  - What is the estimated degree of impact on the target system(s)?
  - What is the functional recuperation time estimated for the target system(s) if the target's function is neutralized, delayed, disrupted, or degraded?
  - What distinct short-term and/or long-term military or political advantage/disadvantage do we expect if the target's function is neutralized, delayed, disrupted, or degraded?
  - What is the expected enemy or adversary reaction to affecting the target's function?

Appendix D

Electronic Attack Request Format

Appendix D includes the electronic attack request format and the electronic attack 5-line briefing formats. These formats are used to request specific electronic attack support and on-call electronic attack support.

ELECTRONIC ATTACK REQUEST EXAMPLES

D-1. Request EA effects via normal request processes and provide specific effects requests using the EARF. The EARF normally accompanies the joint tactical air strike request. For more information on this format see ATP 3-09.32. (See table D-1 for an example of the EARF.)

Table D-1. The electronic attack request format

<table>
<tr><th colspan="2">Format 24. Electronic Attack Request Format (EARF)</th></tr>
<tr><td colspan="2">Requesting Major Supported Command:</td></tr>
<tr><td colspan="2">Requesting Unit:</td></tr>
<tr><td colspan="2">Contact Information: This person will be responsible to verify that the EARF has been approved before the mission starts and to relay the information to the executing unit.</td></tr>
<tr><td colspan="2">Joint Tactical Air Request (JTAR) Number: Enter the corresponding JTAR number that will be submitted with this EARF.</td></tr>
<tr><td colspan="2">Concept of Operations: Describe the concept of operations. This will include the objective, forces used, timeline of the mission, and coordination efforts required for mission success. Relate the impact of mission success to specific objectives for the integrated tasking order.</td></tr>
<tr><td colspan="2">Electronic Attack (EA) Concept of Operations: Define desired effect(s) and timeline.</td></tr>
<tr><td colspan="2">Cease Buzzer Procedures: This will be in accordance with theatre special instructions (SPINS). Provide frequency to communicate between jamming control authority (JCA) and EA asset. Very/ultra-high frequency (V/UHF) is the primary means to talk to a supporting aircraft. If unable to establish communications, consider using another asset to relay information. Some aircraft may be Internet Relay Chat (IRC) client (mIRC) capable.</td></tr>
<tr><td colspan="2">Friendly Frequency Use for Operation:</td></tr>
<tr><td>Target Communications System(s) to be Jammed/Denied:</td><td>Target Requested (List type and frequency, if known.)

Intelligence Assessment (Intelligence assessment required for each request. Do not copy and paste frequencies from one day to the next without intelligence validation/assessment.)</td></tr>
<tr><td colspan="2">Target Location (in Lat/Long or military grid reference system [MGRS]):</td></tr>
<tr><td colspan="2">Jamming date-time group(s): From – To, in Zulu Time (preferred)</td></tr>
<tr><td colspan="2">Type of EA Requested: Preplanned – Scheduled/On-Call</td></tr>
</table>

ELECTRONIC ATTACK 5 LINE

D-2. Request immediate and on-call EA requests using a 5-line format. This is used to prepare the aircrew for an EA. For more information on this format see ATP 3-09.32. (See table D-2 for an example of the EA 5-line briefing format.)

Table D-2. The electronic attack 5-line briefing

Electronic Attack 5-Line Briefing
Do not transmit line numbers. Units of measure are standard unless briefed. Lines 1, 2 and 4 are mandatory readback(*). Jam Control Authority (JCA) may request additional readback. JCA: **"**_____, **this is** _____" (Aircraft Callsign) (JCA Callsign) **"Type 3 Control"** 1.* Target/Effect Description:"_____" A. Rapper/Target Name (if applicable, not required) B. Frequency (if known) C. Modulation (if known, not required) 2.* Target Location: "_____" (Lat/Long, MGRS) 3. Location of Friendlies: "_____" 4.* Time on Target: " _____" 5. Remarks (as appropriate): "_____"

Glossary

The glossary lists acronyms and terms with Army, multi-Service, or joint definitions, and other selected terms. Where Army and joint definitions are different, (Army) follows the term. The proponent publication for a term is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ARCYBER	United States Army Cyber Command
CEMA	cyberspace electromagnetic activities
CERF	cyber effects request format
COA	course of action
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations – internal defensive measures
DCO-RA	defensive cyberspace operations – response action
DOD	Department of Defense
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network - Army
EA	electronic attack
EARF	electronic attack request format
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWO	electronic warfare officer
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-5	assistant chief of staff, plans
G-6	assistant chief of staff, signal
G-9	assistant chief of staff, civil affairs operations
IO	information operations
IPB	intelligence preparation of the battlefield
IRC	information-related capabilities
J-3	operations directorate of a joint staff
JFC	joint force commander
MDMP	military desion-making process
OCO	offensive cyberspace operations
OPE	operational preparation of the environment
ISR	intelligence, surveillance, & reconnaissance
SCIF	sensitive compartmented information facility
SIGINT	signals intelligence
SMO	spectrum management operations
USC	United States Code
USCYBERCOM	United States Cyber Command

SECTION II – TERMS

aimpoint

A point associated with a target and assigned for a specific weapon impact. (JP 3-60)

Army design methodology

A methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them. (ADP 5-0)

countermeasures

That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 3-13.1)

cyberspace electromagnetic activities

The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. (ADRP 3-0)

cyberspace

A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12[R])

cyberspace operations

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

cyberspace superiority

The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 3-12[R])

defensive cyberspace operations

Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 3-12[R])

defensive cyberspace operation response action

Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend the Department of Defense cyberspace capabilities or other desiganted systems. (JP 3-12[R])

denial operations

Actions to hinder or deny the enemy the use of space, personnel, supplies, or facilities. (FM 3-90-1)

Department of Defense information network

The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 6-0)

Department of Defense information network operations

Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 3-12[R])

destroy

A tactical mission task that physically renders an enemy force combat-ineffective until it is reconstituted. Alternatively, to destroy a combat system is to damage it so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. (FM 3-90-1)

directed energy

(DOD) An umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles. Also called DE. (JP 3-13.1)

disrupt

1. A tactical mission task in which a commander integrates direct and indirect fires, terrain, and obstacles to upset an enemy's formation or tempo, interrupt his timetable, or cause enemy forces to commit prematurely or attack in piecemeal fashion. 2. An obstacle effect that focuses fire planning and obstacle effort to cause the enemy to break up his formation and tempo, interrupt his timetable, commit breaching assets prematurely, and attack in a piecemeal effort. (FM 3-90-1)

electrmagnetic compatibility

(DOD) The ability of systems, equipment, and devices that use the electromagnetic spectrum to operate in their intended environments without causing or suffering unacceptable or unintentional degradation because of electromagnetic radiation or response. Also called EMC. (JP 3-13.1)

electromagnetic hardening

(DOD) Action taken to protect personnel, facilities, and/or equipment by blanking, filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy. (JP 3-13.1)

electromagnetic interference

(DOD) Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. (JP 3- 13.1)

electromagnetic intrusion

(DOD) The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. (JP 3-13.1)

electromagnetic jamming

(DOD) The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. (JP 3-13.1)

electromagnetic pulse

(DOD) The electromagnetic radiation from a strong electronic pulse, most commonly caused by a nuclear explosion that may couple with electrical or electronic systems to produce damaging current and voltage surges. Also called EMP. (JP 3-13.1)

electromagnetic spectrum

The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-13.1)

electromagnetic spectrum management

Planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. (JP 6-01)

electronic intelligence

(DOD) Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. (JP 3-13.1)

electronic masking

(DOD) The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-13.1)

electronic probing

(DOD) Intentional radiation designed to be introduced into the devices or systems of potential enemies for the purpose of learning the functions and operational capabilities of the devices or systems. (JP 3-13.1)

electronic reconnaissance

The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 3-13.1)

electronics security

(DOD) The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations, e.g., radar. (JP 3-13.1)

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-13.1)

electronic warfare reprogramming

(DOD) The deliberate alteration or modification of electronic warfare or target sensing systems, or the tactics and procedures that employ them, in response to validated changes in equipment, tactics, or the electromagnetic environment. (JP 3-13.1)

electro-optical-infrared countermeasures

(DOD) A device or technique employing electro-optical-infrared materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Also called EO-IR CM. (JP 3-13.1)

emission control

(DOD) The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. Also called EMCON. (JP 3-13.1)

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

information operations

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

intelligence preparation of the battlefield

(Army) The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. (ATP 2-01.3)

key terrain

Any locality, or area, the seizure or retention of which affords a marked advantage to either combatant. (JP 2-01.3)

measure of effectiveness

A criterion used to assess changes in system or enemy behavior, capability, or operational environment that is tied to measuring the attainment of an endstate, achievement of an objective, or creation of an effect. (JP 3-0)

offensive cyberspace operations

Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 3-12[R])

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 3-0)

planning

The art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. (ADP 5-0)

radio frequency countermeasures

(DOD) Any device or technique employing radio frequency materials or technology that is intended to impair the effectiveness of enemy activity, particularly with respect to precision guided weapons and sensor systems. Also called RF CM. (JP 3-13.1)

situational understanding

The product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables to facilitate decisionmaking. (ADP 5-0)

spectrum management operations

The interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. (FM 6-02)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADRP 3-0)

wartime reserve modes

(DOD) Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. Also called WARM. (JP 3-13.1)

This page intentionally left blank.

References

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

ADRP 1-02. *Terms and Military Symbols*. 16 November 2016.

DOD Dictionary of Military and Associated Terms. March 2017.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new_pubs/jointpub.htm.

CJCSI 3370.01B. *Target Development Standards*. 6 May 2016.

CJCS Manual 3139.01. *(U) Review and Approval Process for Cyberspace Operations (S/NF)*. 22 October 2013.

CJCS Manual 3320.02D. *Joint Spectrum Interference Resolution (JSIR)*. 3 June 2013.

DODI 4650.01. *Policy and Procedures for Management and Use of the Electromagnetic Spectrum*. 9 January 2009.

DoD Manual 5240.01. *Procedures Governing the Conduct of DOD Intelligence Activities*. 8 August 2016.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 21 May 2014.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-12(R). *Cyberspace Operations*. 5 February 2013.

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.

JP 3-60. *Joint Targeting*. 31 January 2013.

JP 5-0. *Joint Operation Planning*. 11 August 2011.

JP 6-0. *Joint Communications System*. 10 June 2015.

JP 6-01. *Joint Electromagnetic Spectrum Management Operations*. 20 March 2012.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: www.apd.army.mil.

ADP 2-0. *Intelligence*. 31 August 2012.

ADP 3-0. *Operations*. 11 November 2016.

ADP 5-0. *The Operations Process*. 17 May 2012.

ADP 6-0. *Mission Command*. 17 May 2012.

ADRP 2-0. *Intelligence*. 31 August 2012.

ADRP 3-0. *Operations*. 11 November 2016.

ADRP 5-0. *The Operations Process*. 17 May 2012.

ADRP 6-0. *Mission Command*. 17 May 2012.

AR 5-12. *Army Use of the Electromagnetic Spectrum.* 16 February 2016

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

AR 380-10. *Foreign Disclosure and Contacts with Foreign Representatives*. 14 July 2015.

AR 381-10. *U.S. Army Intelligence Activities*. 3 May 2007.

AR 530-1. *Operations Security*. 26 September 2014.

ATP 2-01.3. *Intelligence, Preparation of the Battlefield/Battlespace*. 10 November 2014.

ATP 3-09.32/MCRP 3-16.6A/NTTP 3-09.2/AFTTP 3-2.6. *JFIRE Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower*. 21 January 2016.

ATP 3-13.10/NTTP 3-51.2/AFTTP 3-2.7. *EW Reprogramming Multi-Service Tactics, Techniques, and Procedures for Reprogramming Electronic Warfare (EW) Systems*. 17 June 2014.

ATP 3-36. *Electronic Warfare Techniques*. 16 December 2014.

ATP 3-60. *Targeting*. 7 May 2015.

ATP 5-0.1. *Army Design Methodology*. 1 July 2015.

ATP 5-19. *Risk Management*. 14 April 2014.

ATP 6-02.70. *Techniques for Spectrum Management Operations*. 31 December 2015.

FM 2-0. *Intelligence Operations*. 15 April 2014.

FM 3-13. *Information Operations*. 6 December 2016.

FM 3-55. *Information Collection*. 3 May 2013.

FM 3-90-1. *Offense and Defense Volume 1*. 22 March 2013.

FM 3-94. *Theater Army, Corps, and Division Operations*. 21 April 2014.

FM 6-0. *Commander and Staff Organization and Operations*. 5 May 2014.

FM 6-02. *Signal Support to Operations*. 22 January 2014.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

OTHER PUBLICATIONS

Army Strategic Planning Guidance. 2014. http://www.g8.army.mil/index.html

Executive Order 12333. *United States Intelligence Activities.* 4 December 1981. https://www.archives.gov/federal-register/codification

Strategic Instruction 714-04. *Satellite Communications*. 14 October 2014. https://vela.stratcom.mil/sites/publications/Pubs/SIs/714-04.pdf

Trilateral Memorandum of Agreement among the Department of Defense and the Department of Justice and the Intelligence Community regarding Computer Network Attack and Computer Network Exploitation Activities (S/NF). 9 May 2007.

United States Code. http://uscode.house.gov/

United States Constitution. https://www.whitehouse.gov/1600/constitution

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA Forms are available on the Army Publishing Directorate (APD) web site: www.apd.army.mil.
DD Forms are available on the Office of the Secretary of Defense (OSD) web site: http://www.dtic.mil/whs/directives/forms/index.htm.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DD Form 1494. *Application for Equipment Frequency Allocation*.

Index

Entries are by paragraph number unless indicated otherwise.

FM 3-12
11 April 2017

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1709701

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: To be distributed in accordance with the initial distrubution number (IDN) 116045, requirements for FM 3-12.

PIN: 201561-000