FM 3-38

CYBER ELECTROMAGNETIC ACTIVITIES

FEBRUARY 2014

DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 3-38

Headquarters
Department of the Army
Washington, DC, 12 February 2014

Cyber Electromagnetic Activities

Contents

Figures

Tables

Preface

FM 3-38, *Cyber Electromagnetic Activities*, provides overarching doctrinal guidance and direction for conducting cyber electromagnetic activities (CEMA). This manual describes the importance of cyberspace and the electromagnetic spectrum (EMS) to Army forces and provides the tactics and procedures commanders and staffs use in planning, integrating, and synchronizing CEMA.

This manual provides the information necessary for Army forces to conduct CEMA that enable them to shape their operational environment and conduct unified land operations. It provides enough guidance for commanders and their staffs to develop innovative approaches to seize, retain, and exploit advantages throughout an operational environment. CEMA enable the Army to achieve desired effects in support of the commander's objectives and intent.

The principal audience for FM 3-38 is all members of the profession of arms. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should see applicable joint or multinational doctrine concerning cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO). Trainers and educators throughout the Army will also use this manual.

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

FM 3-38 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

FM 3-38 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 3-38 is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCK-D (FM 3-38), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by e-mail to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

Introduction

United States (U.S.) forces operate in an increasingly network-based world. The proliferation of information technologies is changing the way humans interact with each other and their environment, including interactions during military operations. This broad and rapidly changing operational environment requires that today's Army must operate in cyberspace and leverage an electromagnetic spectrum that is increasingly competitive, congested, and contested.

FM 3-38, *Cyber Electromagnetic Activities,* is the first doctrinal field manual of its kind. The integration and synchronization of cyber electromagnetic activities (CEMA) is a new concept. The Army codified the concept of CEMA in Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*, and ADP 6-0, *Mission Command*. The mission command warfighting function now includes four primary staff tasks: conduct the operations process (plan, prepare, execute, assess), conduct knowledge management and information management, conduct inform and influence activities (IIA), and conduct CEMA. The purpose of FM 3-38 is to provide an overview of principles, tactics, and procedures on Army integration of CEMA as part of unified land operations.

At its heart, CEMA are designed to posture the Army to address the increasing importance of cyberspace and the electromagnetic spectrum (EMS) and their role in unified land operations. CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO).

The Army continues to support the Secretary of Defense and joint requirements for information operations, EW, and cyberspace operations through the execution of IIA, CEMA, and the integration of other information-related activities. These separate activities are tied through mission command, but they have distinctly different processes for carrying out their operating requirements.

FM 3-38 contains seven chapters:

Chapter 1 defines CEMA and provides an understanding of the fundamentals of the CEMA staff tasks. It briefly describes each activity and provides a framework for the emerging operational environment that includes cyberspace.

Chapter 2 begins with a discussion of the commander's role in the conduct of CEMA. It then describes the CEMA element, its role in the operations process, and how it interacts with, supports, and receives support from other staff members.

Chapter 3 provides tactics and procedures specific to cyberspace operations.

Chapter 4 provides tactics and procedures specific to EW.

Chapter 5 provides tactics and procedures specific to SMO and the functions executed by the spectrum manager.

Chapter 6 describes how CEMA are executed through the operations processes, including other integrating processes.

Chapter 7 describes considerations unique to CEMA when conducting operations with unified action partners.

Appendix A provides guidance on CEMA input to operations orders and plans.

This page intentionally left blank.

Chapter 1

Fundamentals of Cyber Electromagnetic Activities

This chapter discusses the fundamentals of cyber electromagnetic activities (CEMA), introduces the cyberspace domain, and describes the electromagnetic spectrum within an operational environment and the information environment. Chapter one concludes with a discussion of the implications of CEMA in support of unified land operations.

CYBER ELECTROMAGNETIC ACTIVITIES DEFINED

1-1. *Cyber electromagnetic activities* are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system (ADRP 3-0). CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO) (see figure 1-1 on page 1-2).

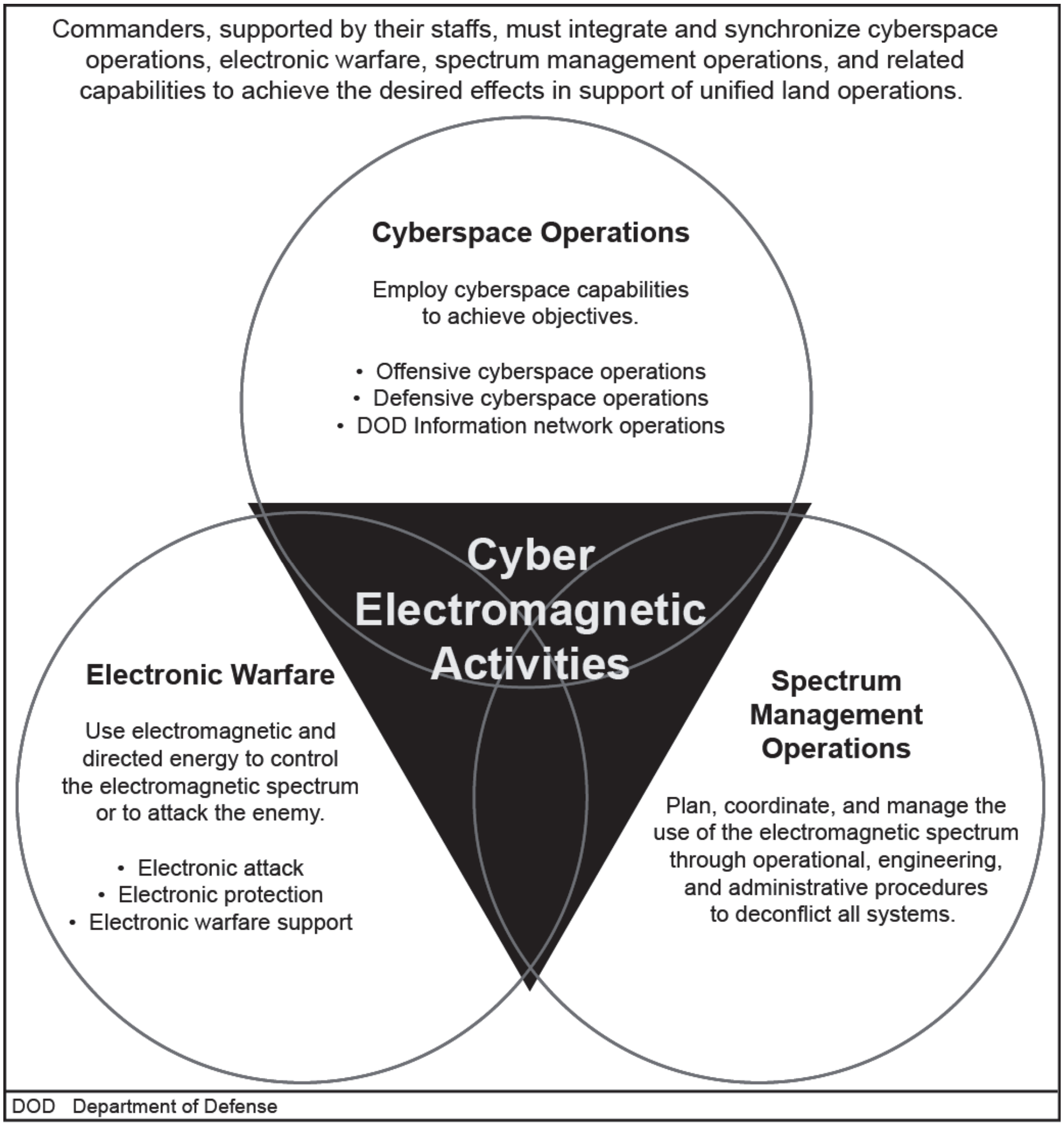

Commanders, supported by their staffs, must integrate and synchronize cyberspace operations, electronic warfare, spectrum management operations, and related capabilities to achieve the desired effects in support of unified land operations.
Cyberspace Operations
Employ cyberspace capabilities to achieve objectives.
• Offensive cyberspace operations
• Defensive cyberspace operations
• DOD Information network operations
Cyber Electromagnetic Activities
Electronic Warfare
Use electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.
• Electronic attack
• Electronic protection
• Electronic warfare support
Spectrum Management Operations
Plan, coordinate, and manage the use of the electromagnetic spectrum through operational, engineering, and administrative procedures to deconflict all systems.
DOD Department of Defense

Figure 1-1. Cyber electromagnetic activities

1-2. Army forces conduct CEMA as a unified effort. *Integration* is the arrangement of military forces and their actions to create a force that operates by engaging as a whole (JP 1-02). *Synchronization* is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time (JP 1-02). CEMA integrates and synchronizes the functions and capabilities of CO, EW, and SMO to produce complementary and reinforcing effects. Conducting these activities independently may detract from their efficient employment. If uncoordinated, these activities may result in conflicts and mutual interference between them and with other entities that use the electromagnetic spectrum (EMS). CO, EW, and SMO are synchronized to cause specific effects at decisive points to support the overall operation.

1-3. The CEMA element is responsible for planning, integrating, and synchronizing CO, EW, and SMO to support the commander's mission and desired end state within cyberspace and the EMS. During execution the CEMA element is responsible for synchronizing CEMA to best facilitate mission accomplishment. (See chapter 2 for more information on the CEMA element.)

1-4. Cyberspace operations, EW, and SMO are essential to the conduct of unified land operations. While these activities differ in their employment and tactics, their functions and capabilities must be integrated and synchronized to maximize their support to unified land operations. The integration of these activities requires an understanding of the functions and capabilities being employed.

CYBERSPACE OPERATIONS

1-5. *Cyberspace operations* are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). Cyberspace operations consist of three functions: offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations (see chapter 3).

ELECTRONIC WARFARE

1-6. *Electronic warfare* is any 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 consists of three functions: electronic attack, electronic protection, and electronic warfare support. These functions are referred to as divisions in joint doctrine (see chapter 4).

SPECTRUM MANAGEMENT OPERATIONS

1-7. SMO are the interrelated functions of spectrum management, frequency assignment, host-nation coordination, and policy that enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. SMO are the management portions of electromagnetic spectrum operations (EMSO). EMSO also include electronic warfare (see chapter 5)

CEMA IN AN OPERATIONAL ENVIRONMENT

1-8. 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). An analysis of an operational environment must consider the five domains and the EMS. The four traditional domains (air, land, maritime, and space) and the EMS exist naturally. The fifth domain, cyberspace, is manmade (see figure 1-2 on page 1-4).

1-9. Cyberspace and the EMS provide commanders the ability to share information, communicate, integrate, and synchronize operations across all warfighting functions and echelons. Conversely, cyberspace and the EMS provide adversaries and enemies an effective, inexpensive, and anonymous means for recruitment, information activities, training, and command and control. CEMA provide commanders with the ability to gain and maintain an advantage in cyberspace and the EMS.

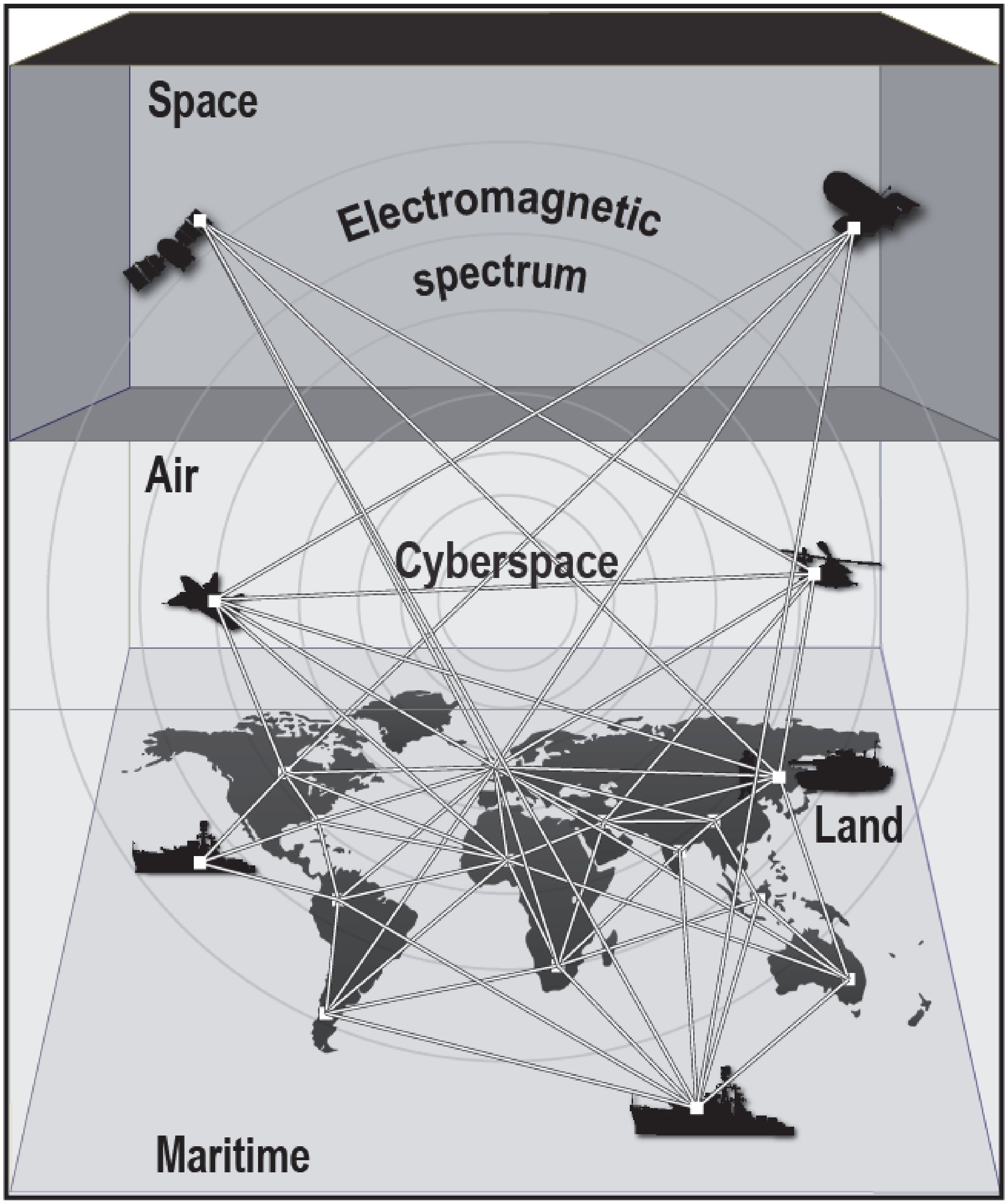


Figure 1-2.The relationships among the five domains and the electromagnetic spectrum

CYBERSPACE DOMAIN

1-10. *Cyberspace* is 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 1-02). Operations in cyberspace contribute to gaining a significant operational advantage for achieving military objectives.

1-11. Cyberspace resides in components throughout the four naturally occurring domains. For example, network servers may reside in a land-based data complex or at sea, aboard warships. Operations in cyberspace rely on the links and nodes that exist in the natural domains. Therefore, operations in cyberspace enable freedom of action for operations in the four natural domains and the EMS. Operations in the other domains create effects in and through cyberspace by affecting the EMS, the data, or the physical infrastructure.

1-12. The cyberspace and space domains are uniquely interrelated primarily because of their current role in telecommunications and networks. Operations in the space domain depend on cyberspace and the EMS to execute space support. Space capabilities provide cyberspace with a global reach. These interrelationships are important considerations when planning for CEMA.

Characteristics of the Cyberspace Domain

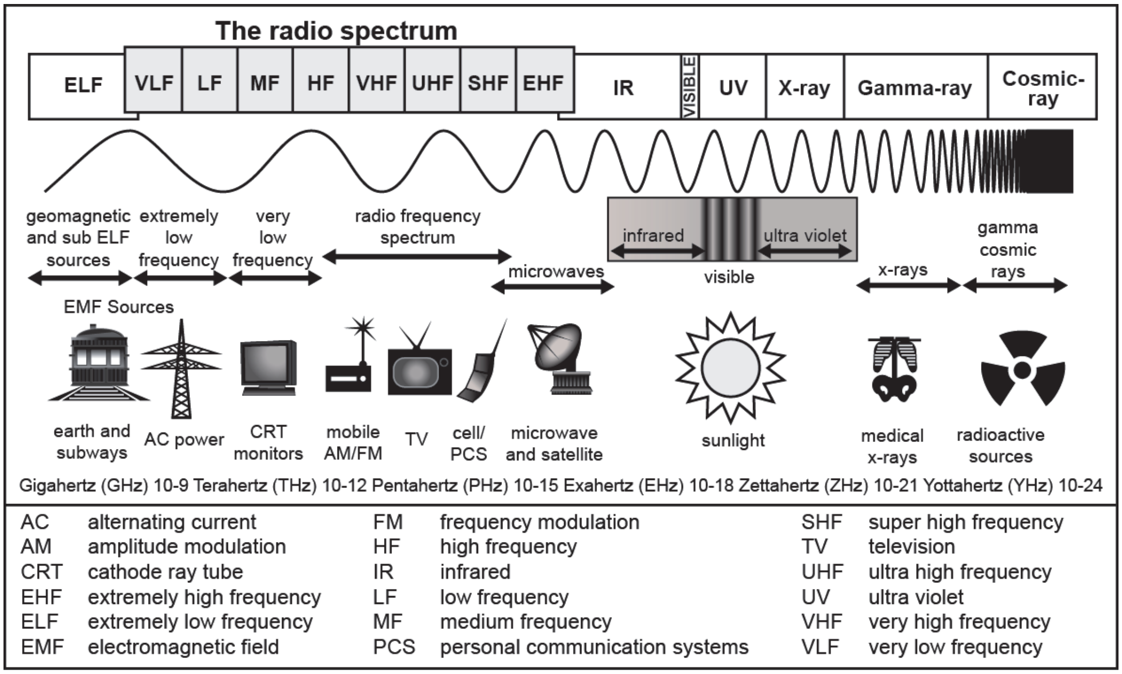
1-13. Cyberspace has characteristics that significantly differ from the land, air, maritime, and space domains. Cyberspace is a system of systems in that many small and diverse systems comprise the structure as a whole. These systems exist throughout each of the four natural domains. Changes in cyberspace are often driven by private industry research and development, making the domain dynamic and continually evolving as information technology capabilities continue to expand and evolve. Because cyberspace is man-made, it is only through continued attention and maintenance that cyberspace persists.

1-14. Cyberspace reinforces the fact that an operational framework is not confined to a physical place. Traditional battlefields were confined to physical space. While the repercussions of what happens on the traditional battlefield can create social and political effects around the world, the actual physical impact is limited to the physical battlefield. The inclusion of cyberspace and the EMS greatly expands and complicates the operational framework, transforming a limited physical battlefield to a global battlefield. A computer virus executed in cyberspace may strike its intended target and also indiscriminately strike other systems in several nations around the world, including the United States (U.S.). Collateral damage from this type of attack is not always predictable.

1-15. Cyberspace is an environment created and maintained for the purpose of facilitating the use and exploitation of information, human interaction, and intercommunication. This domain co-exists with the EMS through telecommunications systems. These systems utilize the EMS and have converged into a worldwide network to create cyberspace. Effective CO holistically address the physical infrastructure, data networks, and the EMS.

ELECTROMAGNETIC SPECTRUM

1-16. 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). (See figure 1-3 on page 1-6.**)**



AC	alternating current	FM	frequency modulation	SHF	super high frequency
AM	amplitude modulation	HF	high frequency	TV	television
CRT	cathode ray tube	IR	infrared	UHF	ultra high frequency
EHF	extremely high frequency	LF	low frequency	UV	ultra violet
ELF	extremely low frequency	MF	medium frequency	VHF	very high frequency
EMF	electromagnetic field	PCS	personal communication systems	VLF	very low frequency

Figure 1-3. The electromagnetic spectrum

1-17. The increased use of wireless systems – including the use of commercial off-the-shelf items – makes the available EMS a high-demand resource. The resulting electromagnetic environments in which forces operate are highly contested and congested, making unencumbered access to the EMS problematic.

THE INFORMATION ENVIRONMENT

1-18. Cyberspace and the EMS are part of 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 three dimensions of the information environment (physical, informational, and cognitive) apply to the conduct of CEMA. CEMA is conducted in the physical and informational dimensions and CEMA supports objectives in the cognitive dimension. The EMS resides within the physical dimension of the information environment. The three layers of cyberspace (physical, logical, and cyber persona) reside within the physical and informational dimensions of the information environment. (See chapter 3 for a detailed discussion of the layers of cyberspace.)

1-19. The physical dimension is composed of tangible elements such as telecommunications networks, information systems and infrastructures, satellites, broadcast facilities, meeting places, printed publications, billboards, flyers, statues, symbolic objects, organizations, groups, and people. In effect, tangible elements are the means and methods used to enable the flow of information among producers, users, audiences, and systems. The physical dimension also includes elements such as transmission paths in the EMS. It is within the physical dimension that the components, or physical layer, of cyberspace exist on land, air, sea, or space and are the easiest to measure.

1-20. The informational dimension consists of the information itself, whether it is static (at rest) or in transit. The informational dimension refers to content and flow of the information, such as text or images, or data that staffs can collect, process, store, disseminate, and display. For the conduct of CEMA, the informational dimension is represented by computer data moving in and through cyberspace and electromagnetic transmissions moving in and through the EMS. This dimension is where the logical and cyber persona layers of cyberspace reside. The informational dimension provides the necessary link between the physical dimension and the cognitive dimension.

1-21. The cognitive dimension is composed of the knowledge, values, beliefs, concepts, intentions, and perceptions of individuals and groups transmitting and receiving information. This dimension focuses on the societal, cultural, religious, and historical contexts that influence the perceptions of those producing the information and of the target audiences receiving the information. Governments, societies, military forces, enemy forces, and other actors all think, perceive, visualize, understand, and decide within this dimension. These actors are the creators and users of the information that moves in and through the physical dimension. While cyberspace and the EMS do not exist within the cognitive dimension, CEMA is sometimes leveraged as an information-related capability to affect this portion of the information environment.

Cyber Electromagnetic Activities as an Information-Related Capability

1-22. *Information-related capabilities* are capabilities, techniques, or activities employing information to effect any of the three dimensions within the information environment to generate an end(s) (FM 3-13). These capabilities include, but are not limited to, public affairs operations, military information support operations, combat camera, Soldier and leader engagement, civil affairs operations, civil and cultural considerations, operations security, military deception, and CEMA.

1-23. CEMA are leveraged by inform and influence activities (IIA) to effect the information environment. CEMA are considered an information-related capability that must be integrated and synchronized with other information-related capabilities. *Inform and influence activities* is the integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking (ADRP 3-0). These activities occur within, through, or by means of the information environment. The information environment can have a consequential affect on the operational environment, and it can impact military operations and outcomes. (For additional information on IIA, see FM 3-13.)

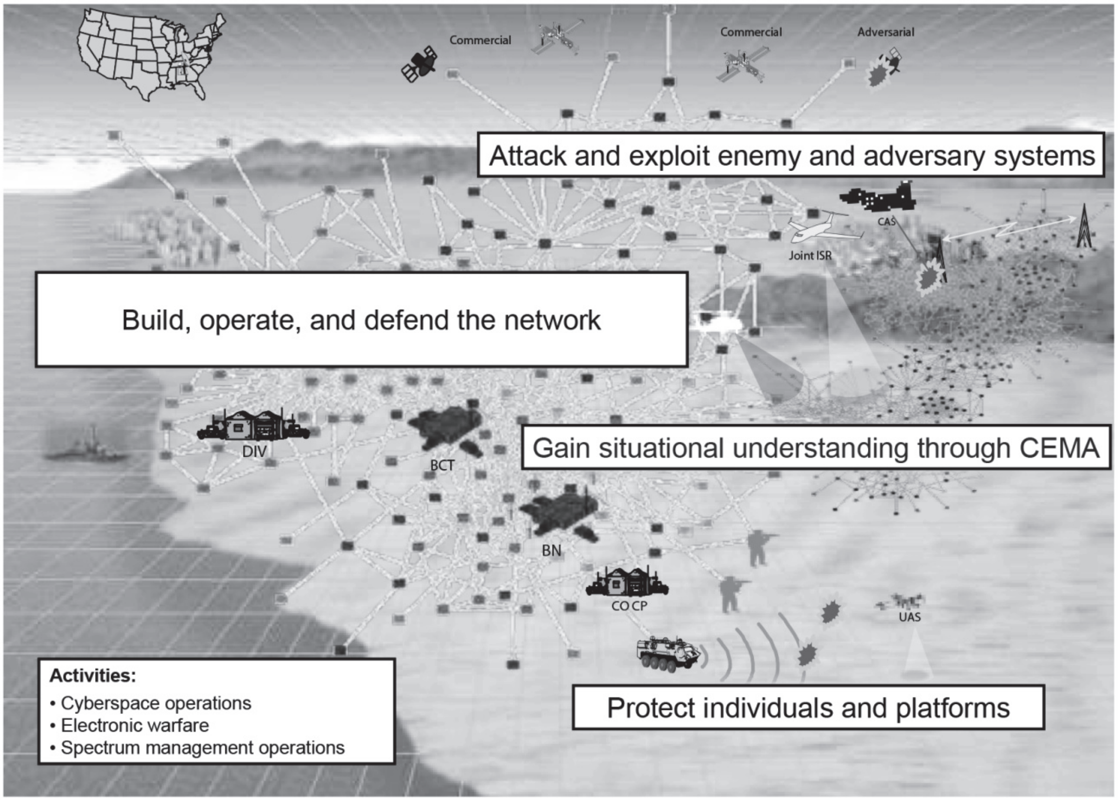
1-24. Although IIA and CEMA are interrelated, IIA focuses on the holistic information environment. Both IIA and CEMA are integrating and mutually supporting functions that contribute to affecting perceptions and decisionmaking. For example, CEMA can reinforce messaging efforts by providing additional means for message distribution. Additionally, there are offensive and defensive related CEMA capabilities that can help reinforce the goals of other information-related capabilities, such as protecting friendly information.

1-25. Both CEMA and IIA require uniquely different skill sets to perform the required planning processes effectively. While both are integrated actions, effective planning requires a general understanding of the capabilities being employed and consultation with the respective subject matter experts. CEMA can be planned separately from IIA. However, when possible, CEMA and IIA should be planned to achieve simultaneous and complementary effects.

CYBER ELECTROMAGNETIC ACTIVITIES IN UNIFIED LAND OPERATIONS

1-26. Figure 1-4 on page 1-8 depicts the CEMA operational view. The ability to gain and maintain an advantage in cyberspace and the EMS requires that the Army employ the capabilities of CEMA to conduct the following:

- Build, operate, and defend the network.
- Attack and exploit enemy and adversary systems.
- Gain situational understanding through CEMA.
- Protect individuals and platforms.


Commercial
Commercial
Adversarial
Attack and exploit enemy and adversary systems
CAS
Joint ISR
Build, operate, and defend the network
Gain situational understanding through CEMA
DIV
BCT
BN
CO CP
UAS
Protect individuals and platforms
Activities:
• Cyberspace operations
• Electronic warfare
• Spectrum management operations

BCT	brigade combat team	CEMA	cyber electromagnetic activities	ISR	intelligence, support, reconnaissance
BN	battalion	COCP	company command post		
CAS	close air support	DIV	division	UAS	unmanned aerial systems

Figure 1-4. Cyber electromagnetic activities operational view

BUILD, OPERATE, AND DEFEND THE NETWORK

1-27. Unified land operations are increasingly dependent on net-enabled capabilities to collect, process, store, and disseminate information. Net-enabled capabilities are supported by LandWarNet. LandWarNet is the Army's portion of the Department of Defense information networks (DODIN). LandWarNet is a technical network that encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide. It provides commanders the information they need, when they need it, in any environment, to facilitate decisive action with unified action partners. CEMA establish this network infrastructure. Once established, the network must be operated in a way that allows it to be shaped and preserved to meet dynamic mission requirements. This is achieved through the management of network configurations, performance, resource allocations, faults, and security aligned with the commander's intent and priorities throughout the full range of military operations.

1-28. Because of the increased dependence on net-enabled capabilities, unified land operations are very sensitive to cyberspace and EW threats that can jeopardize the confidentiality and integrity of the mission command system and information. Enemy offensive operations in cyberspace and the EMS can affect all friendly operations. An adversary's ability to access Army cyberspace can result in the manipulation of information in Army systems. This change can influence future friendly actions (for example, delay an attack) and lead to reduced confidence in friendly systems. Reduced confidence results in a degraded situational understanding of the Army's information environment.

1-29. Inherent to the operation of the network are the actions to defend it by monitoring for, detecting, analyzing, and responding to anomalous network activity. Defense of the network provides a greater understanding of the operational environment through finding and fixing cyber-related threats and vulnerabilities. Attack sensing can offer leads to indications and warnings. The integration of network build, operate, and defend operations (known as LandWarNet network operations) establishes the portion of cyberspace commanders require to assure network and system availability, information delivery, and information protection. (See FM 6-02.71 for more information on LandWarNet network operations.)

ATTACK AND EXPLOIT ENEMY AND ADVERSARY SYSTEMS

1-30. Attacking enemy and adversary networks and systems can disrupt and deny them freedom of action in cyberspace and the EMS. CEMA provide the commander with capabilities that can be employed to deceive, degrade, disrupt, deny, destroy, or manipulate across the continuum, and CEMA can exploit enemy and adversary systems to facilitate intelligence collection. These capabilities may be used to target enemy and adversary cyberspace and EW functions or create first-order effects in cyberspace and the EMS to create cascading effects into natural domains to affect weapons systems, command and control processes, and critical infrastructure and key resources.

1-31. CEMA enhance the lethality of traditional weapons systems. Examples include the use of data links and network based targeting systems, targeting and terminal guidance through laser designators, laser range finders, global positioning systems, and seeker weapons.

SITUATIONAL UNDERSTANDING THROUGH CEMA

1-32. To gain understanding, commanders and staffs process data to develop meaning. At the lowest level, processing transforms data into information. Analysis then refines information into knowledge. Commanders and staffs then apply judgment to transform knowledge into situational understanding. CEMA provide capabilities that greatly enhance situational understanding of an operational environment. These capabilities provide the networks, information systems, and equipment, such as blue force tracking, command post of the future, and force XXI battle command brigade and below, that provide the common operational picture. CEMA also provide the means for communication that facilitate a commander's situational understanding of an environment. Cyberspace and the EMS are leveraged by Army forces to provide communication through voice, data, chat, video, teleconferencing, e-mail, and web interfaces such as SharePoint and Defense Connect Online. U.S. sensors, whether optical, electro-optical, thermal, millimeter wave, or multi-spectral, use cyberspace and the EMS to provide near real-time information to commanders and Soldiers. Mobile global positioning enabled systems that provide awareness of Soldiers' battlefield locations are also examples of systems that use cyberspace and the EMS.

PROTECT INDIVIDUALS AND PLATFORMS

1-33. CEMA provide Army forces with capabilities to increase survivability. Examples of survivability enhanced by EW include the use of expendables such as flares, electronic countermeasures against radio-controlled improvised explosive devices, and jamming to disable an enemy's equipment or capability. SMO enhances survivability through mitigating electromagnetic interference in systems from friendly use of EW. Survivability is also enhanced by CO through the secure and uninterrupted flow of data and information that allows Army forces to multiply their combat power and synchronize with other joint capabilities.

This page intentionally left blank.

Chapter 2

Roles, Responsibilities, and Organization

This chapter discusses roles and responsibilities of the commander, introduces the cyber electromagnetic activities (CEMA) element, and follows with the roles of the assistant chief of staff, operations (G-3 [S-3]) and staff within CEMA. It concludes with a discussion of the roles of supporting agencies and the Soldier's role in conducting CEMA.

THE COMMANDER'S ROLE IN CEMA

2-1. The commander is a central and critically important figure in the conduct of CEMA. Commanders leverage CEMA as part of combined arms operations to achieve objectives in the natural domains, cyberspace, and the electromagnetic spectrum (EMS) though lethal and nonlethal means. Commanders conduct CEMA to seize, retain, and exploit an advantage over adversaries and enemies in the natural domains, cyberspace, and the EMS, thereby facilitating overall mission success.

2-2. Commanders integrate and synchronize CEMA across all command echelons and warfighting functions as part of the operations process. They develop the commander's guidance for planning which informs the development of desired end states and supporting desired effects. They develop the commander's intent which establishes key tasks that shape actions to achieve and maintain freedom of action in cyberspace and the EMS. Specific to execution, commanders direct the timely delivery of actions to enable simultaneous and complementary effects in support of the concept of operations.

2-3. Commanders make decisions based on recommendations provided by the G-3 (S-3) through information received from the CEMA element. Through this process, commanders guide the integration and synchronization of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO) into their concept of operations. Commanders designate resources to employ in support of CEMA.

COMMANDER'S CONSIDERATIONS

2-4. Unified land operations require commanders to consider what will affect an operational environment. Staffs, when integrating and synchronizing CEMA with other capabilities available to them, must take into account the following considerations:

- Execution of CEMA can involve significant legal and policy considerations.
- Execution of CEMA may require long lead times due to availability of assets and approval authority considerations.
- CO require extensive coordination (for example, national level authorities) for most missions that extend outside of LandWarNet.
- EW can be enabled and executed at all levels and can emphasize supporting the tactical commander.
- CEMA offer the option to employ alternative effects to achieve objectives formerly attained only by physical destruction.
- CEMA can create simultaneous and near instantaneous effects across multiple domains. These effects may occur within friendly, neutral, and adversary portions of cyberspace and the EMS.
- Possibilities of unintended or cascading effects exist and may be difficult to predict.
- Situational understanding of the operational environment is incomplete without the inclusion of cyberspace and the EMS.
- CEMA must be leveraged to protect and ensure access to the mission command system.

THE CYBER ELECTROMAGNETIC ACTIVITIES ELEMENT

2-5. The CEMA element consists of personnel who can plan, prepare, and synchronize CO, EW, and SMO. The CEMA element is led by the electronic warfare officer (EWO) and provides staffs expertise for the planning, integration, and synchronization of CO, EW, and SMO. Commanders organize their staffs based on mission requirements, strengths, and weaknesses. When the mission dictates, the CEMA element can leverage other additional skill sets of the CEMA working group as needed to conduct both joint and unified land operations. When operating in a joint, multinational, or intergovernmental environment, commanders may reorganize their staffs to better align with higher headquarters. The CEMA element is an organic organization in brigade, division, corps, and theater Army staffs. (See figure 2-1.)

2-6. The CEMA element integrates CEMA into the operations process from theater Army through brigade. The CEMA element is responsible for coordinating organic and nonorganic CEMA capabilities in support of the concept of operations. As a staff element, the CEMA element participates in the planning and targeting processes to determine desired effects in support of the concept of operations. During execution, the CEMA element is responsible for integrating and synchronizing CEMA to best facilitate mission accomplishment. For additional information on Army planning methodologies, see ADP 5-0 and ADRP 5-0. (See chapter 6 for a detailed discussion of how the CEMA element participates in the operations process).

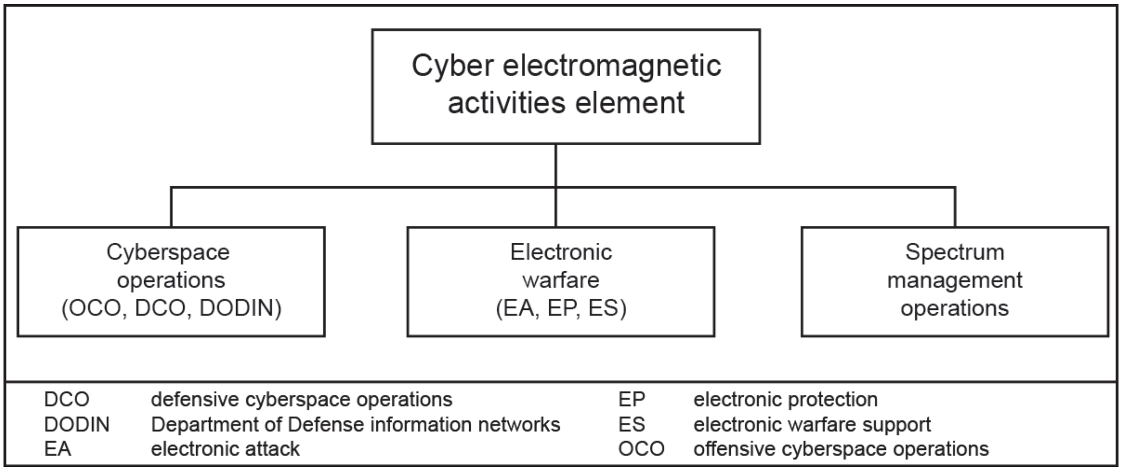

Cyber electromagnetic activities element
Cyberspace operations (OCO, DCO, DODIN)
Electronic warfare (EA, EP, ES)
Spectrum management operations
DCO defensive cyberspace operations
DODIN Department of Defense information networks
EA electronic attack
EP electronic protection
ES electronic warfare support
OCO offensive cyberspace operations

Figure 2-1. The cyber electromagnetic activities element

2-7. CO, EW, and SMO differ in their employment and tactics; however, their functions and capabilities must be integrated and synchronized to ensure synergy with one another and other combined arms capabilities. Throughout the operations process, staffs—

- Consider CEMA as part of a combined arms team.
- Integrate CEMA with other information-related capabilities through inform and influence activities (IIA).
- Determine how CEMA, combined with physical actions, achieve the commander's desired end state.

The staff determines how CEMA create effects in the operational environment. They identify internal and external CEMA requirements and capabilities, and they comply with legal and policy constraints.

2-8. The CEMA element works to ensure that both cyberspace and the EMS are leveraged to maximum effect in achieving the unit's overall mission. This could include setting conditions in cyberspace and the EMS to facilitate a unit's mission.

2-9. The CEMA element coordinates the offensive and defensive aspects of CEMA. The element orients on the commander's desired end state and this informs the development and implementation of actions designed to gain and maintain freedom of action across cyberspace and the EMS. The element informs commanders and staffs about its activities and continually assesses progress toward desired conditions. It integrates and synchronizes all appropriate capabilities in order to achieve these desired conditions. It performs vertical and lateral coordination across Army command echelons to achieve the best results from assigned and supporting capabilities.

2-10. The CEMA element coordinates the functions and capabilities of CEMA across all the warfighting functions and staff elements, both vertically and horizontally, which includes integration with external staffs, organizations, and multinational partners. Given the dynamic nature of CEMA, the CEMA element requires a presence in the current operations integrating cell, and will need co-located representatives from other staff elements to achieve real time awareness and direct dynamic actions and response actions to unfolding challenges and opportunities.

KEY PERSONNEL IN PLANNING AND COORDINATING CEMA

2-11. There are several key personnel involved in the planning and coordination of CEMA in the CEMA element. They are the—

- EW staff.
- Spectrum manager.
- Assistant chief of staff, intelligence (G-2 [S-2]) staff.
- Assistant chief of staff, signal (G-6 [S-6]) staff.

ELECTRONIC WARFARE STAFF

2-12. The EWO serves as the commander's designated staff officer for the planning, integration, synchronization, and assessment of CEMA and uses other members of the staff to integrate CEMA into the commander's concept of operations. The EWO is responsible for understanding all applicable classified and unclassified policy relating to cyberspace, EW, and EMS in order to properly inform the commander on the proper planning, coordination, and synchronization of CO, EW and SMO. The EWO—

- Integrates, coordinates, and synchronizes all CEMA related functions and capabilities being executed.
- In coordination with the appropriate legal support, advises the commander on CEMA associated rules of engagement impact and constraints.
- Develops and maintains the consolidated CEMA target synchronization matrix.
- Nominates offensive cyberspace operations and electronic warfare targets for approval from the fire support coordinator and commander.
- Receives, vets, and processes offensive cyberspace operations and EW targets from subordinate units.
- Develops and prioritizes CEMA effects and targets with the fire support coordinator.
- Monitors execution of capabilities employed through CEMA.
- Continuously assesses measures of performance and effectiveness against the intended plan.
- Coordinates targeting and assessment collection with higher, adjacent, and subordinate organizations or units.
- Advises the commander and staff for adjustments in the plan based on the assessment.
- Advises the commander on how CEMA can impact an operational environment.
- Prepares to receive and integrate cyberspace operations team(s) and capabilities.
- Coordinates with the expeditionary cyberspace support element for offensive cyberspace operations support for approved targets.
- Provides recommendations on commander's critical information requirements and priority intelligence requirements.
- Prepares and processes the cyber effects request format and the electronic attack request format.
- Participates in other cells and working groups as required to ensure integration of CEMA.

2-13. The EWO or EW noncommissioned officer plans, coordinates, and supports the execution of EW within the CEMA element. The EWO or EW noncommissioned officer—

- Plans, coordinates, and assesses electronic attack, protect, and support requirements.
- Supports the G-2 (S-2) during intelligence preparation of the battlefield.
- Provides information collection requirements to the G-2 (S-2) to support the assessment of EW.
- Supports the fire support coordinator to ensure the integration of electronic attack with all other effects.
- Provides electronic warfare support derived tactical targeting information to the fire support coordinator.
- Coordinates with the G-6 (S-6) to plan, assess, and implement electronic protection measures.
- Prioritizes EW effects and targets with the fire support coordinator.
- Plans and coordinates EW operations across functional and integrating cells.
- Deconflicts EW operations with the spectrum manager within the CEMA element.
- Maintains a current assessment of available EW resources.
- Participates in other cells and working groups (as required) to ensure EW integration.
- Serves as EW subject matter expert on existing EW rules of engagement.
- Serves as the EW jamming control authority when designated.
- Prepares, submits for approval, and supervises the issuing and implementation of fragmentary orders for EW operations.
- Ensures EW operations are synchronized and deconflicted with intelligence collection activities.

Spectrum Manager

2-14. The spectrum manager coordinates EMS use for a wide variety of communications and electronic resources. The spectrum manager—

- Issues the signal operating instructions.
- Provides all spectrum resources to the task force.
- 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 eliminate, moderate, or mitigate electromagnetic interference.
- 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, CO, and intelligence collection.

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

2-15. The G-2 (S-2) works with the rest of the staff including the CEMA element to provide intelligence support. The G-2 (S-2)—

- Provides the same all-source intelligence support to CEMA as to other operations.
- Coordinates with the intelligence community to help establish attribution for associated adversary initiated cyberspace, electronic attack, or exploitation activities.
- Requests reachback intelligence support and collaborates with the intelligence community for intelligence support to CO. This support serves as a force multiplier for the CEMA element when leveraged effectively.

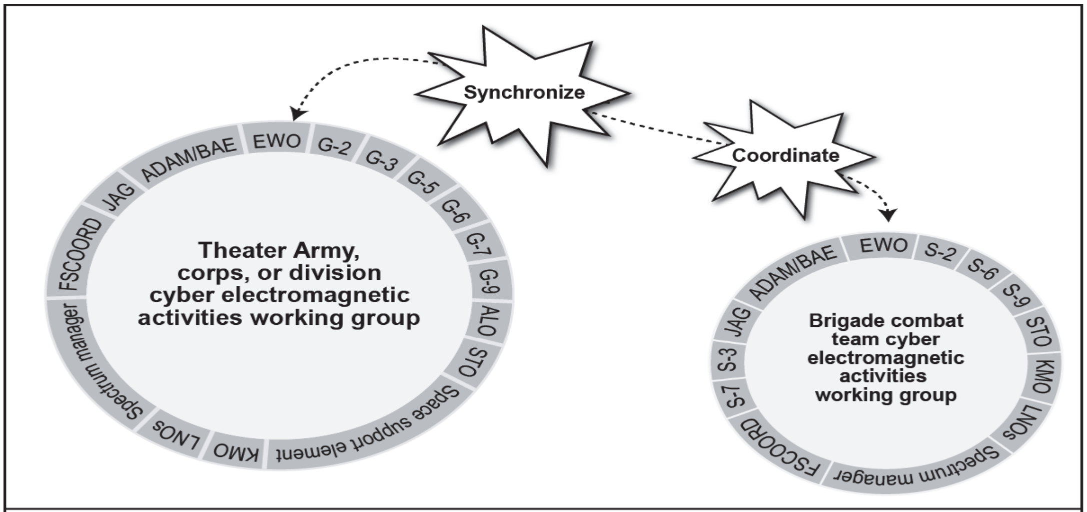
Assistant Chief of Staff, G-6 (S-6), Signal

2-16. The G-6 (S-6) conducts the following LandWarNet network operations actions within the CEMA element. The G-6 (S-6)—

- Shares and integrates the friendly force network common operational picture with information on adversary, allied, neutral, or other specified cyberspace areas in order to contribute to the situational understanding of cyberspace and the EMS.
- Receives and requests intelligence information from the G-2 (S-2) in reference to potential threats and associated threat tactics, techniques, and procedures used against mission command networks and systems.
- Plans, integrates, and synchronizes Department of Defense information network operations including LandWarNet network operations, network transport, and information services into the unit's operations processes and scheme of maneuver.
- Reports information on unauthorized network activity to be integrated with other indications and warning of adversary activities.
- Presents a timely and accurate estimate of technical impacts resulting from threat activity and determines detrimental effects to the unit's mission.
- Plans, coordinates, and synchronizes pre-approved response actions to threat activity and assesses risk to networks and information systems, in coordination with the CEMA element.
- Plans, requests, and coordinates the implementation of defensive cyberspace operations and countermeasures provided by entities external to the unit, in coordination with the CEMA element.
- Participates in the after action reviews of an incident to determine the effectiveness and efficiency of incident handling.
- Assists in the prioritization of CEMA effects and targets.
- Deconflicts defensive cyberspace operations with unified land operations, including vulnerability assessments, in coordination with the CEMA element.
- Supports development of techniques, tactics, and procedures for capabilities within CEMA, in coordination with the CEMA element.
- Assesses defensive requirements for CEMA, in coordination with the CEMA element.
- Provides current assessment of defensive cyberspace operations resources available to the unit, in coordination with the CEMA element.

THE CYBER ELECTROMAGNETIC ACTIVITIES WORKING GROUP

2-17. The CEMA working group, when established, is accountable for integrating CEMA 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 a collaborative staff meeting led by the EWO to analyze, coordinate, and provide recommendations for a particular purpose, event, or function. 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-6 (S-6), G-7 (S-7), G-9 (S-9), fire support officer, space support element, judge advocate general representative (or appropriate legal advisor), and a joint terminal attack controller when assigned (see figure 2-2 on page 2-6). Deletions or modifications to the CEMA working group staff are based on requirements for certain capabilities and assets. (See table 2-1 on page 2-8 for an outline of the functions of the CEMA working group.) The CEMA working group augments the function of the permanently established CEMA element. When scheduled, the CEMA working group is a critical planning event integrated into the staff's battle rhythm.



ADAM/BAE	air defense air space management/brigade aviation element	JAG	judge advocate general
ALO	air liaison officer	KMO	knowledge management officer
EWO	electronic warfare officer	LNO	liaison officer
FSCOORD	fire suppvort coordinator	S-2	intelligence staff officer
G-2	assistant chief of staff, intelligence	S-3	operations staff officer
G-3	assistant chief of staff, operations	S-6	signal staff officer
G-5	assistant chief of staff, plans	S-7	inform and influence activities staff officer
G-6	assistant chief of staff, signal	S-9	civil affairs staff officer
G-7	assistant chief of staff, inform and influence activities	STO	special technical officer
G-9	assistant chief of staff, civil affairs		

Figure 2-2. Cyber electronic activities working group

ADDITIONAL KEY PERSONNEL IN THE CEMA WORKING GROUP

2-18. The key personnel found in the CEMA element are central to the CEMA working group. The working group members will vary. The personnel most likely to be involved in the majority of CEMA working groups are—

- G-7 (S-7) staff.
- G-9 (S-9) staff.
- Staff judge advocate general.
- Space support element staff.
- Liaisons.

ASSISTANT CHIEF OF STAFF, G-7 (S-7), INFORM AND INFLUENCE ACTIVITIES STAFF OFFICER

2-19. The G-7 (S-7) integrates designated information-related capabilities and other organic capabilities a commander may use for IIA (including the capabilities of CEMA). This staff officer is the information environment subject matter expert and primary advisor to the commander when operational activity and its direct or indirect message or perception could influence the information environment. The IIA staff officer—

- Integrates all information related capabilities being executed as part of the commander's IIA.
- Continuously assesses measures of effectiveness and measures of performance against the intended plan.
- Identifies information capacity and infrastructure in the area of operations.
- Nominates and coordinates targets to the CEMA working group to ensure IIA are integrated and deconflicts information-related capability requirements.
- Provides requirements for the information collection plan.
- Prioritizes effects and targets with the fire support coordinator and staff.

ASSISTANT CHIEF OF STAFF, G-9 (S-9), CIVIL AFFAIRS OPERATIONS

2-20. The G-9 (S-9) advises the commander and CEMA working group on the potential effects of CO and EW on the civilian population. The civil affairs operations officer—

- Creates conditions that contribute to CEMA in the area of operations.
- Provides requirements for the information collection plan.
- Identifies civilian and commercial cyber-related capacity and infrastructure within the area of operations.
- Assists in the prioritization of CEMA effects and targets in the area of operations.

STAFF JUDGE ADVOCATE GENERAL

2-21. The staff judge advocate advises the commander and the CEMA working group with respect to operational law and cyberspace actions, particularly if CO may affect non-combatants. The staff judge advocate—

- Ensures CEMA actions comply with applicable policies and laws.
- Reviews potential CEMA actions in accordance with relevant legal frameworks and authorities granted at national and regional command levels.

SPACE SUPPORT ELEMENT

2-22. The space support element coordinates and synchronizes space-related activities and operations during unified land operations. The space support element—

- Plans, coordinates, and assesses space situational awareness, space force enhancement, space control, space force application, and space support requirements.
- Provides space-based expertise and services that enhance CEMA.
- Supports the G-2 (S-2) during intelligence preparation of the battlefield.
- Develops and maintains space segment threat assessment (in conjunction with the G-2 [S-2] and appropriate DOD organizations), including environmental threats and potential adversary employment counter-space activities against friendly on-orbit and ground based supporting infrastructure, and proposes and coordinates required activities to mitigate these threats and activities.
- Participates in other cells and working groups (as required) to ensure space integration into CEMA.
- Supports the G-6 (S-6) in developing and maintaining the network common operating picture.
- Integrates space-related capabilities into CEMA planning.
- Analyzes and recommends the potential employment of additional space-related capabilities to support CEMA.

THE ROLE OF OTHERS IN CYBER ELECTROMAGNETIC ACTIVITIES

2-23. The CEMA element collaborates internally with subordinate units and externally with supported, supporting, and adjacent units and centers. The CEMA element neither owns nor controls any of the unit's CO or EW assets, but it must coordinate with many who do. Therefore, CEMA staff personnel cannot support the element's mission by themselves. To plan, integrate, and synchronize successfully, the CEMA element, in coordination with the G-2 (S-2), collaborates via several means both internally to its unit and externally to its supporting units. The organization's knowledge management section can assist in establishing mechanisms to facilitate collaboration and reachback. (See table 2-1 on page 2-8.)

Table 2-1. Functions of the cyber electromagnetic activities working group

CEMA Working Group Participants	*CEMA Working Group Functions*
Division and above ADAM/BAE ALO EWO G-2 G-3 G-5 G-6 G-7 G-9 FSCOORD JAG KMO LNOs Spectrum manager Space support element STO	• Plan and integrate CEMA in support of operations or command requirements. • Plan and nominate targets within cyberspace and the EMS for offensive CEMA capabilities to achieve effects that support the commander's intent. • Develop and integrate CEMA actions into operation 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 functions and capabilities. • Plan, coordinate, and assess offensive and defensive CEMA requirements. • Plan, coordinate, synchronize, deconflict, and assess CEMA functions and capabilities. • Maintain current assessment of resources available to the commander for CEMA. • Prioritize effects and targets for functions and capabilities within CEMA. • Predict effects of friendly and enemy CEMA. • Coordinate spectrum management and radio frequency deconfliction with G-6 and J-6. • Plan, assess, and implement friendly electronic security measures. • Plan, coordinate, integrate, and deconflict CEMA within the operations process. • Ensure CEMA actions comply with applicable policy and laws. • Identify civilian and commercial CEMA-related capacity and infrastructure within the area of operations.
Brigade ADAM/BAE ALO EWO FSCOORD JAG KMO S-2 S-3 S-6 S-7 S-9 LNOs Spectrum manager STO	• Develop and integrate CEMA actions into operation plans and exercises. • Support CEMA policies. • Plan, prepare, execute, and assess CEMA. • Integrate intelligence preparation of the battlefield into the operations process. • Identify and coordinate intelligence support requirements for BCT and subordinate units' CEMA. • Assess offensive and defensive requirements for CEMA functions and capabilities. • Maintain current assessment of CEMA resources available to the unit. • Nominate and submit approved targets within cyberspace and the EMS for offensive CEMA capabilities to division. • Prioritize BCT targets for functions and capabilities within CEMA. • Plan, coordinate, and assess friendly CEMA. • Implement friendly electronic and network security measures (for example, electromagnetic spectrum mitigation and network protection). • Ensure CEMA actions comply with applicable policy and laws. • Identify civilian and commercial CEMA-related capacity and infrastructure within the area of operations.

ADAM/BAE	air defense air space element/brigade aviation element
ALO	air liaison officer
BCT	brigade combat team
CEMA	cyber electromagnetic activities
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-7	assistant chief of staff, inform and influence activities
G-9	assistant chief of staff, civil affairs operations
JAG	judge advocate general
J-6	communications system directorate of a joint staff
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-7	inform and influence activities staff officer
S-9	civil affairs staff officer

THE SOLDIER'S ROLE IN CEMA

2-24. Routine uses of cyberspace, such as sending e-mail, using the Internet to complete an online training course, and developing a briefing document, may occur in cyberspace, but they do not amount to what is defined as CO. However, it is through these routine uses of cyberspace that most of the vulnerabilities on U.S. networks are exposed to, and exploited by, adversaries. This includes communications that enter the

EMS. By following accepted operations security procedures, every Soldier contributes to CEMA. Commanders, leaders, and non-commissioned officers educate Soldiers on threats in cyberspace and the EMS. Soldiers understand the relationship between cyberspace and the EMS and maintain the necessary protection measures when using devices that leverage this relationship between capabilities.

This page intentionally left blank.

Chapter 3

Cyberspace Operations

This chapter provides an overview of cyberspace operations (CO) as an activity that is integrated into operations through cyber electromagnetic activities (CEMA). It discusses the three functions of CO and operations in and through cyberspace.

FUNCTIONS OF CYBERSPACE OPERATIONS

3-1. Army forces coordinate and integrate CO through CEMA. They do this to gain and maintain freedom of action in cyberspace and as required to achieve periods of cyberspace superiority.

3-2. *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 adversary (JP 1-02). Such interference is possible because large portions of cyberspace are not under the control of friendly forces. Cyberspace superiority establishes conditions describing friendly force freedom of action while denying this same freedom of action to enemy and adversary actors. Ultimately, Army forces conduct CO to create and achieve effects in support of the commander's objectives and desired end state.

3-3. CO are categorized into three functions including offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense information network operations. These functions are described in joint doctrine as missions in cyberspace that require specific actions in cyberspace (see joint doctrine for CO). Figure 3-1 on page 3-2 depicts the three interdependent functions of CO.

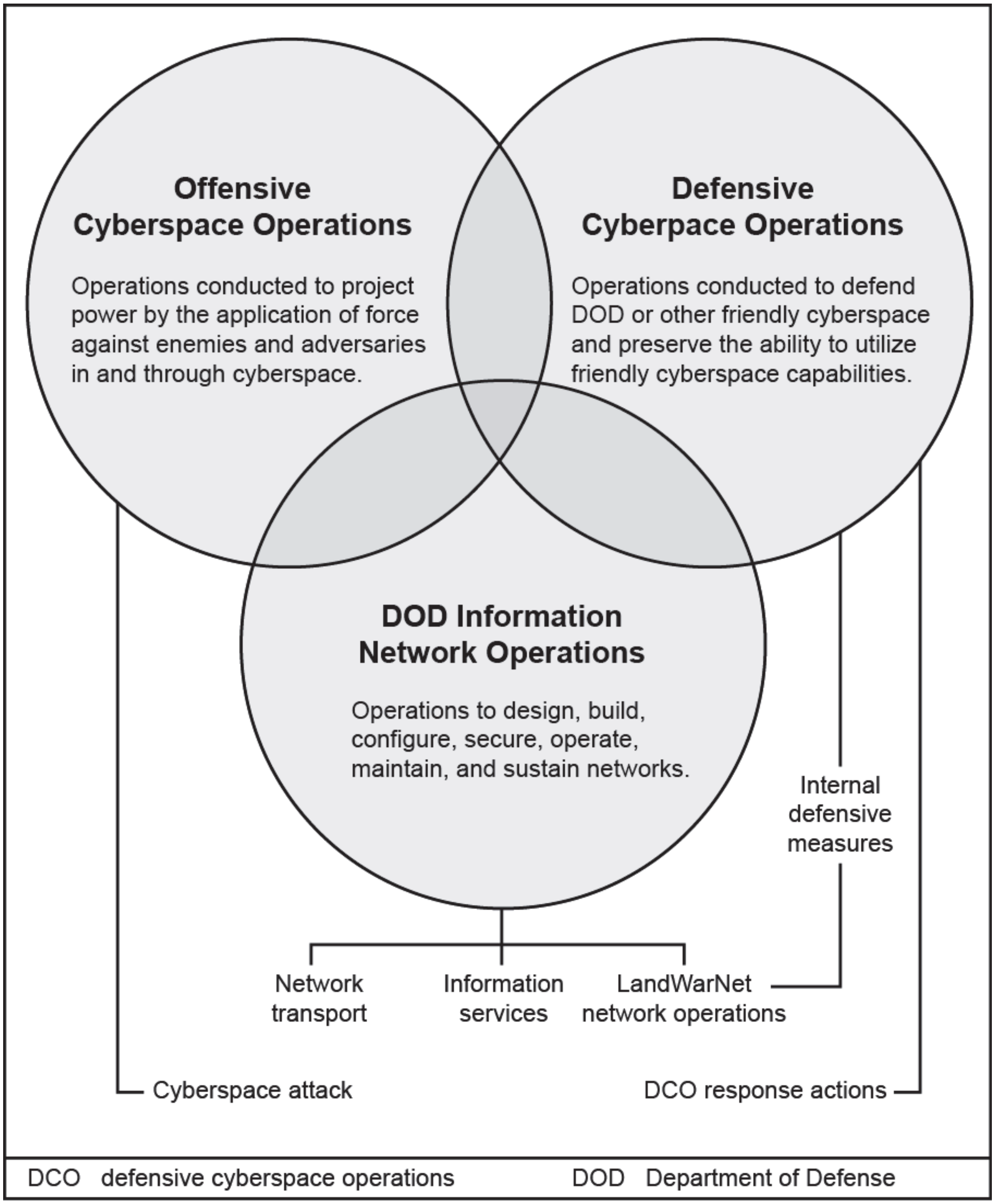

Offensive Cyberspace Operations
Operations conducted to project power by the application of force against enemies and adversaries in and through cyberspace.
Defensive Cyberpace Operations
Operations conducted to defend DOD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.
DOD Information Network Operations
Operations to design, build, configure, secure, operate, maintain, and sustain networks.
Internal defensive measures
Network transport
Information services
LandWarNet network operations
Cyberspace attack
DCO response actions
DCO defensive cyberspace operations
DOD Department of Defense

Figure 3-1. Three interdependent functions

OFFENSIVE CYBERSPACE OPERATIONS

3-4. *Offensive cyberspace operations* are cyberspace operations intended to project power by the application of force in or through cyberspace (JP 1-02). Army forces conduct OCO across the range of military operations by targeting enemy and hostile adversary activity and related capabilities in and through cyberspace. OCO are designed to support the commander's objectives and intent consistent with applicable authorities and legal frameworks. (See paragraph 3-38 for additional information on authorities and other legal considerations.)

3-5. OCO are conducted in and through cyberspace where information technology infrastructures, along with the people and systems that use them, exist in an area of operations and pervade an operational environment. To varying degrees, host-nation populations, governments, security forces, businesses and other actors rely upon these infrastructures and supporting networks or systems. Given these conditions, OCO require deliberate coordination and integration to ensure desired effects (changes in behavior which do not suggest the ways or means those changes were created) are created and focused at the right place and time in support of the commander's objectives.

3-6. Using OCO, commanders can mass effects through the employment of lethal and nonlethal actions leveraging all capabilities available to gain advantages in cyberspace that support objectives on land. For example, cyberspace capabilities and other information-related capabilities may be directed at an enemy weapons system consisting of the targeted platform and its operators. The cyberspace capability could create degrading effects on the platform while an information-related capability influences, disrupts, corrupts, or usurps the decisionmaking of the operator. (See FM 3-13 for additional information on inform and influence activities (IIA) and information-related capabilities.)

CYBERSPACE ATTACK

3-7. A cyberspace attack consists of actions that create 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. For the Army, cyberspace attacks are a type of cyberspace operation employed primarily in support of OCO. Cyberspace attacks are primarily employed outside of LandWarNet, but they are coordinated and deconflicted inside of the Department of Defense information networks (DODIN). (See paragraph 3-24 for additional information on the DODIN.)

3-8. Army forces conduct or facilitate cyberspace attacks in support of OCO within designated areas of operation. For example, when employed as part of an offensive cyberspace operation, a cyberspace attack may be directed at information resident in, or in transit between, computers (including mobile phones and personal digital assistants) and computer networks used by an enemy or adversary. Enemy or adversary actors may be denied the ability to use resources or have their information resources used for friendly proposes as a result of a cyberspace attack. In every instance, commanders and staffs follow appropriate authorities and legal guidance. (See paragraph 3-38 for additional information on authorities and other legal considerations.)

3-9. Using specific portions of cyberspace and the electromagnetic spectrum (EMS) as primary pathways or avenues of approach, cyberspace attacks may employ capabilities such as tailored computer code in and through various network nodes such as servers, bridges, firewalls, sensors, protocols, operating systems, and hardware associated with computers or processors. Tailored computer code is only one example of a cyberspace capability (a device, computer program, or technique, including any combination of software, firmware, or hardware) designed to create an effect in or through cyberspace. The development and employment of tailored computer code represents the core and unique technical nature of CO capabilities. Computer code is designed to create specific effects, and when employed this code moves in the form of data packets in and through cyberspace across wired and wireless driven communication technology and systems. Cyberspace attacks must therefore be coordinated and integrated in support of the commander's objectives and consistent with applicable assessment measures and indicators.

3-10. Cyberspace attack capabilities are employed to support maneuver operations by creating simultaneous and complementary effects. For example, a cyberspace attack capability may be employed in conjunction with electronic attack, offensive space control, fires, and information related capabilities to deceive, degrade, destroy, and disrupt a specific enemy integrated air defense system or enemy safe haven (see table 3-1 on page 3-4).

Table 3-1. Examples of simultaneous and complementary 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)

3-11. In table 3-1, 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 intelligence preparation of the battlefield, cyber-enabled intelligence, the targeting process, and cyberspace information collection. Cyberspace attacks may employ manipulation which includes deception, decoying, conditioning, and spoofing to control or change information, information systems, and networks. Ultimately, decisions to employ cyberspace attack capabilities alone or in conjunction with other capabilities will be determined by commanders, with the assistance of their staffs, throughout the operations process. (See chapter 6 for additional information on the operation process.)

CYBERSPACE INFORMATION COLLECTION

3-12. Cyberspace information collection is an extension of information collection consisting of actions that facilitate CO primarily through deliberate network reconnaissance and surveillance and other enabling activities (including access to or control of those networks) in and through cyberspace. Cyberspace information collection includes activities in cyberspace conducted to gather intelligence from target and adversary systems that may be required to support future operations and enabling activities conducted to plan and prepare for follow-on military operations. Cyberspace information collection aligns with joint constructs for cyberspace intelligence, surveillance, and reconnaissance and cyberspace operational preparation of the environment as discussed in paragraphs 3-13 through 3-15 and depicted in figure 3-2.

3-13. Consistent with joint doctrine, cyberspace intelligence, surveillance, and reconnaissance includes activities in cyberspace conducted to gather intelligence from target and adversary systems that may be required to support future operations, including OCO or DCO. These activities synchronize and integrate the planning and execution of cyberspace sensors, assets, and processing, exploitation, and dissemination systems, in direct support of current and future operations. For the Army, cyberspace information collection expands joint cyberspace intelligence, surveillance, and reconnaissance by focusing on answering the commander's critical information requirements thereby enabling understanding and decisionmaking.

3-14. Consistent with joint doctrine, cyberspace operational preparation of the environment consists of the non-intelligence enabling activities conducted to plan and prepare for follow-on military operations. This includes identifying data, software, system and network configurations and identifiers, or physical structures connected to, or associated with, the network for the purposes of determining system vulnerabilities. This also includes actions taken to assure future access or control of the system, network, or data during anticipated hostilities. (See joint doctrine for cyberspace operations for more information.) For the Army, cyberspace information collection expands joint cyberspace operational preparation of the environment and enables commanders and staffs to plan, prepare, and facilitate the employment of cyberspace capabilities.

3-15. Cyberspace information collection is employed primarily in support of OCO. Accordingly, cyberspace information collection is employed outside of LandWarNet and coordinated and deconflicted inside of the DODIN. In every instance of cyberspace information collection, commanders and staffs follow appropriate authorities, legal guidance, and international law. (See paragraph 3-24 for additional information on the DODIN.)

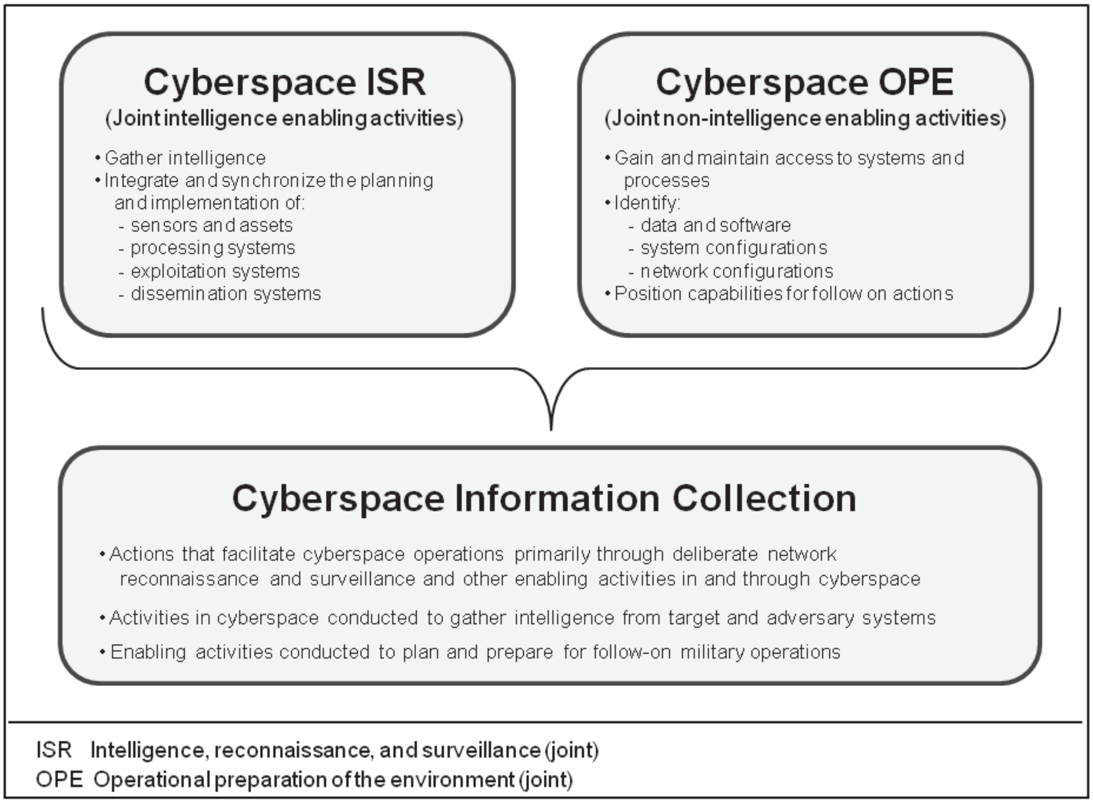

Cyberspace ISR
(Joint intelligence enabling activities)
• Gather intelligence
• Integrate and synchronize the planning and implementation of:
- sensors and assets
- processing systems
- exploitation systems
- dissemination systems
Cyberspace OPE
(Joint non-intelligence enabling activities)
• Gain and maintain access to systems and processes
• Identify:
- data and software
- system configurations
- network configurations
• Position capabilities for follow on actions
Cyberspace Information Collection
• Actions that facilitate cyberspace operations primarily through deliberate network reconnaissance and surveillance and other enabling activities in and through cyberspace
• Activities in cyberspace conducted to gather intelligence from target and adversary systems
• Enabling activities conducted to plan and prepare for follow-on military operations
ISR Intelligence, reconnaissance, and surveillance (joint)
OPE Operational preparation of the environment (joint)

Figure 3-2. Cyberspace information collection from joint cyberspace actions

DEFENSIVE CYBERSPACE OPERATIONS

3-16. *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 1-02). Army forces conduct DCO across the range of military operations by detecting, identifying, and responding to enemies and adversaries taking or about to take offensive actions against friendly networks and information resident in these networks, particularly LandWarNet. (See paragraph 3-45 for information on enemy and adversary cyberspace activity.)

3-17. DCO are designed to detect and respond to unauthorized activity or indications of activity (alerts and threat information) against friendly networks including LandWarNet and DOD communications systems and networks. Army forces may be required to dynamically reestablish, resecure, reroute, reconstitute, or isolate degraded or compromised networks to ensure continuous access to specific portions of cyberspace that enable the friendly mission command system. Enemy or adversary actions involving attack, exploitation, intrusion, or effects of malware on friendly networks may require the notification of counterintelligence or law enforcement agencies and it may trigger certain pre-authorized response actions requiring the creation of effects outside of LandWarNet.

3-18. There are two major types of DCO. They are—

- DCO response actions.
- Internal defensive measures.

DCO Response Actions

3-19. *Defensive cyberspace operation response actions* are deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems (JP 1-02). DCO response actions are initiated by various sensors and capabilities. Once these sensors and capabilities detect and identify sources of cyber attack, response actions (for example, employment of tailored computer code) may be employed with the intent to protect and defend friendly force cyberspace capabilities or other designated systems.

3-20. DCO response actions may rise to a level of physical damage or destruction of enemy or adversary systems. In this situation, DCO response actions may require cyberspace information collection in the same manner in which it is required for OCO. As a result of these conditions, response actions require deliberate coordination and integration to ensure desired effects are created and achieved at the right place and time in support of the commander's objectives.

3-21. DCO response actions may involve countermeasures. Countermeasures are designed to identify the source of the threat to LandWarNet and use nonintrusive techniques to stop or mitigate the threat. Countermeasures are nondestructive in nature, typically impact only malicious activity but not the associated threat system, and are terminated when the threat stops. Countermeasures in cyberspace should not destroy or significantly impede the operations or functionality of the network they are being employed against, nor should they intentionally cause injury or the loss of life. In every instance of DCO response actions and countermeasures, commanders and staffs follow appropriate authorities, legal guidance, and international law.

Internal Defensive Measures

3-22. Internal defensive measures are those DCO that are conducted within the DODIN. (See joint cyberspace doctrine for more information on the DODIN.) Internal defensive measures may involve counter reconnaissance measures within LandWarNet or other DODIN to locate internal threats and respond to unauthorized activity or alerts and threat information. Internal defensive measures share similar objectives and tasks associated with the defense of LandWarNet. For example, tailored computer code may be employed inside LandWarNet to identify and mitigate threats that have bypassed routine defense measures. (See FM 6-02.71 for additional information on network operations.)

3-23. Army forces employ various internal defensive measures to protect and defend LandWarNet. DCO include the employment of internal defensive measures in response to an attack, exploitation, intrusion, or an effect of malware on LandWarNet. To assist in the defense of LandWarNet, the Army uses a defense-in-depth concept, which incorporates a layered approach for the implementation of defensive tools and procedures. At a minimum, this includes a perimeter router, firewall, intrusion detection system or intrusion protection system, domain name server, web proxy, and host-based security system that blocks, deceives, or redirects the threat. Defensive tools and techniques are designed to find, fix, and finish anomalous network activity using rule, signature, and behavioral-based techniques.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

3-24. *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 networks (JP 1-02). Accordingly, *Department of Defense information networks* are the globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security (JP 1-02). The coordination and integration of CO for the Army will occur primarily within LandWarNet, which is the Army's portion of the DODIN.

3-25. LandWarNet is a technical network that encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide. LandWarNet is a single, secure, standards-based, versatile infrastructure linked by networked, redundant transport systems, sensors, warfighting and business applications, and services that provides Soldiers and civilians timely and accurate information in any environment and enables decisive action with our joint, interagency, and multinational partners. (See FM 6-02.71 for additional information on LandWarNet.)

3-26. Army forces are involved in Department of Defense information network operations across the range of military operations to gain and maintain access to specific portions of cyberspace by planning, engineering, installing, operating, maintaining, controlling, and defending LandWarNet in support of both the generating force and the operational Army. This includes the proactive technical functions of configuration control, system patching, information assurance and user training, physical security, secure architecture design, host-based security systems and firewalls, and encryption of data at rest.

3-27. There are three major types of Department of Defense information network operations for the Army. They are—

- LandWarNet network operations.
- Network transport.
- Information services.

LANDWARNET NETWORK OPERATIONS

3-28. LandWarNet network operations are an integrated construct of Department of Defense information network operations involving enterprise management, network assurance, content management, situational understanding, and the mission command activities that guide signal entities in the installation, management, and defense of communications networks and information services necessary to support operational forces. LandWarNet network operations are therefore a subset of the overarching network operations which are activities conducted to operate and defend the DODIN. LandWarNet network operations involve network and systems management to engineer, install, operate, manage, service, and restore communication and computer networks, systems, and applications.

3-29. LandWarNet network operations protect and defend communications and computer networks, systems, and information services. Computer network defense protects, monitors, analyzes, detects and responds to unauthorized activity within information systems. Defending in the context of LandWarNet network operations involves those DCO that are conducted inside of friendly force networks to respond to unauthorized activity and to leverage intelligence, counterintelligence, law enforcement, and other military capabilities as required. Defending may also involve DCO response actions that occur outside of LandWarNet when deemed necessary. (See paragraph 3-19 for additional information on DCO response actions.)

3-30. LandWarNet network operations also involve information assurance, information dissemination management, and content staging capabilities that allow users to collect, process, store, discover, and disseminate information. (See FM 6-02.71 for additional information on LandWarNet network operations.)

NETWORK TRANSPORT

3-31. Network transport is a system of systems including the people, equipment, and facilities that provide end-to-end communications connectivity for network components. The system of systems and end-to-end communications connectivity relative to network transport enables network transport systems to transmit and receive voice, video, and date in order to execute warfighting functions in support of unified land operations. Network transport encompasses the integrated space, aerial, and terrestrial capabilities that provide access from Soldier and sensor through joint and strategic levels. (See FM 6-02.71 for additional information on LandWarNet network operations.)

INFORMATION SERVICES

3-32. Through a full suite of information services, commanders and Soldiers collect, process, store, transmit, display, and disseminate information. They also share information and collaborate with unified action partners through all phases of an operation anywhere in the world. Information sharing allows for the mutual use of information services or capabilities.

OPERATIONS IN AND THROUGH CYBERSPACE

3-33. Paragraphs 3-1 through 3-32 describe the functions of CO. The employment of these functions in and through cyberspace requires a full understanding of the following:

- The layers of cyberspace.
- Authorities and other legal considerations.
- The functions and the networks.
- Enemy and adversary cyberspace activity.
- Targeting in cyberspace.

THE LAYERS OF CYBERSPACE

3-34. The layers of cyberspace consist of the interdependent networks of information technology infrastructures and resident data within those structures. The interdependent networks of information technology infrastructures and resident data that define cyberspace exist in one or more layers of cyberspace. Commanders and staffs must consider these layers as they relate to the information environment, the operational environment, and the area of operations. Table 3-2 provides a sample of this analysis using the dimensions of the information environment, the operational variables associated with the operational environment, and the mission variables associated with activities in the area of operations.

3-35. The physical network layer includes geographic and physical network components. The geographic component is the physical location of elements of the network. The physical network component includes all the physical equipment associated with links (wired, wireless, and optical) and the physical connectors that support the transfer of code and data on the networks and nodes. For example, physical networks components may include wires, cables, radio frequencies, routers, servers, computers, radars, weapons systems, telecommunications systems, personal digital assistants, and other networked devices where data is created, manipulated, processed and stored. Commanders and staffs identify physical entities in cyberspace that may require specific effects and prioritize them for information collection, targeting, and assessment.

3-36. The logical network layer consists of the components of the network that are related to one another in ways that are abstracted from the physical network. For instance, nodes in the physical layer may logically relate to one another to form entities in cyberspace that are 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 another example. Commanders and staffs identify logical entities in cyberspace that may require specific effects and prioritize them for cyberspace information collection, targeting, and assessment.

3-37. The cyber-persona layer is an abstraction of the logical network, and it uses the rules of the logical network layer to develop 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 cell phone numbers. Cyber-personas hold important implications for Army forces in terms of attributing responsibility and targeting the source of a cyberspace threat. Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities may be required. Commanders and staffs identify cyber-persona entities in cyberspace that may require specific effects and prioritize them for information collection, targeting, and assessment.

Table 3-2. Sample application of the layers of cyberspace

Layers of Cyberspace	*Information Environment*	*Operational Environment*	*Area of Operations*
Physical network	• Command and control facilities and systems • Key decisionmakers • Computers and laptops • Smart phones and tablet computers	• Information technology infrastructures - Hardware - Systems software - Embedded processors - Controllers • Resident data • Critical infrastructure and key resources • Supervisory control and data acquisition systems • Distributed control systems	• Identification of physical entities in cyberspace that may require specific effects • Priorities for information collection and assessment • Priorities for targeting
Logical network	• Abstraction from the physical layer • Content and flow of information (data)	• Multiple nodes forming entities in cyberspace • Logical relationships between nodes • Data collection, processing, storage, usage	• Technical considerations for actions inside and outside of LandWarNet • Information collection and exploitation
Cyber-persona		• Digital representations of individuals - e-mail addresses - web site or similar identities • Abstraction from the logical layer	• Emphasis on positive target identification • Priorities for targeting and second-order effects

AUTHORITIES AND OTHER LEGAL CONSIDERATIONS

3-38. Commanders and staffs coordinate with key agencies, including the staff judge advocate, as they apply the functions of CO in accordance with authorities and relevant legal frameworks. The legal framework applicable to CO depends on the nature of the activities conducted, such as offensive or defensive military operations, stability operations, defense support to civilian authorities, service provider actions, intelligence operations, or defense of the homeland. Army forces conducting CO will comply with the law of war. (For more information on the law of war, see JP 1-04 and CJCSI 5810.01D.) Some functions of CO require deconfliction in accordance with current policies.

3-39. Authorities relevant to CO are derived from the United States (U.S.) Constitution and federal laws. These authorities establish roles and responsibilities that provide focus for organizations to develop capabilities and expertise, including those for cyberspace.

3-40. There are several key statutory authorities that apply to the Department of Defense (DOD). They include the United States Code (USC) Title 10 (Armed Forces) addressing the conduct of military operations in cyberspace to secure U.S. interests; USC Title 50 (War and National Defense) addressing intelligence gathering through cyberspace on foreign intentions, operations, and capabilities; and USC Title 32 (National Guard) addressing domestic consequence management.

3-41. In addition to the key statutory authorities described in paragraph 3-40, Army CO may involve USC Title 18 (Crimes and Criminal Procedure) addressing law enforcement actions to include prosecution of criminals operating in cyberspace. They may also involve USC Title 40 (Public Buildings, Property, and Works) addressing the establishment and enforcement of standards for acquisition and security of information technologies and USC Title 44 (Public Printing and Documents) addressing the implementation of information security policies and practices as required by standards and guidelines for national security systems.

3-42. Commanders and staffs must ensure compliance with all relevant authorities and associated legal frameworks before conducting CO. For instance, during armed hostilities involving Army forces deployed to a foreign nation state, an OCO may involve the disruption of a target which is being used by enemy forces but is located within public accessed infrastructure. USC Title 10 and Title 50 directly apply to Army forces as would DOD policies and standing rules of engagement. However, given the nature of the mission, international laws (for example, the law of war), international agreements, treaties, host-nation domestic laws, and other legal considerations may also be applicable. Table 3-3 provides an example of authoritative references and associated execution authorities for the three functions of CO.

Table 3-3. Example of alignment to authorities

Functions	***References***	***Executive Authority***
Offensive Cyberspace Operations	• USC Title 10 and Title 50 • Joint doctrine for cyberspace operations • Guidance from unified command plan • Guidance from presidential policy directive for cyberspace operations	• President of the United States • Secretary of Defense
Defensive Cyberspace Operations	• USC Titles 10, Title 18, and Title 50 • Joint doctrine for cyberspace operations • Guidance from unified command plan • Guidance from presidential policy directive for cyberspace operations SROE	• Combatant commanders (IDM) • Joint force commanders (IDM) • SROE - as required
Department of Defense Information Network Operations	• USC Titles 10, 18, 40, 44, and 50 • Guidance from unified command plan • Joint doctrine for cyberspace operations • DODD 8000.01 - management of the DOD information enterprise	• Defense Information Systems Agency • Network Enterprise Center • Army Network Enterprise Technology Command
CJCSI - Chairman of the Joint Chiefs of Staff Instruction DODD - Department of Defense Directive IDM - internal defensive measures	SROE - standing rules of engagement USC - United States Code	

THE FUNCTIONS AND THE NETWORKS

3-43. Commanders and staffs identify physical entities in cyberspace and the location where effects are desired. It is necessary to establish this geographic location and its relation to cyberspace because aligned authorities (see table 3-3) and other legal considerations will be applied in each situation. The functions of CO occur both outside and inside of the DODIN as depicted in figure 3-3.

3-44. OCO are employed primarily outside of the DODIN. DCO are employed primarily inside the DODIN and may extend outside of the DODIN. For the Army, Department of Defense information network operations are employed inside the DODIN and consist of LandWarNet network operations, network transport, and information services. Cyberspace information collection expands joint cyberspace intelligence, surveillance, and reconnaissance and joint cyberspace operational preparation of the environment to enable commanders and staffs to plan, prepare, and facilitate the employment of cyberspace capabilities.

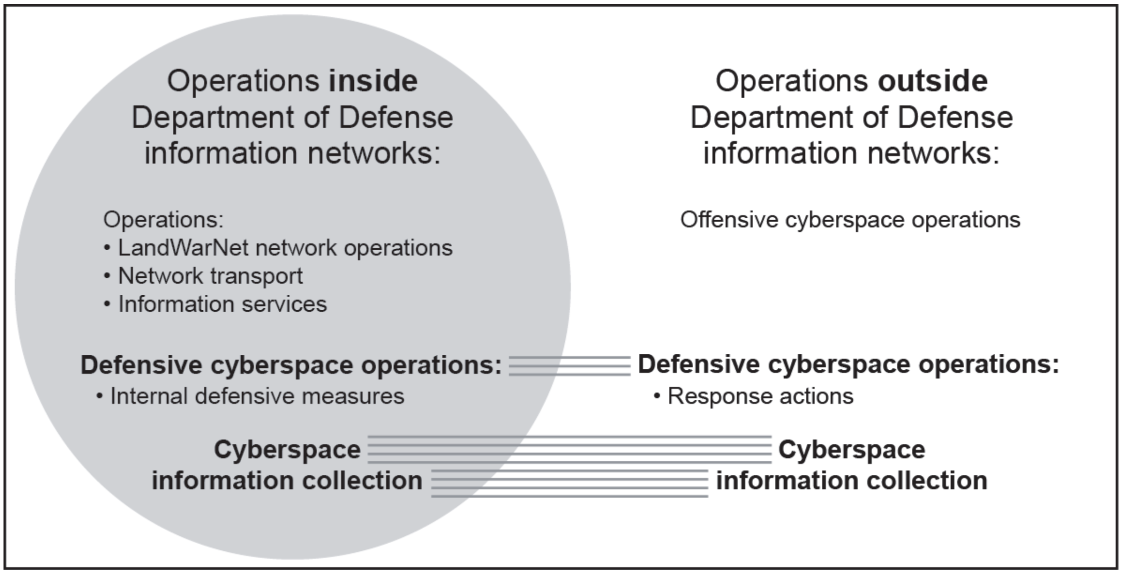

Operations inside Department of Defense information networks:
Operations:
• LandWarNet network operations
• Network transport
• Information services
Defensive cyberspace operations:
• Internal defensive measures
Cyberspace information collection
Operations outside Department of Defense information networks:
Offensive cyberspace operations
Defensive cyberspace operations:
• Response actions
Cyberspace information collection

Figure 3-3. Cyberspace operations outside and inside the networks

ENEMY AND ADVERSARY CYBERSPACE ACTIVITY

3-45. Similar to the land domain, cyberspace is used by host-nation populations, governments, security forces, businesses, and other actors. In the context of military operations, in the land domain both friendly and enemy forces strive to achieve freedom of maneuver in support of strategic, operational, and tactical objectives. In cyberspace these same forces strive to achieve freedom of action to seize, retain, and exploit strategic, operational, and tactical advantages. Therefore, enemy and adversary actors present a cyberspace threat to friendly forces in both the cyberspace and land domains.

3-46. A cyberspace threat can be characterized based on intent, sponsorship, training, education, skills, motivation, and tools. Two examples include advanced cyberspace threats and hackers. Advanced cyberspace threats are generally supported by nation-states and have advanced education, training, skills, and tools that allow these threats to remain undetected for extended periods of time on improperly defended networks. Hackers have a broad range of skills, motives, and capabilities and must be assessed independently. The level of the cyberspace threat is the combination of the actor's ability (skills and resources), opportunity (access to target), intent (attack, surveillance, exploit), and motive (national policy, war, profit, fame, personal reasons, and others). Cyberspace provides adversaries an effective and inexpensive means for recruitment, propaganda, training, and command and control. Nations and nonstate actors may use cyberspace, supporting an information campaign in combination with lethal attacks, to forward their interests.

3-47. Specific to CO, a cyberspace threat is any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in friendly force cyberspace, leading to a loss of confidentiality, integrity, or availability. Cyberspace threats not only involve an action but also require actors (enemy and adversary) to execute that action in order to exploit cyber weaknesses. For example, hackers may develop and employ malicious computer code to access and exploit the DODIN including LandWarNet. Such operations adversely affect friendly forces' use of specific portions of cyberspace in support of operations.

TARGETING IN CYBERSPACE

3-48. Targeting to create and achieve desired effects by the employment of cyberspace capabilities follows standard targeting methodologies discussed in joint and Army doctrine (see JP 3-60 and FM 3-60).

Targeting in cyberspace involves the decide, detect, deliver, and assess process. (See chapter 6 for additional information on targeting.)

3-49. Commanders and staffs consider three aspects when targeting in cyberspace. First, they recognize that cyberspace capabilities are viable options for engaging designated targets. Second, commanders and staffs understand that the employment of CO, particularly OCO, may be preferable in some cases because they can have the advantage of low probability of detection. Third, they are aware of that due to the interconnected nature of cyberspace, first order effects may intentionally or unintentionally cascade into second and third order effects, impacting deliberate planning and risk management. (See ADRP 5-0 for additional information on the operations process and risk management.)

3-50. The cyber effects request format is a format used to request effects in support of CO. The cyber effects request format contains baseline information for coordinating and integrating cyberspace capabilities and associated authorities to create effects outside and inside of the DODIN including LandWarNet. Commanders and staffs ensure cyber effects request formats are developed and submitted throughout the operations process to facilitate planning. Also, the cyber effects request format facilitates the achievement of operational and tactical objectives by leveraging the employment of cyberspace capabilities. (See FM 6-99 for additional information on developing and processing the cyber effects request format.)

Chapter 4

Electronic Warfare

This chapter provides an overview of electronic warfare (EW) as an activity integrated into operations through cyber electromagnetic activities (CEMA). It discusses the three functions of EW, their respective tasks, and considerations for employment.

4-1. EW is an activity that is integrated into operations through CEMA. EW capabilities are applied from the air, land, sea, space, and cyberspace by manned, unmanned, attended, or unattended systems. EW capabilities are an increasingly important means by which commanders can shape operational environments to their advantage. For example, electronic warfare may be used to set favorable conditions for cyberspace operations (CO) by stimulating networked sensors, denying wireless networks, or other related actions. Operations in cyberspace and the electromagnetic spectrum (EMS) depend on electronic warfare activities maintaining freedom of action in both. (See FM 3-36 for additional information on electronic warfare.)

4-2. EW consists of three functions. They are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES) (see figure 4-1 on page 4-2).

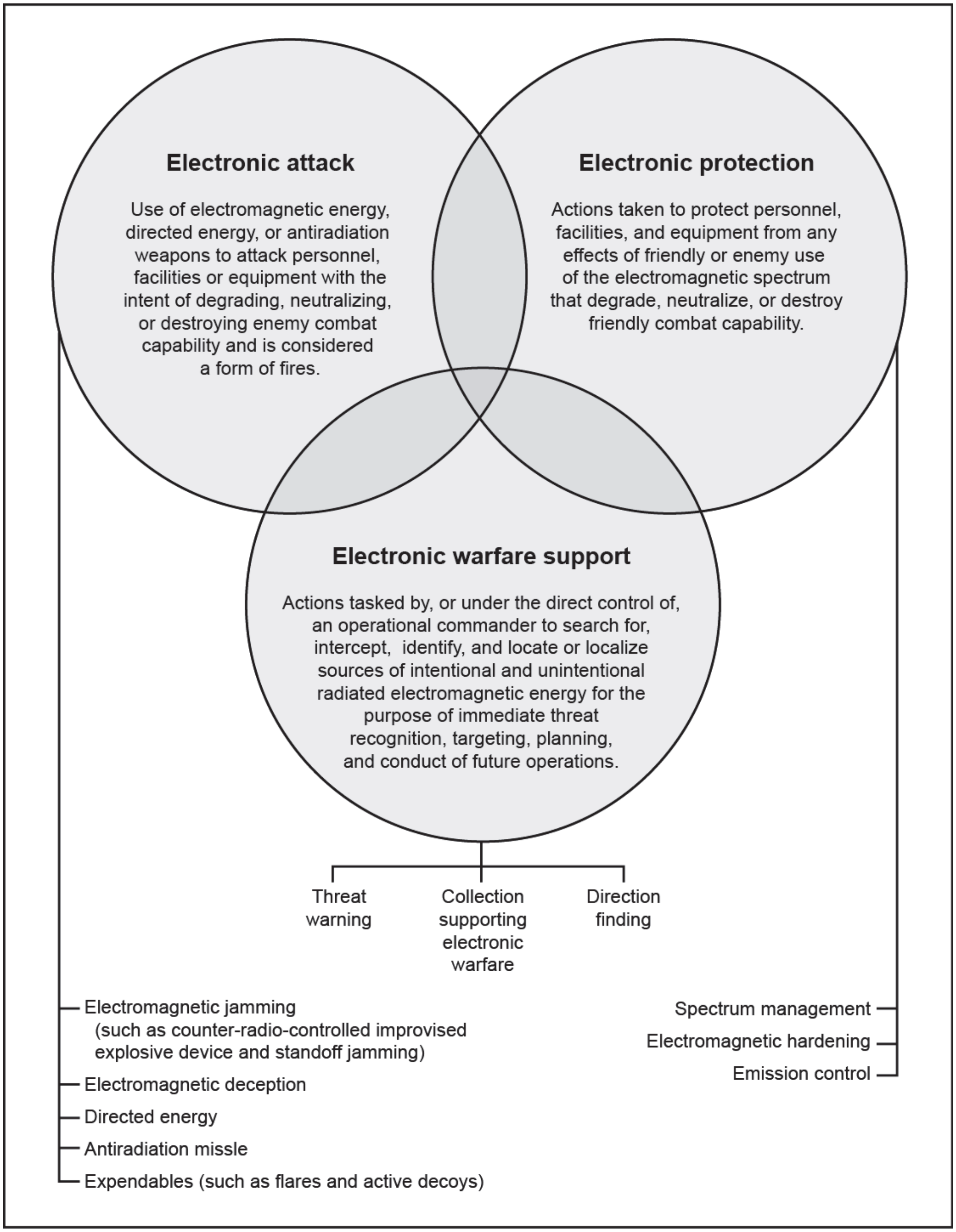

Electronic attack
Use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.
Electronic protection
Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability.
Electronic warfare support
Actions tasked by, or under the 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.
Threat warning
Collection supporting electronic warfare
Direction finding
Electromagnetic jamming (such as counter-radio-controlled improvised explosive device and standoff jamming)
Electromagnetic deception
Directed energy
Antiradiation missle
Expendables (such as flares and active decoys)
Spectrum management
Electromagnetic hardening
Emission control

Figure 4-1. The three functions of electronic warfare

ELECTRONIC ATTACK

4-3. *Electronic attack* is a division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-13.1). 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.

4-4. Actions that prevent or reduce an enemy's effective use of the EMS include spot, barrage, and sweep electromagnetic jamming. EA actions also include various electromagnetic deception techniques such as false target or duplicate target generation.

4-5. 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 directed energy primarily as a direct means to damage or destroy an enemy's equipment, facilities, and personnel. In addition to destructive effects, directed-energy weapons systems support area denial and crowd control.

4-6. Unified land operations use offensive and defensive tasks for EA. Examples of offensive EA include—

- Jamming enemy radar or electronic command and control systems.
- Using antiradiation missiles to suppress enemy air defenses (antiradiation weapons use radiated energy emitted from a target as the mechanism for guidance onto the target).
- Using electronic deception to confuse enemy intelligence, surveillance, and reconnaissance systems.
- Using directed-energy weapons to disable an enemy's equipment or capability.

4-7. 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 PROTECTION

4-8. *Electronic protection* is a division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-13.1). 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 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.

4-9. 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 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.
- Ensure that they safeguard electronic system capabilities during exercises, workups, and pre-deployment training.
- Coordinate and deconflict EMS usage.
- Provide training during routine home station planning and training activities on appropriate EP active and passive measures under normal conditions, conditions of threat electronic attack, 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 all systems is maintained and personnel are well-versed in switching between systems.

4-10. EP also includes spectrum management. The spectrum manager works for the assistant chief of staff, signal (G-6 [S-6]) and plays a key role 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.

4-11. 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 WARFARE SUPPORT

4-12. *Electronic warfare support* is a division of electronic warfare involving 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 (JP 3-13.1). ES enables U.S. forces to identify the electromagnetic vulnerability of an adversary's electronic equipment and systems. Friendly forces take advantage of these vulnerabilities through EW operations.

4-13. 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.
- Initiate self-protection measures.
- Task weapons systems.
- Support EP efforts.
- Create or update EW databases.
- Support information related capabilities.

4-14. ES and signals intelligence missions may use the same or similar resources. The two differ in the person who tasks and controls the assets, 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. (See ADRP 2-0 and FM 2-0 for more information on signals intelligence.)

TASKS AND TERMINOLOGY

4-15. Although new equipment, tactics, techniques, and procedures continue to be developed, the physics of electromagnetic energy remains constant. Hence, effective EW tasks remain the same despite changes in hardware and tactics.

PRINCIPAL TASKS

4-16. Principal EW functions support unified land operations by exploiting the opportunities and vulnerabilities inherent in the use of the EMS. The EW activity is categorized by the EW functions with which they are most closely associated (EA, EP, and ES).

Electronic Attack Tasks

4-17. Tasks related to EA are either offensive or defensive. These activities differ in their purpose. Defensive EA protects friendly personnel and equipment or platforms. Offensive EA denies, disrupts, or destroys enemy capability. Tasks related to EA include—

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

Countermeasures

4-18. *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.

4-19. *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, smokes, aerosols, signature suppressants, decoys, pyrotechnics, pyrophorics, high-energy lasers, or directed infrared energy countermeasures.

4-20. *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 missle systems are an example of radio frequency countermeasures.

Electromagnetic Deception

4-21. 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

4-22. *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

4-23. *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 that are subject to jamming include radios, radars, navigational aids, satellites, and electro-optics.

Electromagnetic Pulse

4-24. *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 Probing

4-25. *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.

Electronic Warfare Support Tasks

4-26. There are several tasks related to ES. They include—

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

Electronic Reconnaissance

4-27. *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 enemy threat characteristics information. The enemy electronic threat characteristics information is used in the planning and integrating processes.

Electronic Intelligence

4-28. *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). Examples of non-communications electromagnetic radiations include radars, surface-to-air missile systems, and aircraft.

Electronics Security

4-29. *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 electromagnetic spectrum mitigation and network protection.

Electronic Protection Tasks

4-30. There are several tasks related to EP. They include—

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

Electromagnetic Hardening

4-31. *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.

Electronic Masking

4-32. *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/signals intelligence without significantly degrading the operation of friendly systems (JP 3-13.1).

Emission Control

4-33. *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.

Electromagnetic Spectrum Management

4-34. *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.

Wartime Reserve Modes

4-35. *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, if ever, applied or intercepted prior to such use.

Electromagnetic Compatibility

4-36. *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 electromagnetic spectrum management; system, equipment, and device design configuration that ensures interference-free operation. It also involves clear concepts and doctrines that maximize operational effectiveness.

ELECTROMAGNETIC INTERFERENCE

4-37. *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 electronic warfare, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and other similar products. Once electromagnetic interference is identified, a joint spectrum interference report is initiated and forwarded through spectrum manager channels.

ELECTRONIC WARFARE REPROGRAMMING

4-38. *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, adversary, or third parties; or they may be brought about by electromagnetic interference or other inadvertent phenomena. The purpose of electronic warfare reprogramming is to maintain or enhance the effectiveness of electronic warfare and target sensing system equipment. Electronic warfare reprogramming includes changes to self defense systems, offensive weapons systems, ES, and intelligence collection systems. The key consideration for EW reprogramming is joint and multinational coordination. Joint and multinational coordination of service reprogramming efforts ensures all friendly forces consistently identify, process, and implement reprogramming requirements. (For more information on EW reprogramming, see ATTP 3-13.10.)

EMPLOYMENT CONSIDERATIONS

4-39. EW has specific ground-based, airborne, and functional (EA, EP, or ES) employment considerations. The electronic warfare officer (EWO) properly articulates EW employment considerations early in the operations process. Each employment consideration has certain advantages and disadvantages that commanders and staffs weigh when planning operations. Staffs plan for EA, EP, and ES before executing EW operations.

Electronic Attack Considerations

4-40. There are several considerations are involved in planning for employing EA. They include—

- Friendly communications.
- Intelligence collection.
- Other effects.
- Non-hostile local EMS use.
- Hostile intelligence collection.
- Persistency of effect.

4-41. The electronic warfare officer (EWO), the assistant chief of staff, intelligence (G-2 [S-2]), the assistant chief of staff, operations (G-3 [S-3]), the G-6 (S-6), the spectrum manager, and the assistant chief of staff, inform and influence activities (G-7 [S-7]) coordinate closely to ensure effects produced by electronic warfare operations are properly coordinated and integrated with other users of the EMS in the operational environment. Coordination and integration ensures that EA systems' frequencies are employed to maximize synergies with other EMS dependent systems and to eliminate, moderate, or mitigate potential electromagnetic interference on friendly systems. Conducting proper coordination and integration of EMS dependent systems results in friendly EMS control while denying EMS control to the adversary and enemy.

4-42. The number of information systems, EW systems, and sensors operating simultaneously on the battlefield makes deconfliction with communications and other EMS dependent 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.

4-43. If not properly coordinated with the G-2 (S-2) staff, EA operations may interrupt intelligence collection by jamming or inadvertently interfering with a particular frequency being used to collect data on the threat or by jamming a given enemy frequency or system that deprives friendly forces of that means of collecting data. Either interruption can significantly deter intelligence collection efforts and their ability to answer critical information requirements. Conversely, signals intelligence collectors need to be aware that CEMA elements are charged with controlling the EMS and that this can take precedence over collections. Coordination between the EWO, the fire support coordinator, and the G-2 (S-2) mitigates this interference. In situations where a known conflict between the intelligence collection effort and the use of EA exists, the CEMA working group brings the problem to the G-3 (S-3) for resolution.

4-44. Planners need to consider other effects that rely on EMS when planning for EA. For example, military information support operations may include plans to use certain frequencies to broadcast messages, or a military deception plan may include the broadcast of friendly force communications. In both examples, the use of EA could unintentionally interfere or disrupt such broadcasts if not properly coordinated. To ensure EA does not negatively impact planned operations, the EWO coordinates between fires, network operations, and other functional or integrating cells as required.

4-45. Like any other form of electromagnetic radiation, EA can adversely affect local media and communications systems and infrastructure. EW planners consider unintended consequences of EW operations and deconflict these operations with the various functional or integrating cells. For example, friendly jamming could deny the functioning of essential services such as ambulance or firefighters to a local population. EWOs routinely synchronize EA with the other functional or integrating cells responsible for information related capabilities. In this way, they ensure that EA efforts do not cause fratricide or unacceptable collateral damage to their intended effects.

4-46. The potential for hostile intelligence collection also affects EA. A well-equipped enemy can detect friendly EW activities 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 adversaries and others [JP 2-0].)

4-47. The effects of jamming only persist as long as the jammer itself is emitting and is in range to affect the target. Normally these effects last a matter of seconds or minutes, which makes the timing of such missions critical. This is particularly true when units use jamming in direct support of aviation platforms. For example, in a mission that supports suppression of enemy air defense, the time on target and duration of the jamming must account for the speed of attack of the aviation platform. They must also account for the potential reaction time of enemy air defensive countermeasures. The development of directed-energy weapons may change this dynamic in the future. However, at present (aside from antiradiation missiles), the effects of jamming are less persistent than effects achieved by other means.

Electronic Protection Considerations

4-48. Electronic protection is achieved through physical security, communications security measures, system technical capabilities (such as frequency hopping and shielding of electronics), spectrum management, redundancy of systems, and emission control procedures. Planning for EP operations have the following considerations:

- Vulnerability analysis and assessment.
- Monitoring and feedback.
- Electronic protection measures and their effects on friendly capabilities.

Vulnerability Analysis and Assessment

4-49. Vulnerability analysis and assessment forms the basis for formulating EP plans. The Defense Information Systems Agency operates the vulnerability analysis and assessment program, which specifically focuses on automated information systems and can be useful in this effort.

Monitoring and Feedback

4-50. The National Security Agency monitors communications security. The National Security Agency's programs focus on telecommunications systems using wire and electronic communications, and it has programs that can support and remediate a command's communications security procedures when required.

Electronic Protection Measures and Their Effects on Friendly Capabilities

4-51. Electronic protection measures include any measure taken to protect the force from hostile EA actions. However, these measures can also limit friendly capabilities or operations. For example, denying frequency usage to counter radio-controlled-improvised-explosive-device EW systems on a specific 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

4-52. Operational commanders task assets to conduct ES for the purpose of immediate threat recognition, targeting, planning the conduct of future operations, and other tactical actions (such as threat avoidance and homing). The EWO coordinates with the G-2 (S-2) to ensure they identify all ES needed for planned EW operations and submit that needed support to the G-3 (S-3) for approval by the commander. This ensures that the required collection assets are properly tasked to provide the ES. In cases where planned 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 work-ups.

Chapter 5

Spectrum Management Operations

This chapter describes spectrum management operations (SMO). It lists and briefly discusses the four functions of SMO. Finally, it provides tasks conducted by the spectrum manager.

ELECTROMAGNETIC SPECTRUM OPERATIONS

5-1. Electromagnetic spectrum operations (EMSO) are comprised of electronic warfare (EW) and SMO. The importance of the electromagnetic spectrum (EMS) and its relationship to the operational capabilities of the Army is the focus of EMSO.

5-2. EMSO include all activities in military operations to successfully control the EMS. Figure 5-1 illustrates EMSO and how they relate to SMO and EW.

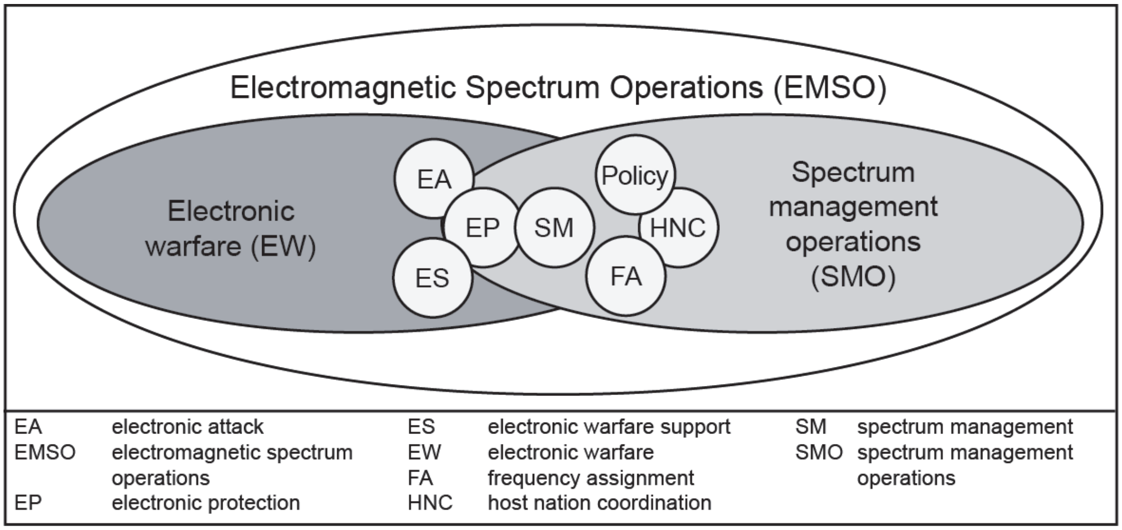

Electromagnetic Spectrum Operations (EMSO)
Electronic warfare (EW)
Spectrum management operations (SMO)
EA
EP
ES
SM
Policy
HNC
FA
EA electronic attack
EMSO electromagnetic spectrum operations
EP electronic protection
ES electronic warfare support
EW electronic warfare
FA frequency assignment
HNC host nation coordination
SM spectrum management
SMO spectrum management operations

Figure 5-1. Electromagnetic spectrum operations

SPECTRUM MANAGEMENT OPERATIONS FUNCTIONS

5-3. 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.

5-4. The conduct of SMO enables and supports the execution of cyberspace operations (CO) and EW. SMO are also critical to all other spectrum dependent devices, including air defense radars, navigation, sensors, EMS using munitions, manned and unmanned systems of all types (ground and air, radar, sensor), and a host of other future systems that will 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.

5-5. The planning and coordinating of SMO is a responsibility of the assistant chief of staff, signal (G-6 [S-6]). SMO are normally performed by trained electromagnetic 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. To maximize use of the EMS, coordination between EW, the assistant chief of staff, operations (G-3 [S-3]), network operations, the assistant chief of staff, intelligence (G-2 [S-2]), and other known users is required.

5-6. Understanding the SMO process in planning, managing, and employing EMS resources is a critical function within cyber electromagnetic activities (CEMA) to the conduct of operations. SMO provides the resources necessary for the implementation of the wireless portion of net-centric warfare (see FM 6-02.70). SMO are comprised of four inter-related core capabilities: Spectrum management, frequency assignment, host-nation coordination, and policy implementation.

SPECTRUM MANAGEMENT

5-7. Spectrum management consists of evaluating and mitigating electromagnetic environmental effects, managing frequency records and databases, deconflicting frequencies, frequency interference resolution, allotting frequencies, and EW coordination. Spectrum management ensures electromagnetic dependent systems operate as intended.

5-8. The objective of Army spectrum management is to ensure access to the frequency spectrum in order to support users conducting the Army's operational mission. Spectrum management enables the allotment of the vital, but limited, natural resources that directly support operational forces throughout the world. The Army is dependent upon the radio spectrum to communicate from the strategic to the tactical levels of war to carry out its responsibilities for national security. Spectrum management enables electronic systems, including networks that leverage the spectrum, to perform their functions in the intended environment without causing or suffering unacceptable interference.

FREQUENCY ASSIGNMENT

5-9. The frequency assignment function of SMO entails requesting and issuing authorizations to use frequencies for specific equipment. Examples of frequency assignment include providing the frequencies for combat net radio network, unmanned aerial systems, or line of sight network.

HOST-NATION COORDINATION

5-10. A *host nation* is a nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory (JP 3-57). Each nation has the sovereign right to manage the use of the EMS within its borders. Unlike the United States (U.S.), most nations have a single agency responsible for spectrum management. For many of these nations that office will be with the ministry of communications or some similar agency. In nations where the Army has established posts, camps, or stations there will normally be a liaison with the ministry established through which the spectrum manager negotiates for spectrum support.

5-11. There is no standard format or process for negotiating spectrum usage with individual nations and spectrum managers should become familiar with respective formats and processes for each nation with which they interact. Spectrum managers should also be familiar with host-nation radio service allocations and channeling plans. A useful tool to assist the spectrum manager in determining whether or not a piece of equipment may be supportable in a given region is the host-nation spectrum worldwide database. The host-nation spectrum worldwide database is a portal based tool located on the SECRET Internet Protocol Router Network (SIPRNET). The host-nation spectrum worldwide database automates the distribution of host-nation coordination requests and combatant command submission of host-nation supportability comments (data).

POLICY ADHERENCE

5-12. It is critical that all levels of command understand the inherent risk of violating the rules of proper spectrum management. Generally, a radio signal is all that connects a Soldier, platoon, or company to safety, by providing awareness or communications. Emitters that are turned on in a geographic area of operations without the proper clearance and certification have the same effect as “bootlegging” a frequency. The term bootlegging in reference to spectrum resources is considered the unauthorized use of frequencies to provide communication support. In the past, “bootlegging” a frequency usually only affected the communications network. Today, this practice can have first, second, or third order effects on other systems that are undesirable. Some of the effects of these actions have included the damaging of multi-million dollar unmanned aerial systems, lack of communications between elements during critical situations, and interference with safety of life frequencies (frequencies used for medical evacuation and search and rescue).

5-13. Commanders should be informed of any equipment that does not have spectrum supportability and the implications or consequences of employing such equipment. Spectrum managers must also be particularly aware of equipment that potentially interferes with safety of life systems such as search and rescue, medical, or air operations systems.

SPECTRUM MANAGEMENT OPERATIONS TASKS

5-14. The tasks necessary to accomplish these functions are generally the same across higher and lower echelons. The difference is the size and scope of the tasks. For example, developing a corps signal operating instructions is a much larger task than developing a signal operating instructions for a brigade, even though the same process and tool are used to create both signal operating instructions. The SMO tasks are staff coordination, EW coordination, joint restricted frequency list coordination, communications security coordination, satellite coordination, frequency deconfliction, and frequency interference resolution.

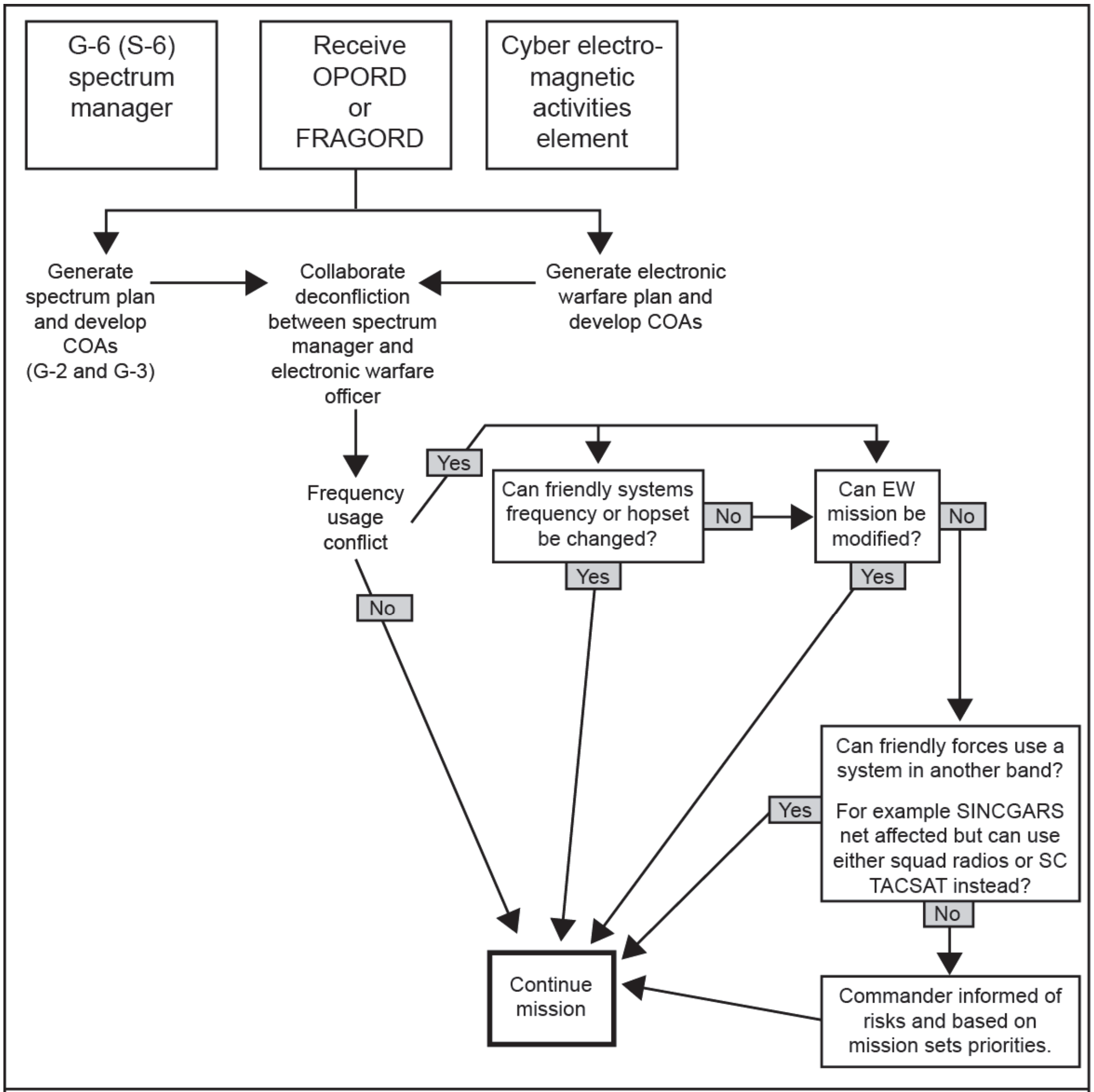
STAFF COORDINATION

5-15. Spectrum managers work with many systems that are not solely communications systems. They must be involved with other staff members to provide guidance and advice to the commander regarding the use and prioritization of the EMS. Systems such as unmanned aerial systems, common user jammers, radars, navigational aids, and sensors all use the EMS for operation. Their widespread use and unique operating characteristics require special planning and coordination to mitigate frequency fratricide.

5-16. The spectrum manager must be engaged with the appropriate staffs or liaisons for these systems to ensure that spectrum support is available. Many of these systems, particularly radars, operate on fixed frequencies and, depending on proximity to other systems, they may induce harmful interference unless proper coordination takes place.

5-17. The spectrum manager should be knowledgeable on the spectrum requirements of all spectrum dependent devices. Most spectrum dependent devices are operator owned and maintained. Many of these systems, such as high frequency automatic link establishment, airborne systems, and tactical satellite systems, have their own communications planning software necessary to configure the systems for operation. It is the unit’s or operator’s responsibility to configure these systems for operations. For example, the spectrum manager provides the frequencies for a high frequency automatic link establishment radio, but it is the unit’s responsibility to configure and operate the radio.

Note: The single channel ground and airborne radio system is an exception due to a legacy requirement for communications planning for these radios.


G-6 (S-6) spectrum manager
Receive OPORD or FRAGORD
Cyber electro-magnetic activities element
Generate spectrum plan and develop COAs (G-2 and G-3)
Collaborate deconfliction between spectrum manager and electronic warfare officer
Generate electronic warfare plan and develop COAs
Frequency usage conflict
Yes
No
Can friendly systems frequency or hopset be changed?
No
Yes
Can EW mission be modified?
No
Yes
Can friendly forces use a system in another band?
For example SINCGARS net affected but can use either squad radios or SC TACSAT instead?
Yes
No
Continue mission
Commander informed of risks and based on mission sets priorities.

COA	course of action	G-6 (S-6)	assistant chief of staff, signal
EW	electronic warfare	OPORD	operations order
FRAGORD	fragmentary order	SC TACSAT	single channel tactical satellite
G-2 (S-2)	assistant chief of staff, intelligence	SINCGARS	single-channel ground and airborne radio system
G-3 (S-3)	assistant chief of staff, operations		

Figure 5-2. The spectrum management operations and electronic warfare deconfliction process

ELECTRONIC WARFARE COORDINATION

5-18. The spectrum manager should be an integral part of all EW planning in order to be aware of spectrum conflicts initiated by friendly systems for personnel protection, enemy exploitation, or enemy denial. 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 take place in the CEMA element. It may take place in the EW cell if it is operating under a joint construct or operating at a special echelon. (See figure 5-2 for SMO and EW deconfliction process.)

5-19. Although in some respects the functions of the electronic warfare officer (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 threat focused and works to protect the EMS for friendly forces while denying the enemy use of the EMS. Commanders and staffs must realize this distinction and avoid relying on one person or cell to manage both functions.

JOINT RESTRICTED FREQUENCY LIST

5-20. A joint restricted frequency list is normally a corps or theater product. The spectrum manager must work closely with the G-2, G-3, and the EWO to coordinate publication of the joint restricted frequency list. To make this product useful, the spectrum manager should work to keep it as current and brief as possible. A restricted frequency list may be developed and published at lower levels, depending upon need and mission.

COMMUNICATIONS SECURITY COORDINATION

5-21. The spectrum manager must work closely with communications security personnel to ensure that the proper keying material is matched to the appropriate frequency resource for single channel ground and airborne radio systems loadsets. Spectrum managers are concerned only with the necessary communications security for single channel ground and airborne radio systems loadsets and do not handle or manage communications security for other emitters.

SATELLITE COORDINATION

5-22. The spectrum manager coordinates with satellite managers to maintain awareness of channels (frequencies) being used by satellite communications systems. The satellite manager generates and processes satellite access requests for all very high frequency (VHF), ultra high frequency (UHF), super high frequency (SHF), and extremely high frequency (EHF) satellite systems. Once a request is approved, the spectrum manager enters the frequencies into the database in order to do frequency deconfliction with all other emitters in the area of operations.

FREQUENCY DECONFLICTION

5-23. *Frequency deconfliction* is a systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management (JP 3-13.1). The limitations of today’s spectrum management tools make it impossible for the spectrum manager to keep a real-time database of frequency use. This is due to the highly dynamic nature of tactical operations and the inability of the tools to do real-time updates automatically. In fast-paced operations the spectrum manager will mainly be concerned with interference resolution or deconfliction by exception.

FREQUENCY INTERFERENCE RESOLUTION

5-24. 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* 714-5.)

5-25. 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.

5-26. 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 are 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, the operator makes an internal equipment check 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.

5-27. 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 in accordance with CJCSM 3320.02D.

Chapter 6

The Operations Process

This chapter discusses cyber electromagnetic activities (CEMA) in the operations process of unified land operations. Specifically, it discusses planning, preparing, executing, and assessing CEMA.

THE OPERATIONS PROCESS AND CYBER ELECTROMAGNETIC ACTIVITIES

6-1. CEMA are integrated through the operations process. Figure 6-1 is a depiction of the operations process. CEMA are planned, prepared for, executed, and assessed as part of all Army operations. (See ADP 5-0, ADRP 5-0, and ATTP 5-01.1 for more information on the operations process.)

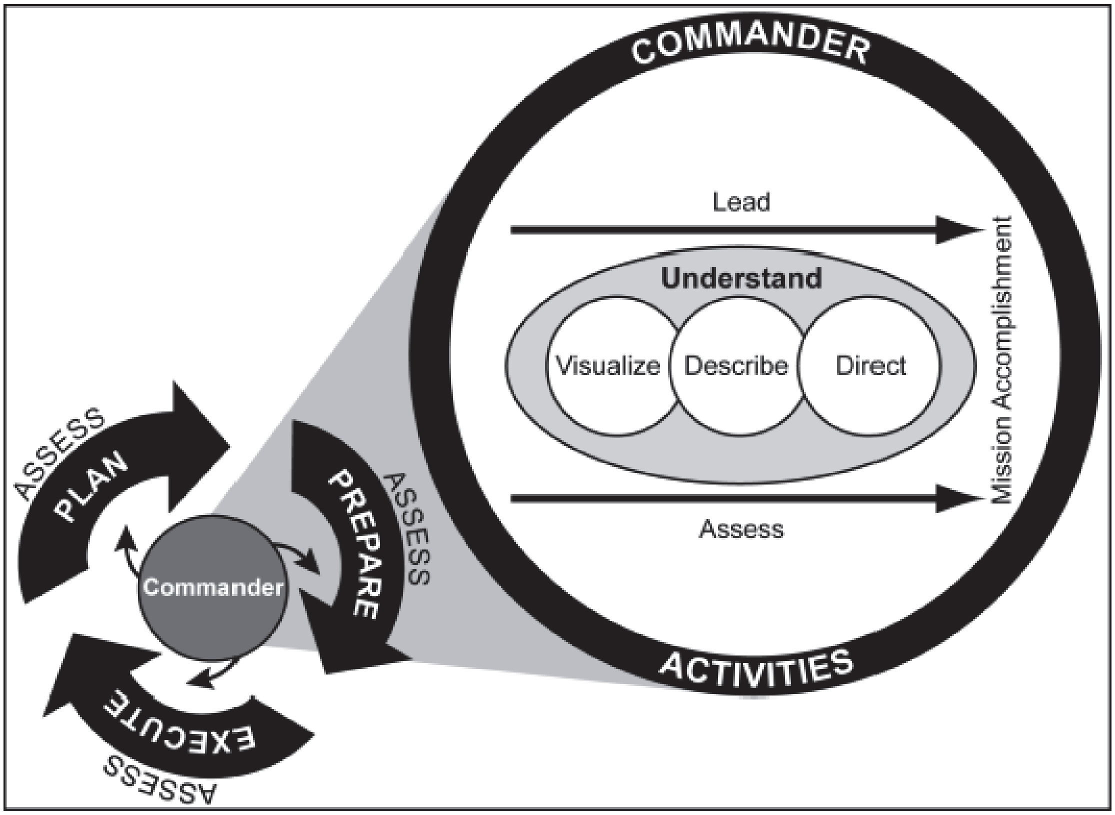


Figure 6-1. The operations process

CYBER ELECTROMAGNETIC ACTIVITIES IN PLANNING

6-2. CEMA involve unique planning considerations. These considerations include—

- Planning with interagency partners, other nations, and non-government organizations requires close coordination, as these unified action partners may have authorities greater than or different from the Army.
- Understanding that possible second and third order effects in and through cyberspace and the electromagnetic spectrum (EMS) can be difficult to predict. These unintended effects manifest during the execution stage of operations. This does not preclude the possibility of their occurrence from being incorporated into the planning.
- Planning based on the physical elements of cyberspace and the EMS mapped out geographically in the traditional domains is insufficient.
- Understanding that the effects of cyberspace operations (CO) and electronic warfare (EW) can take place almost instantaneously. This does not preclude these activities from moving through the entirety of the operations process. In a time-constrained environment, the staff might not be able to conduct a detailed military decisionmaking process. The process may be abbreviated, but all seven steps will be accomplished.
- Understanding that CEMA provide the commander with lethal and nonlethal actions. Choosing a specific capability depends on the desired effect on the target and other considerations, such as time sensitivity or limiting collateral damage. A desired outcome, such as assured information protection or disruption of adversary communications systems, can also influence capability choice.
- Anticipating a protracted period between initial request for application of an effect and execution. Even if pre-approved at the national level, significant time may be required to develop tools, establish target access, and return a battle damage assessment.
- Understanding that CEMA involve significant legal and policy constraints.

Military Decisionmaking Process

6-3. CEMA are integrated into plans and orders through the military decisionmaking process. (For more information on the military decisionmaking process, see ADP 5.0, ADRP 5-0, ATTP 5-0.1, and FM 6-02.71.)

Receipt of Mission

6-4. During the receipt of mission, the CEMA element participates in the commander's initial assessment actions and gathers the resources required for mission analysis. Unique to CEMA, part of the initial assessment determines whether resources can be brought to bear on the mission at hand within a reasonable timeframe or context through the reachback and support processes. (See table 6-1.)

Table 6-1. The military decisionmaking process, step 1: receipt of mission

Inputs	*CEMA Element Actions*	*CEMA Element Outputs*
• Higher headquarters' plan or order or a new mission anticipated by the commander. • All documents related to the mission and area of operations. • Additional intelligence and assessment products (assessment of operational variables including political, military, economic, social, information, infrastructure, physical, and time). • Existing CEMA running estimates.	• Begin updating the CEMA running estimate, especially the status of friendly units and resources and key civil considerations. • Determine and contact outside agencies and organizations included in the planning process. • Provide CEMA input to the development of the staff planning timeline. • Provide CEMA input during formulation of the commander's initial guidance. • Provide CEMA input to the initial warning order.	• Updated CEMA running estimate. • CEMA input to initial intelligence preparation of the battlefield and information collection taskings.
CEMA - cyber electromagnetic activities		

Mission Analysis

6-5. The CEMA element contributes to mission analysis in order to help commanders understand the operational environment and frame the problem. An effective mission analysis considers the potential impact cyberspace and the EMS on an operational environment. The CEMA element does this by participating in planning actions that help form the problem statement, mission statement, commander’s intent, planning guidance, initial commander’s critical information requirements, essential elements of friendly information, and updated running estimates. This analysis is conducted from the separate perspectives of CO and EW, taking note where the two activities converge. The CEMA element coordinates with the assistant chief of staff, intelligence (G-2 [S-2]), assistant chief of staff, operations (G-3 [S-3]), assistant chief of staff, signal (G-6 [S-6]), and other staff elements in reference to mission critical systems, risk assessments, current defense posture, and overall operational requirements. When utilized as an information-related capability the CEMA element works closely with the assistant chief of staff, inform and influence activities (G-7 [S-7]) to identify the desired effects for the information environment.

6-6. The CEMA element further contributes to overall mission analysis by participating in the intelligence preparation of the battlefield and closely coordinates with the G-2 (S-2) by providing information, advice, and assistance. This ensures the G-2 (S-2) understands what CEMA products are needed in order for the G-2(S-2) to tailor intelligence preparation of the battlefield products. Threats and vulnerabilities are identified in accordance with adversary offensive cyberspace capabilities, EW capabilities, or both. A friendly center of gravity analysis is conducted to ensure thorough planning. A key portion of this analysis is to assess the potential impact of CEMA on friendly assets. For example, increasing security in cyberspace or deploying additional tools to analyze networks can cause slower network operational speeds.

6-7. The CEMA element then analyzes the commander’s intent and mission from a CEMA perspective and determines if forces have sufficient assets to perform the identified tasks for all three activities within the CEMA construct. If organic assets are insufficient, the CEMA element drafts requests for support and augmentation. If offensive cyberspace operations (OCO) are to be conducted a cyberspace support element may be required to support the CEMA element. By the conclusion of the mission analysis, the CEMA element generates or gathers the products and information listed in table 6-2 on page 6-4.

Table 6-2. The military decisionmaking process, step 2: mission analysis

Inputs	***CEMA Element Actions***	***CEMA Element Outputs***
• Commander's initial guidance. • Higher headquarters' plan or order. • Higher headquarters' rules of engagement (specific to cyberspace operations and electronic warfare). • Higher headquarters' intelligence and knowledge products. • Knowledge products from other organizations. • Army design methodology products.	• Analyze the higher headquarters' plan or order and develop requests for information as needed. • Collaborate with the intelligence staff to perform initial intelligence preparation of the battlefield. • Develop cyber and electronic warfare threat (for example, enemy, adversary, and neutral) characteristics. • Identify and analyze key threat networks, capabilities, and use of cyberspace and the electromagnetic spectrum. • Determine CEMA-related high-value targets. • Identify CEMA-related specified and implied tasks. • Determine CEMA-related limitations and constraints. • Identify CEMA-related critical facts and assumptions. • Identify gaps in standing rules of engagement specific to cyberspace operations and electronic warfare. • Conduct initial assessment of spectrum requirements and supportability including spectrum dependent devices. • Coordinate with higher headquarters and the host-nation government to develop initial spectrum plan. • Identify and nominate CEMA-related commander's critical information requirements. • Identify and nominate CEMA-related essential elements of friendly information. • Provide CEMA input to the development of: - The information collection plan. - Initial themes and messages. - Proposed problem statement. - Proposed mission statement. - The mission analysis brief. - The commander's initial intent. - The commander's initial planning guidance. • Participate in the mission analysis brief as required. • Provide CEMA input to the warning order.	• List of CEMA-related requests for information. • CEMA specified and implied tasks. • Specified targets from higher headquarters' plan or order requiring effects by cyberspace operations or electronic warfare means. • Request for CEMA-related capabilities and resources. • List of CEMA-related assumptions. • Requests to modify standing rules of engagement specific to cyberspace operations and electronic warfare. • List of CEMA-related essential elements of friendly information. • CEMA portion of the mission analysis brief. • Updated CEMA running estimate including: - Maps. - Overlays. - Network infrastructure diagrams and charts. - List of high-value targets for potential offensive and defensive cyberspace operations or electronic warfare effects. - Updated assessment of operational variables including political, military, economic, social, information, infrastructure, physical, and time.
CEMA - cyber electromagnetic activities		

Course of Action Development

6-8. The CEMA element members contribute to course of action (COA) development by determining possible friendly and enemy operations and which friendly CO and EW capabilities are available to support the operations. The CEMA element focuses planning efforts on achieving an operational advantage at the decision point of each COA. By the conclusion of the COA development, the CEMA element generates a list of CEMA objectives and desired effects. It also generates a list of capabilities, information, and intelligence required to perform the tasks for each COA (see table 6-3).

Table 6-3. The military decisionmaking process, step 3: COA development

Inputs	*CEMA Element Actions*	*CEMA Element Outputs*
• Mission statement. • Initial commander's intent. • Initial commander's planning guidance. • Initial commander's critical information requirements. • Initial essential elements of friendly information. • Updated intelligence preparation of the battlefield. • CEMA specified and implied tasks. • List of high-value targets that may require effects by cyberspace operations or electronic warfare means. • Updated CEMA running estimate. • List of CEMA-related assumptions.	• Provide CEMA input to the assessment of relative combat power. • Identify vulnerabilities of friendly, enemy, adversary, and neutral actors. • Provide CEMA input to the development of options for decisive, shaping, and sustaining operations. • Provide CEMA input to the development of military deception courses of action. • Develop initial scheme of CEMA for each course of action. • Develop CEMA statements and sketches for each course of action. • Analyze high-value targets and develop list of tentative high-payoff targets for offensive and defensive cyberspace operations or electronic warfare effects. • Begin cyber effects request formats. • Begin electronic attack request formats. • Begin evaluation request messages. • Develop primary, alternate, contingency, and emergency communications plan for each course of action. • Develop CEMA input for the fire support plan. • Develop CEMA input for the operations execution matrix. • Provide CEMA input and participate in the course of action development brief as required.	• For each course of action developed include: - Draft CEMA concept of operations with tasks. - Draft CEMA input to high-payoff target list. - Draft CEMA input to target information folders. - Draft CEMA input to target synchronization matrix. - Draft maps and overlays. - Draft network infrastructure diagrams and charts. - Draft spectrum plan including the joint restricted frequency list. • Updated CEMA running estimate including assumptions. • Draft Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations). • Draft Appendix 6 (Spectrum Management Operations) to Annex H (Signal).
CEMA - cyber electromagnetic activities		

Course of Action Analysis

6-9. During COA analysis the CEMA element plans and coordinates with each of the warfighting function staff members to integrate and synchronize CO and EW capabilities into each COA, thereby identifying which COA best accomplishes the mission. The CEMA element addresses how CO and EW capabilities support each COA and applies them to timelines, critical events, and decision points (see table 6-4 on page 6-6).

Table 6-4. The military decisionmaking process, step 4: COA analysis

Inputs	*CEMA Element Actions*	*CEMA Element Outputs*
• Updated CEMA running estimate including assumptions. • Revised planning guidance specific to CEMA. • Consolidated course of action statements and sketches. • Draft Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations). • Draft Appendix 6 (Spectrum Management Operations) to Annex H (Signal).	• In collaboration with the staff, war-game enemy and adversary cyber and electronic warfare capabilities against friendly capabilities and vulnerabilities for each course of action. • Integrate and synchronize CEMA into the concept of operations for each course of action. • Develop and complete the war-game synchronization matrix tool from a CEMA perspective. • Identify and record strengths and weaknesses associated with each course of action from a CEMA perspective. • Integrate and synchronize CEMA into the fire support plan for each course of action. • Integrate and synchronize CEMA in support of military deception courses of action. • Provide input for the development of the decision support matrix and decision support template. • Provide input to CEMA-related operation order appendices and tabs. • Provide CEMA input and participate in the war-game briefing as required.	• For each course of action war-gamed include: - Refined CEMA input to the concept of operations with tasks. - Refined CEMA-related information requirements. - Refined CEMA-related essential elements of friendly information. - Refined CEMA input to high-payoff target list. - Refined CEMA input to target information folders. - Refined CEMA input to target synchronization matrix. - Refined maps and overlays. - Refined network infrastructure diagrams and charts. - Refined spectrum plan including the joint restricted frequency list. - Refined draft cyber effects request formats. - Refined draft electronic attack request formats. - Refined draft evaluation request messages. • Refined draft Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations). • Refined draft Appendix 6 (Spectrum Management Operations) to Annex H (Signal).
CEMA - cyber electromagnetic activities		

Course of Action Comparison

6-10. During COA comparison all staff members evaluate the advantages and disadvantages of each COA from their perspectives. The CEMA element lead presents the CEMA's element's findings for the others' consideration. At the conclusion of the COA comparison, the CEMA element generates a list of pros and cons for each COA relative to CEMA. The CEMA element also develops a prioritized list of the COAs from a CEMA perspective (see table 6-5).

Table 6-5. The military decisionmaking process, step 5: COA comparison

Inputs	*CEMA Element Actions*	*CEMA Element Outputs*
• Updated CEMA running estimate including assumptions. • Refined courses of action. • Evaluation criteria. • War-game results.	• In collaboration with the staff, conduct an analysis of advantages and disadvantages for each course of action, emphasizing CEMA aspects. • Provide input to the decision matrix tool as required. • Recommend for the most supportable course of action from a CEMA perspective. • Provide CEMA input and participate in the course of action decision briefing as required.	• For each course of action include final draft: - CEMA input to the concept of operations with tasks. - CEMA-related information requirements. - CEMA-related essential elements of friendly information. - CEMA input to high-payoff target list. - CEMA input to target information folders. - CEMA input to target synchronization matrix. - Maps and overlays. - Network infrastructure diagrams and charts. - Spectrum plan including the joint restricted frequency list. - Cyber effects request formats. - Electronic attack request formats. - Evaluation request messages.
CEMA - cyber electromagnetic activities		

Course of Action Approval

6-11. The CEMA staff officer attends the COA decision briefing to help finalize the commander’s intent based on the COA selected. The commander’s final guidance provides the CEMA element the commander’s intent, any new critical information requirements, risk acceptance, and guidance on the priorities for the elements of combat power, orders preparation, rehearsal, and preparation. The output from the CEMA element is a finalized CEMA execution matrix (see table 6-6 on page 6-8).

Table 6-6. The military decisionmaking process, step 6: COA approval

Inputs	*CEMA Element Actions*	*CEMA Element Outputs*
• Updated CEMA running estimate including assumptions. • Evaluated courses of action. • Recommended course of action.	• Receive and respond to final planning guidance from the commander. • Assess implications and take actions to finalize CEMA element outputs. • Provide CEMA input to the warning order.	• For the approved course of action include refined: - CEMA input to the concept of operations. - CEMA tasks. - CEMA-related information requirements. - CEMA-related essential elements of friendly information. - CEMA input to high-payoff target list. - CEMA input to target information folders. - CEMA input to target synchronization matrix. - Maps and overlays. - Network infrastructure diagrams and charts. - Spectrum plan including the joint restricted frequency list. - Cyber effects request formats. - Electronic attack request formats. - Evaluation request messages.
CEMA - cyber electromagnetic activities		

Orders Production, Dissemination, and Transition

6-12. The CEMA element provides the appropriate input for several sections of the operation order or plan and associated annexes or appendixes as required. This may include input to other functional area annexes such as intelligence, fire support, signal, and civil affairs operations as required (see table 6-7).

Table 6-7. The military decisionmaking process, step 7: orders production, dissemination, and transition

Inputs	*CEMA Element Actions*	*CEMA Element Outputs*
• Commander approved course of action and any modifications. • Refined commander's intent. • Refined commander's critical information requirements. • Refined essential elements of friendly information. • Updated CEMA running estimate including assumptions. • Refined draft Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations). • Refined draft Appendix 6 (Spectrum Management Operations) to Annex H (Signal).	• Conduct a more detailed war game of the selected course of action as required. • Participate in the staff plans and orders reconciliation as required. • Participate in the staff plans and orders crosswalk as required. • Finalize cyber effects request formats. • Finalize electronic attack request formats. • Finalize evaluation request messages. • Finalize input to CEMA-related operation order appendices and tabs. • Provide CEMA input and participate in the operations order brief. • Provide CEMA input and participate in confirmation briefings as required.	• Final Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations). • Final CEMA input to Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal). • Final CEMA input to Appendix 2 (Information Network Operations) to Annex H (Signal). • Final Appendix 6 (Spectrum Management Operations) to Annex H (Signal). • Final CEMA input to Appendix 2 (Military Deception) to Annex J (Inform and Influence Activities).
CEMA - cyber electromagnetic activities		

CYBER ELECTROMAGNETIC ACTIVITIES IN PREPARATION

6-13. The CEMA element participates in the preparation phase of the operations process in order to create conditions in cyberspace and the EMS that improve friendly forces' opportunities for success throughout all domains.

6-14. Many effects of CEMA require considerable legal and policy review. This often creates lengthy lead times during the planning and preparation phases, even though the effects may occur nearly instantaneously once executed. Initial preparations for many operations specific to cyberspace begin during peacetime, although execution of operations occurs during a time of war. EW operations are generally conducted under the authority of the tactical commander, subject to higher level rules of engagement and the laws of armed conflict. Operations against targets in cyberspace are generally conducted under national or combatant commander authority, subject to higher level rules of engagement and the laws of armed conflict. Tactical level commanders may prepare for lethal actions against known enemy cyberspace assets within an area of operations.

6-15. Preparation includes an assessment of a unit's readiness to conduct CEMA. A unit's readiness includes its ability to operate in degraded conditions. Degradation to friendly networks can occur based on many internal, external, intentional, and unintentional threats. Because most CEMA defensive measures are executed continuously throughout all phases of the operation, during peacetime and war, preparation occurs not only by the CEMA element and applicable staff entities, for example, the G-6 (S-6), but at the individual level as well. Individual Soldiers not directly involved in CEMA contribute to the preparation process by adhering to the basic tenets of information assurance and operations security.

6-16. During preparation the CEMA element conducts several actions. They include—

- Revising and refining the CEMA estimate and tasks in support of the overall plan.
- Rehearsing the synchronization of CEMA in support of the plan including integration into the targeting process, procedures for requesting assets, procedures for deconfliction, and asset determination and refinement.

- Synchronizing the collection plan and intelligence synchronization matrix with the attack guidance matrix and CEMA input to the operation plan or order annexes and appendices.
- Assessing the planned task organization developed in support of CEMA, including liaison officers and organic and nonorganic capabilities required by echelon.
- Coordinating procedures with information collection operational elements.
- Training the supporting staff of the CEMA working group during rehearsals.
- Completing precombat checks and inspections of CEMA assets.
- Completing sustainment preparations for CEMA assets.
- Coordinating with the assistant chief of staff, logistics (G-4 [S-4]) to develop CEMA equipment report formats.
- Completing backbriefs by subordinate CEMA working groups on planned operations.
- Refining content and format for the CEMA element's portion of the operation update assessment and briefing.

CYBER ELECTROMAGNETIC ACTIVITIES IN EXECUTION

6-17. Execution puts a plan into action by applying combat power to accomplish the mission and using situational understanding to assess progress and make execution and adjustment decisions. CEMA are integrated and synchronized into the commander's concept of operations. Fires provided by CO and EW are employed in accordance with the targeting plan. These integrations are based on commander's guidance, desired effects, friendly capabilities, and likely enemy or adversary COA. During execution, the CEMA element is responsible for monitoring the proper employment of these capabilities in accordance with the commander's guidance and ensuring the proper integration with other warfighting function capabilities based on the concept of operations.

6-18. Each capability within CEMA has diverse operational functions and requirements. These capabilities often require wide variances in times to achieve effects. The CEMA element accounts for these time variances and ensures synchronization between the capabilities during execution. The effects from each capability being utilized are then realized at the appropriate phase in the commander's scheme of maneuver.

6-19. During execution the CEMA element performs several actions. They are to—

- Serve as CEMA experts for the commander.
- Maintain a running estimate for CEMA.
- Monitor CEMA in operations and recommend adjustments during execution.
- Recommend adjustments to the commander's critical information requirements based on the situation.
- Recommend adjustments to control measures and procedures related to CEMA.
- Maintain direct liaison with the fires, signal, and intelligence cells to ensure integration and deconfliction of CEMA.
- Coordinate and manage CEMA taskings to subordinate units or assets.
- Coordinate requests for nonorganic CEMA assets.
- Continue to assist the targeting working group in target and access development and to recommend targets to attack through CO or electronic attack.
- Receive, process, and coordinate subordinate requests for CEMA assets during operations.
- Provide input to the overall assessment regarding the effectiveness of CO and EW missions.
- Maintain, update, and distribute the status of CEMA assets.

CYBER ELECTROMAGNETIC ACTIVITIES IN ASSESSMENT

6-20. The CEMA element conducts an assessment of CEMA by following the same general procedures as the assessment of all other operations. The CEMA assessment contributes to the overall assessment of the operation.

6-21. Assessment requires direct feedback from those closest to observing the intended effects. Assessment of CEMA relies heavily on sensors capable of monitoring networks, systems, and the EMS. Visual systems can contribute to the assessment by detecting changes in the flights of enemy weapons and trajectory profiles, or observing changes in adversary patterns of behavior.

6-22. During planning, assessment focuses on gathering information on cyberspace and its contribution to the assigned area of operations to assist the commander and staff with understanding the current situation. The CEMA element provides the commander with an understanding of the linkage between cyberspace and the EMS to the supported mission or operation. During preparation and execution, assessment focuses on monitoring the current situation and evaluating the operation's progress.

6-23. During assessment, the CEMA element performs several actions. The CEMA element—

- Continuously assesses the enemy's reactions and vulnerabilities.
- Continuously monitors the situation and progress of CEMA support of the operation towards the commander's desired end state.
- Evaluates CEMA against measures of effectiveness and measures of performance.

THE INTEGRATING PROCESSES

6-24. The CEMA element ensures the integration of CEMA into the intelligence preparation of the battlefield, targeting process, risk management, and continuing activities processes. These processes require the involvement of the CEMA element throughout the operations process.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

6-25. The G-2 (S-2), as part of threat characteristics of intelligence preparation of the battlefield, evaluates the threat's ability to conduct cyberspace attack and electronic attack. This includes evaluating the threat forces' ability to protect their networks and command and control systems from attack. This can consist of threat servers, websites, towers, satellites, and spectrum wavelengths. Because cyberspace is man-made, new threat capabilities can be created in a relatively short period of time. The G-2 (S-2) determines possible threat courses of action. The CEMA element assists the G-2 (S-2) in these efforts and their integration into the concept of operations. An area of operations involves a portion of cyberspace as a part of its whole. An area of influence may be a geographic area, a portion of cyberspace, or both. Due to the global nature of cyberspace, it can be difficult to conceptualize cyberspace within the boundaries of an area of operations and map out the physical elements of cyberspace geographically in the naturally occurring domains. A geographic area is too limiting, and it is insufficient to contain cyberspace. Cyberspace may expand the geographic area of local interest to a worldwide interest.

6-26. The CEMA element assists the G-2 (S-2) in describing how the variables of an operational environment impact CEMA and vice versa. The element also assists with the assessment of enemy cyberspace and EW capabilities, including an examination of doctrinal principles; tactics, techniques, and procedures; and observed patterns of enemy operations in cyberspace and the EMS leading to a determination of possible enemy courses of action. Enemy or adversary courses of action may involve avenues of approach that reside solely within cyberspace or the EMS. (For more information on intelligence preparation of the battlefield see FM 2-01.3.)

TARGETING

6-27. Fires provided by CEMA are integrated and synchronized into the concept of operations during the planning process and adjusted based on the targeting guidance. Both CO and EW, when authorized, provide the commander with lethal and nonlethal actions in support of unified land operations. Targets and problem sets may exist within or be accessible through all five domains.

6-28. The CEMA element participates in the targeting process to assist with the integration of fires provided by both CO and EW. OCO provide a strike option in the form of cyberspace attack. EW provides electronic attack. Targeting provides the process to match these capabilities (in addition to physical attack) against targets. The commander's intent plays a critical role and largely determines which form of fires or combination of fires is necessary to produce the required effect—deny, degrade, disrupt, delay, deceive, or destroy.

6-29. OCO, defensive cyberspace operations (DCO)-response actions, and electronic attack provide advantages and disadvantages with regards to their use. OCO can be more enduring. For instance, the means by which these missions are executed involves the deployment of tailored computer code which can reside on one or more enemy or adversary networks. DCO-response actions share similar characteristics. The disadvantages of these CO missions are the additional time needed for careful policy and legal review and strict adherence to rules of engagement and laws of armed conflict. Planners must also consider the time intensive nature of target and capability development, as well as time needed for preparation and execution. Electronic attack fires are likely to be more readily available to units at division echelons and below. These fires are generally less enduring in nature. For instance, electronic attack against enemy communications for denial purposes ends once the platform conducting the mission departs. Physical attack (for example, a precision fires mission) may provide the best option for creating the intended effects on the target. Physical attack may be combined with the OCO, DCO-response actions, and electronic attack missions to create simultaneous and complementary effects.

Decide

6-30. The characteristics of cyberspace and the EMS provide threats and adversaries with considerable measures of anonymity. Individuals, politically motivated groups, and criminals can have a larger cyber persona or role than some nation states. Intelligence collection is a critical step for identifying potential threats or adversaries in cyberspace. Designating targets that reside within cyberspace and the EMS depends heavily on the intelligence collection effort. Each designated target and its required effect is assigned to OCO, electronic attack fires, traditional physical fires, or a combination of each in accordance with their capabilities.

6-31. An important part of this step in the targeting process is identifying potential fratricide situations and providing electronic protection and DCO to mitigate them. This requires intense coordination and synchronization on the part of the CEMA element. Any action in cyberspace and the EMS, either offensive or defensive, must be coordinated and balanced with potential degradation inflicted on friendly systems. The spectrum management operations (SMO) component of CEMA is leveraged to ensure that electronic attack does not cause unwanted interference on friendly systems or degrade friendly networks. The nature of OCO, by design and implementation, mitigates friendly network fratricide.

Detect

6-32. The capabilities that provide situational understanding of cyberspace provide situational data in the form of network topology (terrain), configuration, operating system, and enemy and adversary actions and intentions. Capabilities that provide situational understanding of the EMS provide situational data in the form of geospatial location, signal strength, system type, and frequency of target to focus OCO, electronic attack, or physical attack on the intended target.

Deliver

6-33. The CEMA element ensures the full coordination, integration, deconfliction, and employment of CO, EW, and physical fires in accordance with the commander’s time-phased scheme of maneuver. Close coordination between collecting assets (sensor) and those assets delivering the fires (shooter) is critical during the engagement to avoid unintended effects.

Assess

6-34. Execution of CEMA is often dependent on intelligence. Effects produced by CEMA are not always readily visible. The intelligence community operates many airborne and ground-based sensors. These sensors provide the raw data. This data is converted into intelligence that then supports the conduct of CEMA. In some cases this intelligence can be immediately used by tactical forces. Intelligence is the primary contributor to the assessment of effects produced by CEMA 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 ADP 2-0, ADRP 2-0, FM 2-0, and FM 2-01.3.)

6-35. Close coordination between sensor and shooter regarding the success or failure of the intended effects often provides instant feedback. This coordination can also facilitate necessary, rapid adjustments. (For more information on targeting see FM 3-60.)

RISK MANAGEMENT

6-36. Throughout the operations process, the CEMA element uses risk management to mitigate risks associated with cyberspace and the EMS that have the potential to impact mission effectiveness. The CEMA element begins the risk management process during planning and applies the process to CEMA continuously through preparation and execution. (For more information on risk management, see FM 5-19.)

CONTINUING ACTIVITIES

6-37. While executing tasks throughout the operations process, commanders and staffs plan for and coordinate continuing activities. The CEMA element coordinates with the staff to participate in these continuing activities as necessary, and it ensures that CEMA are fully synchronized and integrated within these processes. As needed, each continuing activity addresses tasks specific to each capability within CEMA. The continuing activities are liaison, information collection, security operations, protection, terrain management, and airspace control. (See ADRP 5-0 for more information on continuing activities.)

This page intentionally left blank.

Chapter 7

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 cyber electromagnetic activities (CEMA) with unified action partners.

JOINT OPERATIONS CONSIDERATIONS

7-1. Army operations that involve the use of cyberspace and the electromagnetic spectrum (EMS) can have joint implications. Each service component has cyberspace operations (CO), EMS requirements, and electronic warfare (EW) capabilities that contribute to an integrated whole, synchronized by a joint force headquarters.

7-2. The CEMA element ensures that the conduct of CEMA aligns with joint information operations, CO, EW, spectrum management operations (SMO), and doctrine. The Army supports joint force objectives by integrating its CO, EW functions, and SMO requirements through the conduct of CEMA.

7-3. 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 element staff to integrate the capabilities within CEMA into the joint operations planning process. The integration of these capabilities into operations occurs at the information operations 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 electronic warfare 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 element separately from the joint electronic warfare cell, integrating the element into the higher CEMA element, or converting to a joint organizational model.

7-4. 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 information operations, see JP 3-13. For more information on joint SMO, see JP 6-01.)

HOMELAND DEFENSE AND DEFENSE SUPPORT OF CIVIL AUTHORITIES CONSIDERATIONS

7-5. Commanders and staffs understand the unique legal and political parameters, and the roles, missions, and capabilities of other United States (U.S.) government agencies when conducting CEMA in support of homeland defense and defense support of civil authorities. During homeland defense and defense support of civil authorities, the supported military command is U.S. Northern Command or U.S. Pacific Command.

7-6. Army commanders may be required to assist with homeland defense and defense support of civil authorities by providing CO, EW, and SMO. This support is provided within the appropriate legal framework that ensures compliance with federal laws. Unless approved by appropriate authorities, Army assets cannot be used to perform attack or exploit operations on U.S. entities. In the event of a homeland defense operation, the Department of Defense (DOD) may be the lead federal agency in formulating CEMA responses, or it may provide support to another federal agency such as the Department of Justice. The U.S. service components criminal investigative and counterintelligence organizations may be able to bring Title 18 or Title 50 authorities to bear in situations involving U.S. and foreign entities actions in cyberspace and the EMS. A state's National Guard forces may play a role in responding to a CEMA related event whether under the command of the governor (either in State Active Duty or Title 32 status), or in

Title 10 status under the command of the President. Army Reserve forces may also be brought onto active duty in Title 10 status to respond to CEMA related events.

7-7. Conducting CEMA in the homeland presents a challenge to the Army commander due to the possibility that the malicious activity originates from within the U.S. The policy and legal restrictions that govern the DOD's domestic activities extend to the Army's operations in cyberspace. The Army works closely with the Department of Justice and Homeland Security, and each State's National Guard works closely with State and local governments, to defeat threats to U.S. cyberspace. Commanders must ensure that the legal, constitutional, and privacy rights of U.S. citizens are protected throughout the planning and execution of CEMA.

7-8. During disaster relief operations Army units may be expected to provide assistance in reconstituting or restoring access to cyberspace which may include SMO or, in unique circumstances, providing EW support to allow military and U.S. government organizations to communicate or be connected for situational awareness. The supported federal agency may be the Department of Homeland Security or the Department of Justice. Army installations currently interface with both government and civilian emergency responders via land mobile radio networks. Army units must be prepared to join those networks during defense support of civil authorities operations.

INTERAGENCY AND INTERGOVERNMENTAL CONSIDERATIONS

7-9. Army commanders must consider the unique capabilities, structures, and priorities of interagency and intergovernmental partners in the planning and execution of CEMA. Successful execution of missions with partners requires a shared understanding and common objective for the operation.

7-10. 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 prior to 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.

7-11. 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 decisionmaking 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

7-12. Army units conducting 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.

7-13. 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.

7-14. 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.

7-15. Intelligence and information sharing with allies and multinational partners is important during multinational operations. When conducting CEMA with multinational partners, Army units must ensure adherence to information assurance and computer network defense 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

7-16. Commanders ensure adherence to information assurance and computer network defense procedures when conducting CEMA 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 be required to coordinate CEMA.

HOST-NATION CONSIDERATIONS

7-17. 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. Host-nation coordination will not be extended to enemy nations or their military. 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

7-18. Tactical cyber electromagnetic 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 tools, systems, and processes necessary to execute CEMA.

7-19. 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 CO, EW, and electromagnetic spectrum operations will be constrained due to laws, policies, and regulations. Third, unique 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.

7-20. The installation as a docking station system allows units to train and exercise the same information technology capabilities they use on the battlefield at home station. This “train as you fight” strategy allows commanders and system operators to maintain skills and ensure equipment readiness. Both EW and SMO capabilities must be integrated with this system in order for CEMA to provide the force multiplication necessary in today’s net-centric environment and support the warfighting functions.

PRIVATE INDUSTRY CONSIDERATIONS

7-21. Private industry plays a significant role in the conduct of CEMA. 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.

7-22. 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.

7-23. 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 in support of national needs.

7-24. The Department of Defense information networks (DODIN) reside on commercial networks that reside in the four traditional domains in the form of 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 CEMA vulnerable to access denial, service interruption, communications intercept and monitoring, infiltration, and data compromise. Army commanders pursue risk mitigation through adherence to operations security, information assurance, inspection of vendor supplied equipment, encryption, and promotion of user and commander education.

Appendix A

CEMA Input to Operation Plans and Orders

This appendix provides fundamental considerations, formats and instructions for developing cyber electromagnetic activities (CEMA) input to Army plans and orders. This appendix provides the format for Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations).

APPENDIX 12 (CYBER ELECTROMAGNETIC ACTIVITIES) TO ANNEX C (OPERATIONS) TO OPERATIONS PLANS/ORDERS

A-1. Commanders and staffs use Appendix 12 (Cyber Electromagnetic Activities) to Annex C (Operations) to operations plans and orders to describe how CEMA) support operations described in a base plan or order. The electronic warfare officer (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 operations plans and orders being conducted, and the content of actual Appendix 12s will vary greatly.

A-2. This appendix describes CEMA support and objectives. Complex CEMA support may require a schematic to show CEMA integration and synchronization requirements and task relationships. This includes a discussion of the overall CEMA 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 CEMA. This appendix also includes CEMA related constraints, if appropriate.

[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 (CYBER 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 cyber electromagnetic activities, if needed.*

1. **(U) Situation.** *Include information affecting cyber electromagnetic activities (CEMA) that paragraph 1 of Annex C (Operations) does not cover or that needs expansion.*

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

[page number]
[CLASSIFICATION]

Figure A-1. Appendix 12 (CEMA) to Annex C (Operations)

[CLASSIFICATION]

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

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

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

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

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

f. (U) Third Party. *Identify and describe other organizations, both local and external to the area of operations that have the ability to influence CEMA or the implementation of CEMA 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 CEMA. 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 CEMA assets that are 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 CEMA in support of the base plan or order.*

3. (U) Execution.

a. Scheme of Cyber Electromagnetic Activities. *Describe how CEMA support the commander's intent and concept of operations. Establish the priorities of support to units for each phase of the operation. State how CEMA tasks will degrade, disrupt, deny, and deceive the enemy. State the defensive and offensive CEMA measures. Identify target sets and effects, by priority. Describe the general concept for the integration of CEMA. List the staff sections, elements, and working groups responsible for aspects of CEMA. Include the CEMA collection methods for information developed in staff section, elements, and working groups outside the CEMA element and working group. Ensure subordinate units and higher headquarters receive the CEMA integration plan. 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 CEMA and how these activities are integrated across the operational plan. It is recommended that this appendix include an understanding of technical requirements.*

[page number]
[CLASSIFICATION]

Figure A-1. Appendix 12 (CEMA) to Annex C (Operations) (continued)

[CLASSIFICATION]

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

This appendix concentrates on the integration requirements for CEMA and references appropriate annexes and appendices 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, constraints, and restraints. Identify risks associated with cyberspace operations. Include collateral damage, discovery, attribution, fratricide (to U.S. or allied or coalition networks or information), and possible conflicts. Describe actions that will prevent 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 indications and 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 adversary actions in the physical domains and cyberspace. Ensure subordinate units are conducting defensive cyberspace operations. Synchronize the CEMA element with the IIA section. Pass requests for offensive cyberspace operations to higher headquarters for approval and implementation. Describe how DOD information network operations support the commander's intent and concept of operations. Synchronize DOD information network operations with elements reconcilable for friendly network operations (G-6 [S-6]). Prioritize the allocation of applications utilizing cyberspace. Ensure the employment of cyber 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 appendices as needed to reduce duplication).*

(1) (U) Defensive Cyberspace Operations. *Describe how defensive cyberspace operations are conducted, coordinated, integrated, synchronized, and support operations to defend DOD or other friendly cyberspace and preserve the ability to utilize friendly cyberspace capabilities.*

(2) (U) Offensive Cyberspace Operations. *Describe how offensive cyberspace operations 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 offensive cyberspace operations.*

(3) (U) DOD Information Network 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.*

c. (U) Scheme of Electronic Warfare. *Describe how electronic warfare 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 electronic warfare 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 electronic warfare operations.*

[page number]

[CLASSIFICATION]

Figure A-1. Appendix 12 (CEMA) to Annex C (Operations) (continued)

[CLASSIFICATION]

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

Synchronize with G-7 (S-7) and the inform and influence activities (IIA) staff. See the following attachments as required: Tab C,D,E (Electronic Warfare) to Appendix 12 (Cyber Electromagnetic Activities); Annex J (Inform and Influence Activities); and Annex C (Operations).

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

d. (U) Scheme of Spectrum Management Operations. *Describe how spectrum management operations support the commander's intent and concept of operations. Outline the effects the commander wants to achieve while prioritizing spectrum management operations 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' spectrum management operations (SMO) capabilities. See Annex H (Signal) as required.*

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

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

4. **(U) Sustainment**. *Identify priorities of sustainment for CEMA 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 CEMA. 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 CEMA. 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 CEMA leaders.*

[page number]
[CLASSIFICATION]

Figure A-1. Appendix 12 (CEMA) to Annex C (Operations) (continued)

[CLASSIFICATION]

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

(2) (U) Liaison Requirements. *State the CEMA liaison requirements not covered in the unit's SOPs.*

b. *(U)* Control.

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

(2) (U) Reports. *List CEMA specific reports not covered in SOPs. See Annex R (Reports) as required.*

c. *(U)* Signal. *Address any CEMA 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]

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 (CYBER 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 A-1. Appendix 12 (CEMA) to Annex C (Operations) (continued)

This page intentionally left blank.

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

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AR	Army regulation
ATTP	Army tactics, techniques, and procedures
CEMA	cyber electromagnetic activities
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CO	cyberspace operations
COA	course of action
DA	Department of the Army
DCO	defensive cyberspace operations
DD	Department of Defense (for forms)
DOD	Department of Defense
DODI	Department of Defense instruction
DODIN	Department of Defense information networks
EA	electronic attack
EHF	extremely high frequency
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWO	electronic warfare officer
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
G-7	assistant chief of staff, inform and influence activities
G-9	assistant chief of staff, civil affairs operations
IIA	inform and influence activities
JP	joint publication
OCO	offensive cyberspace operations
S-2	intelligence staff officer
S-3	operations staff officer
S-6	signal staff officer
S-7	inform and influence activities staff officer
S-9	civil affairs operations staff officer
SHF	super high frequency
SIPRNET	SECRET Internet Protocol Router Network

SMO	spectrum management operations
UHF	ultra high frequency
U.S.	United States
USC	United States Code
VHF	very high frequency

SECTION II – TERMS

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)

cyber electromagnetic activities

Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. (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 1-02)

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 1-02)

defensive cyberspace operation response action

Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. (JP 1-02)

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 1-02)

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 1-02)

Department of Defense information networks

The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. (JP 1-02)

directed energy

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)

electromagnetic compatibility

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)

electromagnetic hardening

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

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

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

The deliberate radiation, re-radiation, 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

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)

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 attack

Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-13.1)

electronic intelligence

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

electronic masking

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

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 protection

Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-13.1)

electronic reconnaissance

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

electronics security

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non-communications 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

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)

electronic warfare support

Division of electronic warfare involving 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. (JP 3-13.1)

electro-optical-infrared countermeasures

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)

emission control

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)

frenquency deconfliction

A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. Frequency deconfliction is one element of electromagnetic spectrum management. (JP 3-13.1)

host nation

A nation which receives the forces and/or supplies of allied nations and/or NATO organizations to be located on, to operate in, or to transit through its territory. (JP 3-57)

inform and influence activities

The integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decisionmaking. (ADRP 3-0)

information environment

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

information-related capabilities

Capabilities, techniques, or activities employing information to effect any of the three dimensions within the information environment to generate an end(s). (FM 3-13)

integration

2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1)

offensive cyberspace operations

Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 1-02)

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)

radio frequency countermeasures

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)

red team

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 adversaries and others. (JP 2-0)

synchronization

The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (JP 1-02)

wartime reserve modes

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)

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*. 24 September 2013.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010, as amended through 15 September 2013.

REQUIRED FORMS

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

DA Form 2028. *Army Electronic Publications and Forms*. February 1974.

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 5810.01D. *Implementation of the DOD Law of War Program*. 30 April 2010.

CJCSM 3320.02D. *Joint Spectrum Interference Resoultion (JSIR) Procedures*. 3 June 2013.

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

JP 1-04. *Legal Support to Military Operations*. 17 August 2011.

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

JP 3-0. *Joint Operations*. 11August 2011.

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

JP 3-13.1. *Electronic Warfare*. 08 February 2012.

JP 3-57. *Civil-Military Operations*. 11 September 2013.

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

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

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: <http://www.apd.army.mil/>. Army regulations are produced only in electronic media and available at the same link.

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

ADP 3-0. *Unified Land Operations*. 10 October 2011.

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. *Unified Land Operations*. 16 May 2012.

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

ATTP 3-13.10. *EW Reprogramming:Multi-Service Tactics, Techniques, and Procedures for the Reprogramming Electronic Warfare (EW) Systems*. 1 February 2011.

ATTP 5-0.1. *Commander and Staff Officer Guide*. 14 September 2011.

FM 2-0. *Intelligence*. 23 March 2010.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 15 October 2009.

FM 3-13. *Inform and Influence Activities*. 25 January 2013.

FM 3-36. *Electronic Warfare*. 9 November 2012.

FM 3-60. *The Targeting Process*. 26 November 2010.

FM 5-19. *Composite Risk Management*. 21 August 2006.

FM 6-02.70. *Army Electromagnetic Spectrum Operations*. 20 May 2010.

FM 6-02.71. *Network Operations*. 14 July 2009.

FM 6-99. *U.S. Army Report and Message Formats*. 19 August 2013.

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

OTHER PUBLICATIONS

Title 10, United States Code. Armed Forces.

Title 18, United States Code. Crimes and Criminal Procedures.

Title 32, United States Code. National Guard.

Title 40, United States Code. Public Buildings, Property, and Works.

Title 44, United States Code. Public Printing and Documents.

Title 50, United States Code. War and National Defense.

RECOMMENDED READINGS

AR 5-12. *Army Use of the Electromagnetic Spectrum*. 15 February 2013.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. July 2011. http://www.defense.gov/news/d20110714cyber.pdf

Office of the President of the United States. *The Comprehensive National Cybersecurity Initiative*. March 2010. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

PRESCRIBED FORMS

None.

REFERENCED FORMS

DA Forms are available on the APD web site (http://www.apd.army.mil/) and DD forms are available on the OSD web site (http://www.dtic.mil/whs/directives/infomgt/forms/).

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

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

Index

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

This page intentionally left blank.

FM 3-38
12 February 2014

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1401704

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with the initial distribution number (IDN) 116045, requirements for FM 3-38.

This page intentionally left blank.

PIN: 103949-000