FM 3-36

ELECTRONIC WARFARE

NOVEMBER 2012

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 3-36

Headquarters
Department of the Army
Washington, DC, 9 November 2012

Electronic Warfare

Contents

***This publication supersedes FM 3-36, dated 25 February 2009.**

Figures

Tables

Preface

Field Manual (FM) 3-36 provides Army doctrine for electronic warfare (EW) planning, preparation, execution, and assessment in support of unified land operations. Users of FM 3-36 must be familiar with unified land operations doctrine established in Army Doctrine Publication (ADP) 3-0 (2011), the operations process established in ADP 5-0 (2012), and EW doctrine described in Joint Publication (JP) 3-13.1 (2012). This manual is not intended to be a major departure from the 2009 version. It aligns Army EW doctrine with ADP 3-0 and addresses numerous administrative and organizational changes since 2009.

The principle audience for FM 3-36 is Army commanders and staffs at all echelons. This FM serves as an authoritative reference for personnel who—

- Develop doctrine (fundamental principles and tactics, techniques, and procedures), materiel, and force structure.
- Develop institutional and unit training.
- Develop standard operating procedures for unit operations.
- Plan, prepare, execute, and assess EW.

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 3-36 uses joint terms where applicable. Selected joint and Army terms 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.

This publication applies to the Active Army, Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and United States Army Reserve (USAR) unless otherwise stated.

The proponent for this publication is the United States Army Combined Arms Center. The preparing agency is the United States Army Electronic Warfare Proponent. Send written 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-MCC-E (FM 3-36), 950 Bluntville Lane, Building 391, Fort Leavenworth, KS 66027-2337; by e-mail to EWPO@conus.army.mil; or submit an electronic DA Form 2028.

Chapter 1
Electronic Warfare Overview

This chapter provides an overview of electronic warfare and the conceptual foundation that leaders require to understand the electromagnetic environment and its impact on Army operations. It first discusses operational environments. Then it discusses the three divisions of electronic warfare. The chapter concludes with a discussion of the electronic warfare activities and terms.

OPERATIONAL ENVIRONMENTS AND ELECTRONIC WARFARE

1-1. *Electronic warfare* is 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 (EW) consists of three divisions: electronic attack, electronic protection, and electronic warfare support. EW capabilities are emerging as an increasingly important means by which commanders can shape operational environments to their advantage.

1-2. 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 operational environment encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment, which includes cyberspace. Commanders employ and integrate their unit's capabilities and actions within an operational environment to achieve a desired end state. Through analyzing their operational environments, to include the electromagnetic spectrum and cyberspace, commanders seek to understand how the results of friendly, adversary, and neutral actions may affect that desired end state.

1-3. 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). These bands include the radio spectrum, infrared, visible light and ultraviolet bands (see figure 1-1, page 1-2). The spectrum is a continuum of all electromagnetic waves arranged according to frequency and wavelength. The electromagnetic spectrum extends from below the frequencies used for modern radio (at the long-wavelength end) through gamma radiation (at the short-wavelength end). It covers wavelengths from thousands of kilometers to a fraction of the size of an atom. The rapid development and distribution of wireless technologies throughout commercial, societal, and military activities make the electromagnetic spectrum an increasingly important factor within an operational environment. Wireless systems work as powerful enablers to modern telecommunications, computer networks, and weapons systems. Additionally, new technologies expand beyond the traditional radio frequency spectrum and include high-power microwave, directed-energy, and electro-optical devices.

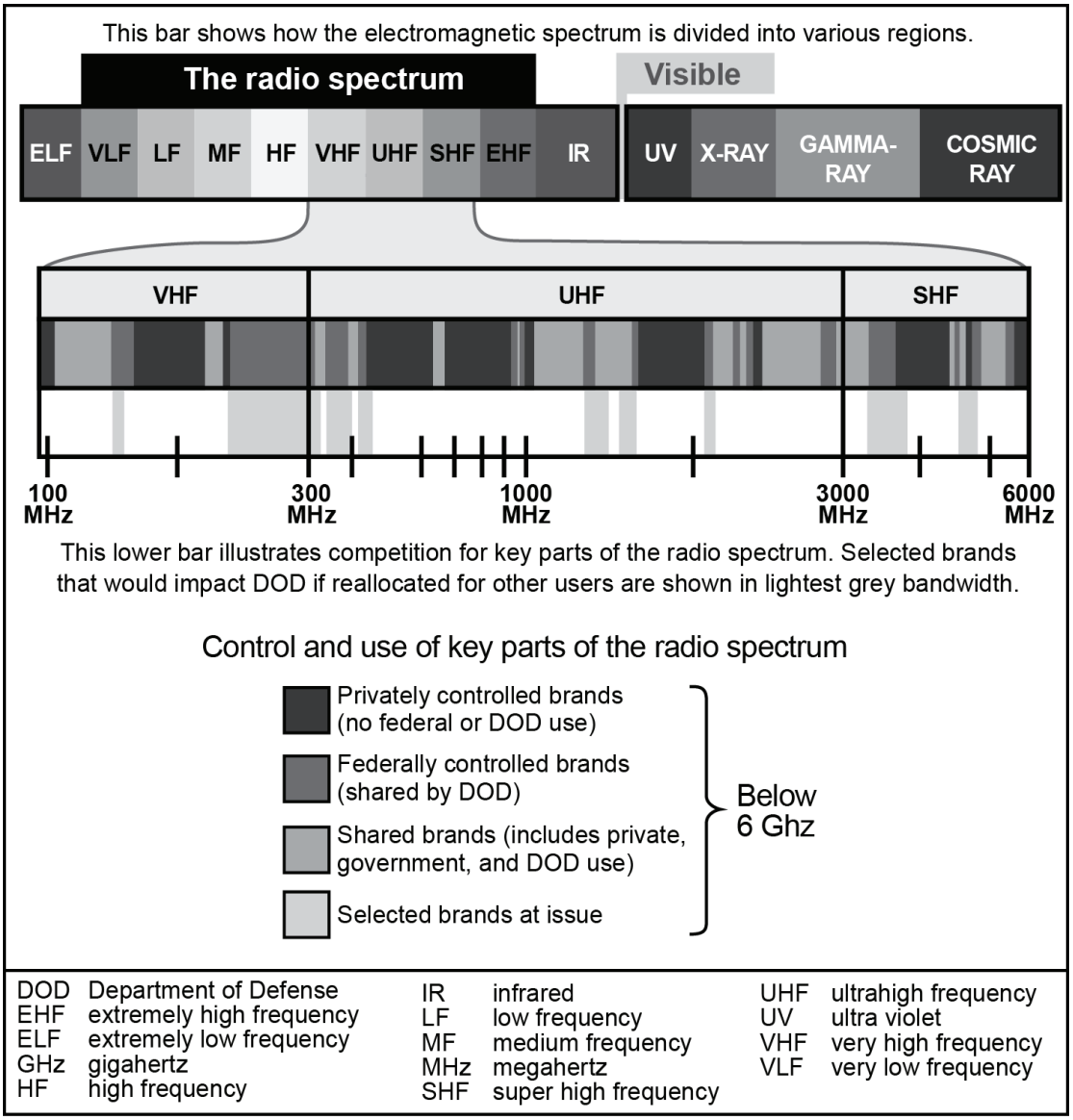


Figure 1-1. The electromagnetic spectrum

1-4. The increased use of wireless systems—including commercial off-the-shelf items—makes the available electromagnetic spectrum a high-demand, low-density resource. The resulting electromagnetic environments in which forces operate tend to be highly contested and congested, making unencumbered access to the electromagnetic spectrum problematic. This challenge is most acute for, but not unique to, U.S. forces that depend on new technologies. However, a plethora of current and potential adversaries increasingly relies on the electromagnetic spectrum, enabling both friendly and enemy forces of exploiting the advantages while being vulnerable to the disadvantages these systems provide (see figure 1-2). Reliance on the electromagnetic spectrum enables commanders to control or, at least, gain and maintain an advantage in unified land operations. EW provides commanders a valuable tool to help achieve the objective.

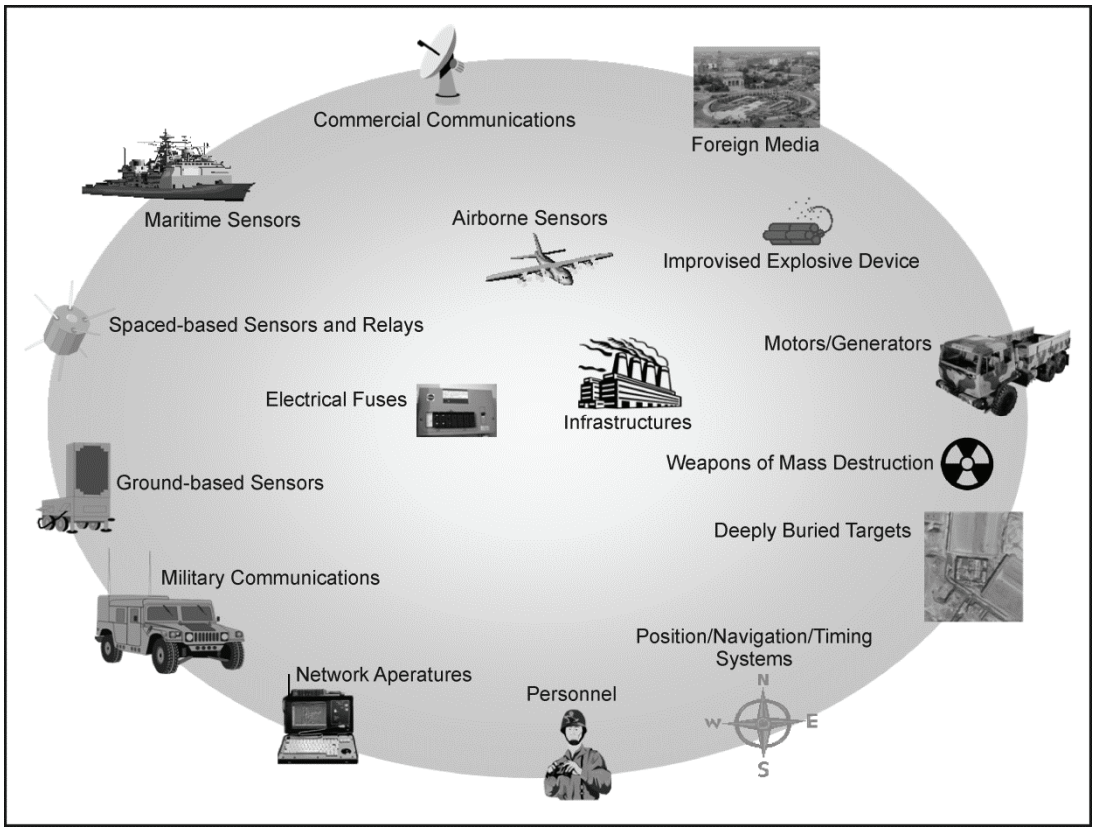


Figure 1-2. Examples of systems and targets dependent on the electromagnetic spectrum

ELECTRONIC WARFARE AND ITS DIVISIONS

1-5. EW is one of the two lines of effort within cyber electromagnetic activities (see appendix E for more information about cyber electromagnetic activities). EW consists of three divisions: electronic attack, electronic protection, and electronic warfare support. (See figure 1-3, page 1-4.)

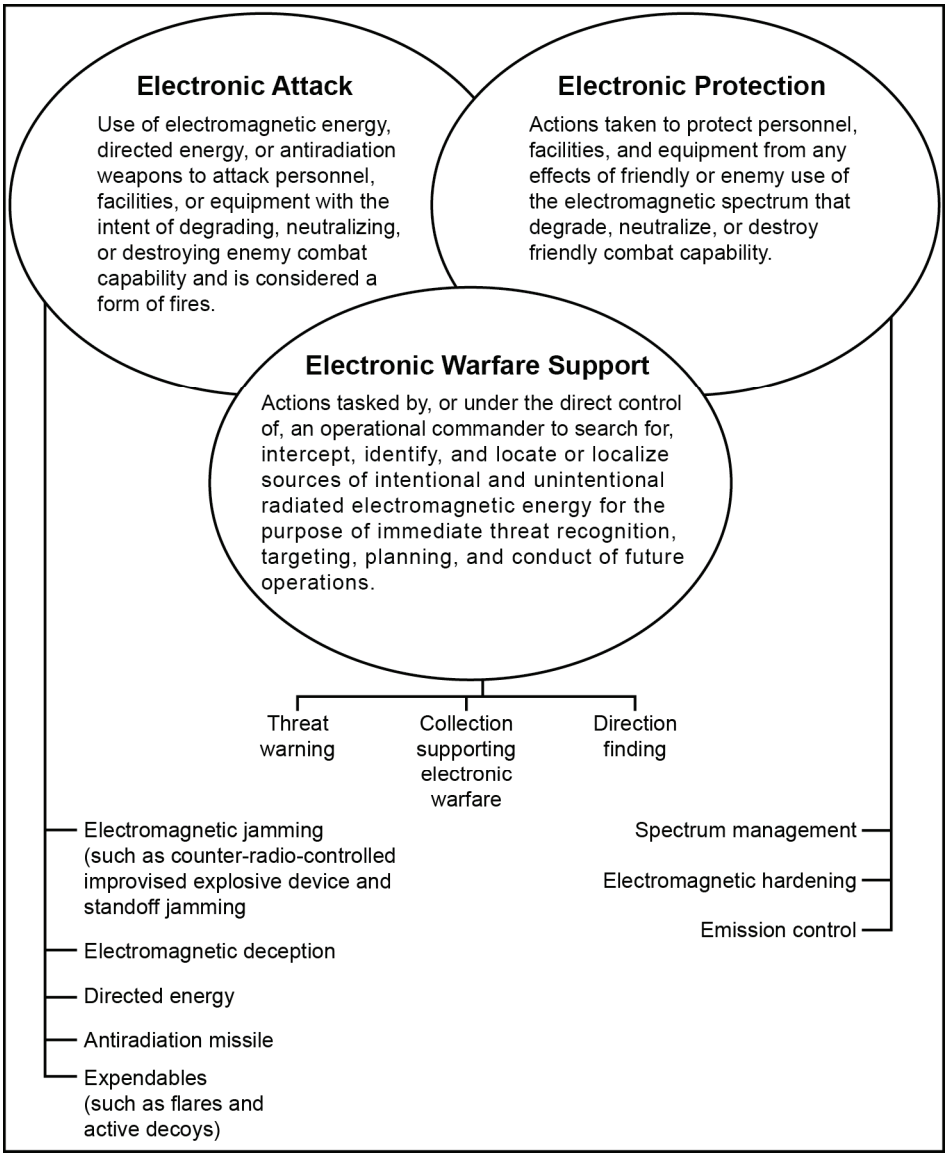


Figure 1-3. The three divisions of electronic warfare

ELECTRONIC ATTACK

1-6. *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). Electronic attack includes—

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

1-7. Actions that prevent or reduce an enemy's effective use of the electromagnetic spectrum include spot, barrage, and sweep electromagnetic jamming (defined in paragraph 1-26). Electronic attack actions also include various electromagnetic deception techniques such as false target or duplicate target generation. (See paragraphs 1-21 through 1-28 for a more detailed discussion of electronic attack activities.)

1-8. Electronic attack 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 electronic attack. 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.

1-9. Unified land operations use offensive and defensive tasks for electronic attack. Examples of offensive electronic attack 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 for guidance onto the target).
- Using electromagnetic deception to confuse enemy intelligence, surveillance, and reconnaissance systems.
- Using directed-energy weapons to disable an enemy's equipment or capability.

1-10. Defensive electronic attack uses the electromagnetic spectrum 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 EW systems.

ELECTRONIC PROTECTION

1-11. *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, electronic protection includes actions taken to ensure friendly use of the electromagnetic spectrum, such as frequency agility in a radio or variable pulse repetition frequency in radar. Commanders avoid confusing electronic protection with self-protection. Both defensive electronic attack and electronic protection protect personnel, facilities, capabilities, and equipment. However, electronic protection protects from the effects of electronic attack (friendly and enemy), while defensive electronic attack primarily protects against lethal attacks by denying enemy use of the electromagnetic spectrum to guide or trigger weapons.

1-12. During operations, electronic protection includes, but is not limited to, the application of training and procedures for countering enemy electronic attack. Army commanders and forces understand the threat and vulnerability of friendly electronic equipment to enemy electronic attack and take appropriate actions to safeguard friendly combat capability from exploitation and attack. Electronic protection measures minimize the enemy's ability to conduct activities of electronic warfare support (defined in paragraph 1-15) and electronic attack operations successfully against friendly forces. To protect friendly combat capabilities, units—

- Regularly brief force personnel on the EW threat.
- Ensure that they safeguard electronic system capabilities during exercises, workups, and predeployment training.
- Coordinate and deconflict electromagnetic spectrum usage.
- Provide training during routine home station planning and training activities on appropriate electronic protection active and passive measures.
- Take appropriate actions to minimize the vulnerability of friendly receivers to enemy jamming (such as reduced power, brevity of transmissions, and directional antennas).

1-13. Electronic protection also includes electromagnetic spectrum management (see paragraph 1-37). The spectrum manager works for the G-6 or 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.

1-14. The development and acquisition of communications and electronic systems includes electronic protection requirements to clarify performance parameters. Army forces design their equipment to limit inherent vulnerabilities. If electronic attack vulnerabilities are detected, then units must review these programs. (See DODI 4650.01 for information on the spectrum certification process and electromagnetic compatibility.)

ELECTRONIC WARFARE SUPPORT

1-15. *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). Electronic warfare support 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.

1-16. Electronic warfare support systems are a source of information for immediate decisions involving electronic attack, electronic protection, avoidance, targeting, and other tactical employment of forces. Directed energy may also support EW, such as a laser-warning receiver designed solely to detect and analyze a laser signal. Electronic warfare support systems collect data and produce information or intelligence to—

- Corroborate other sources of information or intelligence.
- Conduct or direct electronic attack operations.
- Initiate self-protection measures.
- Task weapons systems.
- Support electronic protection efforts.
- Create or update EW databases.
- Support cyber electromagnetic activities.

1-17. Electronic warfare support and signals intelligence missions use the same 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. Like tactical signals intelligence, electronic warfare support missions respond to the immediate requirements of a tactical commander. Signals intelligence above the tactical level is under the operational control of the National Security Agency/Central Security Service and directly supports the overarching national security mission. Resources that collect tactical-level electronic warfare support data can simultaneously collect national-level signals intelligence.

ACTIVITIES AND TERMINOLOGY

1-18. Although new equipment and tactics, techniques, and procedures continue to be developed, the physics of electromagnetic energy remain constant. Hence, effective EW activities remain the same despite changes in hardware and tactics.

PRINCIPAL ACTIVITIES

1-19. This section (paragraphs 1-19 through 1-41) introduces principal EW activities. Principal EW activities support unified land operations by exploiting the opportunities and vulnerabilities inherent in the use of the electromagnetic spectrum. The numerous principal EW activities are categorized by the three EW divisions: electronic attack, electronic warfare support, and electronic protection. (See JP 3-13.1 for a more information about these principal activities.)

Electronic Attack Activities

1-20. Activities related to electronic attack are either offensive or defensive and include—

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

Countermeasures

1-21. *Countermeasures* are that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity (JP 3-13.1). They can be deployed preemptively or reactively. Devices and techniques used for EW countermeasures include electro-optical-infrared countermeasures and radio frequency countermeasures.

1-22. An *electro-optical-infrared countermeasure* is 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 is the part of the electromagnetic spectrum between the high end of the far infrared and the low end of ultraviolet. Electro-optical-infrared countermeasures may use laser and broadband jammers, smokes or aerosols, signature suppressants, decoys, pyrotechnics or pyrophorics, high-energy lasers, or directed infrared energy countermeasures.

1-23. *Radio frequency countermeasures* consist of 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).

Electromagnetic Deception

1-24. Electromagnetic deception refers to the deliberate radiation, reradiation, 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 electromagnetic deception involves actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces. Simulative electromagnetic deception involves actions to simulate friendly, notional, or actual capabilities to mislead hostile forces. Imitative electromagnetic deception introduces electromagnetic energy into enemy systems that imitates enemy emissions.

Electromagnetic Intrusion

1-25. *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 Jamming

1-26. *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).

Electromagnetic Pulse

1-27. *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).

Electronic Probing

1-28. *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 Activities

1-29. Activities related to electronic warfare support include—

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

Electronic Reconnaissance

1-30. *Electronic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-13.1).

Electronic Intelligence

1-31. *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).

Electronics Security

1-32. *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).

Electronic Protection Activities

1-33. Activities related to electronic protection include—

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

Electromagnetic Hardening

1-34. *Electromagnetic hardening* is 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).

Electronic Masking

1-35. *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

1-36. *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).

Electromagnetic Spectrum Management

1-37. *Electromagnetic spectrum management* [also referred to as spectrum management] is planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference (JP 6-0). (See paragraphs 5-8 through 5-10 for more information about coordination and deconfliction of the electromagnetic spectrum.)

Wartime Reserve Modes

1-38. *Wartime reserve modes* are characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance (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

1-39. *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; and clear concepts and doctrines that maximize operational effectiveness.

ELECTROMAGNETIC INTERFERENCE

1-40. *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). Unintentional electromagnetic interference is often the result of spurious emissions, intermodulation products and responses, and inadequate electromagnetic spectrum management.

ELECTRONIC WARFARE REPROGRAMMING

1-41. *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 result from deliberate actions by friendly, adversary or third parties, or they may come from electromagnetic interference or other inadvertent phenomena. The purpose of electronic warfare reprogramming is to maintain or enhance the effectiveness of EW and target sensing system equipment. Electronic warfare reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems.

ADDITIONAL TERMINOLOGY USED IN THE CONTEXT OF ELECTRONIC WARFARE

1-42. This section, (paragraphs 1-42 through 1-50) discusses terms as they apply to the three divisions of EW—electronic attack, electronic protection, and electronic warfare support. In the context of EW application, units use several specific terms: control, detection, denial, deception, disruption, degradation, protection, and destruction.

1-43. EW capabilities are applied from the air, land, sea, space, and cyberspace by manned, unmanned, attended, or unattended systems. Units employ these capabilities to achieve the desired lethal or nonlethal effect on a given target. Units maintain freedom of action in the electromagnetic spectrum while controlling the use of it by the enemy. Regardless of the application, units employing EW capabilities must use appropriate levels of control and protection of the electromagnetic spectrum. In this way, they avoid adversely affecting friendly forces. Improper EW actions must be avoided because they may cause fratricide or inadvertently eliminate high-value intelligence targets.

Control

1-44. EW aims to enable commanders to gain and maintain freedom of action across the physical domains and the information environment (which includes cyberspace) through electromagnetic spectrum control. Commanders achieve control of the electromagnetic spectrum by effectively managing and coordinating friendly electromagnetic spectrum-dependent systems—such as communications, EW, and computer networks—while countering and exploiting adversary systems. Commanders ensure deconfliction and maximum integration among EW, communications, information collection, cyberspace operations, and other capabilities.

Detection

1-45. In the context of EW, detection is the active and passive monitoring of an operational environment for radio frequency, electro-optical, laser, infrared, and ultraviolet electromagnetic threats. Detection is the first step in EW for exploitation, targeting, and defensive planning. Friendly forces maintain the capability to detect and characterize interference as hostile jamming or unintentional electromagnetic interference.

Denial

1-46. In the context of EW, denial is controlling the information an enemy receives via the electromagnetic spectrum and preventing the acquisition of accurate information about friendly forces. Denial uses traditional jamming techniques, expendable countermeasures, destructive measures, or network applications. These range from limited effects up to complete denial of usage.

Deception

1-47. In the context of EW, deception is confusing or misleading an enemy by using some combination of human-produced, mechanical, or electronic means. Through use of the electromagnetic spectrum, EW deception manipulates the enemy's decision loop, hindering the enemy's ability to establish accurate situational awareness.

Disruption

1-48. Disruption aims to confuse or delay enemy action. Forces achieve disruption with electromagnetic jamming, electromagnetic deception, and electromagnetic intrusion. Disruption techniques interfere with the adversary's use of the electromagnetic spectrum to limit adversary combat capabilities. Disruption resembles denial but is not as comprehensive in execution or impact on the enemy. A trained enemy operator can thwart disruption through electronic protection measures, such as procedures to counter communications jamming. Disruption enhances attacks on hostile forces and acts as a force multiplier by increasing adversary uncertainty while reducing uncertainty for friendly forces. Advanced electronic attack activities (discussed in paragraphs 1-20 through 1-28) offer the opportunity to nondestructively disrupt or degrade adversary infrastructure.

Degradation

1-49. Degradation refers to making an enemy incapable of performing the designated mission. It resembles disruption but is not as comprehensive in execution or impact on the enemy. Degradation may confuse or delay the actions of an untrained enemy, but a trained operator can work around the effects. Like disruption, forces achieve degradation with electromagnetic jamming, electromagnetic deception, and electromagnetic intrusion. Degradation may be the best choice to stimulate the enemy to determine their response or for electronic attack conditioning.

Protection

1-50. In the context of EW, protection is the use of physical properties; operational tactics, techniques, and procedures; and planning and employment processes to ensure friendly use of the electromagnetic spectrum. Protection includes ensuring that offensive EW activities do not electronically destroy or degrade friendly intelligence sensors or communications systems. Forces achieve protection by component hardening, emission control, and frequency management and deconfliction. Frequency management and deconfliction include the capability to detect, characterize, geolocate, and mitigate electromagnetic interference that affects operations. Protection includes other means to counterattack and defeat enemy attempts to control the electromagnetic spectrum. Additionally, organizations—such as a joint force commander's EW staff or a joint EW coordination cell—enhance electronic protection by deconflicting EW efforts.

Destruction

1-51. Destruction, in the context of EW, is the elimination of targeted enemy systems. Sensors and command and control nodes are lucrative targets because their destruction strongly influences the enemy's perceptions and abilities to coordinate actions. Various weapons and techniques—ranging from conventional munitions and directed-energy weapons to network attacks—can destroy enemy systems that use the electromagnetic spectrum. Electronic warfare support provides target location and related information. While destroying enemy equipment can effectively deny the enemy use of the electromagnetic spectrum, the duration of denial depends on the enemy's ability to reconstitute. (See JP 3-13.1.)

MEANS VERSUS EFFECTS

1-52. Forces apply EW means against targets to create a full range of lethal and nonlethal effects. Choosing a specific EW capability depends on the desired effect on the target and other considerations, such as time available or risk of collateral damage. EW capabilities provide commanders with additional options for achieving their objectives. During major combat operations, there may be circumstances where commanders want to limit the physical damage on a given target. Under such circumstances, the EW staff clearly articulates to the commander the lethal and nonlethal effects EW capabilities can achieve. For example, a target might be enemy radar mounted on a fixed tower. Two possible EW options to defeat the radar would be to jam the radar or destroy it with antiradiation missiles. If commanders wanted to limit damage to the tower, they could use an electronic attack jamming platform. In circumstances where commanders could not sufficiently limit undesired effects such as collateral damage, they would be constrained from applying physical force. In any case, the EW staff articulates succinctly how EW capabilities can help achieve desired effects by providing lethal and nonlethal options for commanders.

SUMMARY

1-53. As the modern battlefield becomes more technologically sophisticated, forces continue to execute military operations in an increasingly complex electromagnetic environment. Therefore, commanders and staffs need to thoroughly understand and articulate how the electromagnetic environment affects their operations and how they can use friendly EW operations to gain an advantage. Commanders and staffs use the terminology presented in this chapter to describe the application of EW. This ensures a common understanding and consistency within plans, orders, standard operating procedures, and directives.

This page intentionally left blank.

Chapter 2
Electronic Warfare in Unified Land Operations

This chapter describes how commanders apply electronic warfare to support unified land operations. It discusses the role of electronic warfare. It then discusses how electronic warfare enables each of the warfighting functions.

THE ROLE OF ELECTRONIC WARFARE

2-1. The ability to control the electromagnetic spectrum is central to unified land operations. As information technology becomes universally available, more adversaries rely on communications and computer networks to make and implement decisions. Radios remain the backbone of tactical military mission command architectures. Most communications relayed over radio networks are becoming digital as more computers link networks through transmitted frequencies, making computer networks and communications more dependent on the electromagnetic spectrum.

2-2. Army electronic warfare (EW) operations seek to enable the land force commander to support unified land operations through decisive action. Decisive action consists of the simultaneous combination of offense, defense, and stability or defense support of civil authorities appropriate to the mission and environment. The central idea of unified land operations is to seize, retain, and exploit the initiative to gain and maintain a position of relative advantage in sustained land operations in order to create the conditions for favorable conflict resolution. (See ADP 3-0 for more information about unified land operations.)

2-3. The foundation of unified land operations is built on initiative, decisive action, and mission command—linked and nested through purposeful and simultaneous execution of both combined arms maneuver and wide area security—to achieve the commander's intent and desired end state. Appropriately applied, EW enables successful unified land operations. Commanders and staffs determine which resident and joint force EW capabilities to use in support of each element of decisive action. As they apply the appropriate level of EW effort to support these elements, commanders can seize, retain, and exploit the initiative within the electromagnetic environment.

SUPPORT OF THE WARFIGHTING FUNCTIONS

2-4. Once a commander can seize, retain, and exploit the initiative within the electromagnetic environment, then control becomes possible. Commanders plan, prepare, execute, and assess EW operations to control the electromagnetic spectrum.

2-5. To exercise electromagnetic spectrum control (see paragraph 1-44), commanders effectively apply and integrate EW operations across the warfighting functions: mission command, movement and maneuver, intelligence, fires, sustainment, and protection.

MISSION COMMAND

2-6. The mission command warfighting function develops and integrates those activities enabling a commander to balance the art of command and science of control. EW supports the mission command warfighting function by—

- Protecting the mission command system from the effects of friendly and adversary EW operations.
- Controlling friendly EW systems through—
  - Frequency deconfliction.
  - Asset tracking.

  - Controlling EW effects during execution.
  - Reprogramming of EW systems.
  - Registration of all electromagnetic spectrum emitting devices with the spectrum manager (prior to deployment and when new systems or devices are added to the deployed force).
- Developing EW mission command tools to enhance required coordination between Army and joint EW operations.
- Integrating, coordinating, deconflicting, and synchronizing EW operations through the EW working group (see chapter 3).
- Improving input to the common operational picture, related to the electromagnetic spectrum and EW, which enhances the commander's situational understanding.
- Monitoring and assessing EW operations.

MOVEMENT AND MANEUVER

2-7. The movement and maneuver warfighting function is the related tasks and systems that move and employ forces to achieve a position of relative advantage over the enemy and other threats. Direct fire and close combat is inherent in maneuver. EW enables the movement and maneuver of Army forces by—

- Suppressing and destroying enemy integrated air defenses.
- Denying enemy information systems and information collection sensors.
- Designating target and range finding.
- Protecting friendly forces from effects of friendly and enemy EW.
- Providing lethal and nonlethal effects against enemy combat capability (personnel, facilities, and equipment).
- Providing threat warning and direction finding.
- Using the electromagnetic spectrum to counter improvised explosive devices.
- Providing electromagnetic spectrum obscuration, low observability, and multispectral stealth.

INTELLIGENCE

2-8. The intelligence warfighting function is the related tasks and systems that facilitate understanding the enemy, terrain, and civil considerations. It includes the synchronization of collection requirements with the execution of tactical tasks such as reconnaissance, surveillance, and related intelligence operations. EW enables the intelligence warfighting function by—

- Increasing access for intelligence collection assets (systems and personnel) by reducing antiaccess, antipersonnel, and antisystems threats.
- Increasing friendly forces' abilities to search for, intercept, identify, and locate sources of radiated electromagnetic energy in support of targeting and future operations.
- Increasing friendly forces' abilities in providing threat recognition and threat warning to the force.
- Providing indications and warning of threat emitters and radar.
- Denying and destroying threat information collection systems.

FIRES

2-9. The fires warfighting function is the related tasks and systems that provide collective and coordinated use of Army indirect fires, air and missile defense, and joint fires through the targeting process. The integration and synchronization of cyber electromagnetic activities is a task of this warfighting function. EW supports the fires warfighting function by—

- Detecting and locating surface targets.
- Providing electro-optical-infrared and radio frequency countermeasures.
- Providing electromagnetic deception.
- Providing electromagnetic intrusion.

- Providing electromagnetic jamming.
- Disrupting enemy sensors and command and control nodes.
- Disrupting and degrading enemy infrastructure.
- Destroying targeted enemy systems.

SUSTAINMENT

2-10. The sustainment warfighting function is the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance. EW supports the sustainment warfighting function by—

- Protecting sustainment forces from friendly and adversary use of EW in static or mobile environments.
- Enhancing electromagnetic environment situational awareness through the interception, detection, identification, and location of adversary electromagnetic emissions used to provide indications and warnings. (This information can assist in convoy planning, asset tracking, and targeting of potential threats to sustainment operations.)
- Countering improvised explosive devices to support ground lines of communications (using counter radio-controlled improvised explosive device systems and other means to counter threats triggered through the electromagnetic spectrum, such as lasers).
- Providing spectrum deconfliction and emissions control procedures in support of sustainment control.
- Providing electromagnetic spectrum obscuration, low-observability, and multispectral stealth (for protection during sustainment operations).

PROTECTION

2-11. The protection warfighting function is the related tasks and systems that preserve the force so the commander can apply maximum combat power to accomplish the mission. EW enables the protection warfighting function by—

- Enhancing electromagnetic spectrum situational awareness through the interception, detection, identification, and location of adversary electromagnetic emissions used to provide indications and warnings of threat emitters and radars.
- Denying, disrupting, or destroying electromagnetic-spectrum-triggered improvised explosive devices and enemy air defense systems.
- Deceiving enemy forces.
- Providing electromagnetic spectrum obscuration, low-observability, and multispectral stealth.
- Providing EW countermeasures for platform survivability (air and ground).
- Enabling area denial (lethal and nonlethal) against personnel, vehicles, and aircraft.
- Protecting friendly personnel, equipment, and facilities from friendly and enemy electronic attack, including friendly information systems and information. (This includes the coordination and use of airborne and ground-based electronic attack with higher and adjacent units.)

SUMMARY

2-12. EW supports unified land operations by detecting, denying, deceiving, disrupting, or degrading and destroying enemy combat capabilities and by controlling and protecting friendly use of the electromagnetic spectrum. EW applied across the warfighting functions enables commanders to address a broad set of electromagnetic-spectrum-related targets to gain and maintain an advantage within the electromagnetic spectrum.

This page intentionally left blank.

Chapter 3
Electronic Warfare Organization

This chapter discusses an adaptable organizational design for electronic warfare activities that ensures coordination, synchronization, and integration of electronic warfare into unified land operations. It includes a discussion of key personnel for planning and coordination electronic warfare activities.

ORGANIZATIONAL DESIGN FOR ELECTRONIC WARFARE ACTIVITIES

3-1. Operational challenges across the electromagnetic spectrum are expanding rapidly. As Army electronic warfare (EW) capabilities expand to meet these challenges, the organizational design required to coordinate, synchronize, integrate, and deconflict EW capabilities is centered around the EW element and the EW working group. (Figure 3-1, page 3-2, illustrates the EW coordination organizational framework.) A flexible organizational framework and capable, proficient electronic warfare personnel enable the commander's electronic warfare capability on the battlefield.

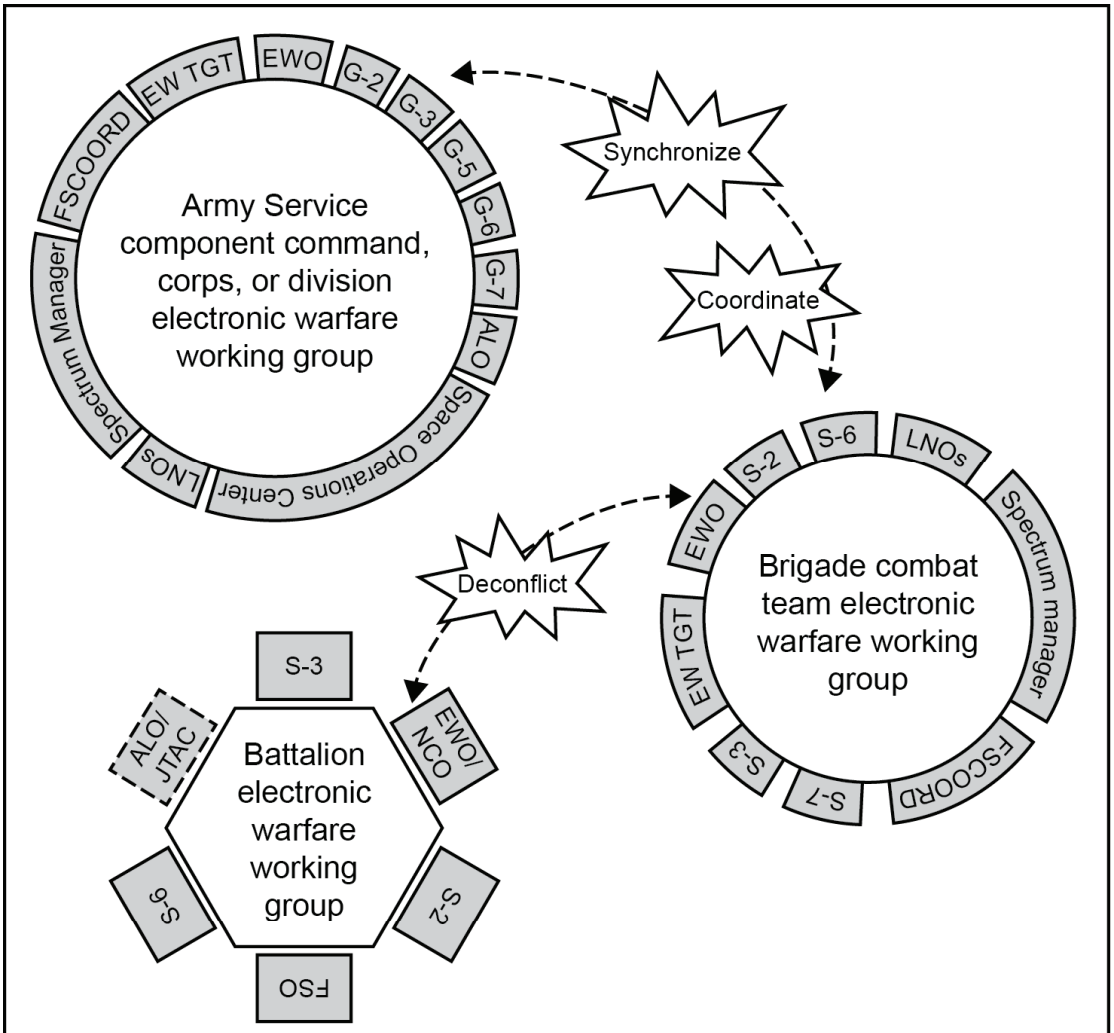
THE ELECTRONIC WARFARE ELEMENT AND ELECTRONIC WARFARE WORKING GROUP

3-2. An EW element is an organic organization in brigade, division, corps, and Army Service component command (ASCC) staffs. The EW element is responsible to the G-3 or S-3 and is located within the mission command cell.

3-3. Primarily, the EW element develops EW plans and monitors EW operations and activities. The EW element plays an important role in requesting and integrating joint air and ground EW assets and manages the organic EW "fight" within the mission command cell. The EW element ensures electromagnetic spectrum management within its specified area of operations and assists the ground commander in coordinating shaping operations. The EW element, usually through the EW working group, leads and facilitates the integration of cyber electromagnetic activities (CEMA).

3-4. A *working group* is a grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function (ATTP 5-0.1). The EW working group, when established, is responsible to the G-3 or S-3 through the mission command cell. An EW working group usually includes representation from across the staff. (Joint doctrine calls this organization the electronic warfare cell [EWC].) The EW working groups depicted in figure 3-1 facilitate the internal (Army) and external (joint) integration, synchronization, and deconfliction of EW actions with mission command, movement and maneuver, intelligence, fires, sustainment, and protection warfighting functions. Normally, EW working groups do not add additional structure to an existing organization. As depicted in figure 3-1, working groups vary in size and composition based on echelon. The EW working group integrates EW actions as part of larger CEMA. (See appendix G for more information on CEMA.)

3-5. Normally, in brigade through ASCC organizations, the senior electronic warfare officer (EWO) heads the EW working group and is accountable to the G-3 or S-3 for integrating EW requirements. Working within the mission command cell, the EWO coordinates directly with the fire support coordinator to integrate EW into the targeting process. This coordination ensures EW is fully integrated with all other effects. Additional staff representation within EW working groups may include a fire support coordinator, a spectrum manager, a space operations officer, and liaison officers as required. Depending on the echelon, liaisons could include joint, interagency, and multinational representatives. When an Army headquarters serves as the headquarters of a joint task force or joint force land component command, the Army headquarters' working group becomes the joint force EWC.



ALO	air liaison officer	JTAC	joint terminal attack controller
EW	electronic warfare	LNO	liaison officer
EWO	electronic warfare officer	NCO	noncommissioned officer
FSCOORD	fire support coordinator	S-2	intelligence staff officer
FSO	fire support officer	S-3	operations staff officer
G-2	assistant chief of staff, intelligence	S-6	signal staff officer
G-3	assistant chief of staff, operations	S-7	inform and influence activities staff officer
G-5	assistant chief of staff, plans		
G-6	assistant chief of staff, signal	TGT	targeting
G-7	assistant chief of staff, inform and influence activities		

Figure 3-1. Electronic warfare coordination organizational framework

3-6. When Army forces are employed as part of a joint or multinational force, they normally have EW representatives supporting higher headquarters' EW coordination organizations. These organizations may include the joint force commander's EW staff or the information operations cell within a joint task force. Sometimes a component EW organization may be designated as the joint EWC. (Chapter 6 discusses joint EW operations in more detail.) The overall structure of the combatant force and the level of EW to be conducted determine the structure of the joint EWC. The organization to accomplish the required EW coordination and functions varies by echelon.

3-7. Regardless of the organizational framework employed, EW working groups perform specific tasks. Table 3-1, page 3-4, details the functions of the EW working groups by echelon, from battalion to ASCC. There is no formal organizational framework for EW at the company level (see paragraph 3-9).

BATTALION-LEVEL STAFFING

3-8. Battalion-level organizations have an EW noncommissioned officer who leads the EW working group and is accountable to the S-3 for integrating EW requirements. This is in contrast to organizations at brigade through ASCC level, which have an EWO and staff organizations to lead planning and coordination. Additional staff representation within EW working groups at the battalion level may include the S-2, S-6, fire support officer, and a joint terminal attack controller, when assigned. The battalion EW working group coordinates battalion EW operations with the brigade combat team EW working group. (See table 3-1, page 3-4 for an outline of the functions of the battalion EW working group.)

COMPANY- LEVEL STAFFING

3-9. At the company level, trained EW personnel holding an additional skill identifier of 1K (CREW Master Gunner Course) or 1J (operational EW operations) perform several tasks. They advise the commander on using EW equipment, track EW equipment status, assist operators in the use and maintenance of EW equipment, and coordinate with higher headquarters EW working groups.

Table 3-1. Functions of electronic warfare working groups

EW Working Group	*Functions*
Division and Above ALO EWO EW Targeting G-2 G-3 G-5 G-6 G-7 G-9 FSCOORD LNOs Spectrum manager Space support officer	• Conduct EW planning in support of theater of operations or combatant command requirements. • Develop and integrate EW actions into operation plans and operational concepts. • Coordinate joint EW training and exercises. • Develop information to support planning (joint restricted frequency list, spectrum management, and deconfliction). • Serve as the joint force land component or JTF EW working group. • When directed, serve as the jamming control authority. • Develop and promulgate EW policies and support higher-level policies. • Identify and coordinate intelligence support requirements for EW. • Plan, coordinate, and assess offensive and defensive EW requirements. • Plan, coordinate, synchronize, deconflict, and assess EW operations. • Maintain current assessment of EW resources available to the commander. • Prioritize EW effects and targets. • Predict effects of friendly and enemy EW. • 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 EW effects within the operations process.
Brigade ALO EWO EW targeting Fires S-2 S-3 S-6 S-7 S-9 LNOs Spectrum manager	• Develop and integrate EW actions into operation plans and exercises. • Support EW policies. • Plan, prepare, execute, and assess EW operations. • Integrate EW intelligence preparation of the battlefield into the operations process. • Identify and coordinate intelligence support requirements for BCT and subordinate units' EW operations. • Assess offensive and defensive EW requirements. • Maintain current assessment of EW resources available to the unit. • Prioritize BCT and subordinate units' EW targets. • Plan, coordinate, and assess friendly EW operations. • Implement friendly electronic security measures (for example, electromagnetic spectrum mitigation and network protection). • When directed, serve as the jamming control authority.
Battalion EW NCO Fires S-2 S-3 S-6 S-9 JTAC	• Support BCT EW requirements to operations and exercises. • Evaluate EW offensive, defensive, and support requirements. • Coordinate EW operations with higher headquarters. • Identify and coordinate intelligence support requirements with higher headquarters. • Execute EW in support of current operations. • Assess EW operations.

ALO air liaison officer
ASCC Army Service component command
BCT brigade combat team
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
J-6 communications system directorate of a joint staff
JTAC joint terminal attack controller
JTF joint task force
LNO liaison officer
NCO noncommissioned officer
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

KEY PERSONNEL FOR PLANNING AND COORDINATING ELECTRONIC WARFARE ACTIVITIES

3-10. Key personnel involved in the planning and coordination of EW activities are—

- G-3 or S-3 staff.
- EWO.
- Fire support coordinator.
- G-2 or S-2 staff.
- G-6 or S-6 staff.
- G-7 or S-7 staff.
- Electromagnetic spectrum manager.
- Liaisons.

G-3 OR S-3 STAFF

3-11. The G-3 or S-3 staff is responsible for the overall planning, coordination, and supervision of EW activities, except for intelligence. The EWO is part of the G-3 or S-3 staff. The G-3 or S-3 staff—

- Plans for and incorporates EW into operation plans and orders, in particular within the fire support plan and the information operations plan (in joint operations).
- Tasks EW actions to assigned and attached units.
- Exercises control over electronic attack, including integration of electromagnetic deception plans.
- Directs electronic protection measures the unit will take based on recommendations from the G-6 or S-6, the EWO, and the EW working group.
- Coordinates and synchronizes EW training with other unit training requirements.
- Issues EW support tasks within the unit information collection plan. These tasks are according to the collection plan and the requirements tools developed by the G-2 or S-2 and the requirement manager.
- Coordinates with the EW working group to ensure planned EW operations support the overall tactical plan.
- Integrates electronic attack within the targeting process.

ELECTRONIC WARFARE OFFICER

3-12. As a member of the G-3 or S-3 staff, the EWO plans, coordinates, and supports the execution of EW and other CEMA (see appendix E). The EWO—

- Leads the EW working group.
- Plans, coordinates, and assesses EW offensive, defensive, and support requirements.
- Supports the G-2 or S-2 during intelligence preparation of the battlefield.
- Supports the fire support coordinator to ensure electronic attack fires are integrated with all other effects.
- Plans, assesses, and implements friendly electronics security 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.
- 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.
- When designated, serves as the jamming control authority (see paragraph 5-11).
- Prepares, submits for approval, and supervises the issuing and implementation of fragmentary orders for EW operations.

G-2 OR S-2 STAFF

3-13. The G-2 or S-2 staff advises the commander and staff on the intelligence aspects of EW. The G-2 or S-2 staff—

- Provides threat data to support programming of unit EW systems and deconfliction of their use by the EW working group.
- Ensures that electronic order of battle requirements is included in the intelligence collection plan.
- Determines enemy EW organizations, disposition, capabilities, and intentions via collection and analysis.
- Determines enemy EW vulnerabilities and high-value targets.
- Assesses effects of friendly EW operations on the enemy.
- Helps prepare the intelligence-related portion of the EW running estimate.
- Provides input to the restricted frequency list (see paragraphs C-9 to C-10) by recommending guarded frequencies.
- Provides updates on the rapid electronic order of battle.
- Maintains appropriate threat EW databases.
- Works with the EW working group to synchronize intelligence collection with EW requirements and deconflict with planned EW actions.
- Ensures deconfliction of EW threat data with friendly electromagnetic spectrum needs.

NETWORK OPERATIONS OFFICER

3-14. The network operations officer (in the G-6 or S-6 staff) coordinates the communications network for the following actions:

- Preparing the electronic protection policy on behalf of the commander.
- Assisting in preparing EW plans and orders.
- Reporting all enemy electronic attack activity detected by friendly communications and electronics elements to the EW working group for counteraction.
- Assisting the unit EWO with resolving EW systems maintenance and communications fratricide problems.

SPECTRUM MANAGER

3-15. The spectrum manager coordinates electromagnetic spectrum 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 or S-6, and applicable host-nation and international agencies as necessary.
- Coordinates the preparation of the 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 reduce electromagnetic interference.
- Coordinates with higher echelon spectrum managers for electromagnetic interference resolution that cannot be resolved internally.

- Assists the EWO in issuing guidance in the unit (including subordinate elements) regarding deconfliction and resolution of interference problems between EW systems and other friendly systems.
- Participates in the EW working group to deconflict friendly electromagnetic spectrum requirements with planned EW operations and intelligence collection.

G-7 OR S-7 STAFF

3-16. The G-7 or S-7 is responsible to the commander for all inform and influence activities. CEMA enable inform and influence activities by undertaking deliberate actions designed to gain and maintain informational advantages in the information environment. Typically, but not solely, these actions occur through cyberspace operations and EW. The G-7 or S-7—

- Ensures that EW is effectively integrated with other inform and influence activities and deconflicts EW actions as required.
- Considers second- and third-order effects of EW on inform and influence activities and proactively plans to enhance intended effects and their consequences.

SUMMARY

3-17. The organizational framework for EW coordination and functions varies by echelon. The necessity to form an EW working group is largely based on the overall structure of the force and the level at which EW is conducted. During the conduct of unified action, other Service EWOs, signals intelligence officers, and EW representatives coordinate with Army EW working groups in the planning, preparation, execution, and assessment of EW operations. Flexible organizational designs ensure adaptable and effective EW support to operations regardless of the force structure.

This page intentionally left blank.

Chapter 4

Electronic Warfare and the Operations Process

This chapter first introduces the operations process. Then it discusses electronic warfare planning. Next, it discusses electronic warfare preparation. Then it discusses electronic warfare execution. It concludes with a discussion of electronic warfare assessment.

THE OPERATIONS PROCESS

4-1. The operations process is commander-centric, informed by the mission command approach to the activities of planning, preparing, executing, and assessing military operations. These activities may occur sequentially or continuously throughout an operation, overlapping and recurring as required (see figure 4-1). The electronic warfare officer (EWO) is actively involved in the operations process. Electronic warfare (EW) planning, preparation, execution, and assessment require collective expertise from operations, intelligence, signal, and mission command staffs. The EWO integrates efforts across the warfighting functions to ensure that EW operations support the commander's objectives.

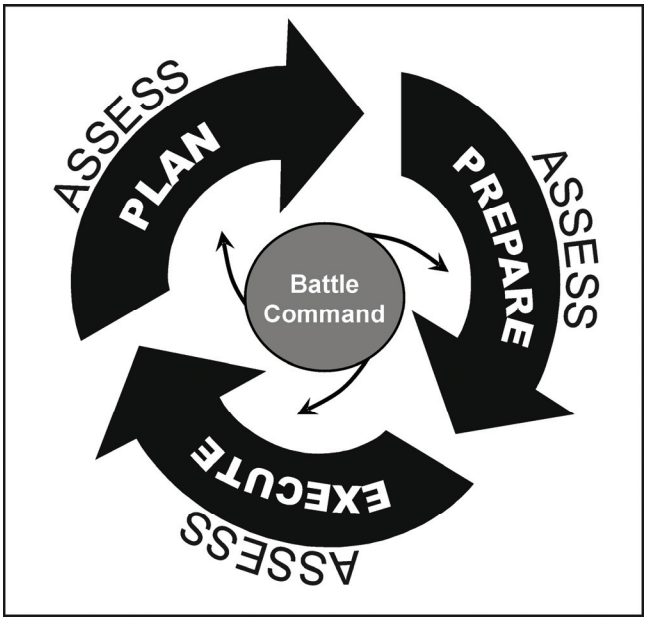


Figure 4-1. The operations process

ELECTRONIC WARFARE PLANNING

4-2. EW planning is based on three main considerations. The first consideration is applying the military decisionmaking process (MDMP). EW planners understand and follow its seven steps. In a time-constrained environment they still follow all seven steps, abbreviating the MDMP appropriately. The second consideration is that EW planners apply integrating processes. They understand how EW actions contribute to operations as a whole. They integrate and synchronize EW actions starting with planning and continuing throughout operations. Finally, EW planners apply specific EW employment considerations.

THE MILITARY DECISIONMAKING PROCESS

4-3. EW planning minimizes fratricide and optimizes operational effectiveness during execution. Therefore, EW planning occurs concurrently with other operational planning during the MDMP. The MDMP synchronizes several processes, including intelligence preparation of the battlefield (IPB), the targeting process (see FM 3-60), and risk management (see FM 5-19). These processes occur continuously during operations.

4-4. Depending on the organizational echelon, the EW staff officer leads EW planning through the EW working group. (The EW working group at echelons above brigade is sometimes referred to as an EW coordination cell.) An EW working group normally has representatives from the G-2 or S-2, G 3 or S-3, G-6 or S-6, and other staff as required. Other staff can include the fire support coordinator or fire support officer, spectrum manager, air liaison officer, space officer, and liaison officers. The next sections (paragraphs 4-5 through 4-30) outline key EW contributions to the processes and planning actions that occur during the seven steps of the MDMP. (ATTP 5-0.1 discusses the MDMP in detail.)

Receipt of Mission

4-5. Commanders begin the MDMP upon receiving or anticipating a new mission. During this first step, commanders issue their initial guidance and initial information requirements or commander's critical information requirements.

4-6. Upon receipt of a mission, the EW staff officer alerts the staff supporting the EW working group. The EWO and supporting staff begin to gather the resources required for mission analysis. Resources might include a higher headquarters operation order or plan, maps of the area of operations, electronic databases, required field manuals and standard operating procedures, current running estimates, and reachback resources (see appendix D). The EWO also provides input to the staff's initial assessment and updates the EW running estimate. As part of this update, the EWO identifies all friendly EW assets and resources and their statuses throughout the operations process. Lastly, the EWO monitors, tracks, and seeks information relating to EW operations to assist the commander and staff.

Mission Analysis

4-7. Planning includes a thorough mission analysis. Both the process and products of mission analysis help commanders refine their situational understanding and determine their restated mission. The EWO and supporting staff of the EW working group contribute to the overall mission analysis by participating in IPB and through the planning actions given in paragraphs 4-8 through 4-13. (Paragraphs 4-34 through 4-39 discuss EW input to IPB during operations.)

4-8. The EWO and working group—

- Determine known facts, status, or conditions of forces capable of EW operations as defined in the commander's planning documents, such as a warning order or operation order.
- Identify EW planning support requirements and develop support requests as needed.
- Determine facts and develop necessary assumptions relevant to EW such as the status of EW capability at probable execution and time available.
- Conduct an initial EW risk assessment and review the risk assessment done by the entire working group.
- Provide an EW perspective when developing the commander's restated mission.
- Help develop the mission analysis briefing for the commander.

4-9. The EWO and working group support the G-2 and S-2 in IPB by—

- Determining the threat's dependence on the electromagnetic spectrum.
- Determining the threat's EW capability.
- Determining the threat's intelligence system collection capability.
- Determining which threat vulnerabilities relate to the electromagnetic spectrum.

- Determining how an operational environment affects EW operations, using the operational variables and mission variables for analysis as appropriate.
- Initiating, refining, and validating information requirements and requests for information.

4-10. The EWO and EW working group determine enemy and friendly decisive points and list their critical capabilities, requirements, and vulnerabilities from an EW perspective. They determine how EW capabilities can best attack an enemy's command and control system. The EWO and EW working group list the critical requirements associated with command and control capability (or command and control nodes) and then identify the critical vulnerabilities associated with the critical requirements. Through this process, the EWO and EW working group help determine which enemy vulnerabilities can be engaged by EW capabilities to produce a decisive outcome.

4-11. The EWO and EW working group identify and list—

- High-value targets that can be engaged by EW capabilities.
- Tasks that EW forces perform according to EW division—electronic attack, electronic warfare support, and electronic protection—in support of the warfighting functions. These include—
  - Specified EW tasks.
  - Implied EW tasks.
- Constraints relevant to EW:
  - Actions EW operations must perform.
  - Actions EW operations cannot perform.
  - Other constraints.

4-12. The EWO and EW working group analyze—

- The commander's intent and mission from an EW perspective.
- Mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations) from an EW perspective.
- The initial EW force structure to determine if forces have sufficient assets to perform the identified EW tasks. (If organic assets are insufficient, they draft requests for support and augmentation.)

4-13. By the conclusion of mission analysis, the EWO and EW working group generate or gather the following products and information:

- The initial information requirements for EW operations.
- A rudimentary command and control nodal analysis of the enemy.
- The list of EW tasks required to support the mission.
- A list of assumptions and constraints related to EW operations.
- The planning guidance for EW operations.
- EW personnel augmentation or support requirements.
- An update of the EW running estimate.
- EW portion or input to the commander's restated mission.

Course of Action Development

4-14. After receiving the restated mission, commander's intent, and commander's planning guidance, the staff develops courses of action (COAs) for the commander's approval. This section (paragraphs 4-15 through 4-29) discusses specific actions the EWO and EW working group perform to support COA development. Figure 4-2, page 4-4, depicts the required input to COA development and identifies the key contributions made by the EWO and EW working group during the process and output stages (center and right of figure 4-2).

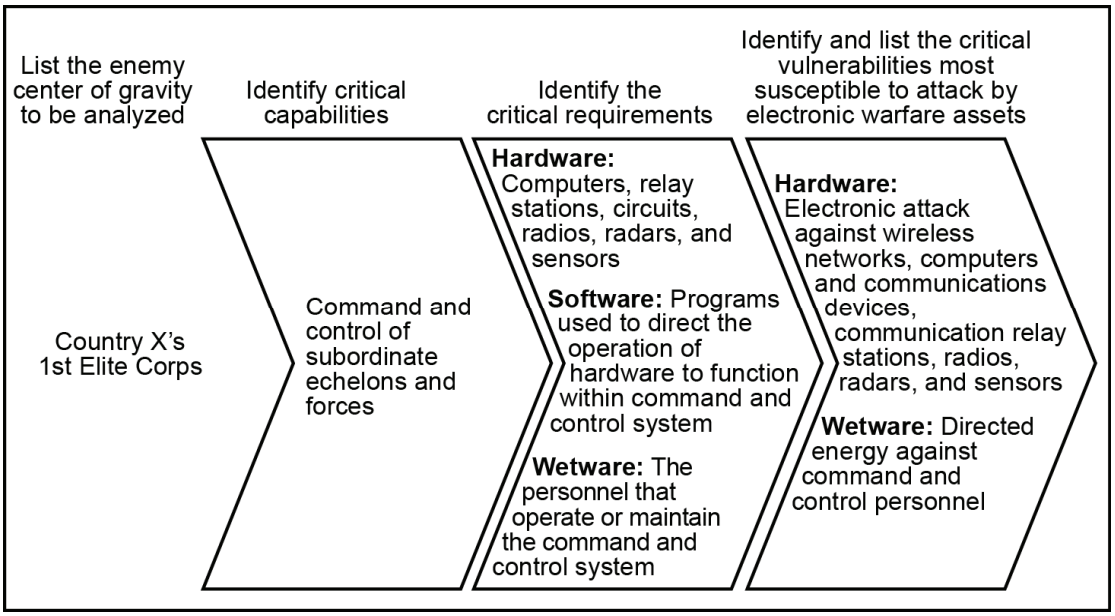


Figure 4-2. Course of action development

4-15. The EWO and EW working group contribute to COA development through the following planning actions:

- Determining which friendly EW capabilities are available to support the operation, including organic and nonorganic capabilities for planning.
- Determining possible friendly and enemy EW operations, including identifying friendly and enemy vulnerabilities.

4-16. Additionally, the EWO and EW working group help develop initial COA options by—

- Identifying COA options that may be feasible based on their functional expertise (while brainstorming of COAs).
- Providing options to modify a COA to accomplish EW tasks more effectively.
- Identifying information (relating to EW options) that may affect other functional areas and sharing that information immediately.
- Identifying the EW tasks required to support the COA options.

4-17. The EWO and EW working group determine the forces required for mission accomplishment by—

- Determining the EW tasks that support each COA and how to perform those tasks based on available forces and capabilities. (They consider available special technical operations capabilities in this analysis.)
- Providing input and support to proposed deception options.
- Ensuring the EW options provided in support of all possible COAs meet the established screening criteria.

4-18. The EWO and EW working group identify EW supporting tasks and their purposes in support of decisive, shaping, and sustaining operations as each COA is developed. These EW tasks include those—

- Focused on defeating the enemy.
- Required to protect friendly force operations.

4-19. The EWO and EW working group assist in developing the COA briefing as required. By the conclusion of COA development, the EWO and EW working group generate or gather the following products and information:

- A list of EW objectives and desired effects related to the EW tasks.
- A list of EW capabilities required to perform the stated EW tasks for each COA.
- The information and intelligence requirements for performing the EW tasks in support of each COA.
- An update to the EW running estimate.

Course of Action Analysis (War-Gaming)

4-20. The COA analysis allows the staff to synchronize the elements of combat power for each COA and to identify the COA that best accomplishes the mission. It helps the commander and staff to—

- Determine how to maximize the effects of combat power while protecting friendly forces and minimizing collateral damage.
- Further develop a visualization of the battle.
- Anticipate battlefield events.
- Determine conditions and resources required for success.
- Determine when and where to apply force capabilities.
- Focus IPB on enemy strengths and weaknesses as well as the desired end state.
- Identify coordination needed to produce synchronized results.
- Determine the most flexible COA.

Paragraphs 4-21 and 4-22 discuss specific actions the EWO and EW working group perform to support COA analysis. (See ATTP 5-0.1 for more information on war-gaming and preparing a synchronization matrix.)

4-21. During COA analysis, the EWO and EW working group synchronize EW actions and assist the staff in integrating EW capabilities into each COA. The EWO and EW working group address how each EW capability supports each COA. They apply these capabilities to associated timelines, critical events, and decision points in the synchronization matrix. During this planning phase, the EWO and EW working group aim to—

- Analyze each COA from an EW functional perspective.
- Recommend any EW task-organization adjustments.
- Identify key EW decision points.
- Provide EW data for the synchronization matrix.
- Recommend EW priority intelligence requirements.
- Identify EW supporting tasks to any branches and sequels.
- Identify potential EW high-value targets.
- Assess EW risks created by telegraphing intentions, allowing time for enemy to mitigate effects, unintended effects of electronic attack, and the impact of asset or capability shortfalls.

4-22. By the conclusion of COA analysis (war-gaming), the EWO and EW working group generate or gather the following products and information:

- The EW data for the synchronization matrix.
- The EW portion of the branches and sequels.
- A list of high-value targets related to EW.
- A list of commander's critical information requirements related to EW.
- The risk assessment for EW operations in support of each COA.
- An update to the EW running estimate.

Course of Action Comparison

4-23. COA comparison starts with all staff analyzing and evaluating the advantages and disadvantages of each COA from their perspectives. The staff presents their findings for the others' consideration. Using the evaluation criteria developed during COA analysis, the staff outlines each COA, highlighting its advantages and disadvantages. Comparing the strengths and weaknesses of the COAs identifies their advantages and disadvantages with respect to each other. (See ATTP 5-0.1 for a further discussion of COA comparison).

4-24. During COA comparison, the EWO and EW working group compare COAs based on the EW-related advantages and disadvantages (see figure 4-3). Typically, planners use a matrix to assist in the COA comparisons. The EWO may develop an EW functional matrix to compare the COAs or to use the decision matrix developed by the staff. Regardless of the matrix used, the evaluation criteria developed before war-gaming are used to compare the COAs. Normally, the chief of staff or executive officer weights each criterion used for the evaluation based on its relative importance and the commander's guidance. (See ATTP 5-0.1 for more information on COA comparison and a sample decision matrix.)

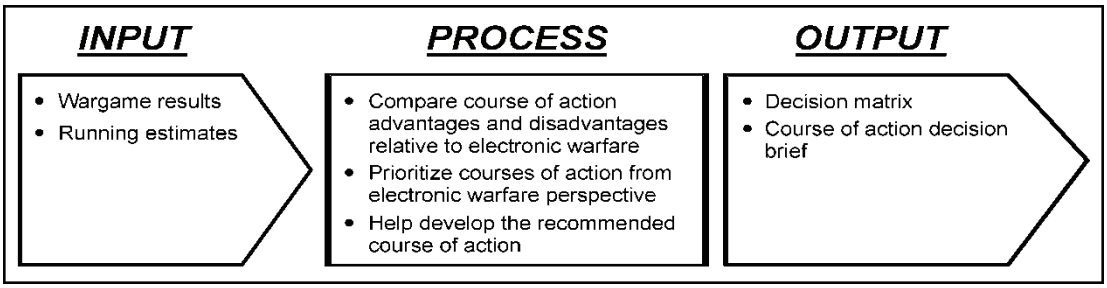


Figure 4-3. Course of action comparison

4-25. By the conclusion of COA comparison, the EWO and EW working group generate or gather the following products and information:

- A list of the pros and cons for each COA, relative to EW.
- A prioritized list of the COAs from an EW perspective.
- An update to the EW running estimate if required.

Course of Action Approval

4-26. The COA approval process has three components. First, the staff recommends a COA, usually in a decision briefing. Second, the commander decides which COA to approve. Lastly, the commander issues the final planning guidance.

4-27. During COA approval, the EWO supports the development of the COA decision briefing and the development of the warning order as required. If possible, the EWO attends the COA decision briefing to receive the commander's final planning guidance. If unable to attend the briefing, the EWO receives the final planning guidance from the G-3 or S-3. The final planning guidance is critical in that it normally provides—

- A refined commander's intent.
- New commander's critical information requirements to support the execution of the chosen COAs.
- Risk acceptance.
- Guidance on priorities for the elements of combat power, orders preparation, rehearsal, and preparation.

4-28. After the COA decision has been made, the EWO and EW working group generate or gather the following products and information:

- An updated command and control nodal analysis of the enemy relevant to the selected COA.
- Required requests for information to refine understanding of the enemy command and control nodal architecture.
- Latest electronic order of battle tailored to the selected COA.
- Any new direction provided in the refined commander's intent.
- A list of any new commander's critical information requirements related to EW.
- The warning order, to assist developing EW operations in support of the operation order or plan.
- Refined input to the initial information collection plan, including—
  - Any additional specific EW information requirements.
  - Updated potential collection assets for the unit's information collection plan.

Orders Production

4-29. Orders production consists of the staff preparing the operation order or plan by converting the selected COA into a clear, concise concept of operations. The staff also provides supporting information that enables subordinates to execute and implement risk controls. They do this by coordinating and integrating risk controls into the appropriate paragraphs and graphics of the order.

4-30. During orders production, the EWO provides the EW operations input for several sections of the operation order or plan. (See appendix A for the primary areas for EW operations input within an Army order or plan. The primary areas for EW input in a joint order, if required, also are shown in appendix A.)

Decisionmaking in a Time-Constrained Environment

4-31. In a time-constrained environment, commanders may alter the steps of the MDMP. In time-constrained conditions, commanders assess the situation, update the commander's visualization, and direct the staff to perform the MDMP activities that support the required decisions. Commanders may direct staffs to shorten the process, and staffs must remain flexible and find ways to save time.

4-32. The EWO and core members of the EW working group meet as a regular part of the unit battle rhythm. However, the EWO calls unscheduled meetings if situations arise that require time-sensitive planning. Regardless of how much they abbreviate the planning process, the EWO and supporting members of the EW working group always—

- Update the EW running estimate in terms of assets and capabilities available.
- Update essential EW tasks with the requirements of the commander's intent.
- Coordinate support requests and intelligence requirements with appropriate staff elements and outside agencies.
- Provide EW input to fragmentary orders through the G-3 or S-3 as necessary to drive timely and effective EW operations.
- Deconflict planned EW actions with other uses of the spectrum, such as communications.
- Synchronize electronic attack and electronic warfare support actions.
- Synchronize other intelligence collection in support of EW requirements.
- Deconflict EW actions specifically with aviation operations.
- Help synchronize and integrate relevant cyber electromagnetic activities through the appropriate staff.

The Integrating Processes and Continuing Activities

4-33. Commanders use several integrating processes and continuing activities to synchronize operations throughout the operations process (see figure 4-4, page 4-8). The EWO ensures EW operations are fully synchronized and integrated within these processes. Other staff supporting the EW working group assist the

EWO. The next sections (paragraphs 4-34 through 4-50) outline some key integrating processes. These processes require EWO involvement throughout the operations process.

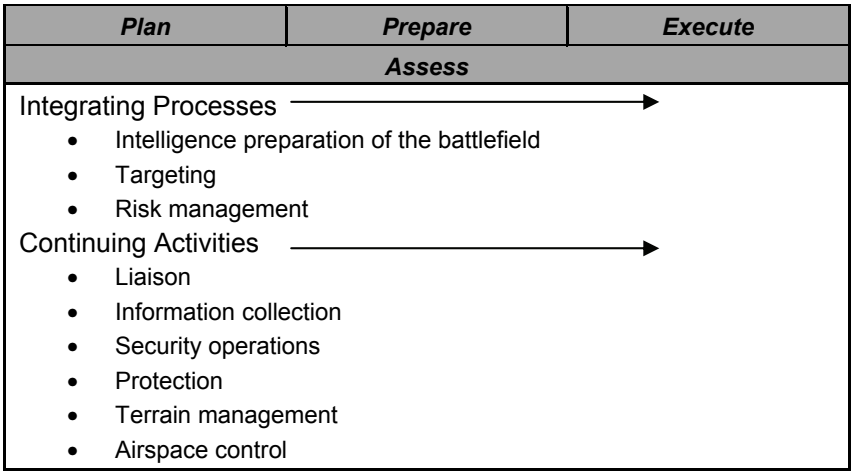


Figure 4-4. Integrating processes and continuing activities

Intelligence Preparation of the Battlefield

4-34. IPB involves systematically and continuously analyzing the threat and certain mission variables (terrain, weather, and civil considerations) in the geographical area of a specific mission. Commanders and staffs use IPB to gain information that supports understanding. The G-2 or S-2 leads IPB planning with participation by the entire staff. This planning activity supports understanding an operational environment, including the options it presents to friendly and adversary forces. Only one IPB planning activity exists within each headquarters; all affected staff cells participate. Paragraphs 4-35 through 4-39 discuss how the EWO and EW working group support IPB during operations.

4-35. In addition to the input provided to the initial IPB (during step 2 of mission analysis), the EWO supports IPB throughout the operations process by providing input related to EW operations. (See figure 4-5, page 4-9.) This input includes, but is not limited to, the following:

- Evaluating an operational environment from an EW perspective.
- Describing how the effects of an operational environment may affect EW operations.
- Evaluating from an EW perspective the threat's capabilities, doctrinal principles, and tactics, techniques, and procedures.
- Determining threat COAs.

4-36. When evaluating an operational environment from an EW perspective, the EWO—

- Determines the electromagnetic environment within the defined physical environment:
  - Area of operations.
  - Area of influence.
  - Area of interest.
- Uses electronic databases to identify gaps.
- Identifies adversary-fixed EW sites, such as electronic warfare support and electronic attack sites.
- Identifies airfields and installations that support, operate, or house adversary EW capabilities.
- In coordination with the G-2 or S-2 and G-6 or S-6, helps identify enemy electromagnetic spectrum usage and requirements within the area of operations and area of interest.

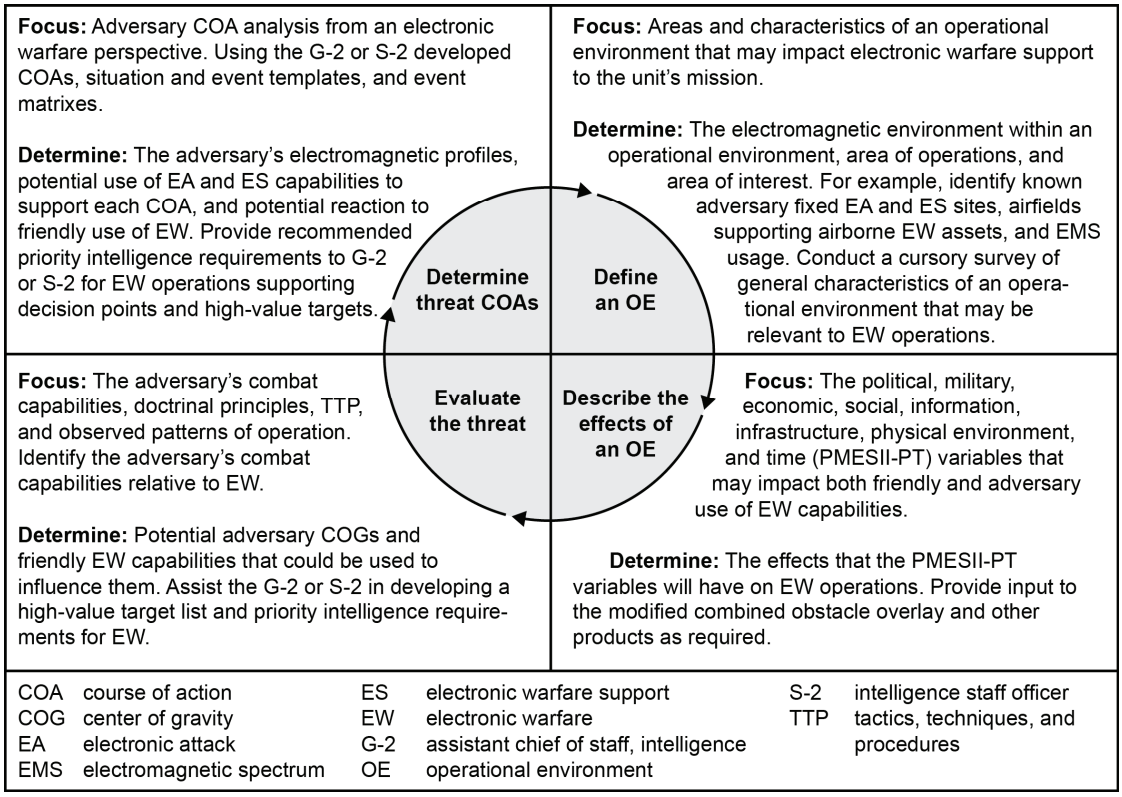


Figure 4-5. Electronic warfare in support of intelligence preparation of the battlefield

4-37. When describing how the variables of an operational environment may impact EW operations, the EWO—

- Focuses on characteristics of both the land and air domains using the factors of observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, and cover and concealment.
- Identifies key terrain that may provide protection for communications and target acquisition systems from exploitation or disruption.
- Identifies how terrain affects line of sight, including effects on both communications and non-communications emitters.
- Evaluates how vegetation affects radio wave absorption and antenna height requirements.
- Locates power lines and their potential to interfere with radio waves.
- Assesses the likely avenues of approach (air and ground), their dangers, and how EW operations could provide support for them.
- If operating within urban terrain, considers how the infrastructure—power plants, power grids, structural heights, and communications and media nodes—may restrict or limit EW capabilities.
- Determines how weather—visibility, cloud cover, rain, and wind—may affect ground-based and airborne EW operations and capabilities (for example, when poor weather conditions prevent airborne EW launch and recovery).
- Assists the G-2 or S-2 with the development of a modified combined obstacle overlay.
- Considers all other relevant aspects of the operational environment that affect EW operations, using the operational variables (PMESII-PT—political, military, economic, social, information, infrastructure, physical environment, and time) and mission variables (METT-TC—mission, enemy, terrain and weather, troops and support available, time available, and civil considerations).

4-38. When evaluating enemy capabilities, the EWO and supporting staff examine doctrinal principles; tactics, techniques, and procedures; and observed patterns of operation from an EW perspective. The EWO—

- Uses the operational and mission variables to help determine the adversary's critical nodes.
- Collects the required data—operational net assessments, electronic order of battle, and electronic databases—to template the command and control critical nodes and the systems required to support and maintain them.
- Assists the G-2 in determining the adversary's EW-related threat characteristics (order of battle) by identifying—
  - Types of communications equipment available.
  - Types of noncommunications emitters.
  - Surveillance and target acquisition assets.
  - Technological sophistication of the threat.
  - Communications network structure.
  - Frequency allocation techniques.
  - Operation schedules.
  - Station identification methods.
  - Measurable characteristics of communications and noncommunications equipment.
  - Command, control, and communications structure of the threat.
  - Tactics, from a communication perspective (such as how the enemy deploys command, control, and communications assets; whether or not communications systems are remote; and the level of discipline in procedures, communications security, and operations security).
  - Electromagnetic deception capabilities.
  - Reliance on active or passive surveillance systems.
  - Electromagnetic profiles of each node.
  - Unique electromagnetic spectrum signatures.
- Assists the G-2 or S-2 in analyzing the center of gravity (identifying its critical system nodes and determining what aspects to engage, exploit, or attack to modify the system's behavior or achieve a desired effect).
- Identifies organic and nonorganic EW capabilities available to achieve desired effects on identified high-value targets.
- Submits initial requests for information describing the intelligence support required for EW operations.
- Obtains the high-value target list, threat templates, and initial priority intelligence requirements list to assist in follow-on EW planning.

4-39. When determining adversary COAs, the EWO—

- Assists the G-2 or S-2 in development of adversary COAs.
- Provides EW input to the situation templates.
- Ensures event templates include EW named areas of interests.
- Assists in providing EW options for target areas of interest.
- Assists in providing EW options to support decision points.
- Provides EW input to the event template and event matrix.

Targeting

4-40. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). A decide, detect, deliver, and assess methodology is used to direct friendly forces to attack the right target with the right asset at the right time. (See figure 4-6.) Targeting provides an effective method to match the friendly force capabilities against targets. Commander's intent plays a critical role in the targeting process. The targeting working group strives to understand the commander's intent and ensure the commander's intended effects on targets are achieved.

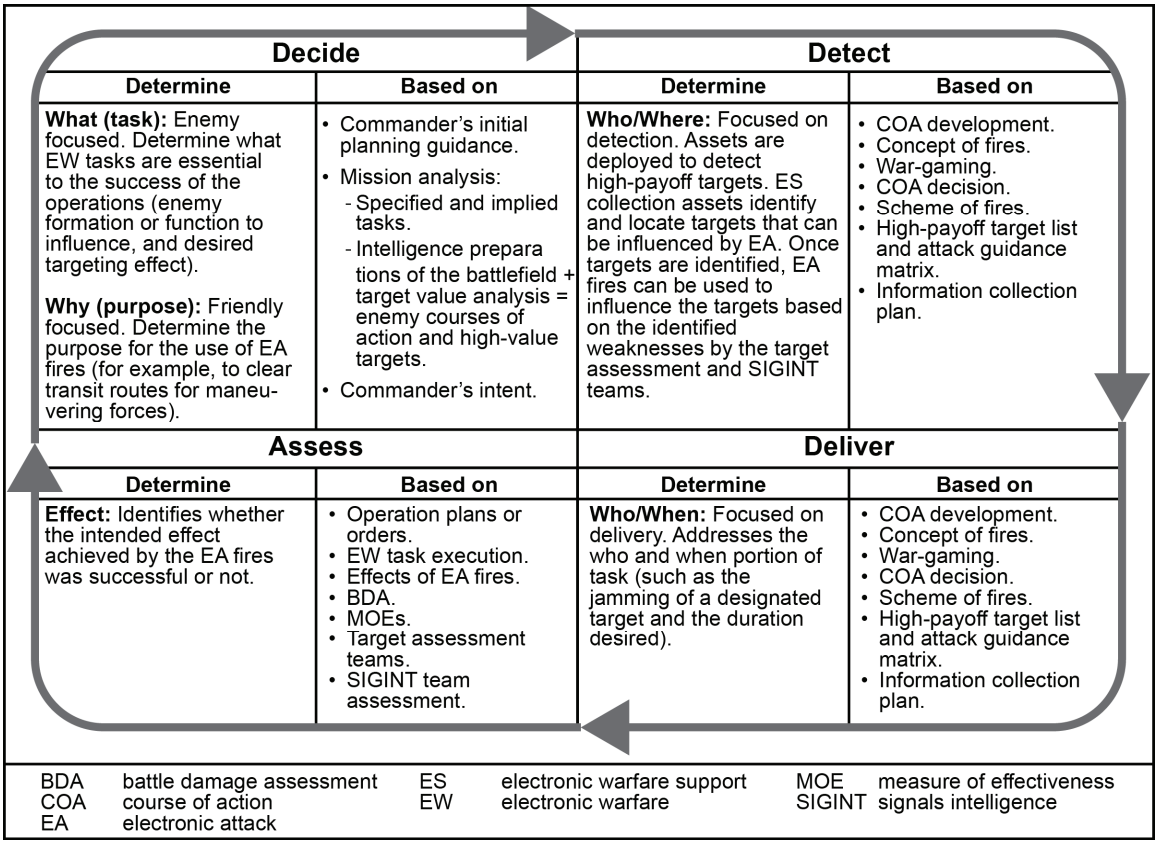


Figure 4-6. Electronic warfare in the targeting process

4-41. An important part of targeting is identifying potential fratricide situations and performing the coordination measures to manage and control the targeting effort positively. The targeting working group and staff incorporate these measures into the coordinating instructions and appropriate annexes of the operation plans and orders. (See ATTP 5-0.1 for detailed information on operation plans and orders. See FM 3-60 for more information on targeting.)

4-42. The EWO thoroughly integrates electronic attack in the targeting process and integrates electronic attack fires into all appropriate portions of the operation plan, operation order, and other planning products. In support of EW targeting, the EWO—

- Helps the targeting working group determine electronic attack requirements against specific high-payoff targets and high-value targets.
- Ensures electronic attack can meet the desired effect (in terms of the targeting objective).
- Coordinates with the signals intelligence staff element through the collection manager to satisfy electronic warfare support and electronic attack information requirements.
- Provides electronic attack mission management through the tactical operations center or joint operations center and the tactical air control party (for airborne electronic attack).

- Provides electronic attack mission management as the jamming control authority (see paragraph 5-11) for ground or airborne electronic attack when designated.
- Determines and requests theater army electronic attack support.
- Recommends to the G-3 or S-3 and the fire support coordinator or fire support officer whether to engage a target with electronic attack.
- Expedites electromagnetic interference reports to the targeting working group.

Decide

4-43. Decide is the first step in the targeting process. This step provides the overall focus for fires, a targeting plan, and some of the priorities for intelligence collection. As part of the staff in the mission command cell, the EWO assists the targeting working group in planning the target priorities for each phase and critical events of the operation. Initially, the targeting working group does not develop electronic attack targets using any special technique or separately from targets for physical destruction. However, as the process continues, these targets are passed through intelligence organizations and further planned using intelligence collection procedures. The planned use of electronic attack is integrated into the standard targeting products (graphic or text-based). Products that involve electronic attack planning may include—

- High-payoff target list.
- Attack guidance matrix.
- Annex D (Fires) of the operation order.

Detect

4-44. Based on what the targeting working group identified as high-payoff targets during the decide step, collection assets are then deployed to detect them. The intelligence enterprise pairs assets to targets based on the collection plan and the current threat situation. When conducting electronic attack tasks, information collection units perform electronic warfare support tasks linked to and working closely with the electronic attack missions. Electronic warfare support units (with support from the target assessment and signals intelligence staff elements) provide the data—location, signal strength, and frequency of the target—to focus electronic attack assets on the intended target. These assets also identify the enemy's command and control system vulnerabilities open to attack by electronic attack assets.

Deliver

4-45. Once friendly force capabilities identify, locate, and track the high-payoff targets, the next step in the process is to deliver fires against those targets. Electronic attack assets must satisfy the attack guidance developed during the decide step. Close coordination between those conducting electronic warfare support and electronic attack is critical during the engagement. The EWO facilitates this coordination and ensures electronic attack fires are fully synchronized and deconflicted with other fires. This officer remains aware of the potential for unintended effects between adjacent units when conducting electronic attack. The EWO continually coordinates with adjacent unit EWOs to mitigate and deconflict these effects during cross-boundary operations. Normally, the G-3, S-3, or fire support coordinator provides requirements and guidance for this coordination and synchronization in the attack guidance matrix, intelligence synchronization matrix, spectrum management plan, and the EW input to the operation plan or operation order annexes and appendixes.

Assess

4-46. Once the target as been engaged, the next step is to assess the engagement's effectiveness. This combat assessment involves determining the effectiveness of force employment during military operations. It consists of three elements:

- Munitions effects assessment.
- Battle damage assessment.
- Re-attack recommendations.

4-47. The first two elements, munitions effects assessment and battle damage assessment, inform the commander on the effects achieved against targets and target sets. From this information, the G-2 or S-2 continues to analyze the threat's ability to further conduct and sustain combat operations (sometimes articulated in terms of the effects achieved against the threat's centers of gravity). The last element involves the assessment and recommendation whether or not to re-attack the targets.

4-48. The assessment of a jamming mission used against an enemy's command and control system is unlike fires that friendly forces can visually observe. The signals intelligence staff element and units executing the electronic attack mission coordinate continuously to assess mission effectiveness. Close coordination between sensor and shooter allows instant feedback on the success or failure of the intended jamming effects. It also can quickly provide the necessary adjustments to produce desired effects.

Risk Management

4-49. Risk management is a process for identifying hazards and controlling risks. Throughout the operations process the EWO uses risk management to mitigate risks associated with all hazards that have the potential impact mission effectiveness. Like targeting, risk management begins in planning and continues through preparation and execution. Risk management consists of the following steps:

- Identify hazards.
- Assess hazards to determine risks.
- Develop controls and make risk decisions.
- Implement controls.
- Supervise and evaluate.

Continuing Activities

4-50. While executing tasks throughout the operations process, commanders and staffs plan for and coordinate continuing activities. The EWO coordinates with the staff to participate in these continuing activities as necessary. The continuing activities address specific EW tasks as needed.

PLANNING REQUIREMENTS

4-51. The EWO ensures that certain planning requirements are completed. Planning requirements include the following:

- Analyzes information requirements and intelligence gaps.
- Evaluates available assets internal and external to the organization and determines gaps in the use of those assets.
- Recommends information collection assets controlled by the organization to collect on the commander's critical information requirements.
- Submits requests for information for adjacent and higher collection support.

The EWO considers all assets—both internal and external to the organization—when determining planning requirements. Effective requirements identify information gaps and the most appropriate assets for collecting information to fill them.

4-52. Planning for information collection begin during mission analysis. Although the G-3 or S-3 lead tasking and information collection, the entire staff, subordinate units, and other unified action partners support it. The staff thoroughly understands, integrates, and synchronizes the information collection plan across all echelons.

4-53. The EWO ensures the information collection plan supports the information requirements related to EW and determined during the planning process. The EWO coordinates these requirements with the signals intelligence staff element through the G-2 or S-2.

ELECTRONIC WARFARE EMPLOYMENT CONSIDERATIONS

4-54. EW employment is based on specific ground-based, airborne, and functional (electronic attack, electronic warfare support, or electronic protection) considerations. The EWO properly articulates EW employment considerations early in the operations process. Each consideration has certain advantages and disadvantages. The staff plans for all of these before executing EW operations.

Ground-Based Electronic Warfare Considerations

4-55. Ground-based EW capabilities support the commander's scheme of maneuver. Soldiers can use ground-based EW equipment when dismounted or on highly mobile platforms. Due to the short-range nature of tactical signals direction finding, electronic attack assets are normally located in the forward areas of the battlefield, with or near forward units.

4-56. Ground-based EW capabilities have certain advantages. They provide direct support to maneuver units (for example, through counter radio-controlled improvised explosive device EW and communications or sensor jamming). Soldiers use ground-based EW capabilities to support continuous operations and to respond quickly to EW requirements of the ground commander. However, to maximize the effectiveness of ground-based EW capabilities, maneuver units must protect EW assets from enemy ground and aviation threats. EW equipment should be as survivable and mobile as the force it supports. Maneuver units must logistically support the EW assets, and supported commanders must clearly identify EW requirements.

4-57. Ground-based EW capabilities have certain limitations. They are vulnerable to enemy attack and can be masked by terrain. They are vulnerable to enemy electromagnetic deceptive measures and electronic protection activities (see paragraphs 1-33 through 1-39). In addition, they have distance or propagation limitations against enemy electronic systems.

Airborne Electronic Warfare Considerations

4-58. While ground-based and airborne EW planning and execution are similar, they significantly differ in their EW employment time. Airborne EW operations are conducted at much higher speeds and generally have a shorter duration than ground-based operations. Therefore, the timing of support from airborne EW assets requires detailed planning.

4-59. Airborne EW requires the following:

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

4-60. Airborne EW capabilities have certain advantages. They can provide direct support to other tactical aviation missions such as suppression of enemy air defenses, destruction of enemy air defenses, and employment of high-speed antiradiation missiles. They can provide extended range over ground-based assets. Airborne EW capabilities can provide greater mobility and flexibility than ground-based assets. In addition, they can support ground-based units in beyond line-of-sight operations.

4-61. Limitations associated with airborne EW capabilities include limited time on station, vulnerability to enemy electronic protection actions, electromagnetic deception techniques, and limited assets (support from nonorganic EW platforms need to be requested). The issue of limited assets is also the result of fixed-wing aircraft being the primary platforms for EW.

Electronic Attack Considerations

4-62. Electronic attack includes both offensive and defensive activities (see paragraphs 1-20 through 1-28 for a list of electronic attack activities). These activities differ in their purpose. Defensive electronic attack protects friendly personnel and equipment or platforms. Offensive electronic attack denies, disrupts, or destroys enemy capability. In either case, certain considerations are involved in planning for employing electronic attack, such as—

- Friendly communications.
- Intelligence collection.
- Other effects.
- Electromagnetic spectrum use by local, nonhostile parties.
- Hostile intelligence collection.
- Persistency of effect.

4-63. The EWO, the G-2 or S-2, the G-3 or S-3, the G-6 or S-6, the spectrum manager, and the G-7 or S-7 coordinate closely to avoid friendly communications interference that can occur when using EW systems on the battlefield. Coordination ensures that electronic attack system frequencies are properly deconflicted with friendly communications and intelligence systems.

4-64. The number of information systems, EW systems, and sensors operating simultaneously on the battlefield makes deconfliction with communications systems a challenge. The EWO, the G-2 or S-2, the G-6 or S-6, and the spectrum manager plan and rehearse deconfliction procedures to ensure they can adjust their use of EW or communications systems quickly.

4-65. Electronic attack operations depend on electronic warfare support and signals intelligence to provide targeting information and battle damage assessment. However, EWOs must keep in mind that not all intelligence collection focuses on supporting EW. If not properly coordinated with the G-2 or S-2 staff, electronic attack operations could inadvertently interrupt intelligence collection by jamming or interfering with a frequency used to collect data on the threat or by jamming an enemy frequency or system that friendly forces are using as a means of collecting data. These conflicts must be avoided, as either type of interruption could significantly deter intelligence collection efforts and their ability to answer critical information requirements. Coordination between the EWO, the fire support coordinator, and the G-2 or S-2 prevents this interference. The EW working group brings known conflicts between intelligence collection and electronic attack efforts to the G-3 or S-3 for resolution.

4-66. Planners consider other efforts that rely on electromagnetic spectrum when planning for electronic attack. For example, military information support operations (formerly known as psychological operations or PSYOP) 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 electronic attack could unintentionally interfere or disrupt such broadcasts if not properly coordinated. To ensure electronic attack does not negatively affect planned operations, the EWO coordinates between fires, network operations, and other functional or integrating cells as required.

4-67. Like any other form of electromagnetic radiation, electronic attack 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 potentially deny the functioning of essential services such as ambulance or firefighters to a local population. EWOs routinely synchronize electronic attack with the other functional or integrating cells responsible for information-related capabilities. In this way, they ensure that electronic attack efforts do not cause fratricide or unacceptable collateral damage to their intended effects.

4-68. The potential for hostile intelligence collection also affects electronic attack. 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 or 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 electronic attack. (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].)

4-69. 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. Aside from antiradiation missiles, the effects of jamming are less persistent than effects achieved by other means. The development of directed-energy weapons may change this dynamic in the future.

Electronic Protection Considerations

4-70. Electronic protection is achieved through physical security, communications security measures, system technical capabilities (such as frequency hopping and shielding of electronics), spectrum management, and emission control procedures. (See paragraphs 1-33 through 1-39 for a list of electronic attack activities.) The EWO and EW working group consider the following functions when planning for electronic protection operations:

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

Vulnerability Analysis and Assessment

4-71. Vulnerability analysis and assessment forms the basis for formulating electronic protection plans. The Defense Information Systems Agency provides a variety of information assurance services, including vulnerability analysis and assessment, that focus on automated information systems and can be useful in this effort.

Monitoring and Feedback

4-72. The National Security Agency/Central Security Service monitors communications security. Its programs focus on telecommunications systems using wire and electronic communications. The programs can support and remediate a command's communications security procedures when required.

Electronic Protection Measures and Their Effects on Friendly Capabilities

4-73. Electronic protection measures include any measure taken to protect the force from hostile electronic attack actions. However, these measures can also limit friendly capabilities or operations. For example, denying a given frequency to counter radio-controlled improvised explosive device EW systems in order to preserve it for a critical friendly information system could leave friendly forces vulnerable to radio-controlled improvised explosive devices. The EWO and the G-6 or S-6 carefully consider these second-order effects when advising the G-3 or S-3 regarding electronic protection measures.

Electronic Warfare Support Considerations

4-74. The distinction between a signals intelligence and an electronic warfare support mission is determined by who tasks and controls the assets, what they are tasked to provide, and the purpose for which they are tasked. Operational commanders task assets to conduct electronic warfare support for immediate threat recognition, targeting, planning future operations, and other tactical actions such as threat avoidance and homing. (See paragraphs 1-29 through 1-32 for a list of electronic warfare support activities.) The EWO coordinates with the G-2 or S-2 to ensure identification of all electronic warfare support needed for planned EW operations and to submit electronic warfare support requests to the G-3 or S-3 for approval by the commander. This ensures that the required collection assets are tasked to provide the electronic warfare support. In cases where planned electronic attack actions may conflict with the G-2 or S-2 intelligence collection efforts, the G-3, S-3, or commander decides which has priority. The EWO and the G-2 or S-2

develop a structured process within each echelon for conducting this intelligence gain-loss calculus during mission rehearsal exercises and predeployment planning.

Electronic Warfare Reprogramming Considerations

4-75. Electronic warfare reprogramming refers to modifying friendly EW or target sensing systems in response to validated changes in enemy equipment and tactics or the electromagnetic environment (see paragraph 1-41 for the complete definition of electronic warfare reprogramming). Reprogramming of EW and target sensing system equipment falls under the responsibility of each Service or organization through its respective electronic warfare reprogramming support programs. Electronic warfare reprogramming includes changes to self-defense systems, offensive weapons systems, and intelligence collection systems. During joint operations, swift identification and reprogramming efforts are critical in a rapidly evolving hostile situation. The key consideration for electronic warfare reprogramming is joint coordination. Joint coordination of Service reprogramming efforts ensures all friendly forces consistently identify, process, and implement reprogramming requirements. During joint operations, electronic warfare reprogramming coordination and monitoring is the responsibility of the joint force commander's EW staff. (For more information on electronic warfare reprogramming, see ATTP 3-13.10).

ELECTRONIC WARFARE PREPARATION

4-76. Preparation consists of activities that units perform to improve their ability to execute an operation. Preparation includes, but is not limited to, plan refinement, rehearsals, information collection, coordination, inspections, and movement. Preparation creates conditions that improve friendly forces' opportunities for success. It facilitates and sustains transitions, including those to branches and sequels.

4-77. During preparation, the EWO and EW working group focus their actions on—

- Revising and refining the EW estimate, EW tasks, and EW in support of the overall plan.
- Rehearsing the synchronization of EW in support of the plan (including integration into the targeting process, procedures for requesting joint assets, procedures for deconfliction, and asset determination and refinement).
- Synchronizing the collection plan and intelligence synchronization matrix with the attack guidance matrix and EW input to the operation plan or order annexes and appendixes.
- Assessing the planned task organization developed to support EW operations, including liaison officers and organic and nonorganic capabilities required by echelon.
- Coordinating procedures with information collection operational elements (such as signals intelligence staff elements).
- Training the supporting staff of the EW working group during rehearsals.
- Completing precombat checks and inspections of EW assets.
- Completing sustainment preparations for EW assets.
- Coordinating with the G-4 or S-4 to develop EW equipment report formats.
- Completing backbriefs by subordinate EW working groups on planned EW operations.
- Refining content and format for the EWO's portion of the operation update assessment and briefing.

ELECTRONIC WARFARE EXECUTION

4-78. 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. Commanders focus their subordinates on executing the concept of operations by issuing their commander's intent and mission orders.

4-79. During execution, the EWO and EW working group—

- Serve as the EW experts for the commander.
- Maintain the running estimate for EW operations.
- Monitor EW 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 EW.
- Maintain direct liaison with the fires and network operations cells to ensure integration and deconfliction of EW operations.
- Coordinate and manage EW taskings to subordinate units or assets.
- Coordinate requests for nonorganic EW.
- Continue to assist the targeting working group in target development and to recommend targets for attack by electronic attack assets.
- Receive, process, and coordinate subordinate requests for EW assets during operations.
- Receive and process immediate support requests for suppression of enemy air defense or EW from joint or multinational forces, and coordinate requests through the fire support officer and fire support coordinator with the battlefield coordination detachment and joint or multinational liaisons.
- Coordinate with the airspace control section on all suppression of enemy air defense or EW missions.
- Provide input to the overall assessment regarding effectiveness of electronic attack missions.
- Maintain, update, and distribute the status of EW assets.
- Validate and disseminate cease-jamming requests.
- Coordinate and expedite electromagnetic interference reports with the analysis and control element for targeting and the spectrum manager for potential deconfliction.
- Perform the jamming control authority function (see paragraph 5-11) for ground-based EW within the area of operations (when designated by the jamming control authority).

ELECTRONIC WARFARE ASSESSMENT

4-80. Assessment is continuously monitoring and evaluating the current situation and the progress of an operation. Commanders, assisted by their staffs, continuously assess the current situation and progress of the operation and compare it with the concept of operations, mission, and commander's intent. Based on their assessment, commanders direct adjustments, ensuring that the operation remains focused on the mission and higher commander's intent.

4-81. Assessment occurs throughout every operations process activity and includes three major tasks:

- Continuously assessing the enemy's reactions and vulnerabilities.
- Continuously monitoring the situation and progress of the operation towards the commander's desired end state.
- Evaluating the operation against measures of effectiveness and measures of performance.

4-82. The EWO and supporting members of the EW working group make assessments throughout the operations process. During planning and preparation, assessments of EW are made during the MDMP, IPB, targeting, information collection synchronization, and risk management integration.

4-83. The EWO, in conjunction with the G-5 or S-5, helps develop the measures of performance and measures of effectiveness for evaluating EW operations during execution. A *measure of performance* is a criterion used to assess friendly actions that is tied to measuring task accomplishment (JP 3-0). A *measure of effectiveness* is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (JP 3-0). In the context of EW, an example of a measure of performance is the percentage of known enemy command and control nodes targeted and attacked by electronic attack means (action) versus the number of enemy command and control nodes that were actually destroyed or rendered inoperable for the desired duration (task accomplishment). Measures of effectiveness are used to determine the degree to which an EW action achieved the desired result. This is normally measured through analysis of data collected by active and passive means. For example, effectiveness is measured by using radar or visual systems to detect changes in enemy weapons flight and trajectory profiles.

4-84. During execution, the EWO and EW working group participate in combat assessments within the targeting process to determine the effectiveness of electronic attack employment in support of operations. Combat assessment consists of three elements: munitions effects assessment, battle damage assessment, and reattack recommendations. (Paragraphs 4-46 to 4-48 discuss combat assessment.)

SUMMARY

4-85. The EWO and staff supporting the EW working group ensure the successful integration of EW capabilities into operations. The EWO leads the EW integration effort throughout the operations process. The effective EWO understands and participates in the applicable integrating processes discussed within this chapter.

This page intentionally left blank.

Chapter 5

Electronic Warfare Coordination, Deconfliction, and Synchronization

This chapter begins by discussing electronic warfare coordination and deconfliction. It concludes with a discussion of synchronization.

COORDINATION AND DECONFLICTION

5-1. Once the commander approves an operation plan or order and preparations are complete, the electronic warfare officer (EWO) and supporting staff turn to coordinating, deconflicting, and synchronizing the electronic warfare efforts. They ensure forces carry out electronic warfare (EW) actions as planned or modify them in response to current operations. A certain amount of EW coordination is part of planning. However, once a plan is approved and an operation begins, the EW staff effort shifts to coordination and deconfliction so units can carry out planned EW actions or modify them to adapt to the dynamics of the operation.

5-2. The EWO and EW working group continuously monitor coordination. This includes general EW coordination across organizations (higher, lower, and adjacent units), coordination of requests for EW activities in support of operations, electromagnetic spectrum management, jamming control authority (see paragraph 5-11), EW asset management, other coordinating actions, and EW deconfliction. Normally, EW personnel on watch in the operations center monitor the coordination. They alert the EWO or other EW personnel to address any required actions.

COORDINATION ACROSS ORGANIZATIONS

5-3. At the joint level, the information operations division of the J-3 performs EW coordination. The EW section of the information operations staff engages in all EW functions. This section performs peacetime contingency planning, completes day-to-day planning and monitoring of routine theater of operations EW activities, and completes crisis action planning for contingencies as part of emergent joint operations. The EW section coordinates closely with other appropriate staff sections and larger joint planning groups as required. (JP 3-13.1 discusses joint EW coordination.)

5-4. In the early stages of contingencies, the joint force commander's EW staff assesses the staffing requirements for planning and execution. This staff also coordinates EW planning and course of action development with the joint force commander's components. Services begin component EW planning and activate their EW working groups per combatant command or Service guidelines. When the scope of a contingency becomes clearer, the command EWO may request that the joint force commander establish a joint electronic warfare cell (EWC). If a joint EWC is formed, it normally requires additional augmentation from the Service or functional components. Depending on the size of the force, EW personnel from the division, corps, or theater army are expected to augment the joint EWC to form a representative EW organization. The senior Army organization's staff EWO anticipates this requirement and prepares to support the augmentation if requested.

5-5. Coordination occurs through EW working groups from theater army level to battalion level. Within Army organizations, the coordination of EW activities occurs horizontally and vertically. At every level, the EW staff officer ensures the necessary coordination. Normally, coordination of EW activities between the Army and joint force air component command flows through the battlefield coordination detachment at the joint air operations center. EW staffs at higher echelons monitor EW activities and resolve conflicts when necessary.

5-6. Normally the senior Army headquarters (the ARFOR) G-3 or S-3 coordinates with external EW organizations, unless direct liaison is authorized at lower echelons. Other components requesting Army EW coordinate their requirements with the EWO located at the ARFOR headquarters or tactical operations center. Often, a liaison from the requesting organization completes these requests. If other Service or functional components have an immediate need for Army EW, they send the request to the operational fires directorate or mission command cell and the senior headquarters EW working group (sometimes referred to as an EW coordination cell) via the Global Command and Control System or Global Command and Control System–Army. In support of external EW coordination, the EW staff officer within the J-3, G-3, or S-3—

- Provides an assessment of EW capabilities to other component operation centers.
- Coordinates preplanned EW operations with other Service components (within prescribed timelines).
- Updates preplanned EW operations in coordination with other components as required.

COORDINATING REQUESTS FOR ELECTRONIC WARFARE ACTIVITIES

5-7. Units requesting electronic attack forward requests to the appropriate EW working group. (See appendix C for the electronic attack request format.) Each EW working group prioritizes the requests and forwards them to the higher headquarters through G-2 or S-2 channels. The commander responsible for the EW assets approves the requests. The EW working group integrates new EW requests into the intelligence synchronization process. If the EW working group approves the new requests, they appear in the requirements tool and the unit information collection plan. The technical data required to support electronic warfare support requests pass via signals intelligence channels within the G-2 or S-2 by classified means.

ELECTROMAGNETIC SPECTRUM MANAGEMENT

5-8. The electromagnetic spectrum is a finite resource. Military forces must manage the limited spectrum allocated to them effectively. Electromagnetic spectrum management (defined in paragraph 1-37) enables electronic systems to perform their functions in the area of operations without causing or experiencing unacceptable interference. Electromagnetic spectrum management deconflicts electronic systems in the area of operations, including electronic protection systems, communications systems, sensors, and weapons systems. Deconfliction efforts must account for electronic systems belonging to unified action partners.

5-9. Electromagnetic spectrum management involves planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. Primarily, it involves determining specific activities that will occur in each part of the available spectrum. For example, some frequencies are assigned to the counter radio-controlled improvised explosive device EW systems operating in the area of operations. These frequencies then are deconflicted with ground tactical communications. The spectrum manager ensures all necessary functions that require use of the electromagnetic spectrum have sufficient allocation of that spectrum to accomplish their purpose. Where a conflict (two or more functions require the same portion of the spectrum) exists, the spectrum manager resolves the conflict through direct coordination. (Figure 5-1, page 5-3, shows the basic procedures the spectrum manager follows to deconflict spectrum use.)

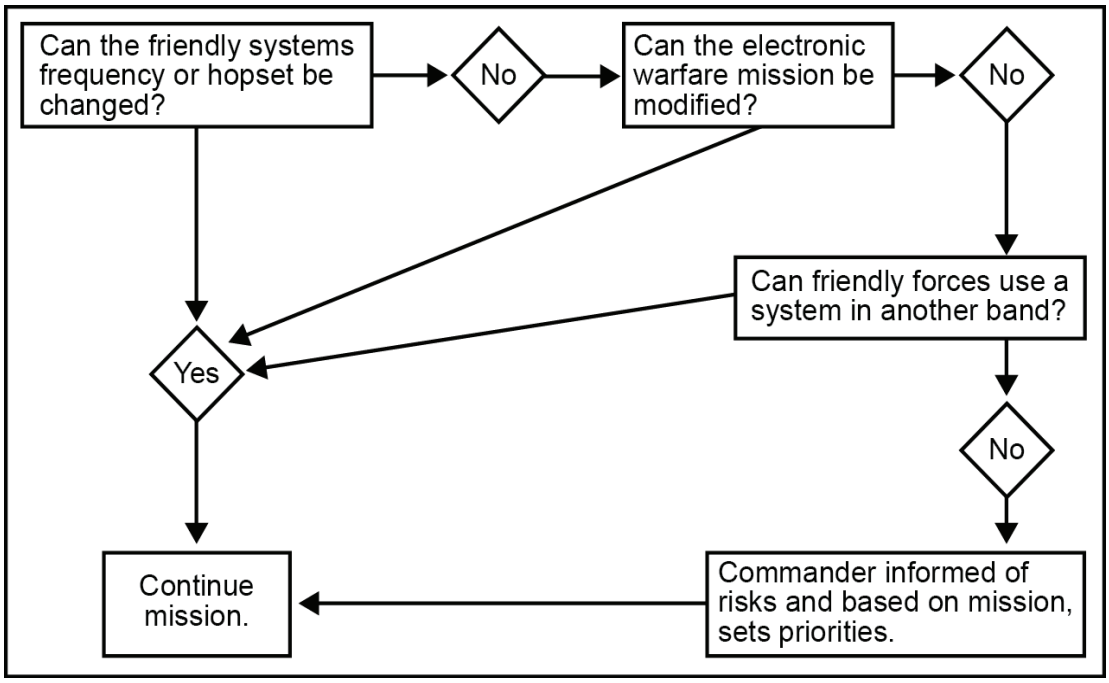


Figure 5-1. Spectrum deconfliction procedures

5-10. The spectrum manager is a member of two groups. First, the manager belongs to the G-6 or S-6 section that has staff responsibility for spectrum management in the unit. The manager also belongs to the unit's EW working group. When conflicts arise regarding spectrum use and allocation that the spectrum manager cannot resolve through direct coordination, the spectrum manager refers them to the G-3 or S-3 for resolution.

JAMMING CONTROL AUTHORITY

5-11. Depending on the situation, an Army headquarters may be designated as the jamming control authority. This authority serves as the senior jamming control authority in the area of operations. It establishes guidance for jamming on behalf of the joint force commander. If designated as the jamming control authority, the senior EW staff officer normally is tasked with the following responsibilities:

- Participating in development of and ensuring compliance with the joint restricted frequency list (see paragraphs C-9 to C-10).
- Validating and approving or denying cease-jamming requests.
- Maintaining situational awareness of all jamming-capable systems in the area of operations.
- Acting as the joint force commander's executive agent for developing intelligence gain-or-loss recommendations when electronic attack or electronic warfare support conflicts occur.
- Coordinating jamming requirements with joint force components.
- Investigating unauthorized jamming events and implementing corrective measures.

(See JP 3-13.1 for further information on jamming control authority.)

ELECTRONIC WARFARE ASSET MANAGEMENT

5-12. Regardless of echelon, the EWO monitors and tracks the organization's EW assets and their status. The EWO makes recommendations to the G-3 or S-3 concerning EW asset allocation and reallocation when required. The EWO monitors and tracks EW asset status within the EW working group and reports this information to higher echelons.

OTHER COORDINATING ACTIONS

5-13. Several coordinating actions must also take place between the EW working groups (at all echelons) and the other planning and execution cells within the headquarters. These actions include—

- Detailed coordination between the EW activities and the intelligence activities supporting an operation.
- Coordination of electronic warfare reprogramming.
- Coordination among EW, cyber electromagnetic activities (CEMA), and inform and influence activities.

Coordination Between Electronic Warfare Activities and Intelligence Activities

5-14. Most of the intelligence effort, before and during an operation, relies on collection activities targeted against various parts of the electromagnetic spectrum. Electronic warfare support depends on the timely collection, processing, and reporting of intelligence and combat information to alert EW operators and other military activities about intelligence collected in the electromagnetic spectrum. The EWO and G-2 or S-2 integrate EW collection priorities and electronic warfare support collection assets into a complete intelligence collection plan. This plan ensures that units maximize the use of scarce intelligence and collection assets to support the commander's objectives.

Coordination of Electronic Warfare Reprogramming

5-15. The EWO and G-2, at division and corps levels, track and coordinate electronic warfare reprogramming input submitted by lower echelons. These officers forward this input to the Army Service component command headquarters for submission to the Army Reprogramming Analysis Team. EWOs promptly submit the input to ensure the command staff completes urgent reprogramming actions for assigned systems. (See ATTP 3-13.10 for detailed procedures for reprogramming EW and target sensing systems.)

Coordination Among Electronic Warfare, Cyber Electromagnetic Activities, and Inform and Influence Activities

5-16. EW working groups coordinate their supporting actions with the elements responsible for inform and influence activities and CEMA. Although EW is one of two lines of effort under CEMA, it also coordinates with inform and influence activities. For example, enemy radio and television broadcasts can be disrupted or replaced with friendly radio and television messages as part of larger military information support operations. Electromagnetic deception capabilities can support and enhance an overall military deception operation.

ELECTRONIC WARFARE DECONFLICTION

5-17. Friendly forces depend on electromagnetic energy and the electromagnetic spectrum to sense, process, store, measure, analyze, and communicate information. This dependency creates the potential for significant interference between various friendly systems. Without proper deconfliction, interference could damage friendly capabilities or lead to operational failure. This is especially true with regard to EW systems. EW deconfliction includes—

- Friendly electromagnetic spectrum use for communications and other purposes (such as navigation systems and sensors) with electronic attack activities (such as counter radio-controlled improvised explosive device EW systems).
- Electronic attack activities with electronic warfare support activities (potential electromagnetic interference of collection assets).
- Electronic attack and electronic warfare support activities with inform and influence activities involving electromagnetic emissions (such as counter radio-controlled improvised explosive device EW systems interfering with a military information support operations radio broadcast).
- Electronic attack activities with host-nation electromagnetic spectrum users (such as commercial broadcasters, local first responders, and law enforcement).

5-18. The forum for deconfliction is the unit's EW working group. As such, the specific composition of the working group may expand to include more than the standard staff representation described in chapter 3. Regardless of echelon, to perform its critical deconfliction function, the EW working group retains knowledgeable representation from and ready access to decisionmakers. The EW working group also retains knowledge of and access to higher headquarters assistance and reachback capabilities available.

SYNCHRONIZATION

5-19. EW, particularly in electronic attack, can produce both intended and unintended effects. Therefore, units thoroughly synchronize its use with other forms of fires and with friendly systems using the electromagnetic spectrum to avoid negative effects such as communications fratricide by jammers. The EWO ensures all EW activities are integrated into the appropriate sections of plans and orders. This officer also synchronizes EW activities for maximum contribution to the commander's desired effects while preventing EW from inhibiting friendly force capabilities. The primary forum for this synchronization is the unit's EW working group. The EWO attends the regular targeting meetings and may also participate (perhaps as a standing member) in other functional or integrating cells and working groups. These may include fires, inform and influence activities, network operations, or future operations. The EWO's participation in these other cells and working groups helps to synchronize EW operations.

SUMMARY

5-20. EW capabilities yield many advantages for the commander. The EW working group's sole purpose is to facilitate the integration, coordination, deconfliction, and synchronization of EW operations to ensure advantages are achieved. This effort requires constant coordination with the unit's other functional cells and working groups. As conflicts are identified during the planning and execution of operations, the EWO and supporting staff coordinate solutions to those conflicts within the EW working group.

This page intentionally left blank.

Chapter 6

Electronic Warfare in Joint and Multinational Operations

This chapter describes the joint and multinational organizational frameworks and guidelines for integrating Army electronic warfare.

JOINT ELECTRONIC WARFARE OPERATIONS

6-1. During joint operations, Services work together to accomplish a mission. In multinational operations, forces of two or more nations work together to accomplish a mission. During both joint and multinational operations, forces operate under established organizational frameworks and coordination guidelines.

6-2. One strength of operating as a joint force is the ability to maximize combat capabilities through unified action. However, the ability to maximize the capabilities of a joint force requires guidelines and an organizational framework that can be used to integrate them effectively. To facilitate integration of Army electronic warfare (EW) operations with joint EW operations, this chapter briefly introduces the guidelines and organizational framework for joint EW operations established in JP 3-13.1.

6-3. Joint task forces are task-organized. Therefore, their composition varies based on the mission. Normally the EW organization within a joint force centers on the—

- Component commands.
- Supporting joint centers.
- Joint force staff.
- Joint force commander's EW staff, joint electronic warfare cell (EWC), or information operations cell.

The supporting centers for EW operations may include the joint operations center, joint intelligence center, joint frequency management office, and joint targeting coordination board.

JOINT FORCE PRINCIPAL STAFF FOR ELECTRONIC WARFARE

6-4. In EW, the principal staff consists of the J-2, J-3, and J-6. The J-2 collects, processes, tailors, and disseminates all-source intelligence for EW. The J-3 has primary staff responsibility for EW activity. This director also plans, coordinates, and integrates joint EW operations with other combat disciplines in the joint task force. Normally, the joint force commander's EW staff or a joint EWC and an information operations cell assist the J-3. The joint force staff network operations director (in the J-6) coordinates electromagnetic spectrum use for information systems with electromagnetic-dependent weapons systems used by the joint force. The information operations officer is the principal information operations advisor to the J-3. This officer is the lead planner for integrating, coordinating, and executing information operations. The command electronic warfare officer (EWO) is the principal EW planner on the J-3 staff. This officer coordinates with the information operations cell to integrate EW operations fully with other information operations core, supporting, and related capabilities (see JP 3-13.1 for further information).

JOINT FORCE COMMANDER'S ELECTRONIC WARFARE STAFF

6-5. A joint force commander's EW staff supports the joint force commander in planning, coordinating, synchronizing, and integrating joint force EW operations. The joint force commander's EW staff ensures that joint EW capabilities support the joint force commander's objectives. The joint force commander's EW staff is an element within the J-3. It consists of representatives from each component of the joint force. An EWO appointed by the J-3 leads this element. The joint force commander's EW staff includes representatives from the J-2 and J-6 to facilitate intelligence support and EW frequency deconfliction.

6-6. On many joint staffs, the intra-staff coordination previously accomplished through a joint force commander's EW staff is performed by an information operations cell or similar organization. An information operations cell, if established, coordinates EW activities with other information operations activities to maximize effectiveness and prevent mutual interference. If both a joint force commander's EW staff and an information operations cell exist, a joint force commander's EW staff representative may be assigned to the information operations cell to facilitate coordination. (For more information about the organization and procedures of the joint information operations cell, see JP 3-13.)

JOINT ELECTRONIC WARFARE CELL

6-7. The decision to form a joint EWC depends on the anticipated role of EW in an operation. When EW is expected to play a significant role in the joint force commander's mission, a Service component command's EW coordination organization may be designated as the joint EWC to handle the EW aspects of the operation. The joint EWC may be part of the joint force commander's staff, be assigned to the J-3 directorate, or remain within the designated Service component commander's structure. The joint EWC plans operational-level EW for the joint force commander. (JP 3-13.1 discusses the joint EWC in more detail.)

JOINT TASK FORCE COMPONENT COMMANDS

6-8. Joint task force component commanders exercise operational control of their EW assets. Each component is organized and equipped to perform EW tasks in support of its basic mission and to provide support to the joint force commander's overall objectives. If a component command (Service or functional) is designated to stand up a joint EWC, it executes the responsibilities and functions outlined in JP 3-13.1.

6-9. A major consideration for standing up a joint EWC at the component command level is access to a special compartmented information facility to accomplish the cell's required coordination functions. A joint EWC should have special technical operations personnel cleared to coordinate and deconflict special technical operations issues. Special technical operations are associated with the planning and coordination of advanced special programs and the integration of new capabilities into operational units.

6-10. Under current force structure, the special technical operations requirement limits the activation of a joint EWC to organizations at corps and above levels. Organizations below corps level require significant joint augmentation to meet the special technical operations requirement.

JOINT FREQUENCY MANAGEMENT OFFICE

6-11. Joint policy tasks each geographic combatant commander to establish a structure to manage electromagnetic spectrum use and establish procedures that support ongoing operations. This structure must include a joint frequency management office. The joint frequency management office may be assigned from the supported combatant commander's J-6 staff, from a component's staff, or from an external command such as the Joint Spectrum Center (see paragraph 7-8). The joint frequency management office coordinates the information systems use of the electromagnetic spectrum, frequency management, and frequency deconfliction. The joint frequency management office develops the frequency management plan and makes recommendations to alleviate mutual interference.

6-12. The G-6 or S-6 coordinates the Army's use of the electromagnetic spectrum, frequency management, and frequency deconfliction with the joint frequency management office through the network operations cell. If established, coordination with the joint spectrum management element is required. (See figure 6-1, page 6-3.)

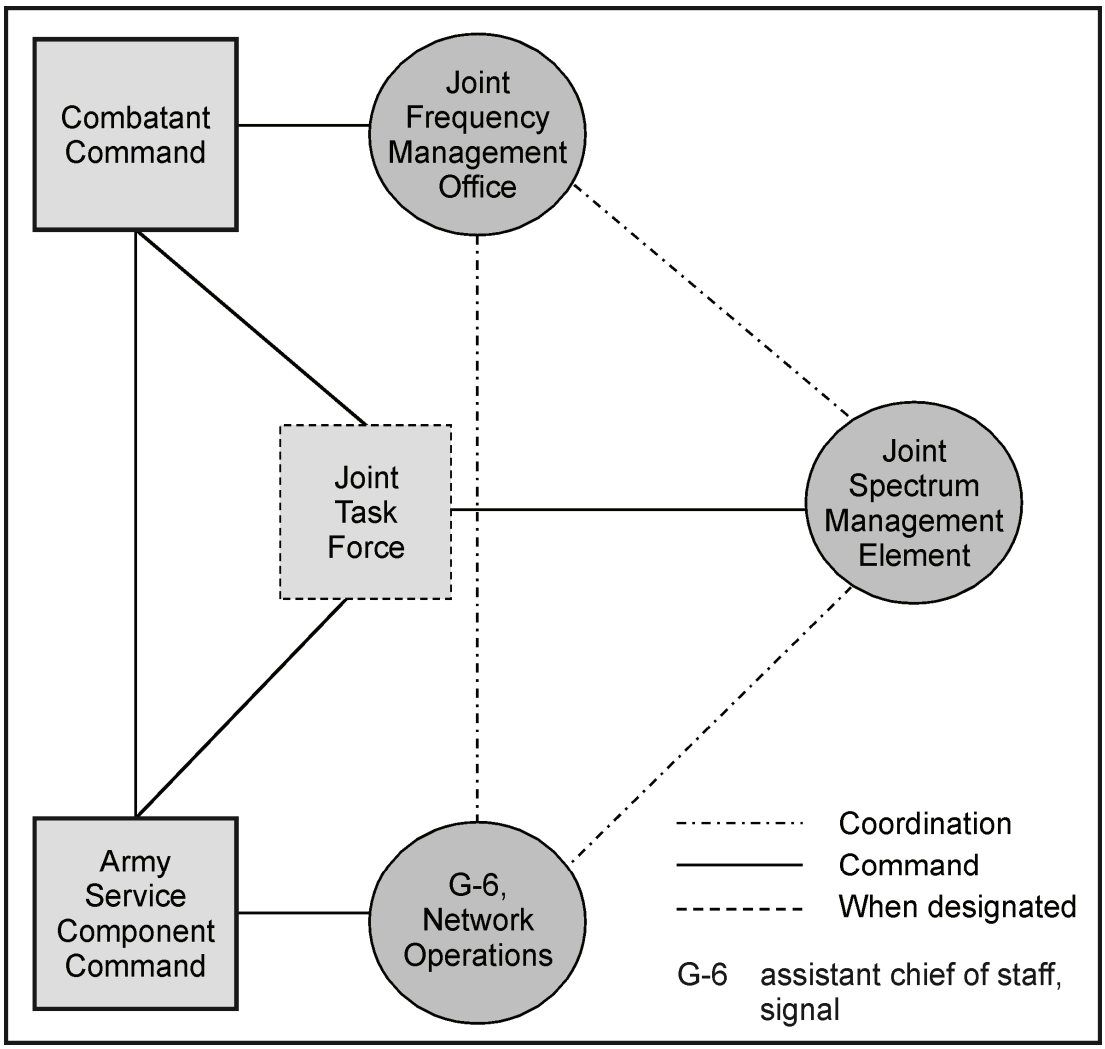


Figure 6-1. Joint frequency management coordination

JOINT INTELLIGENCE CENTER

6-13. The joint intelligence center is the focal point for the intelligence structure supporting the J-2. Directed by the J-2, the joint intelligence center communicates directly with component intelligence agencies and monitors intelligence support to EW operations. This center can adjust intelligence gathering to support EW missions. Within the G-2, EW requests for support are coordinated through the requirement cell and then forwarded to the requirements division within the joint intelligence center. (See figure 6-2, page 6-4.)

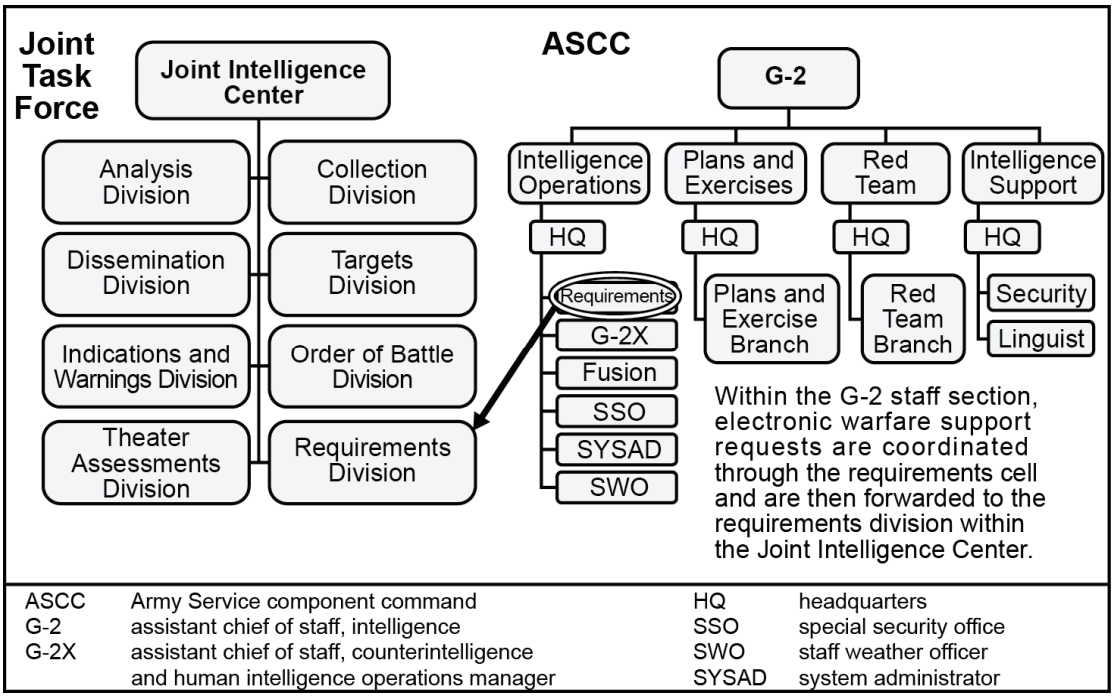


Figure 6-2. Electronic warfare request coordination

6-14. The composition and focus of each joint intelligence center varies by theater of operations. However, each can perform indications and warnings as well as collect, manage, and disseminate current intelligence. Through the joint intelligence center, the Army Service component headquarters (the ARFOR) coordinates support from the Marine Corps, Navy, and Air Force and national, interagency, and multinational sources. In addition to its other functions, the joint intelligence center coordinates the acquisition of national intelligence for the joint task force and the combatant command's staff.

JOINT TARGETING COORDINATION BOARD

6-15. The joint targeting coordination board focuses on developing broad targeting priorities and other targeting guidance in accordance with the joint force commander's objectives as they relate operationally. The joint targeting coordination board remains flexible enough to address targeting issues without becoming overly involved in tactical-level decisionmaking. Briefings conducted at the joint targeting coordination board focus on ensuring that intelligence, operations (by all components and applicable staff elements), fires, and maneuver are on track, coordinated, and synchronized. (For further information on the joint targeting coordination board, see JP 3-60.)

MULTINATIONAL ELECTRONIC WARFARE OPERATIONS

6-16. EW is an integral part of multinational operations. U.S. planners integrate U.S. and multinational EW capabilities into a single, integrated EW plan. U.S. planners provide multinational forces with information concerning U.S. EW capabilities and provide them EW planning and operational support. However, the planning of multinational force EW is difficult due to security issues, differences in levels of training, language barriers, and terminology and procedural issues. U.S. and North Atlantic Treaty Organization (NATO) EW doctrine provide commonality and a framework for using EW in NATO operations.

MULTINATIONAL FORCE COMMANDER

6-17. The multinational force commander provides guidance for planning and executing EW operations with support from the joint EWC. The joint EWC is located at multinational force headquarters. An

information operations cell may also be established to coordinate all information operations activities, including related EW activities.

JOINT OPERATIONS STAFF SECTION

6-18. Within the multinational staff, the joint operations section has primary responsibility for planning and integrating EW activities. A staff EWO is designated with specific responsibilities. These include integrating multinational augmentees, interpreting or translating EW plans and procedures, coordinating appropriate communications connectivity, and integrating multinational force communications into a joint restricted frequency list (see paragraphs C-9 to C-10).

MULTINATIONAL ELECTRONIC WARFARE CELL

6-19. In multinational operations, the multinational force commander uses joint EWC as the mechanism for coordinating EW resources within the area of operations. This cell is an integral part of the multinational joint force headquarters J-3 staff, at whatever level is appropriate. It provides an effective means of coordinating all EW activities by the multinational force. The multinational force joint EWC plans and coordinates all theater of operations EW activities in close liaison with the J-2, J-5, and J-6.

ELECTRONIC WARFARE MUTUAL SUPPORT

6-20. EW mutual support refers to the timely exchange of EW information to make the best use of the available resources. For NATO operations, it is facilitated by the use of a common reference database called the "NATO Emitter Database." Close coordination is required when working with non-NATO partners who do not have access to common databases. EW mutual support procedures developed during EW planning include—

- A review of friendly and enemy information data elements that may be exchanged.
- Mechanisms leading to the exchange of data during peace, crisis, and war.
- Development of peacetime exercises to practice the exchange of data.
- Establishment of EW points of contact with adjacent formations and higher and subordinate headquarters for planning purposes, regardless of whether EW resources exist or not.
- Initial acquisition and maintenance of multinational force EW capabilities.
- Exchange of EW liaison teams equipped with appropriate communications.
- Establishment and rehearsal of contingency plans for the exchange of information on friendly and enemy forces.
- Development of communications protocols in accordance with the appropriate NATO standardization agreements (STANAGs).
- Provision of secure, dedicated, and survivable communications.

OTHER CONSIDERATIONS FOR COORDINATION DURING MULTINATIONAL OPERATIONS

6-21. EW in multinational operations addresses other considerations. Soldiers must consider—

- Exchange of EW information.
- Exchange of signals intelligence information.
- Exchange of the electronic order of battle.
- Electronic warfare reprogramming.

6-22. Army forces participating in multinational EW operations exchange EW information with other forces. Effective Army forces help develop joint information exchange protocols and use those protocols for conducting operations.

6-23. Exchanging signals intelligence information requires care to avoid violating signals intelligence security rules. The policy and relationship between EW and signals intelligence within NATO are set out in a NATO Military Committee document (refer to chapter 5 of JP 3-13.1).

6-24. In peacetime, before forming a multinational force, the exchange of electronic order of battle information is normally achieved under bilateral agreement. During multinational operations, a representative of the joint EWC, through the theater of operations joint analysis center or the joint intelligence center, ensures the maintenance of an up-to-date electronic order of battle. The inclusion of multinational forces is based on security and information exchange guidelines agreed upon by the participating nations.

6-25. Electronic warfare reprogramming is a national responsibility. However, the joint EWC remains aware of reprogramming efforts being conducted within the multinational force. (ATTP 3-13.10 guides the Army's reprogramming effort.)

SUMMARY

6-26. Every joint or multinational operation is uniquely organized to accomplish the mission. Army EWOs integrate EW forces and capabilities with the organizations outlined in this chapter. To coordinate Army EW operations with joint and multinational forces, Army EWOs fully understand the organizational frameworks, policies, and guidelines established for joint and multinational EW operations.

Chapter 7

Electronic Warfare Agencies and Centers

This chapter discusses the agencies and centers of electronic warfare. It first describes integration with other Service electronic warfare capabilities. It then discusses external support agencies and centers. The chapter concludes with a discussion of the United States Cyber Command.

INTEGRATION WITH SERVICE ELECTRONIC WARFARE CAPABILITIES

7-1. Each Service specializes and maintains in certain electronic warfare (EW) capabilities to support operational requirements. Hence, the conduct of EW operations requires joint interdependence. This complex interdependence extends beyond the traditional Service capabilities. It includes national agencies—such as the Central Intelligence Agency, National Security Agency/Central Security Service, and Defense Intelligence Agency—that constantly seek to identify, catalog, and update the electronic order of battle of enemies and adversaries. To support the joint force commander, the subject matter expertise and unique capabilities provided by each Service, agency, and branch or proponent are integrated with all available EW capabilities.

7-2. During operations, the Army depends on organic and nonorganic EW capabilities from higher echelons, joint forces, and national agencies. Army EW planners leverage all available EW capabilities to support Army operations.

EXTERNAL SUPPORT AGENCIES AND CENTERS

7-3. Army EW planners routinely use and receive support from external organizations to assist in planning and integrating EW operations. Support from these organizations may include personnel augmentation, functional area expertise, technical support, and planning support.

DEFENSE INFORMATION SYSTEMS AGENCY

7-4. The Defense Information Systems Agency is a combat support agency. It plans, develops, fields, operates, and supports command, control, communications, and information systems. These systems serve the President, the Secretary of Defense, the Joint Chiefs of Staff, the combatant commanders, and other Department of Defense (DOD) components.

JOINT COMMUNICATIONS SECURITY MONITOR ACTIVITY

7-5. The joint communications security monitor activity was created in 1993 by a memorandum of agreement between the Services' operations deputies, directors of the joint staff, and the National Security Agency/Central Security Service. The joint communications security monitor activity monitors (collects, analyzes, and reports) communications security of DOD telecommunications and automated information systems as well as related noncommunications signals. It aims to identify potentially exploitable vulnerabilities and to recommend countermeasures and corrective actions. The joint communications security monitor activity supports real world operations, joint exercises, and DOD systems monitoring.

JOINT INFORMATION OPERATIONS WARFARE CENTER

7-6. The Joint Information Operations Warfare Center (JIOWC) is subordinate to United States Strategic Command (USSTRATCOM). The JIOWC consists of several directorates including the EW directorate. The JIOWC integrates joint information operations, including EW, into military plans, exercises, and operations. It is a valuable resource for commanders during the planning and execution of joint information operations. It deploys information operations planning teams when the commander of USSTRATCOM approves a request for support. The JIOWC delivers tailored, highly skilled support and sophisticated models and simulations to joint commanders and provides information operations expertise in joint exercises and contingency operations.

7-7. The EW directorate provides specialized expertise in EW. It is an innovation center for existing and emerging EW capabilities and tactics, techniques, and procedures via a network of units, laboratories, test ranges, and academia. The EW directorate manages, as the joint staff's executive agent and technical advisor, U.S. participation in the "NATO Emitter Database" described in paragraph 6-19. The JIOWC also has electronic warfare reprogramming oversight responsibilities for the joint staff. This oversight includes organizing, managing, and exercising joint aspects of electronic warfare reprogramming and facilitating the exchange of joint electronic warfare reprogramming data. The actual reprogramming of equipment, however, is a Service responsibility.

JOINT SPECTRUM CENTER

7-8. The Joint Spectrum Center is a field office within the Defense Spectrum Organization under the Defense Information Systems Agency. Personnel in this center are experts in electromagnetic spectrum planning, electromagnetic compatibility and vulnerability, electromagnetic environmental effects, information systems, modeling and simulation, operations support, and system acquisition. The Joint Spectrum Center provides all services for the electromagnetic spectrum to combatant commands, Services, and other government agencies. It deploys teams in support of the combatant commanders and serves as the DOD focal point for supporting spectrum supremacy aspects of information operations. It assists Soldiers in developing and managing the joint restricted frequency list and helps resolve operational interference and jamming incidents (see paragraphs C-9 through C-10).

JOINT WARFARE ANALYSIS CENTER

7-9. The Joint Warfare Analysis Center is a Navy-sponsored joint command under the J-3. This center assists the Chairman of the Joint Chiefs of Staff and combatant commanders in preparing and analyzing joint operation plans. It provides analysis of engineering and scientific data and integrates operational analysis with intelligence.

MARINE CORPS INFORMATION TECHNOLOGY AND NETWORK OPERATIONS CENTER

7-10. The Marine Corps Information Technology and Network Operations Center is the Marine Corps' enterprise network operations center. The Marine Corps Information Technology and Network Operations Center is the nerve center for the central operational direction and configuration management of the Marine Corps enterprise network. It is co-located with the Marine Corps forces computer network defense, the component to the joint task force for computer network operations, and the Marine Corps computer incident response team. These relationships provide a strong framework for integrated network management and defense.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

7-11. The National Security Agency/Central Security Service is America's cryptologic organization. This organization protects U.S. government information systems and produces foreign signals intelligence information. Executive Order (EO) 12333 describes the responsibility of the National Security Agency/Central Security Service in more detail. The resources of National Security Agency/Central Security Service are organized for two national missions:

- The information assurance mission is to protect U.S. vital national security information and systems from theft or damage by others.
- The signals intelligence mission is to gather information that adversaries of the United States wish to keep secret.

7-12. The Director, National Security Agency/Central Security Service is the principal signals intelligence and information security advisor to the Secretary of Defense, the Director of National Intelligence, and the Chairman of the Joint Chiefs of Staff. The Director, National Security Agency/Central Security Service provides signals intelligence support to combatant commanders and others in accordance with their expressed requirements.

UNITED STATES CYBER COMMAND

7-13. United States Cyber Command fuses cyberspace operations and plans for Department of Defense (DOD). It coordinates, integrates, synchronizes, and conducts activities to lead day-to-day defense and protection of DOD information networks. It coordinates DOD support to military missions and directs the operations and defense of specified DOD information networks. It conducts military cyberspace operations, when directed.

7-14. United States Cyber Command centralizes command of cyberspace operations, strengthens DOD cyberspace capabilities, and integrates and bolsters DOD's cyber expertise. It helps DOD provide reliable information and communications networks, counter cyberspace threats, and ensure access to cyberspace. It also supports U.S. forces by protecting information systems and the cyberspace infrastructure supporting weapons systems platforms from disruptions, intrusions, and attacks.

SUMMARY

7-15. This chapter provides a sampling of available joint and Service EW capabilities, activities, and agencies that support ground force commanders in unified land operations. To leverage these capabilities for EW support, Army EW officers acquire a working knowledge of the capabilities available and the procedures for requesting support. Appendix D provides additional information on available tools and resources related to EW.

This page intentionally left blank.

Appendix A

Electronic Warfare Input to Operation Plans and Orders

This appendix discusses electronic warfare input to Army and joint plans and orders.

ARMY OPERATION PLANS AND ORDERS

A-1. Electronic warfare (EW) information is required for Army operation plans and orders. (ATTP 5-0.1 provides doctrine on plans and orders.) Under the current operation order format, EW information is provided in Annex D (Fires), Appendix 7 (Cyber electromagnetic activities) base order or plan (see figure A-1, pages A-1 through A-3):

- Sub-subparagraph e (Scheme of Fires) to paragraph 3 (Execution).
- Annex D (Fires):
  - Sub-subparagraph (4) (Electronic Warfare Operations) to subparagraph c (Scheme of Air Support) to paragraph 3 (Execution).
  - Subparagraph e (Scheme of cyber electromagnetic activities) to paragraph 3 (Execution).
  - Appendix 7 (Cyber electromagnetic activities).

[CLASSIFICATION]

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

ANNEX D (FIRES) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

(U) References: *Add any specific references to electronic warfare, if needed.*

(U) Time Zone Used Throughout the Plan/Order: *Nothing specific to electronic warfare is needed.*

1. (U) Situation. *Include information affecting fires that paragraph 1 of the OPLAN or OPORD does not cover or that needs expansion.*

a. (U) Area of Interest. *Nothing specific to electronic warfare is needed.*

b. (U) Area of Operations. *Nothing specific to electronic warfare is needed.*

c. (U) Enemy Forces. *Identify the vulnerabilities of enemy information systems and electronic warfare systems. Identify the enemy capability to interfere with accomplishment of the electronic warfare mission.*

d. (U) Friendly Forces. *Identify friendly electronic warfare assets and resources that affect electronic warfare planning by subordinate commanders. Identify friendly forces with which subordinate commanders may operate. Identify potential conflicts within the friendly electronic warfare, especially if conducting joint or multinational operations. Identify and deconflict methods and priority of spectrum distribution.*

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. *Nothing specific to electronic warfare is needed.*

[page number]
[CLASSIFICATION]

Figure A-1. Sample operation plan for Annex D

[CLASSIFICATION]

ANNEX D (FIRES) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

f. (U) Civil Considerations. *Nothing specific to electronic warfare is needed.*

g. (U) Attachments and Detachments. *List the electronic warfare assets that are attached or detached. List the electronic warfare resources available from higher headquarters.*

h. (U) Assumptions. *Nothing specific to electronic warfare is needed.*

2. (U) Mission. *State how electronic warfare will support the commander's objectives.*

3. (U) Execution.

a. (U) Scheme of Fires. *Nothing specific to electronic warfare is needed.*

b. (U) Scheme of Field Artillery Support. *Nothing specific to electronic warfare is needed.*

c. (U) Scheme of Air Support. *Briefly describe the maneuver commander's guidance for the use of air power. Refer to Appendix 5 (Air Support) to Annex D (Fires) as required.*

(1) (U) Organization for Combat. *Nothing specific to electronic warfare is needed.*

(2) (U) Air Interdiction Operations. *Nothing specific to electronic warfare is needed.*

(3) (U) Close Air Support Operations. *Nothing specific to electronic warfare is needed.*

(4) (U) Electronic Warfare Operations. *Provide the concept for use of electronic warfare aircraft and if the joint force air component commander can provide the resources. State the electronic warfare tasks.*

(5) (U) Air Reconnaissance Operations. *Nothing specific to electronic warfare is needed.*

d. (U) Scheme of Naval Fire Support. *Nothing specific to electronic warfare is needed.*

e. (U) Scheme of Cyber Electromagnetic Activities. *Describe the concept for use of electronic warfare (electronic attack). Include specific tasks to supporting units. Refer to the Appendix 7 (Cyber Electromagnetic Activities) to Annex D (Fires) as required.*

f. (U) Battlefield Obscuration Support. *Nothing specific to electronic warfare is needed.*

g. (U) Target Acquisition. *Nothing specific to electronic warfare is needed.*

h. (U) Tasks to Subordinate Units. *Identify the electronic warfare tasks for each unit.*

i. (U) Coordinating Instructions. *Identify electronic warfare instructions applicable to two or more units. Identify the requirements for the coordination of electronic warfare actions between units. Identify the emission control guidance.*

4. (U) Sustainment. *Identify sustainment priorities for electronic warfare operations.*

5. (U) Command and Signal.

a. (U) Command. *Nothing specific to electronic warfare is needed.*

b. (U) Control. *Nothing specific to electronic warfare is needed.*

[CLASSIFICATION]

Figure A-1. Sample operation plan for Annex D (continued)

[CLASSIFICATION]

ANNEX D (FIRES) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

c. (U) Signal. *Identify, if any, the special or unusual communications equipment related to electronic warfare operations.*

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

[page number]

ACKNOWLEDGE: *Nothing specific to electronic warfare is needed.*

OFFICIAL:

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

ATTACHMENTS: *Add any specific references to electronic warfare operations, if needed.*

Appendix 1 – Fire Support Overlay
Appendix 2 – Fire Support Execution Matrix
Appendix 3 – Targeting
Appendix 4 – Field Artillery Support
Appendix 5 – Air Support
Appendix 6 – Naval Fire Support
Appendix 7 – Cyber Electromagnetic Activities

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

[page number]
[CLASSIFICATION]

Figure A-1. Sample operation plan for Annex D (continued)

A-2. Under the current operation order format, electromagnetic spectrum operations information is provided in Annex H (Signal) (see figure A-2, pages A-3 through A-5):

- Sub-subparagraph 5 (Electromagnetic Spectrum Operations) to subparagraph a (Scheme of Signal Operations) to paragraph 3 (Execution).
- Appendix 5 (Electromagnetic Spectrum Operations).

[CLASSIFICATION]

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

ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

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

(U) Time Zone Used Throughout the Order: *Nothing specific to electromagnetic spectrum operations is needed.*

[page number]
[CLASSIFICATION]

Figure A-2. Sample operation plan for Annex H

[CLASSIFICATION]

ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

1. (U) Situation. *Include information affecting signal operations that paragraph 1 of the OPLAN or OPORD does not cover or that needs expansion.*

a. (U) Area of Interest. *Nothing specific to electromagnetic spectrum operations is needed.*

b. (U) Area of Operations. *Nothing specific to electromagnetic spectrum operations is needed.*

c. (U) Enemy Forces. *Identify the vulnerabilities of enemy information systems and electromagnetic spectrum systems. Identify the enemy capability to interfere with accomplishment of the electromagnetic spectrum mission.*

d. (U) Friendly Forces. *Identify friendly electromagnetic spectrum assets and resources that affect electromagnetic spectrum planning by subordinate commanders. Identify friendly forces with which subordinate commanders may operate. Identify potential conflicts within the friendly 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. *Nothing specific to electromagnetic spectrum operations is needed.*

f. (U) Civil Considerations. *Nothing specific to electromagnetic spectrum operations is needed.*

g. (U) Attachments and Detachments. *List the electromagnetic spectrum assets that are attached or detached. List the electromagnetic spectrum resources available from higher headquarters.*

h. (U) Assumptions. *Nothing specific to electromagnetic spectrum operations is needed.*

2. (U) Mission. *State how electromagnetic spectrum operations will support the commander's objectives.*

3. (U) Execution.

a. (U) Scheme of Signal Operations. *Nothing specific to electromagnetic spectrum operations is needed.*

(1) (U) Scheme of Information Assurance. *Nothing specific to electromagnetic spectrum operations is needed.*

(2) (U) Scheme of Voice and Data Network Diagrams. *Nothing specific to electromagnetic spectrum operations is needed.*

(3) (U) Scheme of Satellite Communications. *Nothing specific to electromagnetic spectrum operations is needed.*

(4) (U) Scheme of Foreign Data Exchanges. *Nothing specific to electromagnetic spectrum operations is needed.*

(5) (U) Electromagnetic Spectrum Operations. *Describe how electromagnetic spectrum operations supports the commander's intent and concept of operations described in the base plan or order. Outline the effects the commander wants to achieve while prioritizing tasks for electromagnetic spectrum operations. List objectives and the primary tasks to achieve those objectives. Refer to Appendix 5 (Electromagnetic Spectrum Operations) to Annex H (Signal) as required.*

(6) (U) Network Diagram. *Nothing specific to electromagnetic spectrum operations is needed.*

b. (U) Tasks to Subordinate Units. *Identify the electromagnetic spectrum tasks for each unit.*

[page number]
[CLASSIFICATION]

Figure A-2. Sample operation plan for Annex H (continued)

[CLASSIFICATION]

ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]

c. (U) Coordinating Instructions. *Identify electromagnetic spectrum instructions applicable to two or more units. Identify the requirements for the coordination of electromagnetic spectrum actions between units. Identify the emission control guidance.*

4. (U) Sustainment. *Nothing specific to electromagnetic spectrum operations is needed.*

5. (U) Command and Signal.

a. (U) Command. *Nothing specific to electromagnetic spectrum operations is needed.*

b. (U) Control. *Nothing specific to electromagnetic spectrum operations is needed.*

c. (U) Signal. *Identify, if any, the special or unusual communications equipment related to electromagnetic spectrum operations.*

ACKNOWLEDGE: *Nothing specific to electromagnetic spectrum operations is needed.*

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

OFFICIAL:

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

ATTACHMENTS: *Nothing specific to electromagnetic spectrum operations is needed.*

Appendix 1 – Information Assurance
Appendix 2 – Voice and Data Network Diagrams
Appendix 3 – Satellite Communications
Appendix 4 – Foreign Data Exchanges
Appendix 5 – Electromagnetic Spectrum Operations

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

[page number]
[CLASSIFICATION]

Figure A-2. Sample operation plan for Annex H (continued)

JOINT OPERATION PLANS AND ORDERS

A-3. If required to provide electronic warfare input to portions of a joint order, the primary areas for input are the following:

- Paragraph 3 (Execution) to appendix 3 (Information Operations) to Annex C (Operations).
- Tab B (Electronic Warfare) to appendix 3 (Information Operations) to Annex C (Operations).

This page intentionally left blank.

Appendix B
Electronic Warfare Running Estimate

This appendix discusses the electronic warfare running estimate. It first describes a running estimate. Then it illustrates a sample running estimate for electronic warfare.

DESCRIPTION OF RUNNING ESTIMATE

B-1. A running estimate is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ATTP 5-0.1 discusses running estimates in detail.) The electronic warfare (EW) running estimate is used to support the military decisionmaking process (MDMP) throughout the conduct of operations. During planning, the EW running estimate provides an assessment of the supportability of each proposed course of action from an EW perspective.

B-2. The format of the EW running estimate closely parallels the steps of the MDMP. It serves as the primary tool for recording the electronic warfare officer's (EWO's) assessments, analyses, and recommendations for EW operations. The EWO and staff in the EW working group are responsible for conducting the analysis and providing recommendations based on the EW running estimate.

SAMPLE OF RUNNING ESTIMATE

B-3. A complete EW running estimate should contain the information necessary to answer any question the commander may pose. If there are gaps in the EW running estimate, the staff identifies the gaps as information requirements and submits them to the intelligence cell. The EW running estimate can form the basis for EW input required in other applicable appendixes and annexes within operation plans and orders. Figure B-1, page B-2, provides a sample EW running estimate for use during planning.

B-4. Once the commander approves the order, the EW running estimate is used to inform current and future operations. During execution, the EW running estimate is used to help determine if current EW operations are proceeding according to plan and if future EW operations are supportable. The EWO and supporting staff members within the EW working group produce and update the running estimate. The staff frequently updates the running estimate so that the information remains current and relevant.

1. **SITUATION AND CONSIDERATIONS.**
   a. **Area of Interest.** *Identify and describe those factors of the area of interest that affect functional area considerations.*
   b. **Characteristics of the Area of Operations.**
      (1) Terrain. *State how terrain may impact electronic warfare operations*.
      (2) Weather. *State how weather may impact electronic warfare operations*.
      (3) Enemy Forces. *Describe enemy disposition, composition, strength, and systems as well as enemy capabilities and possible courses of action (COAs) with respect to their effects on electronic warfare operations*.
      (4) Friendly Forces. *List current status of the forces' electronic warfare resources. List the current status of additional electronic warfare resources. Provide a comparison of electronic warfare requirements with available capabilities and recommend solutions for any discrepancies. Identify friendly force's electronic warfare vulnerabilities and recommend solutions*.
      (5) Civilian Considerations. *State how rules of engagement and incident management requirements may impact electronic warfare operations*.
   c. **Assumptions.** *List any assumptions used that may affect the employment of electronic warfare capabilities.*
2. **MISSION.** *Show the restated mission resulting from mission analysis*.
3. **COURSES OF ACTION.**
   a. *List friendly COAs that were war-gamed.*
   b. *List enemy actions or COAs that were templated that affect the functional area*.
   c. *List the evaluation criteria identified during COA analysis. All staffs use the same criteria*.
4. **ANALYSIS.** *Analyze each COA using the evaluation criteria from COA analysis*.
5. **COMPARISON.** *Compare COAs. Rank order COAs for each electronic warfare key consideration identified*.
6. **RECOMMENDATIONS AND CONCLUSIONS.** *This paragraph translates the best COA (as determined in paragraph 5) into a complete recommendation. It should outline who, what, where, when, how, and why from the electronic warfare point of view. It states which COA can best be supported by friendly electronic warfare, and is less vulnerable to enemy electronic warfare force capabilities*.
   a. Recommend the most supportable COAs from an electronic warfare perspective.
   b. *Prioritize and list and electronic warfare issues, deficiencies, and risks and make recommendations on how to mitigate them*.

Figure B-1. Sample of electronic warfare running estimate

Appendix C

Reports and Messages Related to Electronic Warfare

This appendix provides information and references for electronic warfare and related reports and message formats, including counter-improvised explosive device activities.

MESSAGES AND SUMMARIES

C-1. The following messages and summaries are associated with the planning, synchronization, deconfliction, and assessment of electronic warfare (EW) operations.

ELECTRONIC ATTACK DATA MESSAGE

C-2. An electronic attack data message reports an electronic attack strobe from an affected or detecting unit's position to an aircraft emitting an electronic attack. It is used to report the location of a hostile or unknown aircraft emitting an electronic attack. The detecting unit reports its detection to all units using a given network when the data link is degraded or not operational. Upon receipt of several messages, the source of enemy electronic attack can be determined by comparing lines of bearing from the different origins by triangulation. (See FM 6-99.2 for the message format for the *EA (Electronic Attack) Data Message [EADAT],* report number E001.)

ELECTRONIC ATTACK REQUEST FORMAT

C-3. Electronic fires fall within three categories: preplanned, preplanned on-call, and immediate. Requesting airborne electronic attack support for ground operations is similar to requesting close air support. Requests for an electronic attack are sent via the normal joint air request process. Requesters use a DD Form 1972 (Joint Tactical Air Strike Request). They should reference JP 3-09.3 for instructions on completing this form. A theater-specific electronic attack request format may complement a DD Form 1972. When submitting a DD Form 1972, requesters, at a minimum, require the following information:

- Target location.
- Prioritized target description and jam frequencies.
- Time on target (window).
- Joint terminal attack controller.
- Jamming control authority call sign and frequency.
- Friendly force disposition (for example, troop movement route).
- Friendly frequency restrictions.
- Other remarks to clarify the requested electronic attack.

ELECTRONIC WARFARE FREQUENCY DECONFLICTION MESSAGE

C-4. An EW frequency deconfliction message promulgates a list of protected, guarded, and taboo frequencies. This list helps friendly forces to use frequencies in the electromagnetic spectrum without adverse impact from friendly electronic attack. (See FM 6-99.2 for the format for *Electronic Warfare Frequency Deconfliction Message [EWDECONFLICT],* report number E005.)

ELECTRONIC WARFARE MISSION SUMMARY

C-5. The EW mission summary summarizes significant EW missions and reports the status of offensive EW assets. EW and electronic-attack-capable surface and air units use it to provide information on EW

operations. Service components use it to report significant events for subsequent analysis. (See FM 6-99.2 for the format for the *Electronic Warfare Mission Summary [EWMSNSUM]*, report number E010.)

ELECTRONIC WARFARE REQUESTING TASKING MESSAGE

C-6. Joint task force commanders use the EW requesting tasking message to task component commanders to perform EW operations in support of the joint EW plan and to support component EW operations. Component commanders use this message to request EW support from sources outside their command. (See FM 6-99.2 for the format for the *Electronic Warfare Requesting/Tasking Message [EWRTM],* report number E015.)

JOINT TACTICAL AIR STRIKE REQUEST

C-7. The DD Form 1972 (Joint Tactical Air Strike Request) is used to request electronic attack (see paragraph C-3.) (See also JP 3-09.3 and FM 3-09.32 for more information.)

JOINT SPECTRUM INTERFERENCE RESOLUTION

C-8. The joint spectrum interference resolution (JSIR) program replaced the Department of Defense meaconing, intrusion, jamming, and interference program. (CJCSI 3320.02E provides JSIR policy and reporting guidance.)

JOINT RESTRICTED FREQUENCY LIST

C-9. Operational, intelligence, and support elements use the joint restricted frequency list to identify the level of protection desired for various networks and frequencies. The list should be limited to the minimum number of frequencies necessary for friendly forces to accomplish objectives.

C-10. The joint restricted frequency list format (shown in Annex A to appendix B to JP 3-13.1) is used by the joint automated communications–electronics operations instruction system. The format is unclassified but should show the proper classification of each paragraph when filled in. (See CJCSI 3320.01C and JP 3-13.1 for additional information.)

COUNTER IMPROVISED EXPLOSIVE-DEVICE ACTIVITIES

C-11. Certain reports and references are associated with counter improvised explosive device activities. Most of these reports include information for counter radio-controlled improvised explosive device EW (sometimes referred to as CREW) activities. EW working groups have the responsibility to monitor these reports to assess planned counter radio-controlled improvised explosive device EW activities and to support future operations. These reports typically use formats established in FM 6-99.2 modified to include improvised explosive device considerations and current operations.

Appendix D

Tools and Resources Related to Electronic Warfare

This appendix discusses tools and reachback resources related to electronic warfare. Successful electronic warfare officers, noncommissioned officers, and supporting staff know these tools and resources and understand how to use them to support electronic warfare. Some tools and resources require an approved user account for access.

ARMY REPROGRAMMING ANALYSIS TEAM

D-1. The Army Reprogramming Analysis Team (ARAT) supports tactical commanders. It provides timely reprogramming of any Army-supported software used for target acquisition, target engagement, measurement and signature intelligence, and vehicle and aircraft survivability (including software operated by other Services). The team provides software changes not readily possible by operator input to respond to rapid deployments or changes in an operational environment. The ARAT Web site, https://ako.sec.army.mil/arat/index.html, requires Army Knowledge Online login.

D-2. The ARAT provides reprogramming support for counter radio-controlled improvised explosive device electronic warfare (EW) activities and other electronic systems.

D-3. The team is accessible via the ARAT's Warfighter Survivability Software Support Portal. A SECRET Internet Protocol Router Network (SIPRNET) account is required to access the portal.

NATIONAL GROUND INTELLIGENCE CENTER

D-4. The National Ground Intelligence Center provides all-source analysis of the threat posed by improvised explosive devices produced and used by foreign terrorist and insurgent groups. The center supports U.S. forces during training, operational planning, deployment, and redeployment.

D-5. The center maintains a counter improvised explosive device targeting program (often called CITP) portal on its SIPRNET site. This portal provides information concerning improvised explosive device activities, incidents, and assessments.

ELECTRONIC ORDER OF BATTLE

D-6. An electronic order of battle details all known combinations of emitters and platforms in a particular area of operations. It consists of several reachback resources:

- National Security Agency–Electronic Intelligence Parameter Query.
- U.S. electromagnetic systems database.
- National Ground Intelligence System parametric information relational intelligence tool database.
- Military equipment parametrics and engineering database.

JOINT INFORMATION OPERATIONS WARFARE CENTER

D-7. The Joint Information Operations Warfare Center (known as JIOWC) is the only joint EW center of expertise for the Department of Defense. It provides EW subject matter expertise from a range of backgrounds, including people with current multi-service operational experience. The center has a limited capability to perform modeling and simulation studies and EW red team support. It can deploy in a support role if approved by United States Strategic Command. (See paragraphs 7-6 through 7-7.)

JOINT IMPROVISED EXPLOSIVE DEVICE DEFEAT ORGANIZATION

D-8. The Joint Improvised Explosive Device Defeat Organization (known as JIEDDO) leads Department of Defense (DOD) actions to rapidly provide counter-improvised explosive device (sometimes called C-IED) capabilities in support of the combatant commanders and to enable the defeat of the improvised explosive device as a weapon of strategic influence.

JOINT SPECTRUM CENTER

D-9. The Joint Spectrum Center ensures DOD effectively uses the electromagnetic spectrum in support of national security and military objectives. The center serves as DOD's center of excellence for electromagnetic spectrum management matters in planning, acquisition, training, and operations. It provides information on a quick-reaction basis in various formats and media to support EW planners and electromagnetic spectrum managers.

D-10. The center maintains databases and provides data about friendly force command and control systems for locational and technical characteristics. This information is used to plan electronic protection measures. These databases provide EW planners with information covering communication, radar, navigation, broadcast, identification, and EW systems operated by the DOD, other government agencies, and private businesses and organizations. (See also paragraph 7-8.)

KNOWLEDGE AND INFORMATION FUSION EXCHANGE

D-11. The Knowledge and Information Fusion Exchange (sometimes called KnIFE) is a program sponsored by United States Joint Forces Command. It provides Soldiers with observations, insights, and lessons from operations around the world.

Appendix E

Cyber Electromagnetic Activities Support to Electronic Warfare

This appendix introduces cyber electromagnetic activities in the context of the mission command warfighting function staff tasks. It lists integration tasks performed by an electronic warfare working group and required expertise for an electronic warfare staff element and working group.

MISSION COMMAND WARFIGHTING FUNCTION STAFF TASKS

E-1. Staffs support the commander in the exercise of mission command by performing the four staff tasks:

- Conduct the operations process.
- Conduct knowledge management and information management.
- Conduct inform and influence activities.
- Conduct cyber electromagnetic activities.

Through these tasks, the staff supports the commander in understanding situations, making effective decisions, and implementing those decisions throughout the conduct of operations. The application of cyber electromagnetic activities (CEMA) as an information-related capability directly supports mission command to ensure freedom of movement within the information environment.

CYBER ELECTROMAGNETIC ACTIVITIES

E-2. CEMA consist of two lines of effort: cyberspace operations and electronic warfare (EW), supported by electromagnetic spectrum operations. (See table E-1, page E-2.) The electromagnetic spectrum is essential for communications, lethality, sensors, and self-protection. The cyberspace line of effort aims to achieve objectives in and through cyberspace. The EW line of effort aims to control the electromagnetic spectrum or to attack the enemy. These lines of effort may rely on the same information-related capabilities to accomplish these effects, so planners must synchronize and integrate them closely to ensure unity of effort in words, images, and actions. Components of the cyberspace line of effort include cyber situational awareness, network operations, and cyber warfare. These components integrate with the divisions of the EW line of effort—electronic attack, electronic protection, and electronic warfare support. Components of both lines of effort integrate with electromagnetic spectrum operations.

E-3. The EW working group integrates and synchronizes information related to CEMA to achieve desired conditions in cyberspace and the electromagnetic spectrum. The EW working group seeks to unify the offensive and defensive aspects of CEMA (including cyber warfare, network operations, electronic attack, electronic protection, and electronic warfare support). The working group focuses on the commander's stated conditions to gain and maintain advantages for cyberspace and the electromagnetic spectrum. To this end, the working group supports situational awareness related to cyberspace and the electromagnetic spectrum and continually assesses progress toward desired conditions. The working group coordinates vertically and horizontally across echelons to achieve the best results from assigned and supporting information-related capabilities. The working group integrates all appropriate capabilities (cyber electromagnetic and physical) to achieve these desired conditions. The working group also leverages both cyberspace and the electromagnetic spectrum to maximize support of the unit's overall mission. This support could include setting conditions in cyberspace and the electromagnetic spectrum to facilitate a unit's main effort or perhaps providing the means for successful inform and influence activities. The EW element is a primary supporting member of the inform and influence activities working group for this purpose.

Table E-1. Cyber electromagnetic activities

Task: Conduct cyber electromagnetic activities as part of combined arms operations. **Purpose:** To seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and across the electromagnetic spectrum, denying and degrading adversary and enemy use of the same and protecting friendly mission command systems.	
Cyberspace Operations Line of Effort	***Electronic Warfare Line of Effort***
Task: Employ cyber capabilities. **Purpose:** To achieve objectives in and through cyberspace.	**Task:** Use electromagnetic and directed energy. **Purpose:** To control the electromagnetic spectrum or to attack the enemy.
Cyber situational awareness: The knowledge of relevant information regarding activities in and through cyberspace and the electromagnetic spectrum.	**Electronic attack:** Use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment.
Network operations: Activities conducted to operate and defend the Global Information Grid.	**Electronic protection:** Actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum.
Cyber warfare: Warfare that extends cyber power beyond the defensive boundaries of the Global information Grid to deny, degrade, disrupt, destroy, and exploit enemies.	**Electronic warfare support:** Actions 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.
Electromagnetic spectrum operations: Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures.	

E-4. CEMA tasks are coordinated across the integrating cells: current operations integration, future operations, and plans integrating cells. The working group coordinates, both vertically and horizontally, the critical components of CEMA across all the warfighting functions and staff elements (the G-2 or S-2, G-3 or S-3, G-6 or S-6, and G-6 or S-7). This includes integration with external staffs, organizations, and unified action partners.

INTEGRATION TASKS PERFORMED BY ELECTRONIC WARFARE WORKING GROUP

E-5. The EW working group may perform the following CEMA integration tasks:

- Plan, integrate, coordinate, and assess the holistic employment of the full range of CEMA capabilities in unit operations.
- Plan and request offensive and defensive CEMA capabilities and actions to support the scheme of maneuver, including degraded operations.
- Synchronize and integrate offensive and defensive CEMA capabilities and actions into the scheme of maneuver.
- Facilitate and conduct CEMA vertical and horizontal integration and synchronization of operations across the warfighting functions.
- Synchronize operations with CEMA capabilities in other domains such as aerial, high altitude and space.
- Plan, assess, and direct friendly electronics security measures.
- Prioritize CEMA effects and targets.
- Deconflict CEMA with operations, including intelligence.
- Determine, adjudicate, and forward spectrum user requirements.

- Conduct frequency deconfliction and interference resolution for electronic attack.
- Integrate CEMA into the operations process.
- Identify and coordinate intelligence support requirements for unit CEMA operations.
- Assess offensive and defensive CEMA requirements.
- Maintain current assessment of CEMA resources available to the unit.
- Recommend and assess friendly protection measures related to CEMA.

ELECTRONIC WARFARE STAFF ELEMENT AND WORKING GROUP EXPERTISE

E-6. A few of the core capabilities that must reside within the EW element or EW working group to coordinate CEMA effectively consist of the following:

- Knowledge of network operations.
- Ability to access intelligence.
- Electronic warfare.
- Electromagnetic spectrum management (also referred to as spectrum management).
- Employment of offensive CEMA and dynamic defense capabilities (such as cryptologic capabilities).
- Ability to access support activities (for example, higher-level CEMA capabilities, forensics, and vulnerability assessment).
- Synchronization and integration.

This page intentionally left blank.

Glossary

The glossary lists terms and acronyms with Army or joint definitions. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ARAT	Army Reprogramming Analysis Team
ASCC	Army Service component command
ATTP	Army tactics, techniques, and procedures
CEMA	cyber electromagnetic activities
CJCSI	Chairman of the Joint Chiefs of Staff instruction
COA	course of action
DA	Department of the Army
DD	Department of Defense (for forms)
DOD	Department of Defense
DODI	Department of Defense instruction
EW	electronic warfare
EWC	electronic warfare cell
EWO	electronic warfare officer
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-6	assistant chief of staff, signal
G-7	assistant chief of staff, inform and influence activities
IPB	intelligence preparation of the battlefield
J-2	intelligence directorate of a joint staff
J-3	operations directorate of a joint staff
J-6	communications system directorate of a joint staff
JIOWC	Joint Information Operations Warfare Center
JP	joint publication
MDMP	military decisionmaking process
NATO	North Atlantic Treaty Organization
S-2	intelligence staff officer
S-3	operations staff officer
S-4	logistics staff officer
S-6	signal staff officer
S-7	inform and influence activities staff officer
U.S.	United States

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)

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

electromagnetic pulse

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 joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (JP 6-0)

electronic attack

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

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)

electronic reconnaissance

The detection, location, identification, and evaluation of foreign electromagnetic radiations. (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

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)

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 noncommunications electromagnetic radiations, for example, radar. (JP 3-13.1)

electro-optical-infrared countermeasure

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)

measure of effectiveness

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

measure of performance

A criterion used to assess friendly actions that is tied to measuring task accomplishment. (JP 3-0)

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)

targeting

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

wartime reserve modes

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

working group

A grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. (ATTP 5-0.1)

References

Field manuals and selected joint publications are listed by new number followed by old number.

REQUIRED PUBLICATIONS

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

ADRP 1-02. *Operational Terms and Military Symbols*. 31 August 2012.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: < http://www.apd.army.mil/>.

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

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

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

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

FM 3-09.32. *Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower*. 20 December 2007.

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

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

FM 6-99.2 (FM 101-5-2). *U.S. Army Report and Message Formats*. 30 April 2007.

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

JOINT PUBLICATIONS

Most joint publications are available online: <http://www.dtic.mil/doctrine/doctrine/doctrine.htm.>

CJCSI 3320.01C. *Electromagnetic Spectrum Use in Joint Military Operations*. 22 February 2011.

CJCSI 3320.02E. *Joint Spectrum Interference Resolution (JSIR)*. 15 October 2010.

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

JP 2-0. *Joint Intelligence*. 22 June 2007.

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

JP 3-09. *Joint Fire Support*. 30 June 2010.

JP 3-09.3. *Close Air Support*. 8 July 2009.

JP 3-13. *Information Operations*. 13 February 2006.

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

JP 3-60. *Joint Targeting*. 13 April 2007.

JP 6-0. *Joint Communications System*. 10 June 2010.

OTHER PUBLICATIONS

EO 12333. *United States Intelligence Activities*. 4 December 1981. Available at <http://www.archives.gov/federal-register/codification/executive-order/12333.html >.

WEB SITES

Army Reprogramming Analysis Team (ARAT) <https://ako.sec.army.mil/arat/index.html>.

REFERENCED FORMS

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

DD Form 1972. *Joint Tactical Air Strike Request*.

Index

Entries are by paragraph number unless indicated otherwise.

FM 3-36
9 November 2012

By order of the Secretary of the Army:

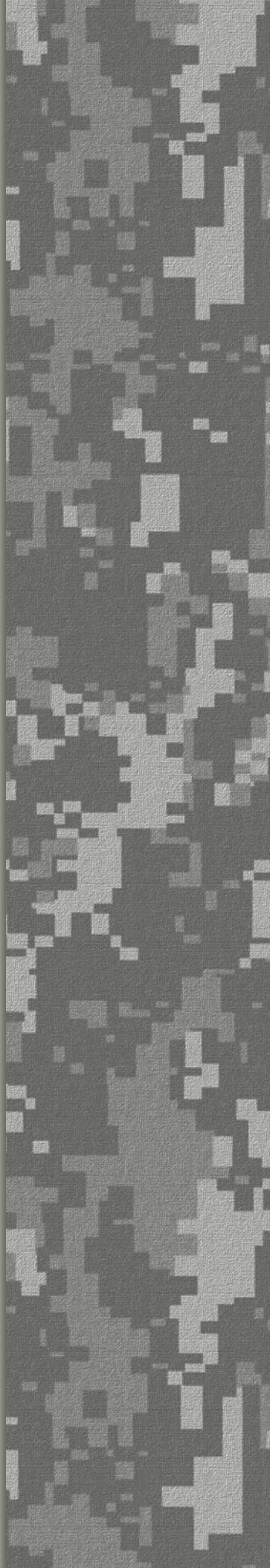
RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1214206

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: Not to be distributed. Electronic media only.



PIN: 085321-000