ATP 3-36 (FM 3-36)

ELECTRONIC WARFARE TECHNIQUES

December 2014

Headquarters, Department of the Army

Army Techniques Publication
No. 3-36

Headquarters
Department of the Army
Washington, DC, 16 December 2014

ELECTRONIC WARFARE TECHNIQUES

Contents

***This publication supersedes FM 3-36, 9 November 2012.**

Figures

Tables

Preface

ATP 3-36 provides techniques for the application of electronic warfare in unified land operations. ATP 3-36 expands the discussion of the role of electronic warfare in cyber electromagnetic activities started in FM 3-38.

The principal audience for ATP 3-36 is all members of the profession of arms. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (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.)

ATP 3-36 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. ATP 3-36 is not the proponent publication (the authority) for any terms. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

ATP 3-36 applies to the Active Army, the Army National Guard/the Army National Guard of the United States, and the United States Army Reserve unless otherwise stated.

The proponent of ATP 3-36 is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCD (ATP 3-36), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by e-mail to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

ATP 3-36 expands upon electronic warfare tasks, their role in unified land operations, and considerations specific to electronic warfare.

It contains five chapters and three appendixes.

Chapter 1 provides a brief description of the three divisions of electronic warfare, describes the key personnel involved in planning and coordinating electronic warfare, explains its relationship to cyber electromagnetic activities, and concludes with electronic warfare contributions to the integrating processes and continuing activities.

Chapter 2 discusses the operations process and applying electronic warfare considerations. It provides guidance on preparing the electronic warfare running estimate.

Chapter 3 addresses electronic warfare preparation, execution, and assessment. More detailed information is provided on the joint restricted frequency list, airborne electronic attack, and electromagnetic interference considerations.

Chapter 4 looks at coordinating electronic warfare through the targeting process.

Chapter 5 introduces joint and multinational electronic warfare staff structures and organizations, as well as, unique information security considerations when working with multinational organizations.

Appendix A discusses electronic warfare forms and message formats. Appendix B provides information on calculating jammer effectiveness. Appendix C describes electronic warfare equipment used by each of the Services.

This publication completes the transition of Army electronic warfare doctrine to the Doctrine 2015 structure. Electronic warfare tactics and procedures contained in the legacy FM 3-36 (2012, now obsolete) have been transitioned to FM 3-38. FM 3-38 introduced the basic concept behind electronic warfare including the electronic warfare principles. FM 3-38 also identified and described the primary electronic warfare tasks for electronic attack, electronic protection, and electronic warfare support. The information from the following chapters from the legacy FM 3-36 (now obsolete) that did not transfer to FM 3-38 was updated in ATP 3-36:

- Chapter 3 that described electronic warfare organization is updated in chapter 1 of this ATP to reflect the replacement of the electronic warfare working group with the cyber electromagnetic activities working group.
- Appendix B that provided a sample electronic warfare running estimate is updated in chapter 2 of this ATP.
- Appendix C that discussed reports and message formats is updated in appendix A of this ATP by removing reports and messages already provided in FM 6-99, and including important forms and message formats used by electronic warfare officers.

ATP 3-36 is not the proponent for any terms.

This page intentionally left blank.

Chapter 1
Overview of Electronic Warfare

This chapter provides an overview of electronic warfare and its relationship to cyber electromagnetic activities. It also discusses the key personnel for planning and coordinating electronic warfare activities. Finally, electronic warfare input to integrating processes and continuing activities closes out the chapter and lays the groundwork for the ensuing chapters.

DEFINITION OF 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) is one of three capabilities of cyber electromagnetic activities (CEMA). The other activities are cyberspace operations and spectrum management operations.

DIVISIONS OF ELECTRONIC WARFARE

1-2. Electronic warfare is further composed of three divisions: electronic attack (EA), electronic protection, and electronic warfare support (ES). Each division has its own purposes and effects that support unified land operations. See JP 3-13.1 for full discussion on EW.

ELECTRONIC ATTACK

1-3. EA uses electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA may be an offensive or defensive action. Offensive EA includes jamming enemy electronic systems, using a missile guided by radiated energy against the energy source, or using directed energy such as a laser against enemy equipment. Defensive EA focuses on protection of personnel, facilities, capabilities, and equipment, such as counter radio-controlled improvised explosive device electronic warfare (CREW) systems. Tasks related to EA include—

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

Countermeasures

1-4. *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).

Electromagnetic Deception

1-5. Electromagnetic deception is 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.

Electromagnetic Intrusion

1-6. *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

1-7. *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

1-8. *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

1-9. *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).

ELECTRONIC PROTECTION

1-10. Electronic protection involves actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Electronic protection (EP) focuses on the effects of friendly or threat use of the electromagnetic spectrum. EP tasks include—

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

Electromagnetic Hardening

1-11. *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

1-12. *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

1-13. *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

1-14. *Electromagnetic spectrum management* is planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures (JP 6-01).

Wartime Reserve Modes

1-15. *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).

Electromagnetic Compatibility

1-16. *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).

ELECTRONIC WARFARE SUPPORT

1-17. ES actions search for, intercept, identify, and locate sources of radiated electromagnetic energy for future operations including EW operations. ES tasks include—

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

Electronic Reconnaissance

1-18. *Electronic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-13.1).

Electronic Intelligence

1-19. *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

1-20. 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 communications and noncommunications electromagnetic radiations.

KEY PERSONNEL FOR PLANNING AND COORDINATING ELECTRONIC WARFARE ACTIVITIES

1-21. Key personnel involved in the planning and coordination of EW activities are—

- G-3 (S-3) staff.
- Electronic warfare officer.
- G-2 (S-2) staff.
- Network operations officer.
- Spectrum manager.
- Information operations officer.
- Staff judge advocate or representative.
- Electronic warfare control authority.

1-22. Other key personnel involved in the planning and coordination of EW activities include—

- Fire support coordinator.
- G-5 (S-5) staff.
- G-6 or S-6 staff.
- Liaison officers.
- Space support element.
- Special technical operations staff.

G-3 (S-3) STAFF

1-23. The G-3 (S-3) staff is responsible for the overall planning, coordination, and supervision of EW activities, except for intelligence. The G-3 (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 EA, including integration of electromagnetic deception plans.
- Directs EP measures the unit will take based on recommendations from the G-6 (S-6), the electronic warfare officer, and the CEMA 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 (S-2) and the requirement manager.
- Coordinates with the CEMA working group to ensure planned EW operations support the overall tactical plan.
- Integrates EA within the targeting process.

ELECTRONIC WARFARE OFFICER

1-24. The electronic warfare officer (EWO) plans, coordinates, and supports the execution of EW and other CEMA. The EWO—

- Leads the CEMA working group.
- Plans, coordinates, and assesses EW offensive, defensive, and support requirements.
- Supports the G-2 (S-2) during intelligence preparation of the battlefield.
- Supports the fire support coordinator to ensure EA 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 elements, cells, and working groups to ensure EW integration.
- Serves as EW subject matter expert on existing EW rules of engagement (ROE).
- When designated, serves as the electronic warfare control authority.
- Prepares, submits for approval, and supervises the issuing and implementation of fragmentary orders for EW operations.

G-2 (S-2) STAFF

1-25. The G-2 (S-2) staff advises the commander and staff on the intelligence aspects of EW. The G-2 (S-2) staff—

- Provides threat data to support programming of unit EW systems and deconfliction of their use by the CEMA working group.

- Ensures that electronic threat characteristics requirements are included in the information collection plan.
- Determines enemy EW organizations, disposition, capabilities, and intentions via collection, analysis, reporting, and dissemination.
- Determines enemy EW vulnerabilities and high-value targets.
- Provides intelligence support to lethal and nonlethal targeting operations.
- Assesses effects of friendly EW operations on the enemy.
- Conducts intelligence gain or loss analysis for EW targets with intelligence value.
- Helps prepare the intelligence-related portion of the EW running estimate.
- Provides input to the restricted frequency list by recommending guarded frequencies.
- Provides updates on the rapid electronic threat characteristics.
- Maintains appropriate threat EW data.
- Works with the CEMA working group to synchronize information collection with EW requirements and deconflict planned EW actions.
- Provides guidance to the EWO to deconflict ES and signals intelligence (SIGINT) operations.

NETWORK OPERATIONS OFFICER

1-26. The network operations officer (in the G-6 [S-6] staff) coordinates the communications network for the following actions:

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

SPECTRUM MANAGER

1-27. 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 (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 CEMA working group to deconflict friendly electromagnetic spectrum requirements with planned EW operations and information collection.

INFORMATION OPERATIONS OFFICER

1-28. The information operations officer is responsible to the commander for all information operations. As an enabler of information operations, CEMA undertakes 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 information operations officer—

- Ensures that EW effectively integrates with other information operations and deconflicts EW actions as required.
- Considers second- and third-order effects of EW on information operations and proactively plans to enhance intended effects and their consequences.

STAFF JUDGE ADVOCATE OR REPRESENTATIVE

1-29. The staff judge advocate (known as SJA) is responsible to the commander for all legal advice. The staff judge advocate or representative reviews all EW operations to ensure they comply with existing Department of Defense directives and instructions, ROE, and applicable domestic and international laws, including the law of armed conflict. The staff judge advocate may also obtain any necessary authorities that are lacking.

ELECTRONIC WARFARE CONTROL AUTHORITY

1-30. Depending on the situation, an Army headquarters may be designated as the electronic warfare control authority (formerly known as the jamming control authority) and may serve as the senior EA authority in the area of operations. It establishes guidance for EA on behalf of the joint force commander. If designated as the electronic warfare 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.
- Validating and approving or denying cease jamming requests.
- Maintaining situational awareness of all EA capable systems in the area of operations.
- Acting as the joint force commander's executive agent for developing EW intelligence gain or loss recommendations when EA or ES conflicts occur.
- Coordinating EA requirements with joint force components.
- Investigating unauthorized EA events and implements corrective measures.

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

RELATIONSHIP WITH CYBER ELECTROMAGNETIC ACTIVITIES

1-31. EW belongs to a category of activities known as CEMA. The other activities are cyberspace operations and spectrum management operations. By definition, CEMA are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading threat use of the same and protecting the mission command system. (See FM 3-38.)

1-32. CEMA, through the CEMA element, supports unified land operations by integrating and synchronizing the functions and capabilities of cyberspace operations, electronic warfare, and spectrum management operations to cause specific effects at decisive points in the operation. *Unified land operations* is how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution (ADP 3-0). The electronic warfare element forms the nucleus of the CEMA element.

ELECTRONIC WARFARE ELEMENT

1-33. An electronic warfare element (EWE) is an organic organization in brigade, division, corps, and Army Service component command (ASCC) staffs. The EWE is located with the CEMA element and is

responsible to the chief of staff. Battalions do not have a EWE but rather a single EW representative on the battalion staff.

1-34. Primarily the EWE develops EW plans and monitors EW operations and activities. The EWE plays an important role in requesting and integrating joint air and ground EW and manages the organic EW "fight" within the main command post. The EWE ensures electromagnetic spectrum management within its specified area of operations and assists the ground commander in coordinating shaping operations. The EWE, through the CEMA working group, leads and facilitates the integration of CEMA, with assistance and coordination from the G-6 (S-6) and G-2 (S-2).

1-35. C*yber electromagnetic activities* is defined as activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system (ADRP 3-0). CEMA consist of cyberspace operations, EW, and spectrum management operations. The EWE does not have the resident expertise to advise the commander or complete the detailed planning for all CEMA capabilities and must be augmented by other functional area experts. For example, cyberspace operations include offensive cyberspace operations and defensive cyberspace operations that are the responsibility of the G-2 (S-2) and G-6 (S-6), respectively, in coordination with the G-3 (S-3) who specifies the desired effects. Both offensive and defensive cyberspace operations are enabled by cryptologic platforms coordinated by the intelligence staff.

1-36. The process for integrating CEMA in an operation involves both the EWE and the CEMA working group. For example, units requesting EA forward a request to the appropriate EWE. Coordination of the request, as time permits, is performed through the CEMA working group, which prioritizes the requests and makes a recommendation to the commander. Once approved, the request is forwarded to the higher headquarters. The commander responsible for the EW assets ultimately approves the request based on the mission variables. The CEMA working group integrates new EW requests into the intelligence synchronization process. If the CEMA working group recommends to approve the new request, then it appears in the requirements tool and the unit information collection plan. The technical data required to support EW requests pass via SIGINT channels within the G-2 (S-2) by classified means.

1-37. The EWE plays an important role in requesting and integrating joint air and ground EW support and manages the organic EW fight. The EWE plans the frequencies to be targeted by EA, analyzes the probability of frequency fratricide, and collaborates with the G-6 (S-6) to mitigate harmful effects from EW to friendly personnel, equipment, and facilities. The personnel who make up the EWE are predominantly EW trained, but also include Soldiers trained in spectrum management. Table 1-1 depicts the structure of a fully resourced EWE at each level.

Table 1-1. Electronic warfare element organization

Organization	***Personnel***	
ASCC	1 x 29A O6 1 x 29A O5 1 x 290A W5	
Corps	1 x 29A O6 1 x 29A O5 1 x 29A O4	1 x 290A W4 1 x 29E E9 1 x 25E E7
Division	1 x 29A O5 1 x 29A O4 1 x 290A W4	1 x 29E E8 1 x 25E E7
BCT *Aviation, fires, battlefield surveillance, maneuver enhancement, and other special function brigades have similar electronic warfare element structure.	1 x 29A O3 1 x 290A W2 1 x 29E E8	1 x 29E E6 1 x 29E E5 1 x 25E E6
ASCC Army Service component command BCT brigade combat team		

1-38. The EWE has the following personnel: electronic warfare officer, electronic warfare technician, electronic warfare noncommissioned officer, and spectrum manager.

1-39. The electronic warfare officer (29A)—

- Serves as the commander's subject matter expert and advisor on all EW matters.
- Plans, coordinates, synchronizes, and deconflicts EW tasks to support unified land operations.
- Integrates EW intelligence preparation of the battlefield (IPB) into the military decisionmaking process (MDMP).
- Provides input to fragmentary orders for EW tasks to support unified land operations.
- Identifies the potential for frequency fratricide in the MDMP.
- Plans, coordinates, and synchronizes EW activities and assets into unified land operations.
- Recommends priorities for EW effects and targets, and integrates EW into the targeting process.
- Coordinates, synchronizes, and deconflicts with collection manager and G-2 (S-2).
- Coordinates and reviews EW battle damage assessment.
- Coordinates CEMA in units conducting cyberspace operations.
- Maintains current assessment of EW resources available.
- Leads the CEMA working group.
- When designated, serves as the electronic warfare control authority.
- Supervises and manages EW activities for the commander.
- Oversees the creation of all EW products for dissemination.

1-40. The electronic warfare technician (290A)—

- Serves as the technical subject matter expert for EW to the EWO and CEMA working group.
- Plans, coordinates, and assesses EW offensive, defensive, and support requirements.
- Provides input to the integration of enemy electronic threat characteristics information into IPB.
- Provides subject matter expertise on technical and tactical employment of EW systems.
- Integrates EW in the targeting process, monitors EW target requests, and conducts battle damage assessments.
- Plans and coordinates EW operations across functional and integrating cells.
- Recommends employment and operation of available EW assets and maintains current resource status for CEMA working group.
- Provides technical oversight and supervision of the maintenance of EW equipment.
- Plans, manages, and executes EW collective tasks.
- Incorporates EW assets and plans into the collection and targeting staff processes.
- Develops EW products for inclusion into the targeting process.
- Facilitates CEMA working group efforts.
- Conducts, maintains, and updates an electromagnetic energy survey.
- Identifies EW enemy and friendly effects in the ES.
- Coordinates, synchronizes, and deconflicts with collection manager and G-2 (S-2).
- Ensures the EWO has all pertinent EW information to maintain situational awareness (maintains EW smart book, follows standard operating procedures, and briefs EWO as needed).

1-41. The electronic warfare noncommissioned officer (NCO) (29E)—

- Plans, manages, and executes EW individual tasks.
- Conducts organic and nonorganic EW asset visibility and management.
- Serves as senior developer and trainer for EW tasks.
- Distributes, maintains, and consolidates EW products.
- Conducts all administrative actions for CEMA working group.
- Collects logs and data for electromagnetic energy surveys.
- Coordinates and deconflicts with 25E (spectrum manager).
- Coordinates, synchronizes, and deconflicts with collection manager and G-2 (S-2).

- Manages the EW current operations situational awareness.
- Ensures all subordinate EW personnel maintain proficiency and adequately support their assigned unit.

1-42. The spectrum manager (25E)—

- Assists with mitigation of offensive and defensive EA on friendly emitters.
- Provides input to the ES plan.
- Conducts analysis of EW requests to determine impact on friendly emitters and recommend mitigation.
- Issues the signal operating instructions.
- Provides all spectrum resources to the task force.
- Coordinates the preparation of the joint restricted frequency list and issuance of emissions control guidance.
- Coordinates electromagnetic deception plans and operations in which assigned communications resources participate.
- Coordinates measures to eliminate, moderate, or mitigate electromagnetic interference.
- Coordinates with higher echelon spectrum managers for electromagnetic interference resolution that cannot be resolved internally.
- Assists the EWO in issuing guidance in the unit (including subordinate elements) regarding deconfliction and resolution of interference problems between EW systems and other friendly systems.

WORKING GROUPS

1-43. 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 (FM 6-0). The CEMA working group, when established, is accountable to the chief of staff but must coordinate with the G-3 (S-3) and fire support coordinator to integrate EW with all other effects. The CEMA working group replaces and assumes the duties and functions formerly performed by the EW working group. To effectively integrate CEMA, the working group usually includes representation from across the staff. The recommended structure and functions of the CEMA working group is described in detail in FM 3-38.

1-44. In brigade through ASCC organizations, the senior EWO heads the CEMA working group. Additional staff representation within the CEMA working group may include a fire support coordinator, a spectrum manager, a space operations officer, a representative of the staff judge advocate, and liaison officers as required. Depending on the echelon, liaison elements 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' CEMA working group becomes the joint force electronic warfare cell. The joint term for the EW staff organization is electronic warfare cell (rather than electronic warfare element). (See JP 3-13.1.)

1-45. When Army forces are employed as part of a joint or multinational operation, 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 element within a joint task force. Sometimes a component EW organization may be designated as the joint electronic warfare cell (EWC). (Chapter 5 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.

1-46. Regardless of the organizational framework employed, CEMA working groups perform the tasks identified in FM 3-38. The EWE within the CEMA element provides specific support to the CEMA working group. Figure 1-1 on page 1-10 details those supporting functions performed by the EWE.

BATTALION-LEVEL STAFFING

1-47. Battalion-level organizations do not have an EWE. Instead, battalions have an EW NCO responsible for planning and integrating EW requirements. Other staff elements that the EW NCO must coordinate at the battalion level include the S-2, S-6, fire support officer, and the joint terminal attack controller when assigned. The battalion EW NCO coordinates battalion EW operations with the brigade CEMA working group.

Support to CEMA Working Group
• Conduct EW planning to support 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 joint task force EW working group. • When directed, serve as the electronic warfare control authority. • Develop and promulgate EW policies and support higher level policies. • Identify and coordinate intelligence support requirements for EW operations and subordinate unit EW operations. • 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. • Ensure compliance with rules of engagement and applicable domestic and international law. • Plan, prepare, execute, and assess EW operations. • Integrate EW intelligence preparation of the battlefield into the operations process. • Assess offensive and defensive EW requirements. • Implement friendly electronic security measures (for example, electromagnetic spectrum mitigation and network protection). • Support BCT EW requirements to operations and exercises. • Coordinate EW operations with higher headquarters.
BCT brigade combat team J-6 communications system directorate of a joint staff EW electronic warfare G-6 assistant chief of staff, signal

Figure 1-1. Electronic warfare staff support of CEMA working group

1-48. Battalion EW NCO duties and responsibilities include, but are not limited to—

- Advising the battalion commander on employment of EW equipment.
- Coordinating organic and nonorganic ES mission requirements and integration of EW into the MDMP.
- Implementing EP requirements.
- Preparing or assisting in coordinating the CEMA portions of the operation order appendixes.
- Tracking status and monitoring operation of EW equipment and systems.
- Developing, executing, and managing unit EW training and CREW technical advice and assistance.
- Submitting airborne electronic attack (DD Form 1972 [*Joint Tactical Air Strike Request*]), electronic attack request format, and concept of operations to brigade EWE to support battalion operations as needed.

- Establishing a battalion EW standard operating procedure and disseminating guidance to subordinate units that integrates brigade and higher guidance.
- Establishing and enforcing CREW policy, procedures, and reporting guidelines that support brigade policy.
- Maintaining an EW-trained personnel and equipment tracking system.
- Ensuring subordinate command CREW requirements are met, to include the implementation and completion of CREW system upgrades.
- Ensuring that battalion satisfies all EW training requirements.
- Conducting precombat checks and precombat inspections on subordinate CREW programs to ensure compliance with battalion and brigade standard operating procedures.
- Downloading and submitting CREW system event logs as required.
- Administering CREW training to battalion and company personnel.
- Coordinating with the regional support center or field support representative for installation and upgrade of CREW systems.
- Conducting CREW system operational checks.
- Coordinating with airborne electronic warfare assets in order to provide the aircraft situational awareness of the ground unit's operational environment including actions on the desired target.

COMPANY-LEVEL STAFFING

1-49. At the company level, units assigned CREW systems may have trained EW personnel holding an additional skill identifier of 1K—for completion of the CREW Master Gunner Course or 1J for completion of the Army Operational Electronic Warfare Operations Course—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 staff.

1-50. Company CREW specialist duties and responsibilities include but are not limited to—

- Advising company commander on the employment of CREW and other EW equipment.
- Tracking CREW and EW equipment status.
- Training and assisting operators in the use and maintenance of CREW equipment.
- Operating CREW systems.
- Assessing effectiveness of CREW for company operations.
- Training company personnel on CREW system capabilities; company tactics, techniques, and procedures; and precombat checks and precombat inspections.
- Ensuring all CREW systems are fully operational, to include conducting precombat checks and precombat inspections as well as troubleshooting and reporting the malfunction of CREW systems to the chain of command and battalion EW NCO.
- Submitting required CREW reports to the battalion EW NCO.

ELECTRONIC WARFARE AND INTEGRATING PROCESSES AND CONTINUING ACTIVITIES

1-51. Commanders use several integrating processes and continuing activities to synchronize operations throughout the operations process. (See figure 1-2 on page 1-12.) The EWO ensures EW operations are fully synchronized and integrated within these processes. Other staff supporting the CEMA working group assist the EWO. Paragraphs 1-30 through 1-37 outline some key integrating processes. These processes require EWO involvement throughout the operations process.

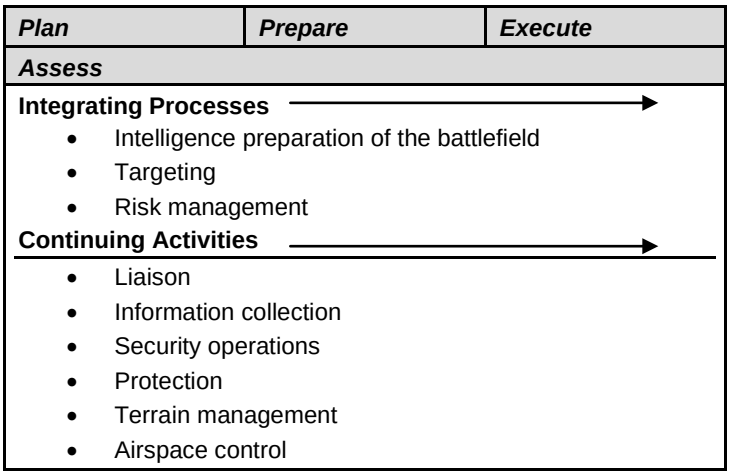

Figure 1-2. Integrating processes and continuing activities

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

1-52. 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 (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 enemy forces. Only one IPB planning activity exists within each headquarters; all affected staff cells participate.

1-53. 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 1-3.) This input includes, but is not limited to, the following:

- Defining an operational environment from an EW perspective.
- Describing effects within an operational environment on EW operations.
- Evaluating from an EW perspective the threat's capabilities, doctrinal principles, and tactics, techniques, and procedures.
- Determining threat courses of action (COAs).

1-54. 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 enemy fixed EW sites, such as ES and EA sites.
- Identifies airfields and installations that support, operate, or house enemy EW capabilities.
- In coordination with the G-2 (S-2) and G-6 (S-6), helps identify enemy electromagnetic spectrum usage and requirements within the area of operations and area of interest.

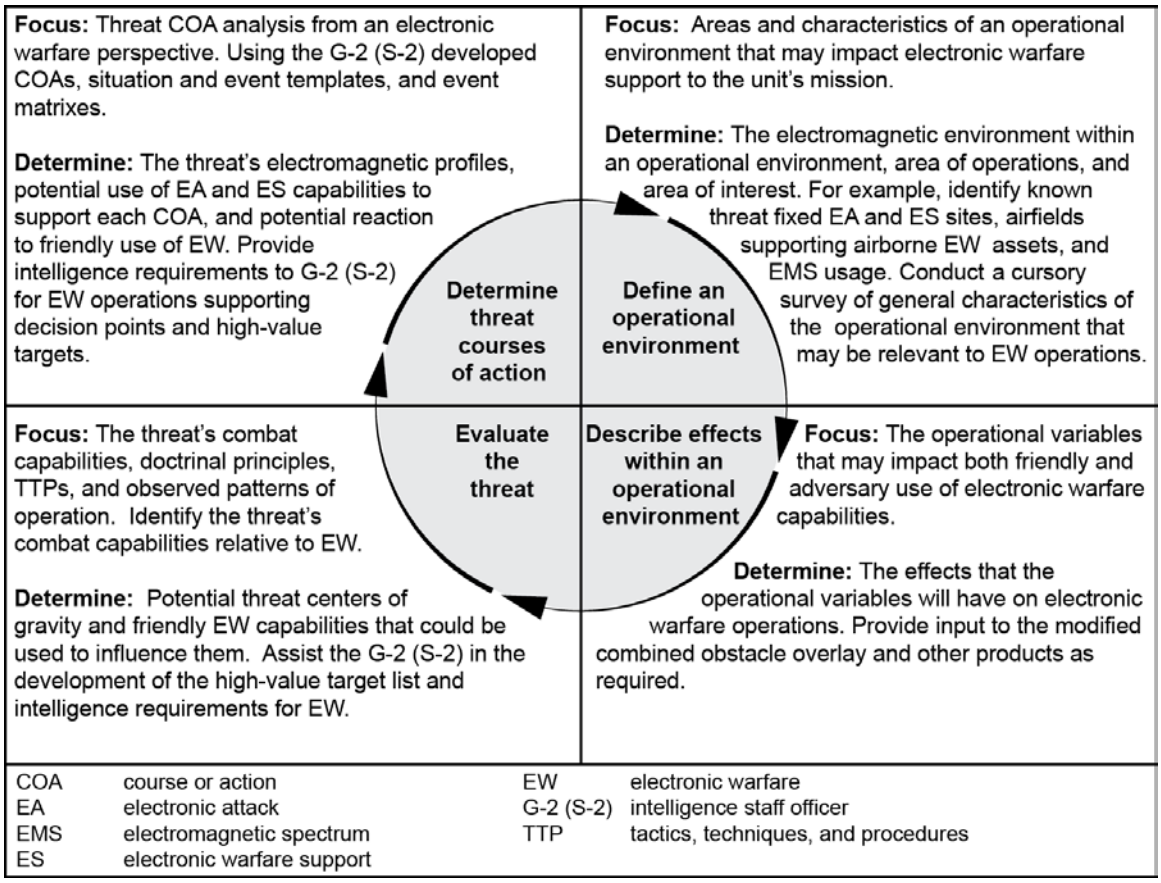

Figure 1-3. Electronic warfare to support intelligence preparation of the battlefield

1-55. When describing the effects of an operational environment on 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 noncommunications 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 potential support that EW operations could provide 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 (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).

1-56. 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 enemy's critical nodes.
- Collects the required data—operational net assessments, electronic threat characteristics, and electronic databases—to template the command and control critical nodes and the systems required to support and maintain them.
- Assists the G-2 (S-2) in determining the enemy's EW-related threat characteristics 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 (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 EW-related requests for information that describe the intelligence support required to support EW operations.
- Obtains the high-value target list, threat templates, and initial priority intelligence requirements list to assist in subsequent EW planning.

1-57. When determining enemy COAs, the EWO—

- Assists the G-2 (S-2) in development of threat 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

1-58. Targeting and the targeting process are more fully described in chapter 4.

RISK MANAGEMENT

1-59. 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 control measures and make risk decisions.
- Implement control measures.
- Supervise and evaluate.

CONTINUING ACTIVITIES

1-60. While executing tasks throughout the operations process, commanders and staffs plan for and coordinate continuing activities. (See figure 1-2 on page 1-12.) The EWO coordinates with the staff to participate in these continuing activities to address specific EW tasks as needed.

This page intentionally left blank.

Chapter 2

Electronic Warfare Planning

Planning for the integration of electronic warfare into operations requires an understanding of the operations process and associated electronic warfare considerations. This chapter discusses electronic warfare contributions during each step of the military decisionmaking process that will ensure electronic warfare is considered as part of the overall operation plan.

THE OPERATIONS PROCESS

2-1. The operations process is a commander-centric activity informed by the mission command approach to planning, preparing, executing, and assessing military operations. These activities may occur sequentially or continuously throughout an operation, overlapping and recurring as required. The EW staff officer is actively involved in the operations process. EW planning, preparation, execution, and assessment require collective expertise from operations, intelligence, signal, and mission command. The EWO integrates efforts across the warfighting functions to ensure that EW operations support the commander's objectives.

2-2. Both the commander and staff have important roles within the operations process. The commander's role is to drive the operations process through the activities of understanding, visualizing, describing, directing, leading, and assessing operations. The staff's role is to assist the commander. Staff planners with the necessary expertise, and in some cases access to sensitive compartmented information facilities (known as SCIF), are essential for planning EW and related capabilities. Integrating EW into operations requires placing experienced planners at the brigade combat team level. More experienced planners with access allows planning for a broader set of capabilities such as special technical operations and special access program effects.

2-3. The EW activities of the operations process frequently involve unique and complex issues. Law, policy, law of armed conflict, and ROE may affect EW activities. These EW activities overlap and recur as circumstances demand. Commanders should seek legal review during all levels of EW planning and execution, including the development of theater ROE. This is best accomplished by integrating a representative of the staff judge advocate into the CEMA working group. While ROE should be considered during the planning process, they should not inhibit developing a plan that employs available capabilities to their maximum potential. If, during the operations process, a ROE-induced restriction is identified, planners work with the staff judge advocate to clarify the ROE or develop supplemental ROE applicable to EW.

ELECTRONIC WARFARE PLANNING CONSIDERATIONS

2-4. EW planning is based on three main considerations. The first consideration is EW planners apply the 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 the operations process. Finally, EW planners apply specific EW employment considerations.

APPLYING THE MILITARY DECISIONMAKING PROCESS

2-5. 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 IPB, the targeting process (see FM 3-60), and risk management (see ATP 5-19). These processes occur continuously during operations.

2-6. Depending on the organizational echelon, the EW staff officer leads EW planning through the CEMA working group and EWE. The next sections outline key EW contributions to the processes and planning actions that occur during the seven steps of the MDMP. (ADRP 5-0 discusses the MDMP in detail.) Table 2-1 summarizes EWE actions during MDMP.

Table 2-1. EWE actions during the MDMP

MDMP Step	*EWE Action*
Step 1: Receipt of Mission	1. Update electronic warfare (EW) running estimate including a detailed description of the electromagnetic environment and electronic order of battle. 2. Identify EW requirements to support mission.
Step 2: Mission Analysis	1. Update EW running estimate. 2. Develop facts, assumptions, and specified, implied, or essential tasks. 3. Develop electronic threat characteristics with S-2. 4. Develop target lists. 5. Develop information requirements.
Step 3: Course of Action (COA) Development	1. Update all EW products. 2. Develop EW effects to support COAs. 3. Update target lists. 4. Conduct target value analysis per COA.
Step 4: COA Analysis (War Game)	1. Refine all EW products. 2. Determine EW data for overall synchronization matrix. 3. Provide EW input on high-value targets (lists). 4. Monitor EW-related commander's critical information requirements.
Step 5: COA Comparison	1. Provide relevant EW input to COA comparison. 2. Prioritize COAs from an EW perspective and support with pros and cons for each COA.
Step 6: COA Approval	1. Prepare (briefing) products as required. 2. Maintain situational understanding of other staff sections, products, and actions.
Step 7: Orders Production, Dissemination, and Transition	1. Update EW running estimates based on selected COA. 2. Draft EW appendixes and tabs in operation order. 3. Synchronize and integrate EW portion of the operation order.

Receipt of Mission

2-7. 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.

2-8. Upon receipt of a mission, the EWE alerts the staff supporting the CEMA working group. The EWO and supporting staff begin to gather 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.

2-9. The EWO also provides input to the staff's initial assessment and updates the EW running estimate. (See figure 2-1.) 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.

1. SITUATION AND CONSIDERATIONS.
- **a. Area of Interest.** Identify and describe those factors of the area of interest that affect electronic warfare (EW) considerations.
- **b. Characteristics of the Area of Operations.**
  1) **Terrain.** State how terrain affects EW capabilities.
  2) **Weather.** State how weather affects EW capabilities.
  3) **Enemy Forces**. Describe enemy EW disposition, composition, strength, and systems. Describe enemy EW capabilities and possible courses of action (COAs) and their effects on friendly EW operations and the friendly mission.
  4) **Friendly Forces.** List current EW resources in terms of equipment, personnel, and systems. Identify additional EW resources available located at higher, adjacent, or other units. List those EW capabilities from other military and civilian partners that may be available to provide support. Compare requirements to current capabilities and suggest solutions for satisfying discrepancies.
  5) **Civilian Considerations.** Describe civil considerations that may affect EW operations, including possible support needed by civil authorities from EW as well as possible interference from civil aspects.
- **c. Facts/Assumptions.** List all facts and assumptions that affect EW.

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 impact EW.
- **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. Review enemy actions that impact EW as they relate to COAs. Identify issues, risks, and deficiencies these enemy actions may create with respect to EW.

5. COMPARISON. Compare COAs. Rank order COAs for each key consideration. Use a decision matrix to aid the comparison process.

6. RECOMMENDATIONS AND CONCLUSIONS.
- **a.** Recommend the most supportable COAs from the perspective of EW.
- **b.** Prioritize and list issues, deficiencies, and risks and make recommendations on how to mitigate them.

Figure 2-1. EW running estimate

Mission Analysis

2-10. 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 members of the CEMA working group contribute to the overall mission analysis by participating in IPB and through the planning actions. (Paragraphs 1-52 through 1-57 discuss EW input to IPB during operations.)

2-11. The CEMA working group and EWO—

- 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 CEMA working group.
- Provide an EW perspective when developing the commander's restated mission.
- Help develop the mission analysis briefing for the commander.

2-12. The CEMA working group and EWO support the G-2 (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 as appropriate.
- Initiating, refining, and validating information requirements and requests for information.

2-13. The CEMA working group and EWO 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 CEMA working group and EWO list the critical requirements associated with the enemy's command and control capability (or command and control nodes) and then identify the critical vulnerabilities associated with the critical requirements. Through this process, the CEMA working group and EWO help determine which enemy vulnerabilities can be engaged by EW capabilities to produce a decisive outcome.

2-14. The CEMA working group and EWO identify and list—

- High-value targets that can be engaged by EW capabilities.
- Tasks that EW forces perform according to EW division—EA, ES, and EP—to support the warfighting functions. These include—
  - Specified EW tasks.
  - Implied EW tasks.
- Constraints relevant to EW such as—
  - Actions EW operations must perform.
  - Actions EW operations cannot perform.
  - Other constraints.

2-15. The CEMA working group and EWO 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.)

2-16. By the conclusion of mission analysis, the CEMA working group and EWO create or gather the following products and information:

- The initial information requirements for EW operations.
- A rudimentary analysis of the enemy command and control nodes.
- 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

2-17. After receiving the restated mission, commander's intent, and commander's planning guidance, the staff develops COAs for the commander's approval. Figure 2-2 depicts the required input to COA development and identifies the key contributions made by the EWO and CEMA working group during the process and output stages (center and right of figure 2-2). Paragraphs 2-18 through 2-22 discuss specific actions the EWO and CEMA working group perform to support COA development.

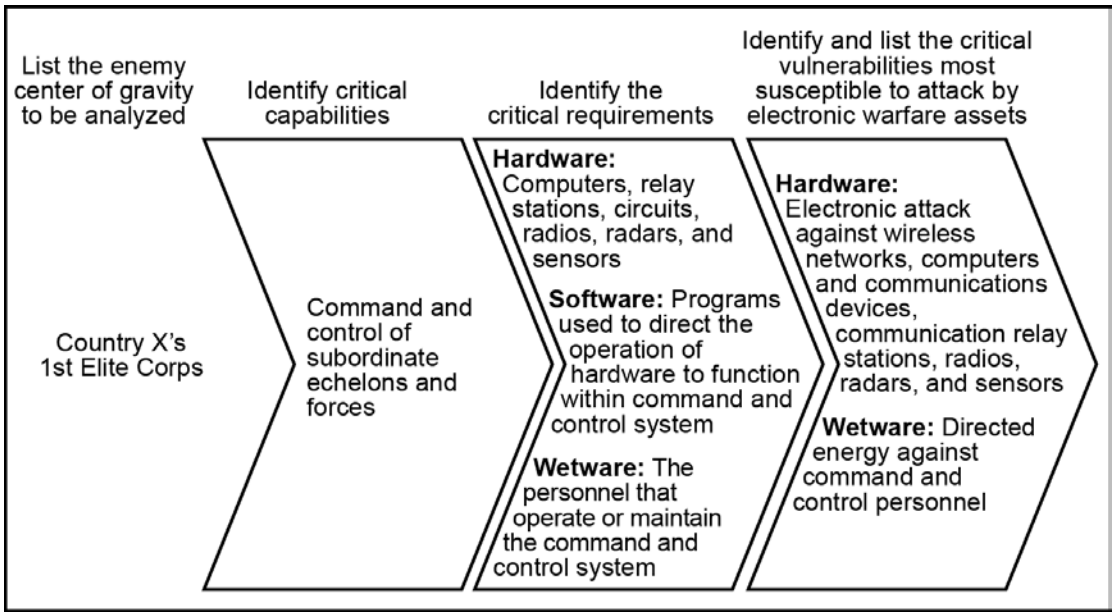

Figure 2-2. Course of action development

2-18. The EWO and CEMA 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.

2-19. Additionally, the EWO and CEMA working group help develop initial COA options by—

- Identifying COA options that may be feasible based on their functional expertise (while brainstorming 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-related tasks required to support the COAs.

2-20. The EWO and CEMA working group determine the forces required for mission accomplishment by—

- Determining the EW tasks that support each COA and the best method 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 to support all possible COAs meet the established screening criteria.

2-21. The EWO and CEMA working group identify EW supporting tasks and their purposes to support decisive, shaping, and sustaining operations as each COA is developed. These EW tasks include those focused on defeating the enemy and those required to protect friendly force operations.

2-22. The EWO and CEMA working group assist in developing the COA briefing as required. By the conclusion of COA development, the EWO and CEMA working group create 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 to support each COA.
- An update to the EW running estimate.

Course of Action Analysis (War Game)

2-23. 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.

2-24. During COA analysis, the EWO and CEMA working group synchronize EW actions and assist the staff in integrating EW capabilities into each COA. The EWO and CEMA 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 CEMA 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.
- Identify EW intelligence gaps.
- 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 EA, and the impact of asset or capability shortfalls.

2-25. By the conclusion of COA analysis (war game), the EWO and CEMA working group create 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 to support each COA.
- An update to the EW running estimate.

Course of Action Comparison

2-26. 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 FM 6-0 for a further discussion of COA comparison).

2-27. During COA comparison, the EWO and CEMA working group compare COAs based on the EW-related advantages and disadvantages. (See figure 2-3.) 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 the war game 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 FM 6-0 for more information on COA comparison and a sample decision matrix.)

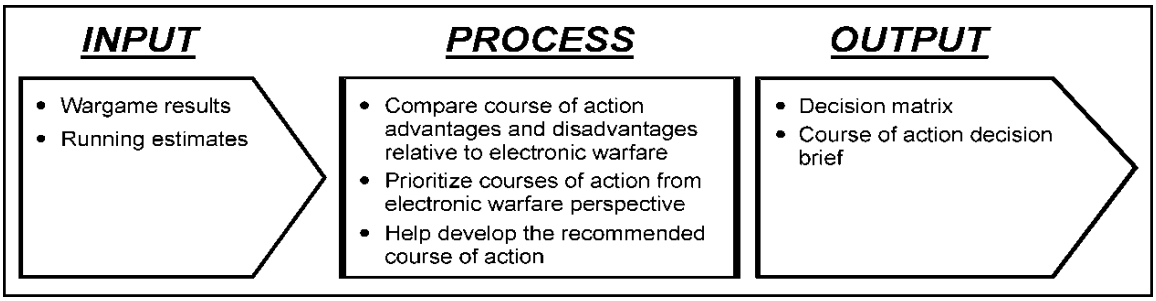

Figure 2-3. Course of action comparison

2-28. By the conclusion of COA comparison, the EWO and CEMA working group create 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

2-29. 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.

2-30. 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 (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 warfighting functions, orders preparation, rehearsal, and preparation.

2-31. After the COA decision has been made, the EWO and CEMA working group create 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 threat characteristics 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 to support 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

2-32. 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 control measures. They do this by coordinating and integrating risk control measures into the appropriate paragraphs and graphics of the order.

2-33. During orders production, the EWO provides the EW operations input for several sections of the operation order or plan. (See FM 6-0 for the primary areas for EW operations input within an Army order or plan.

DECISIONMAKING IN A TIME CONSTRAINED ENVIRONMENT

2-34. In a time constrained environment, the staff might not be able to conduct a detailed MDMP. The staff may choose to abbreviate the process as described in FM 6-0. The abbreviated process uses all seven steps of the MDMP in a shortened and less detailed manner.

2-35. The EWO and core members of the CEMA 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 CEMA 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.
- Provide intelligence requirements to G-2 (S-2).
- Provide EW input to fragmentary orders through the G-3 (S-3) as necessary to drive timely and effective EW operations.
- Deconflict planned EW actions against frequency fratricide of radio systems—including communications, unmanned aircraft systems, weapon systems, Global Positioning System, and sensors—with other uses of the spectrum.
- Synchronize EA and ES actions.
- Assist the G-2 (S-2) to synchronize other information collection to support EW requirements.
- Deconflict EW actions specifically with aviation operations.
- Help synchronize and integrate other relevant CEMA through the appropriate staff.

APPLYING INTEGRATING PROCESSES

2-36. EW planning involves applying the integrating processes. This planning is discussed in chapter 1.

APPLYING EMPLOYMENT CONSIDERATIONS

2-37. EW employment is based on specific ground-based, airborne, and functional (EA, EP, or ES) 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 these considerations before executing EW operations.

Ground-Based Electronic Warfare Considerations

2-38. 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, EA assets are normally located in the forward areas of the battlefield, with or near forward units.

2-39. Ground-based EW capabilities have certain advantages. They provide direct support to maneuver units (for example, through CREW 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.

2-40. 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 EP activities. In addition, they have distance or propagation limitations against enemy electronic systems. As with any spectrum-based system, units must properly program EW equipment to avoid friendly interference and compatibility issues.

Airborne Electronic Warfare Considerations

2-41. 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.

2-42. 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.

2-43. 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.

2-44. Limitations associated with airborne EW capabilities include limited time on station, vulnerability to enemy air defense systems, enemy EP actions, electromagnetic deception techniques, and limited assets.

Electronic Attack Considerations

2-45. EA includes both offensive and defensive activities. These activities differ in their purpose. Offensive EA denies, disrupts, or destroys enemy capability. Defensive EA protects friendly personnel and equipment or platforms. In either case, certain considerations are involved in planning for employing EA, such as—

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

2-46. The EWO, the G-2 (S-2), the G-3 (S-3), the G-6 (S-6), the spectrum manager, and the information operations officer coordinate closely to avoid friendly communications interference that can occur when using EW systems on the battlefield. Coordination ensures that EA system frequencies are properly deconflicted with friendly communications and intelligence systems, or that ground maneuver and friendly information tasks are modified accordingly.

2-47. The number of information systems, EW systems, and sensors operating simultaneously on the battlefield makes deconfliction with communications systems a challenge. The EWO, the G-2 (S-2), the G-6 (S-6), and the spectrum manager plan and rehearse deconfliction procedures to adjust their use of EW or communications systems quickly.

2-48. EA operations depend on ES and SIGINT to provide targeting information and battle damage assessment. However, EWOs must keep in mind that not all information collection focuses on supporting

EW. If not properly coordinated with the G-2 (S-2) staff, EA operations may interrupt information collection by jamming or inadvertently interfering with a particular frequency being used to collect data on the threat or by jamming a given enemy frequency or system that deprives friendly forces of that means of collecting data. Either interruption can significantly deter information collection efforts and their ability to answer critical information requirements. Coordination between the EWO, the fire support coordinator, and the G-2 (S-2) prevents this interference. In situations where a known conflict between the information collection effort and the use of EA exists, the CEMA working group brings the problem to the G-3 (S-3) for resolution.

2-49. Planners consider other effects that rely on electromagnetic spectrum when planning for EA. For example, military information support operations may include plans to use certain frequencies to broadcast messages, or a military deception plan may include the broadcast of friendly force communications. In both examples, the use of EA could unintentionally interfere or disrupt such broadcasts if not properly coordinated. To ensure EA does not negatively affect planned operations, the EWO coordinates between fires, network operations, and other functional or integrating cells as required.

2-50. Like any other form of electromagnetic radiation, EA can adversely affect local media and other 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 EA with the other functional or integrating cells responsible for the information tasks. In this way, they ensure that EA efforts do not cause fratricide or unacceptable collateral damage to their intended effects.

2-51. The potential for hostile intelligence collection also affects EA. A well-equipped enemy can detect friendly EW activities and thus gain intelligence on friendly force intentions. For example, the frequencies Army forces jam could indicate where they believe the enemy's capabilities lie. The EWO and the G-2 (S-2) develop an understanding of the enemy's collection capability. Along with the red team (if available), they determine what the enemy might gain from friendly force use of EA. (A *red team* is an organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others [JP 2-0].)

2-52. 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.

Electromagnetic Deception Considerations

2-53. 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 and denying valid information to the enemy or to enemy electromagnetic-dependent weapons. Each piece of electronic and associated equipment has its own electronic signature. These signatures are exploited in deception.

2-54. There are three types of electromagnetic deception. Manipulative seeks to eliminate, reveal, or convey misleading, telltale indicators that may be used by enemy forces. Simulative attempts to represent friendly, notional, or actual capabilities to mislead enemy forces. Imitative introduces electromagnetic energy into enemy systems to imitate emissions. Electromagnetic deception may take the form of either voice or data transmissions.

2-55. The G-3 usually plans and supervises deceptions. The EWO is responsible to the G-3 for the electromagnetic deception plan and must work with the G-2 to determine the electronic activities most likely to be intercepted by enemy SIGINT.

2-56. Careful integration of electromagnetic deception with other detectable actions is critical. What the enemy detects electronically must remain consistent with other sources of intelligence reports. Because of the reliance placed on electromagnetic radiation (for example, communication, surveillance, and navigation), this aspect of deception requires close attention. Although electromagnetic deception can be the sole act of deception, the effect is often of short duration.

2-57. The enemy's success depends upon its knowledge of friendly emitters. Success in manipulative electromagnetic deception and simulative electromagnetic deception depends on understanding how friendly emitters appear to the enemy. The SIGINT team should keep a database of the friendly command's voice and data emitters. The EW planners can then determine how best to portray a desired portion of that command electronically. The EW planners consider what is occurring and what should occur with all electromagnetic emitters in the unit's area.

2-58. Close control and coordination is necessary to avoid confusing actual activities from deception plan activities. Therefore, when planning an electromagnetic deception, the EW planners consider actions that support the current operation as well as those that will support the deception operation and perform integration and deconfliction as necessary.

2-59. Time is a critical factor in deception planning. Given sufficient time, the enemy can discover even the most complex electromagnetic deception. A maneuver deception plan intended to deceive the enemy for two or three days must include a well-coordinated electromagnetic deception that covers all electronic emitters. However, a deception plan for only a short period just before an attack may be relatively simple since there is less time for the enemy to discover the deception. Regardless of the duration, the enemy's ability to detect emitters is essential to the success of an electromagnetic deception. Therefore false emissions must be—

- On signals strong enough to reach the enemy.
- On a frequency the enemy can intercept.
- In a modulation the enemy can intercept.

2-60. Imitative electromagnetic deception usually requires approval at higher command levels. This restriction ensures that the deception does not jeopardize the SIGINT effort. Imitative electromagnetic deception, if recognized by the enemy, could provide data concerning the friendly ES effort. This could have the unintended effect of causing the enemy to improve its communications security and thereby reduce the effectiveness of the friendly SIGINT.

Electronic Protection Considerations

2-61. 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. The CEMA working group and EWO consider the following functions when planning for EP:

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

Vulnerability Analysis and Assessment

2-62. Vulnerability analysis and assessment forms the basis for formulating EP plans. The Defense Information Systems Agency provides a variety of information assurance services, including vulnerability analysis and assessment, which specifically focus on automated information systems and can be useful in this effort. United States Cyber Command (known as USCYBERCOM) provides information assurance alerts and data through its information assurance vulnerability management system. Another potential source for vulnerability analysis and assessment is the red team officer assigned to division through theater army headquarters. Although not an expert in EP, the red team officer is skilled at developing assessment strategies.

Monitoring and Feedback

2-63. The National Security Agency monitors communications security and provides feedback. Its programs focus on telecommunications systems using wire and electronic communications. Their programs can support and remediate the command's communications security procedures when required.

Electronic Protection Measures and Their Effects on Friendly Capabilities

2-64. Electronic protection measures include any measure taken to protect the force from hostile EA actions. However, these measures can also limit friendly capabilities or operations. For example, denying frequency usage to CREW systems on a given frequency to preserve it for use by a critical friendly information system could leave friendly forces vulnerable to certain remotely detonated improvised explosive devices. The EWO and the G-6 (S-6) carefully consider these second-order effects when advising the G-3 (S-3) regarding EP measures.

Electronic Warfare Support Considerations

2-65. The distinction between a SIGINT mission and an ES 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 ES for the purposes of immediate threat recognition, targeting, future operations planning, and other tactical actions (such as threat avoidance and homing). The EWO coordinates with the G-2 (S-2) to identify ES needed for planned EW operations and to ensure deconfliction of ES operations with SIGINT operations. Once coordinated, the EWO will submit these support requests to the G-3 (S-3) for commander approval. This ensures the required collection assets are properly tasked and managed to provide the requested ES.

2-66. In cases where planned EA actions may conflict with the G-2 (S-2) information collection efforts, the G-3 (S-3) or commander decides which has priority. Communications content and other data may be retained for an operational requirement to support immediate threat recognition, targeting, and planning of future operations. Data that is retained may be transferred to the United States SIGINT System for the production of foreign intelligence. ES personnel are not authorized to analyze the data for generating foreign intelligence. Foreign intelligence is information that relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons. The EWO and the G-2 (S-2) develop a structured process within each echelon for conducting this intelligence gain loss calculus during mission rehearsal exercises and predeployment planning.

Electronic Warfare Reprogramming Considerations

2-67. 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. Reprogramming EW and target sensing system equipment falls under the responsibility of each Service or organization through its respective EW reprogramming support programs. Reprogramming includes changes to self defense systems, offensive weapons systems, and information collection systems. During joint operations, swift identification and reprogramming efforts are critical in a rapidly evolving hostile situation. The key consideration for EW reprogramming is joint coordination. Joint coordination of Service reprogramming efforts ensures all friendly forces consistently identify, process, and implement reprogramming requirements. During joint operations, EW reprogramming coordination and monitoring is the responsibility of the joint force commander's EW staff. (For more information on EW reprogramming, see ATP 3-13.10).

Chapter 3

Electronic Warfare Preparation, Execution, and Assessment

This chapter discusses the preparation, execution, and assessment of EW. It also discusses special considerations during execution. Execution of an electronic warfare plan involves more than passing orders to the elements that will perform the tasks.

ELECTRONIC WARFARE PREPARATION

3-1. 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.

3-2. During preparation, the CEMA working group and EWO focus their actions on—

- Revising and refining the EW estimate, EW tasks, and EW to support the overall plan.
- Rehearsing the synchronization of EW to support 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 SIGINT staff elements).
- Training the supporting staff of the CEMA working group during rehearsals.
- Completing precombat checks and inspections of EW assets.
- Completing sustainment preparations for EW assets.
- Coordinating with the G-4 (S-4) to develop EW equipment report formats.
- Completing backbriefs by subordinate CEMA 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

3-3. 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.

3-4. During execution, the CEMA working group and EWO—

- 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 EW-related control measures and procedures.

- Maintain direct liaison with the fires cell and network operations officer 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 EA assets.
- Receive, process, and coordinate subordinate requests for EW 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 EA missions.
- Maintain, update, and distribute the status of EW assets.
- Validate and disseminate cease jamming requests.
- Coordinate and expedite electromagnetic interference reports with the G-2 (S-2) representative and G-6 (S-6) representative for potential deconfliction.
- Perform electronic warfare control authority function for ground-based EW within the area of operations, when designated.

3-5. Providing an accessible and accurate portrayal of the EW environment challenges the EWE. An updated running estimate is important, but a graphical portrayal in the form of an EW overlay gives relevance to the contributions EW makes to mission accomplishment. Currently, the command post of the future (known as CPOF) is the best tool since the staff uses it to maintain a common operational picture for the commander. However, the staff uses caution when depicting range fans and range rings for EW assets by considering the effects of terrain and weather. Such caution avoids giving a false impression of asset capabilities.

ELECTRONIC WARFARE ASSESSMENT

3-6. 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.

3-7. Assessment occurs throughout planning, preparation, and execution; it 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.

3-8. The EWO and supporting members of the CEMA 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.

3-9. The EWO, in conjunction with the G-5 (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 EA 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. Normally, the EWO measures this by analyzing data collected by both 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. However, use caution in selecting measures of effectiveness to avoid flaws in an analysis of the EW operation. For example, the lack of enemy activity such as communications or improvised explosive device (known as IED) initiation does not necessarily mean it was the result of the EW operation; other factors may be the cause.

3-10. During execution, the EWO and CEMA working group participate in combat assessments within the targeting process to determine the effectiveness of EA employment to support operations. Combat assessment consists of three elements: munitions effects assessment, battle damage assessment, and re-attack recommendations.

SPECIAL CONSIDERATIONS DURING EXECUTION

3-11. During execution, EW planners have special considerations. They consider the joint restricted frequency list, airborne electronic attack, electromagnetic interference, joint spectrum interference resolution program, and electromagnetic interference battle drill.

JOINT RESTRICTED FREQUENCY LIST DECONFLICTION

3-12. The Army is transitioning away from the joint restricted frequency list (JRFL) and adopting spectrum management operations as the technique to deconflict EA from interference with friendly radio frequencies. One reason for this is that the JRFL does not adequately inform communications planners about EA frequencies in use. Therefore, EW planners must utilize the JRFL during mission planning and execution to mitigate the effects of offensive and defensive EA on friendly systems.

3-13. The JRFL is a concise list of highly critical frequencies that should not be jammed or attacked and is used by various operational, intelligence, and support elements. Critical frequencies may include various sensors, exploitation frequencies, full motion video feeds, networks of the mission command system, and aviation safety of flight frequencies. It includes command channels of senior commanders, but unfortunately does not include the frequencies used by maneuver Soldiers in contact with the enemy. The JRFL also does not provide protection from other spectrum users. That protection is provided by a valid frequency assignment coordinated through the G-6 (S-6) spectrum manager. JRFL entries are limited to the minimum number of radio frequencies and intelligence equities necessary for friendly forces to accomplish mission objectives. See FM 6-02.70 for more information about the JRFL.

3-14. The JRFL should not be mistaken as a fix for all deconfliction issues. High priority nets, bands, and frequencies are protected to a certain degree from friendly EA. However, spectrum managers must balance the competing demands that all friendly systems have the ability to operate unimpaired. This can be accomplished by simply adding the offending jammer to a database and using spectrum management techniques (such as changing frequencies, changing assignments, or moving to an unaffected area) to accomplish the mission. The spectrum manager has tools that can identify potential frequency fratricide if properly utilized.

3-15. Spectrum management operations are accomplished using software with a database of radios used in the area of operations, coupled with radio frequency engineering algorithms that calculate the effects any radio in the database will have on other radios in the database. Algorithms exist to determine if a radio circuit will work as intended. Other algorithms calculate the unintended interference a radio may cause to other radios in the database, and recommend alternate frequencies to avoid the interference. The significant change from past practices is to now include frequencies used for EA in the database for deconflicting them from friendly radios.

3-16. Legacy spectrum management operations programs lacked the capability to adequately calculate EA transmissions for deconflicting from friendly operations. New counter-improvised explosive device initiatives have the capability to illustrate the impact that EA transmissions will have on other frequencies included in the database. Due to security concerns, frequencies employed in intelligence roles are not

normally included in the spectrum management operations database limiting the effectiveness of spectrum management operations.

AIRBORNE ELECTRONIC ATTACK

3-17. Airborne electronic attack is an EW capability that delivers EA from aerial platforms. Although some of these platforms are organic to the Army, much of the capability resides in other Services creating a truly joint operation. Effective airborne electronic attack requires good integrating procedures and communications between EWE and the airborne electronic attack asset owner. The techniques described here will assist in getting the most effective airborne electronic attack.

3-18. Although an approved airborne electronic attack mission could be conducted without any communications between the aircraft and EWO, best practices dictate active communications between the two. Communications between aircrews and units they are supporting use specific procedures and terminology. ATP 3-09.32 discusses EA call for fire procedures.

3-19. If no contact can be established between aircrew and EWO or the joint tactical air controller, the supporting aircraft may continue with the airborne electronic attack mission depending on conditions established in the original request. A good technique is to include a note in both the electronic attack request format and the joint tactical air strike request (DD Form 1972) explaining to the aircraft what to do in the event of a communication failure.

3-20. Communications between aircrew and EWO or joint terminal attack controller throughout the mission may also be beneficial for maintaining situational awareness and for making timely adjustments as needed. A good technique is to disseminate key mission status information to staff elements within the command post to support overall understanding and mission command.

Airborne Electronic Attack Cancellations at the Battalion and Brigade Level

3-21. As circumstances change, it may be necessary to cancel a planned airborne electronic attack mission. Assets that perform airborne electronic attacks are generally low density and in high demand. Therefore, EWOs must communicate cancellations through the proper channels to ensure that resources are made available for other taskings. The techniques discussed in paragraphs 3-22 through 3-24 allow the necessary communication to cancel missions and prevent limited assets from sitting idle.

Advanced Cancellation of Preplanned Mission

3-22. Cancellation more than six hours before a preplanned mission may be considered routine and should be communicated as soon as possible to allow for retasking of the asset. One technique may be simply to send the brigade EWO an e-mail with the reason for cancellation and attach the cancellation joint tactical air strike request (JTAR) and electronic attack request format. The brigade EWO forwards the cancellation request to division EWO, brigade fires officer, and brigade air liaison officer. Cancellations made during limited operations should include direct voice communications to ensure someone is available and ready to process the cancellation.

Short Notice Cancellation of Preplanned Mission

3-23. Cancellation less than six hours before a preplanned mission requires immediate action to avoid mission launch and wasting a valuable asset. The EWO informs the EWE that a cancellation is coming by the most expeditious means available, whether internet relay chat, telephone, or radio. If EWOs cannot contact the EWE, then they use the liaison officer channels. After making initial notification has been made, EWOs send the official cancellation JTAR to the EWE as soon as possible. Since the cancellation may require communications that bypass normal chain of command relationships, EWOs include the process in the written unit standard operating procedure and battle drills.

Immediate Cancellation of Preplanned Mission

3-24. EWOs use this technique for cancelling missions within one-hour of the expected execution time. Time is crucial. EWOs use the fastest communication means possible, such as internet relay chat, to

distribute the necessary cancellation information. Immediately after, EWOs e-mail an official cancellation JTAR and electronic attack request format directly to the EWE to ensure units receive information promptly. Effective units include this process in the unit standard operating procedure and battle drills.

Troops-in-Contact and Dynamic Retasking

3-25. When a troops-in-contact is declared, the staff makes every effort to provide support to the on-scene commander, including the allocation of available airborne electronic attack assets. The retasking of airborne electronic attack assets provides the on-scene commander with valuable effects to aid the fight. For example, the airborne electronic attack could jam enemy communications and disrupt its control of the fight. Battalion EW staff and the joint terminal attack controller coordinate swiftly at appropriate levels and pass sufficient details to the EWE to enable coordination with the air operations center to allow retasking of platforms expediently.

Key Personnel

3-26. The following personnel are involved in dynamically retasking an airborne electronic attack:

- Joint tactical attack controller.
- Battalion EW NCO.
- Brigade combat team EWO.
- Electronic warfare element.
- Air operations center.

Joint Tactical Attack Controller

3-27. The joint terminal attack controller (JTAC) aids in the facilitation of air and ground coordination on behalf of the ground commander. The JTAC conducts the following tasks to support airborne electronic attack dynamic retasking:

- Initiates request via available communications systems (may be done by EWO).
- Conducts verbal coordination with airborne electronic attack platform once on station (may be done by the EWO).
- Acts as electronic warfare control authority when dictated on the DD Form 1972. Provides a primary and a secondary frequency for contact and obtains the latest JRFL.
- Assists EWO, if need be, by providing timely feedback of jamming operations.

Battalion Electronic Warfare Noncommissioned Officer

3-28. The battalion EW NCO provides EW advice and guidance to the battalion commander as well as plans and coordinates EW operations. During operations, the EW NCO coordinates with the JTAC on control of airborne electronic attack assets and ensures requested support meets the commander's intent. The battalion EW NCO conducts the following tasks:

- Initiates dynamic retasking request.
- Conducts verbal coordination with airborne electronic attack platform once on station.
- Submits a JTAR and electronic attack request format according to established procedures.
- Serves as electronic warfare control authority when dictated on the DD Form 1972 and electronic attack request format.
- Obtains latest JRFL for deconfliction or obtains approval to override JRFL when applicable.
- Provides timely feedback to airborne electronic attack platform on jamming effectiveness.
- Obtains information on enemy communications and provides input during coordination.

Brigade Combat Team Electronic Warfare Officer

3-29. The brigade combat team EWO coordinates EW operations as part of the headquarters staff. The brigade combat team EWO conducts the following tasks:

- Validates, requests, and prepares JTAR and electronic attack request format information for retask consideration.
- Deconflicts with affected organizations.
- Deconflicts EW effects with information collection efforts, SIGINT, and other EA assets.
- Submits requests to higher EWE for prioritization and final validation.

Electronic Warfare Element

3-30. The EWE coordinates EW operations as part of the headquarters on behalf of the commander. The EWE was formerly called the electronic warfare coordination cell. The EWE conducts the following tasks:

- Validates and prioritizes the retasking request.
- Provides retasking recommendations to the air operations center.
- Confirms retasking with affected unit and air operations center.
- Ensures a new or updated JTAR and electronic attack request format are submitted.

Air Operations Center

3-31. The air operations center (AOC), which can be joint or multinational depending on mission, coordinates all assigned aerospace forces. The AOC conducts the following tasks to support airborne electronic attack dynamic retasking:

- Provides advice and guidance to the EWE and EWO.
- Coordinates and approves required airspace.
- Coordinates aerial refueling support (as required).
- Issues retasking to airborne electronic attack platform.
- Completes air tasking order (ATO) changes, as required.

3-32. The process for retasking airborne electronic attack platforms vary depending on joint command and control arrangements, force disposition, and unit boundaries. The requesting unit submits a request over internet relay chat or other available means to their supporting EW representative or EWE. The electronic attack 9-line is an excellent format for such a request (see ATP 3-09.32 for the format).

3-33. If the requesting unit previously submitted a JTAR for EA support, the EWE modifies the existing JTAR with a numbered change JTAR. If the requesting unit has not submitted a JTAR for the mission, the EWE creates a new JTAR. It is important that the EWE provides status updates to the requesting unit.

3-34. Due to the dynamic nature of a troops-in-contact, there is no way to predict the amount of time needed for airborne electronic attack support. If it is apparent that the duration of support will exceed what was originally requested, the EWO or JTAC notifies the EWE and AOC. The AOC notifies the airborne electronic attack asset and coordinates any additional fuel requirements, or determines the need to retask another airborne electronic attack asset. The AOC then informs the EWO and JTAC of what support to expect. Once the airborne electronic attack support is no longer needed, the JTAC or EWO will contact the AOC to release the airborne electronic attack asset for new tasking.

Air Tasking Order Calendar and Mission Block

3-35. All EWOs should be familiar with the ATO calendar. The ATO calendar is a document used by the AOC to provide detailed information on aircraft, crews, and mission information. The ATO calendar is a valuable tool for an EWO in planning airborne electronic attack missions far in advance based on their unit's battle rhythm or scheduled operations. The ATO calendar is broken down into ATO days. The ATO days are designated based on a letter pairing, which coincide with the numerical Julian date for that particular year. The ATO typically covers a 24-hour duty cycle. Since the ATO calendar is produced at higher echelons, division EWOs may need to push it down to lower echelon EW staffs as needed.

3-36. There are two types of airborne electronic attack requests that may be executed during an ATO day. A preplanned request can be anticipated sufficiently in advance to permit detailed mission coordination and planning. An immediate request cannot be identified sufficiently in advance to permit detailed mission coordination and planning. (See JP 3-09.3 for more details on airborne electronic attack requests.)

3-37. The ATO mission block is annotated at the bottom of the ATO calendar. The EWE assigns each unit a specific set of three digit numbers. The EWE uses these sets of numbers to identify which unit is submitting an airborne electronic attack request. The mission block allows the unit to request several different airborne electronic attacks for that ATO date.

ELECTROMAGNETIC INTERFERENCE

3-38. *Electromagnetic interference* is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment (JP 3-13.1). It can be induced intentionally, as in some forms of EW, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like.

3-39. Electromagnetic interference may be a major concern of commanders, staffs, and operational units during execution. Not all electromagnetic interference (EMI) requires action. Only when the EMI impacts operations by prohibiting friendly use of the spectrum does EMI become an issue. Units should incorporate effective techniques to minimize, reduce, or eliminate prohibitive EMI into every unit's operations.

3-40. EMI mitigation begins with operator-level troubleshooting and reporting. Troubleshooting may identify the source of the interference as truly EMI or an equipment or operator failure. Reporting facilitates situational understanding and supports the development of solutions. See table 3-1 for steps to mitigate EMI problems.

Table 3-1. Operator EMI troubleshooting checklist

Step	*Tasks*
1	Follow equipment troubleshooting (verify frequency, cable and antenna connections, communications security). If EMI continues, then follow remaining steps.
2	Determine start and stop times or duration of EMI.
3	Identify EMI effect (interfering voice, noise, static).
4	Identify other emitters in area of operations.
5	Check adjacent and nearby units for similar problems.
6	Prepare and submit joint spectrum interference resolution report to S-6.
EMI S-6	electromagnetic interference signal staff officer

JOINT SPECTRUM INTERFERENCE RESOLUTION PROGRAM

3-41. All prohibitive EMI is reported and investigated through the joint spectrum interference resolution (JSIR) program. Some procedural guidance in support of the JSIR program may apply to command relationships such as military departments, Army commands, and combatant commands. The G-6 (S-6) and spectrum manager are also good sources of information. CJCSI 3320.02F contains guidance for this program. CJCSM 3320.02D contains procedures for JSIR.

ELECTROMAGNETIC INTERFERENCE BATTLE DRILL

3-42. Prohibitive EMI that has a measureable operational impact and develops into a priority for immediate resolution by the commander may be resolved by an EMI battle drill. (See table 3-2 on page 3-8.) A battle drill helps isolate the cause of EMI and dispel erroneous assumptions about its root cause. For example, knowing that CREW devices are jammers may lead to a hasty assumption that an EMI event is caused by a unit's CREW system that then may lead to a loss of confidence and reluctance to use the CREW system.

3-43. Once the JSIR has been submitted, higher headquarters takes additional actions to solve the problem, avoid future interference, and allow for mission success. An EMI battle drill allows units to respond in a consistent methodical manner.

Table 3-2. Sample EMI battle drill

Responsible party	*Task*	
G-6 (S-6)	• Receive joint spectrum interference resolution report from affected unit. • Check with adjacent units to determine are affected. • Verify frequency assignment or SATCOM authorization. • Perform mitigation as required. • If PNT system is affected, coordinate with space element. • Develop response options.	
EWE	• Determine if electronic attack assets are in the vicinity of the affected unit. • Notify and coordinate with subordinate EWEs and EW staffs. • Report findings to G-6 (S-6) and spectrum manager. • Develop response options.	
Space Element	**SATCOM Interference**	**PNT Interference**
	• Conduct analysis to determine location of EMI. • Determine impact of EMI and recommend countermeasures. • Develop response options.	• Verify affected unit's receivers configured properly. • Discuss jamming mitigation techniques with unit. • Contact other military and nonmilitary organizations to monitor jammer detection and location. • Develop response options or support.
Operations Chief	• Notify command group. • Notify higher headquarters. • Notify host-nation liaison officer. • Reposition information collection assets as required. • Monitor engagement. • Develop response based on staff input. • Provide final report to command group.	

EMI	electromagnetic interference	PNT	positioning, navigation, and timing
EW	electronic warfare	S-6	battalion or brigade signal staff officer
EWE	electronic warfare element	SATCOM	satellite communications
G-6	assistant chief of staff, signal		

Chapter 4

Electronic Warfare Targeting

This chapter discusses electronic warfare targeting. It begins with a discussion of electronic warfare in the targeting process. It concludes with a discussion of calling for electronic attack fires.

ELECTRONIC WARFARE IN THE TARGETING PROCESS

4-1. The modern battlefield presents more targets than available resources can acquire and attack. The commander determines which targets are the most important to the enemy and which ones must be acquired and attacked. As the operation continues, the staff assesses the results.

4-2. *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 4-1.) 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.

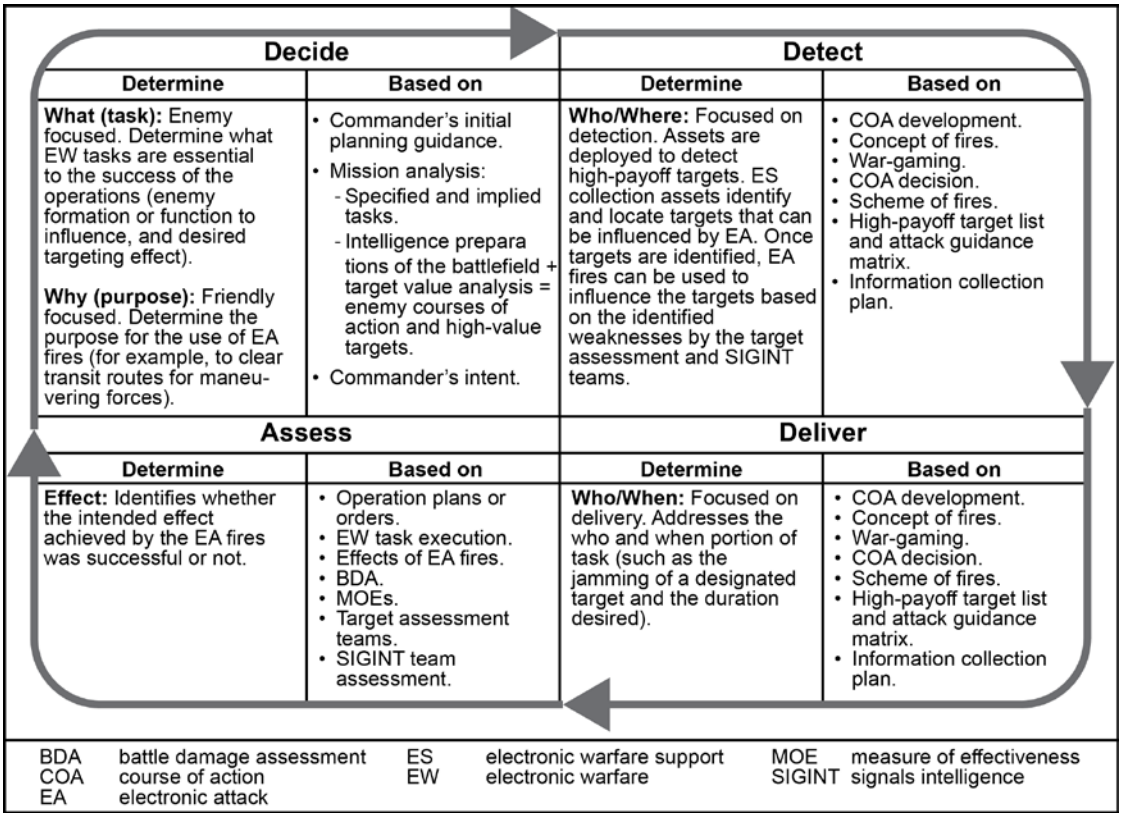

Figure 4-1. Electronic warfare in the targeting process

4-3. 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. (FM 6-0 has detailed information on operation plans and orders. FM 3-60 has more information on targeting.)

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

- Helps the targeting working group determine EA requirements against specific high-payoff targets and high-value targets.
- Ensures EA can meet the desired effect (in terms of the targeting objective).
- Ensures EA will not adversely affect friendly electromagnetic spectrum use.
- Coordinates with the SIGINT staff element through the collection manager to satisfy ES and EA information requirements.
- Provides EA mission management through the command post or joint operations center and the tactical air control party (for airborne electronic attack).
- Provides EA mission management as the electronic warfare control authority for ground or airborne electronic attack when designated.
- Determines and requests theater Army EA support.
- Recommends to the G-3 (S-3) and the fire support coordinator or fire support officer whether to engage a target with EA.
- Expedites EMI reports to the targeting working group.

DECIDE

4-5. 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 information collection. As part of the staff in the main command post, 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 EA 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 information collection procedures. The planned use of EA is integrated into the standard targeting products (graphic or text based). Products that involve EA planning may include—

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

DETECT

4-6. Based on what the targeting working group identified as high-payoff targets during the decide step, collection assets are then allocated and tasked to detect them. The intelligence enterprise pairs assets to targets based on the collection plan and the current threat situation. When conducting EA tasks, information collection units perform ES tasks linked to and working closely with the EA missions. EW support units (with support from the target assessment and SIGINT staff elements) provide the data—location, signal strength, and frequency of the target—to focus EA assets on the intended target. These assets also identify the enemy's command and control system vulnerabilities open to attack by EA assets.

DELIVER

4-7. 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. EA assets must satisfy the attack guidance developed during the decide step. Close coordination between those conducting ES and EA is critical during the engagement. The EWO facilitates this coordination and ensures EA fires are fully synchronized and deconflicted with other fires. This officer remains aware of the potential for unintended effects between adjacent units when

conducting EA. 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

4-8. Once the target has 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.
- Reattack recommendations.

4-9. 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 (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 enemy's centers of gravity). The last element involves the assessment and recommendation whether or not to reattack the targets.

4-10. 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 SIGINT staff element and units executing the EA mission coordinate continuously to assess mission effectiveness. Close coordination between sensor and shooter allows timely feedback on the success or failure of the intended jamming effects. It also can quickly provide the necessary adjustments to produce desired effects.

CALL FOR ELECTRONIC ATTACK FIRES

4-11. Like all forms of fire, EA effects are controlled through a specific call for fire format with specific brevity codes and procedures. Appendix K of ATP 3-09.32 contains detailed instructions for performing these missions. This appendix is classified and available on the SECRET Internet Protocol Router Network at https://www.acc.af.smil.mil/alsa/.

This page intentionally left blank.

Chapter 5

Electronic Warfare in Joint and Multinational Operations

Considering the nature, availability, and allocation of electronic warfare assets, electronic warfare operations are typically joint operations by necessity. This chapter first describes joint electronic warfare operations. It then discusses joint force principal staff for electronic warfare. The chapter concludes with a discussion of multinational electronic warfare operations.

JOINT ELECTRONIC WARFARE OPERATIONS

5-1. 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.

5-2. 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. (JP 3-13.1 establishes the guidelines and organizational framework for joint EW operations.)

5-3. 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 EWC, or information operations element.

5-4. 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

5-5. For joint EW operations, 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 a joint information operations cell assist the J-3. The J-3 organizes the joint information operations cell consisting of the EW staff and other information-related capabilities. (See JP 3-33 for joint task force headquarters organization design.) One of the actions required during the planning process is to work in concert with J-6 electromagnetic spectrum managers to integrate EW spectrum use into the overall spectrum plan for the organization. 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 EWO is the principal EW planner on the J-3 staff. This officer coordinates with the joint 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

5-6. 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, whether Army or other Service, 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.

5-7. On many joint staffs, the intrastaff coordination previously accomplished through a joint force commander's EW staff is performed by a joint information operations cell or similar organization. A joint 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 a joint information operations cell exist, a joint force commander's EW staff representative may be assigned to the joint 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

5-8. 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

5-9. Joint task force component commanders exercise operational control of their EW assets. Each component is organized and equipped to perform EW tasks to support 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. 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 planning and execution organization. The senior Army organization's staff EWO anticipates this requirement and prepares to support the augmentation if requested.

5-10. A major consideration for standing up a joint EWC at the component command level is access to a special compartmented information facility (known as SCIF) 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.

5-11. 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.

5-12. Coordination occurs through CEMA working groups from theater army level to brigade 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 AOC. EW staffs at higher echelons monitor EW activities and resolve conflicts when necessary.

JOINT FREQUENCY MANAGEMENT OFFICE

5-13. Joint policy tasks each geographic combatant commander to establish a structure to manage 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. 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.

5-14. The G-6 (S-6) coordinates the Army's use of the electromagnetic spectrum, frequency management, and frequency deconfliction with the joint frequency management office through network operations. If established, coordination with the joint spectrum management element is required. (See figure 5-1.)

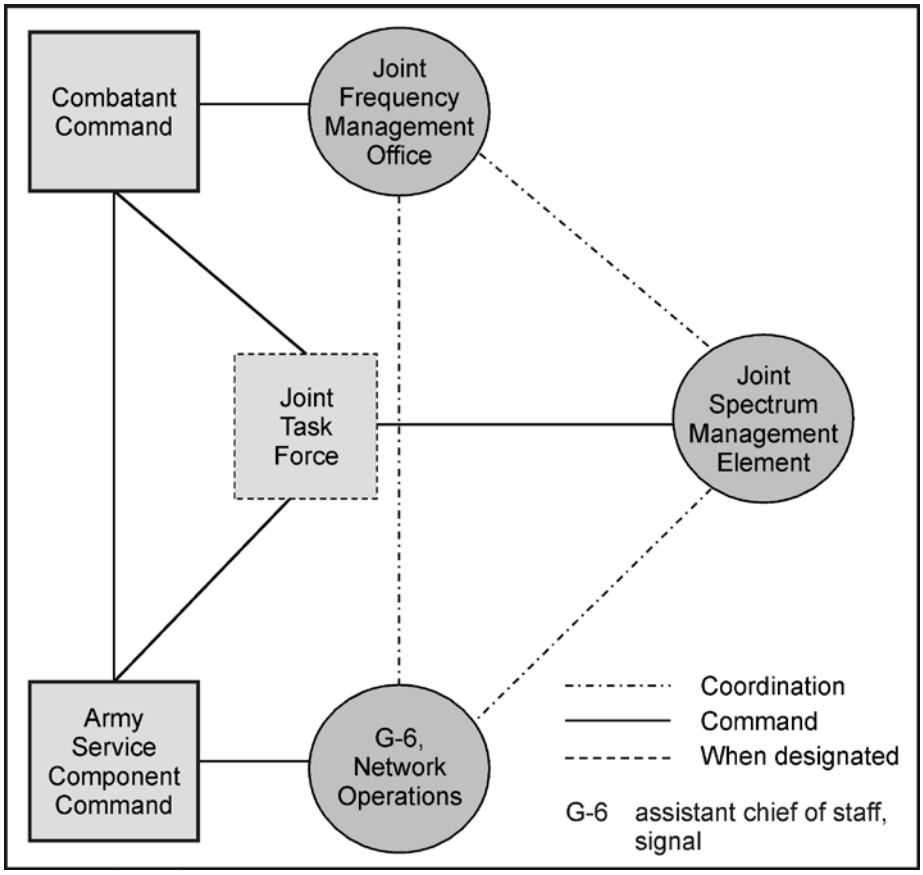

Figure 5-1. Joint frequency management coordination

JOINT INTELLIGENCE CENTER

5-15. 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 support requests are coordinated through the requirement cell and then forwarded to the requirements division within the joint intelligence center. (See figure 5-2 on page 5-4.)

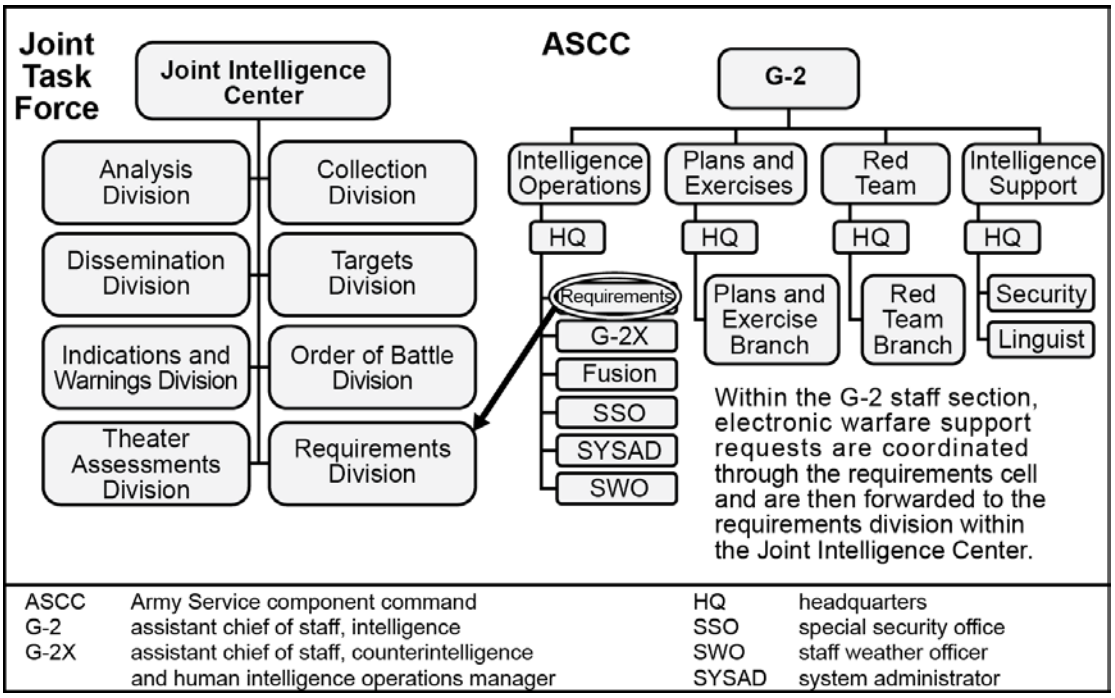

Figure 5-2. Electronic warfare request coordination

5-16. 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 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

5-17. 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

5-18. 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

5-19. The multinational force commander provides guidance for planning and conducting EW operations with support from the joint EWC. The joint EWC is located at multinational force headquarters. A joint information operations cell may also be established to coordinate all information operations activities, including related EW activities.

JOINT OPERATIONS STAFF SECTION

5-20. 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.

MULTINATIONAL JOINT ELECTRONIC WARFARE CELL

5-21. 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 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

5-22. EW mutual support is 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 exchanging information on friendly and enemy forces.
- Development of communications protocols with the appropriate NATO standardization agreements (known as STANAGs).
- Provision of secure, dedicated, and survivable communications.

JOINT SPECTRUM MANAGEMENT ELEMENT

5-23. The joint spectrum management element is an integral part of the multinational joint force headquarters J-6 staff. The joint spectrum management element's primary function is to ensure assigned military forces are authorized sufficient use of the electromagnetic spectrum to accomplish their mission. The joint spectrum management element is also the focal point for EMI investigation for the multinational force commander. For additional information, see CJCSM 3320.01C.

OTHER CONSIDERATIONS

5-24. EW in multinational operations addresses other considerations. Soldiers must consider—

- The exchange of EW information.

- The exchange of SIGINT information.
- The exchange of the electronic threat characteristics.
- Electronic warfare reprogramming.

5-25. 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.

5-26. Exchanging SIGINT information requires care to avoid violating SIGINT security rules. The policy and relationship between EW and SIGINT within NATO are set out in a NATO Military Committee document (refer to chapter 5 of JP 3-13.1).

5-27. In peacetime, before forming a multinational force, the exchange of electronic threat characteristics 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 up-to-date electronic threat characteristics. The inclusion of multinational forces is based on security and information exchange guidelines agreed upon by the participating nations.

5-28. EW reprogramming is a national responsibility. However, the joint EWC acknowledges that multinational forces conduct reprogramming efforts. (ATP 3-13.10 guides the Army's reprogramming effort.)

Appendix A

Forms, Reports, and Messages

Electronic warfare officers use several different forms, reports, and messages in the performance of their duties. The form, message, and report formats contained in this appendix are in addition to those found in FM 6-99 and represent the most common ones used by electronic warfare officers during unified land operations. Techniques for completing each are included and represent processes developed by the operating force and may be modified to fit individual unit needs.

JOINT TACTICAL AIR STRIKE REQUEST

A-1. EWOs use DD Form 1972 to request an airborne electronic attack. JTARs specify the effects desired using air and space power. This is critical to helping air planners in the combat AOC determine both aircraft and effects load required to support the JTAR. To ensure the air component achieves the effects desired by the ground component, the JTARs must describe clear and detailed effects. Most organizations require the submission of a JTAR and an electronic attack request format together. Therefore, the JTAR and electronic attack request format must complement each other. JP 3-09.3 contains the line-by-line instructions for completing both forms. Once completed, DD Form 1972 becomes classified SECRET.

JOINT SPECTRUM INTERFERENCE RESOLUTION REPORT

A-2. The JSIR report is used to report EMI for building situational understanding of the threat and aiding in the development of mitigation procedures. The report preparer provides a copy of the completed form to the EWO, spectrum manager, and G-6 (S-6).

A-3. Affected end users report EMI through JSIR-Online, if available. The JSIR-Online portal is located on the Secure Internet Protocol Network at https://intelshare.intelink.sgov.gov/sites/jsir/default.jspx. Unit standard operating procedures may also require a JSIR be submitted through the chain of command using the JSIR format in figure A-1 on page A-2. The report preparer provides a copy of the completed form to the EWO, spectrum manager, and G-6 (S-6).

Format for Manually Prepared
JOINT SPECTRUM INTERFERENCE RESOLUTION REPORT

Date of Report: *When the report was prepared; not when interference occurred*.

1. Originator/Report Preparer Information: *Identify the person preparing this report to assist with follow-up actions or questions. Include title, name, organization, location, telephone number, and e-mail address in sufficient detail to allow anyone reading the report to identify the preparer of this report.*
2. Organization Experiencing the Interference Information: *Identify the organization by name and location; provide a point of contact with first-hand knowledge of the interference. If the report originator or preparer is the same as the unit point of contact, then state "POC same as originator" or words to that effect.*
3. Where and when interference occurred:
   a) Date(s): *(include entire date range if more than one day).*
   b) Time period: *(use precise hour and minute of start and end time, if known).*
   c) State/country: *(provide geographic name).*
   d) Location: *(briefly describe the location such as, "on a road through a mountain valley…").*
   e) Coordinates: *(military grid or latitude and longitude).*
4. Description of the type of interference: *(meaconing, intrusion, jamming, or interference).*
5. Description of the system and radio frequency disrupted or degraded: *(nomenclature[s] and frequency[ies]).*
6. Impact of interference to the mission: *(describe how the interference is affecting the unit's ability to accomplish the mission).*
7. Report all local actions and troubleshooting that have been taken to resolve the problem: *(attach addition pictures or documents to report troubleshooting) (identify the steps taken and whether those efforts had any effect on the interference).*
8. Type of assistance required: *(indicate specific actions the affected unit would like to occur to mitigate the interference).*
9. Cause of interference (if known): *(identify what caused the interference and how this determination was made).*
10. Recommendation for improving resolution techniques or new frequency allocation: *(only filled out by the spectrum investigating unit or frequency manager).*

Figure A-1. Sample joint spectrum interference resolution format

STOP JAMMING MESSAGE

A-4. An approved jamming task may not have a defined stop time. The stop jamming message may be sent by voice or an internet chat session to end an active jamming task. (See figure A-2.)

Stop Jamming Message

GENERAL INSTRUCTIONS: Use to terminate a jamming task conducted by an electronic attack (EA) asset.

LINE 1 – DATE & TIME: *(Date-time group of when jamming should be terminated).*

LINE 2 – UNIT: *(Unit supported by jamming mission and is requesting termination).*

LINE 3 – FREQUENCY: *(Enter the radio frequency being jammed or enter "ALL" if jamming is to stop on all jammed frequencies).*

LINE 4 – NARRATIVE: *(Any additional information required for clarification).*

LINE 5 – AUTHENTICATION: *(Message authentication if unit standard operating procedures require authentication).*

Figure A-2. Sample stop jamming message format

Appendix B

Jamming Calculations

This appendix discusses jamming formula symbols, the minimum jammer power output, and the jammer maximum distance. Electronic warfare officers use jamming formulas to determine the jamming power output and jammer distance to target. Although the electronic warfare element may never have to use these calculations to plan a jamming mission, this information is provided to enable the electronic warfare officer and staff to better understand the technical aspects of jamming and establish the basis for advising the commander on jamming mission characteristics and effects.

FORMULA SYMBOLS

B-1. Mathematical formulas use the symbols in table B-1. Each symbol identifies a unit of measure that must be used for the calculation to be accurate.

Table B-1. Jammer formula symbols

Symbol	*Use of*
Pj	Minimum amount of jammer power output required in watts (read on power output meter of the jammer).
Pt	Power output of the enemy transmitter in watts.
Hj	Elevation of the jammer location above sea level in feet (does not include antenna height or length).
Ht	Elevation of the enemy transmitter location above the sea level.
Dj	Jammer location-to-target receiver location distance in kilometers.
Dt	Enemy transmitter location-to-target receiver location distance in kilometers.
K	Frequency modulated (FM) jammer tuning accuracy factor.
n	Terrain and ground conductivity factors: 5 = Very rugged terrain (rocky mountains or desert) with poor ground conductivity. 4 = Moderately rugged terrain (rolling to high hills, forests) with fair to good ground conductivity. 3 = Rolling hills (farmland type terrain) with good ground conductivity. 2 = Level terrain (over water, sea, lakes, and ponds) with good ground conductivity.

B-2. The technical data needed to solve the equation are found in technical manuals or specifications written for friendly equipment and technical intelligence publications for enemy systems. The G-2 (S-2) may be able to provide data on enemy systems. Sometimes enemy forces use off-the-shelf equipment whose technical data may be found on the internet. It may be necessary to estimate data when no information is available.

FORMULA 1 – MINIMUM JAMMER POWER OUTPUT

B-3. This formula is used to compute the minimum jammer power output required to jam the target receiver. It is written as—

$$Pj = Pt \times K \times \left(\frac{Ht}{Hj}\right)^2 \times \left(\frac{Dj}{Dt}\right)^n$$

B-4. The difference between Ht and Hj is less than 10 meters, then they are considered to be at the same elevation. When dividing Dj by Dt, include the second decimal place and do not round off. Also, note that this is for a jammer using a whip antenna; divide the result by 2 for a log periodic array (known as LPA) antenna. Figure B-1 provides a sample calculation.

Calculate the minimum power needed to jam an enemy receiver. The enemy receiver is 17 kilometers from the friendly jammer. The enemy transmitter is rated at 5 watts power output and is located 9 kilometers from its intended receiver location. The enemy transmitter is 385 meters above sea level and the friendly jammer is 388 meters above sea level. The terrain is moderately rugged with rolling high hills and forests. The formula data is—

Dt = Enemy transmitter to target receiver distance = 9 kilometers
Dj = Jammer to target receiver distance = 17 kilometers
Pt = Power output of enemy transmitter = 5 watts
Ht = Elevation of enemy transmitter = 385 meters
Hj = Elevation of friendly jammer = 388 meters
K = FM jammer tuning accuracy factor = 2
n = Terrain and ground conductivity factor = 4

$$Pj = Pt \times K \times \left(\frac{Ht}{Hj}\right)^2 \times \left(\frac{Dj}{Dt}\right)^n$$

$$Pj = 5 \times 2 \times \left(\frac{385}{388}\right)^2 \times \left(\frac{17}{9}\right)^4$$

$$Pj = 10 \times (1)^2 \times (1.88)^4$$

$$Pj = 10 \times 12.46$$

$$Pj = 124.60 \; or \; 125 \; watts$$

Therefore, the minimum power output for the friendly jammer must be at least 125 watts with a whip antenna and 62.5 watts with an LPA antenna. Less jammer power output will produce ineffective jamming results.

FM	frequency modulated
LPA	log periodic array

Figure B-1. Sample minimum jammer power output calculation

FORMULA 2 – JAMMER MAXIMUM DISTANCE

B-5. This formula is used to determine the maximum distance a jammer using a whip antenna from the target receiver. For the log periodic array antenna, double the Pj factor. The formula is written as—

$$Dj = Dt \times \sqrt[n]{\frac{Pj}{Pt \times K \times \left(\frac{Ht}{Hj}\right)^2}}$$

B-6. Note that since formula 2 determines maximum distance, the number used for Pj (jammer power output) should be the maximum power the jammer can produce. Figure B-2 provides a sample calculation.

Calculate the maximum distance a friendly jammer may be from an enemy receiver. Using the same tactical situation as in figure B-1, the enemy transmitter is rated at 5 watts power output and is located 9 kilometers from its intended receiver location. The enemy transmitter is 385 meters above sea level and the friendly jammer is 388 meters above sea level. The friendly jammer has a maximum power rating of 1500 watts. The terrain is moderately rugged with rolling high hills and forests. Formula data is—

Dt = Enemy transmitter to target receiver distance = 9 kilometers
Pj = Maximum power output of friendly jammer = 1500 watts
Pt = Power output of enemy transmitter = 5 watts
Ht = Elevation of enemy transmitter = 385 meters
Hj = Elevation of friendly jammer = 388 meters
K = FM jammer tuning accuracy factor = 2
n = Terrain and ground conductivity factor = 4

$$\boldsymbol{Dj = Dt \times \sqrt[n]{\frac{Pj}{Pt \times K \times \left(\frac{Ht}{Hj}\right)^2}}}$$

$$\boldsymbol{Dj = 9 \times \sqrt[4]{\frac{1500}{5 \times 2 \times \left(\frac{385}{388}\right)^2}}}$$

$$\boldsymbol{Dj = 9 \times \sqrt[4]{\frac{1500}{10 \times (1)^2}}}$$

$$\boldsymbol{Dj = 9 \times \sqrt[4]{\frac{1500}{10}}}$$

$$\boldsymbol{Dj = 9 \times \sqrt[4]{150}}$$

$$\boldsymbol{\underline{Dj = 9 \times 3.5 = 31.5\ km}}$$

Therefore, the jammer using a whip antenna may be located a maximum of 31.5 kilometers from the enemy receiver. For a jammer using the LPA antenna, use 3000 watts for Pj and the result is 37.44 kilometers.

FM	frequency modulated
LPA	log periodic array

Figure B-2. Sample jammer maximum distance calculation

This page intentionally left blank.

Appendix C

Electronic Warfare Equipment

This appendix provides information on Army and other Service electronic warfare capabilities. It is not an all-inclusive list. Due to the evolving nature of electronic warfare equipment and systems, this information is perishable and should be augmented, updated, and maintained by the unit electronic warfare officer.

ARMY

C-1. The Army is currently expanding its EW capability. It maintains several EW systems in its inventory. When requested, the Army provides these capabilities to combatant commands for employment at corps and lower echelons.

COUNTER RADIO-CONTROLLED IMPROVISED EXPLOSIVE DEVICE ELECTRONIC WARFARE SYSTEMS

C-2. CREW systems form a family of EA systems. Although the Army has the largest inventory, all U.S. ground forces use these systems to prevent improvised explosive device detonation by radio frequency energy. These forces maintain a mounted, dismounted, and fixed-site CREW capability to protect personnel and equipment. As technology improves, the capabilities of some systems have progressed beyond mere jammers to providing data collection and signal location. The systems currently in use by U.S. forces and multinational partners include—

- Duke V2/V3 (mounted and fixed site).
- Symphony (mounted).
- Thor III (dismounted).
- Baldr (dismounted).
- Guardian (dismounted).

C-3. Jammers may function in an active or reactive mode. Active means the jammer continuously emits a signal to block a preprogrammed frequency. It is effective against multiple low-power signals but may be easily located by direction finding equipment and may not be effective against high-power signals. Reactive jammers search for specific signals and then emit the jamming signal. Reactive jammers are less susceptible to being exploited by location finding and are excellent against high-power signals, but effectiveness may be reduced in a congested signals environment.

AIRCRAFT SURVIVABILITY EQUIPMENT

C-4. Aircraft survivability equipment aims to reduce aircraft vulnerability, thus allowing aircrews to accomplish their immediate mission and survive. Army aviation maintains a suite of aircraft survivability equipment that provides protection against enemy weapon systems employing the electromagnetic spectrum for detection, tracking, and targeting. This protection can include radio frequency warning and countermeasures systems, a common missile warning system, information requirement countermeasures systems, and laser detection and countermeasure systems.

INTELLIGENCE SYSTEMS

C-5. The intelligence community maintains many systems that provide data for use in EW operations. SIGINT systems provide most of this required data. These assets are dual use. Usually the data collected is categorized as SIGINT. The National Security Agency/Central Security Service governs and maintains the data within sensitive compartmented information channels. The data sometimes support EW or, more

specifically, ES. Paragraphs C-6 and C-7 illustrate some SIGINT systems that, when tasked, can provide ES data to support EA and EP actions.

Guardrail Common Sensor

C-6. The Guardrail common sensor is a corps-level airborne SIGINT collection and location system. It provides tactical commanders with near real-time targeting information. Key features include the following: integrated communications intelligence and electronic intelligence reporting, enhanced signal classification and recognition, near real-time direction finding, precision emitter location, and an advanced integrated aircraft cockpit. Preplanned product improvements include frequency extension, computer-assisted online sensor management, upgraded data links, and the capability to exploit a wider range of signals. The Guardrail common sensor shares technology with the ground-based common sensor, airborne reconnaissance-low, and other joint systems.

Prophet

C-7. Prophet enhanced is a dedicated, all-weather, any time, ground-based tactical SIGINT system. This system provides force protection and situational awareness through technologically advanced intelligence support to brigade combat team, Stryker brigade combat team, and enhanced military intelligence brigade commanders. Prophet systems provide commanders flexible, modular components for their mission.

Ground Auto-Targeting Observation/Reactive Jammer

C-8. The ground auto-targeting observation/reactive (known as GATOR) jammer is a fixed-site EW asset providing both ES and EA capabilities. This jammer may be networked with other EW assets or operate as a standalone system. It is particularly useful for detecting and jamming enemy communications.

Communications Electronic Attack Surveillance and Reconnaissance

C-9. Communications electronic attack surveillance and reconnaissance (known as CEASAR) is an aerial EW asset that provides beyond line-of-sight command, control, and communications jamming.

MARINE CORPS

C-10. The Marine Corps has two types of EW units: radio battalions (often called RADBNs), and Marine tactical EW squadrons (referred to as VMAQs). Paragraphs C-11 through C-25 discuss the units' missions, primary tasks, and capabilities currently being employed. (For further information on the Marine Corps EW units and systems, see MCWP 2-22.)

RADIO BATTALION

C-11. Radio battalions are the Marine Corps' tactical level ground-based EW units. During operations, teams from radio battalions are most often attached to the command element (or senior headquarters) of Marine expeditionary units. Each radio battalion has specific mission, tasks, and equipment.

Mission and Tasks

C-12. The mission of the radio battalion is to provide communications security monitoring, tactical SIGINT, EW, and special intelligence communication support to the Marine air-ground task force (MAGTF). The radio battalion's tasks include—

- Executing interception; radio direction finding; recording and analysis of communications and noncommunications signals; and SIGINT processing, analysis, production, and reporting.
- Conducting EW against enemy communications.
- Helping protect MAGTF communications from enemy exploitation by conducting communications security monitoring, analysis, and reporting on friendly force communications.
- Providing special intelligence communications support and cryptographic guard (personnel and terminal equipment) to support the MAGTF command element. Normally, the communications

unit supporting the MAGTF command element provides communications connectivity for special intelligence communications.

- Providing task-organized detachments to MAGTFs with designated SIGINT, EW, special intelligence communication, and other required capabilities.
- Exercising technical control and direction over MAGTF SIGINT and EW operations.
- Providing radio reconnaissance teams with specialized insertion and extraction capabilities (such as combat rubber raiding craft, fast rope, rappel, helocast, and static-line parachute) for specified SIGINT and limited EA support during advance force, preassault, or deep postassault operations.
- Coordinating technical SIGINT requirements and exchanging technical information and material with national, combatant command, joint, and other SIGINT units.
- Providing intermediate, third, and fourth echelon maintenance of the radio battalion's SIGINT and EW equipment.

Equipment

C-13. The radio battalion uses EW capabilities to accomplish the mission and perform the tasks to support the MAGTF.

AN/ULQ-19(V)2 Electronic Attack Set

C-14. The AN/ULQ-19(V)2 EA set allows operators to conduct spot or sweep jamming of single-channel voice or data signals. To provide the required jamming, the system must be employed and operated from a location with an unobstructed signal line of sight to the target enemy's communications transceiver.

AN/MLQ-36 Mobile Electronic Warfare Support System

C-15. The AN/MLQ-36 mobile ES system provides a multifunctional capability that gives SIGINT and EW operators limited armor protection. This equipment can provide SIGINT and EW support to highly mobile mechanized and urban operations where maneuver or armor protection is critical. This system is installed in a logistic variant of the Marine Corps' light armored vehicle. It consists of the following:

- Signals intercept system.
- Radio direction finding system.
- Electronic attack system.
- Secure communications system.
- Intercom system.

AN/MLQ-36A Mobile Electronic Warfare Support System (Product Improved)

C-16. The product-improved AN/MLQ-36A mobile ES system (sometimes called the AN/MLQ-36A MEWSS PIP) is an advanced SIGINT and EW system integrated into the Marine Corps' light armored vehicle. This system replaces the equipment of the AN/MLQ-36.

C-17. The AN/AMLQ-36A has the following capabilities:

- Detect and evaluate enemy communications emissions.
- Detect and categorize enemy noncommunications emissions (such as battlefield radars).
- Determine lines of bearing.
- Degrade enemy tactical radio communications.

When mission-configured and working cooperatively with other AN/MLQ-36As, the system can provide precision location of battlefield emitters.

C-18. This system and its future enhancements will provide the capability to exploit new and sophisticated enemy electronic emissions and conduct EA to support existing and planned national, combatant command, fleet, and MAGTF SIGINT and EW operations.

MARINE TACTICAL ELECTRONIC WARFARE SQUADRON

C-19. Marine tactical EW squadrons are the Marine Corps' airborne tactical EW units. Each squadron has certain mission, tasks, and capabilities.

Mission and Tasks

C-20. The mission of the Marine tactical EW squadron is to provide EW support to the MAGTF and other designated forces. The squadron conducts tactical jamming to prevent, delay, or disrupt the enemy's ability to use the following kinds of radars: early warning, acquisition, fire or missile control, counterfire, and battlefield surveillance. Tactical jamming also denies and degrades enemy communication capabilities. The squadron conducts electronic surveillance operations to maintain electronic orders of battle. These include both selected emitter parameters and nonfriendly emitter locations. The squadron also provides threat warnings for friendly aircraft, ships, and ground units. Squadron tasks include—

- Providing airborne electronic attack and EW support to the aviation combat element and other designated operations by intercepting, recording, and jamming threat communications and noncommunications emitters.
- Processing, analyzing, and producing routine and time-sensitive electronic intelligence reports for updating and maintaining enemy electronic threat characteristics.
- Providing liaison personnel to higher staffs to assist in squadron employment planning.
- Providing an air EW liaison officer to the MAGTF EW coordination cell.
- Conducting EA operations for EP training of MAGTF units.

C-21. The squadron's EW division supports EA-6B Prowler tactical missions with intelligence, the tactical electronic reconnaissance processing and evaluation system (TERPES), and the joint mission planning system. All systems support premission planning and postmission processing of collected data, and production of pertinent intelligence reports. Working with squadron intelligence, these systems provide required electronic intelligence and electronic threat characteristics intelligence products to the aviation combat element, MAGTF, and other requesting agencies.

Equipment

C-22. Marine tactical electronic warfare squadrons maintain the following equipment:

- EA-6B Prowler.
- TERPES.

EA-6B Prowler

C-23. The EA-6B Prowler is a subsonic, all-weather, carrier-capable aircraft. The crew consists of one pilot and three electronic countermeasure officers. The EA-6B Prowler has two primary missions. One is collecting and processing designated threat signals of interest for jamming and subsequent processing, analysis, and intelligence reporting. The other is employing the AGM-88 high-speed antiradiation missile against designated targets. The EA-6B's AN/ALQ-99 tactical jamming system incorporates receivers for the reception of emitted signals and external jamming pods for the transmission of energy to jam targeted radars (principally those associated with enemy air defense radars and associated enemy command and control). In addition to the AN/ALQ-99, the EA-6B Prowler also employs the USQ-113 communications jammer to collect, record, and disrupt threat communications.

AN/TSQ-90 Tactical Electronic Reconnaissance Processing and Evaluation System

C-24. The TERPES (AN/TSQ-90) is an air and land transportable, single-shelter electronic intelligence processing and correlation system. Each of the four Marine tactical EW squadrons includes a TERPES section.

C-25. A TERPES section consists of Marines, equipment, and software. The section identifies and locates enemy radar emitters from data collected by EA-6B aircraft and those received from other intelligence sources. A TERPES section processes and disseminates EW data rapidly to MAGTF and other intelligence

centers and provides mission planning and briefing support. Section support areas include operational support, intelligence analysis support, data fusion, fusion processing, and intelligence reporting. The TERPES section provides the following operational support:

- Translates machine-readable, airborne-collected, digital data into human- and machine-readable reports (such as paper, magnetic tape, secure voice, plots, and overlays).
- Receives and processes EA-6B mission tapes.
- Accepts, correlates, and identifies electronic emitter data from semiautomatic or automatic collection systems using various electronic parameter databases and various analysis techniques.
- Provides tactical jamming analysis.

AIR FORCE

C-26. The Air Force has two primary platforms that provide EW capability: the EC-130H Compass Call and RC-135V/W Rivet Joint. (For further information on Air Force EW, see Air Force Annex 3-51.)

EC-130H COMPASS CALL

C-27. The EC-130H Compass Call is an airborne tactical weapon system.

Mission and Tasks

C-28. The EC-130H's mission is to disrupt enemy command and control information systems and limit the coordination essential for force management. The EC-130H's primary task is to employ offensive counterinformation and EA capabilities to support U.S. and multinational tactical air, surface, and special operations forces.

Capabilities

C-29. The EC-130H is designed to deny, degrade, and disrupt enemy command and control information systems. This includes denial and disruption of enemy surveillance radars; hostile communications being used to support enemy ground, air, or maritime operations; and many modern commercial communication signals that an enemy might employ.

RC-135V/W RIVET JOINT

C-30. The RC-135V/W Rivet Joint is a combatant-command-level surveillance asset that responds to national-level tasks.

Mission and Tasks

C-31. Its mission is to support national consumers, combatant commanders, and combat forces with direct, near real-time reconnaissance information and ES. It collects, analyzes, reports, and exploits information from enemy command and control information systems. During most contingencies, it deploys to the theater of operations with the airborne elements of the theater air control system.

Capabilities

C-32. The RC-135V/W Rivet Joint is equipped with an extensive array of sophisticated information gathering equipment that enables monitoring of enemy electronic activity. The aircraft is integrated into the theater air control system via data links and voice (as required). Refined intelligence data can be transferred from Rivet Joint to an Airborne Warning and Control System platform through the tactical digital information link. Alternatively, this data can be placed into intelligence channels via satellite and the tactical information broadcast service (a near real-time combatant command information broadcast). The aircraft has secure ultrahigh frequency, very high frequency, and high frequency (commonly known as UHF, VHF, and HF, respectively) as well as satellite communications. It can be refueled in the air.

NAVY

C-33. The Navy's primary airborne EW platforms are the EA-6B Prowler and the E/A-18G Growler. The Navy also maintains both surface and subsurface EW shipboard systems for offensive and defensive missions to support the fleet. (For further information on Navy missions and equipment, see NWP 3-13.)

EA-6B PROWLER

C-34. The EA-6B Prowler is a subsonic, all-weather, carrier-capable aircraft. The crew consists of one pilot and three electronic countermeasure officers. Although the Navy's EA-6B Prowler is in the process of being removed from service, the Navy still uses them in current operations.

Mission and Tasks

C-35. The mission of the Navy's EA-6B Prowler is to ensure survivability of U.S. and multinational forces through suppression of enemy air defenses (using the radar-jamming AN/ALQ-99 tactical jamming system), lethal suppression (using the AGM-88 high-speed antiradiation missile), and communications jamming (using the USQ-113 radio countermeasures set). Prowlers have supported U.S. and multinational forces operating from various expeditionary sites throughout the world while maintaining full presence on all Navy aircraft carriers.

Capabilities

C-36. The Navy's EA-6B Prowlers either are outfitted with the improved capability II or improved capability III systems.

Improved Capability II

C-37. The improved capability II program was initiated in the 1980s. It was completed across the fleet of EA-6B aircraft (including U.S. Marine Corps aircraft) in the 1990s. The program incorporated incremental capability improvements that include communications, navigation, and computer interface upgrades; a high-speed antiradiation missile capability; and improved jamming pods. Several system interfaces were also upgraded in preparation for the improved capability III improvements.

Improved Capability III

C-38. The improved capability III program incorporates a highly evolved receiver system and provides upgraded EA-6B aircraft with increased signal detection, geolocation capability, a new selective reactive-jamming capability, and better reliability. High-speed antiradiation missile employment is also improved due to the speed of the receiver and its geolocation accuracy. Increased battlefield situational awareness of joint forces is also provided through Link-16. The improved capability III program provides a new ALQ-218 receiver system, integration of the USQ-113 and the multifunctional information distribution system (often called MIDS). This system incorporates Link-16 and various connectivity avionics into the EA-6B Prowler. The major EW-related subsystems are the AN/ALQ-99 (V) tactical jamming countermeasures set and AN/USQ-113 (V) radio countermeasures set.

C-39. The AN/ALQ-99 (V) tactical jamming countermeasures set has upgraded receivers and processors to provide the following:

- Improved frequency coverage.
- Direction-of-arrival determination capability.
- Narrower frequency discrimination to support narrowband jamming.
- Enhanced interface with onboard systems.

C-40. The AN/USQ-113 (V) radio countermeasures set enhances the aircraft's jamming capability through its integration with the tactical display system. This capability enables the crew to display AN/USQ-113 communications jamming data as well as control AN/USQ-113 operations through the tactical display system.

E/A-18G GROWLER

C-41. The E/A-18G Growler is the Navy's replacement aircraft for the EA-6B Prowler.

Mission and Tasks

C-42. The EA-18G Growler can detect, identify, locate, and suppress hostile emitters. It provides enhanced connectivity to national, combatant command, and strike assets. Additionally, the EA-18G Growler provides organic accurate emitter targeting using on-board suppression weapons, such as the high-speed antiradiation missile.

Capabilities

C-43. The following is a list of the E/A-18G Growler's general capabilities:

- Suppression of enemy air defenses. The EA-18G Growler counters enemy air defenses using both reactive and preemptive jamming techniques.
- Stand-off and escort jamming. The EA-18G Growler is highly effective in the traditional stand-off jamming mission, but with the speed and agility of a Super Hornet, it is effective in the escort role.
- Integrated air and ground airborne electronic attack. Enhanced situational awareness and uninterrupted communications enables the EA-18G Growler to achieve a higher degree of integration with ground operations than previously.
- Self-protect and time-critical strike support. With its active electronically scanned array radar, digital data links, and air-to-air missiles, the EA-18G Growler can protect itself and effectively identify and prosecute targets.
- Growth. High commonality with the F/A-18E and F/A-18F, nine available weapon stations, and modern avionics enable cost-effective synergistic growth, setting the stage for continuous capability enhancement.

C-44. The following is a list of the E/A-18G Growler's airborne electronic attack capabilities:

- Entire spectrum. The EA-18G Growler's ALQ-218 wideband receiver combined with the ALQ-99 tactical jamming system is effective against any surface-to-air threat.
- Precision airborne electronic attack. Selective-reactive technology enables the EA-18G Growler to rapidly sense and locate threats much more accurately than before. This improved accuracy enables greater concentration of energy against threats.
- Advanced communication countermeasures. Its modular communication countermeasure set enables the EA-18G Growler to counter a wide range of communications systems and is readily adaptable to an ever changing threat spectrum.
- EMI cancellation system. This system dramatically enhances aircrew situational awareness by enabling uninterrupted communications during jamming operations.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AOC	air operations center
ASCC	Army Service component command
ATO	air tasking order
ATP	Army techniques publication
CEMA	cyber electromagnetic activities
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff memorandum
COA	course of action
CREW	counter radio-controlled improvised explosive device electronic warfare
DA	Department of the Army
DD	Department of Defense (forms)
EA	electronic attack
EMI	electromagnetic interference
EP	electronic protection
ES	electronic warfare support
EW	electronic warfare
EWE	electronic warfare element
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-5	assistant chief of staff, plans
G-6	assistant chief of staff, signal
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
JP	joint publication
JRFL	joint restricted frequency list
JSIR	joint spectrum interference resolution
JTAC	joint terminal air controller
JTAR	joint tactical air strike request

MAGTF	Marine air-ground task force
MCWP	Marine Corps warfighting publication
MDMP	military decisionmaking process
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
NWP	Navy warfare publication
ROE	rules of engagement
S-2	intelligence staff officer
S-3	operations staff officer
S-4	logitics staff officer
S-5	plans staff officer
S-6	signal staff officer
SIGINT	signals intelligence
TERPES	tactical electronic reconnaissance processing and evaluation system
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)

cyber electromagnetic activities

Activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. (ADRP 3-0)

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

electromagnetic spectrum

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

electromagnetic spectrum management

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

electronic attack

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

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, e.g., radar. (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)

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)

unified land operations

How the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution. (ADP 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

(Army) A grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. (FM 6-0)

References

All URLS accessed on 12 November 2014.

REQUIRED PUBLICATIONS

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

ADRP 1-02. *Terms and Military Symbols*. 24 September 2013.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 08 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

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

CJCSI 3320.02F. *Joint Spectrum Interference Resolution*. 08 March 2013.

CJCSM 3320.01C. *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*. 14 December 2012.

CJCSM 3320.02D. *Joint Spectrum Interference Resolution (JSIR) Procedures*. 03 June 2013.

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

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

JP 3-09.3. *Close Air Support*. 08 July 2009.

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

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

JP 3-33. *Joint Task Force Headquarters*. 30 July 2012.

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

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

ARMY PUBLICATIONS

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

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

ADRP 3-0. *Unified Land Operations*. 16 May 2012.

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

ATP 3-09.32. *JFIRE Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower*. 30 November 2012.

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

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

FM 3-38. *Cyber Electromagnetic Activities*. 12 February 2014.

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

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

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

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

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

OTHER PUBLICATIONS

Annex 3-51. *Electronic Warfare Operations*. 28 July 2011. Available at https://doctrine.af.mil/.

MCWP 2-22. *Signals Intelligence*. 22 February 1999. Available at https://www.doctrine.usmc.mil/currentPubsListing.asp.

NWP 3-13. *Navy Information Operations*. February 2014. Available at https://ndls.nwdc.navy.mil/FilterDocList.aspx.

RECOMMENDED READINGS

FM 1-04. *Legal Support to the Operational Army*. 18 March 2013.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate web site: http://www.apd.army.mil/. DD Forms are available on the Office of the Secretary of Defense web site: http://www.dtic.mil/whs/directives/infomgt/forms/index.htm.

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

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

Index

Entries are by paragraph number.

Entries are by paragraph number.

ATP 3-36 (FM 3-36)
16 December 2014

By Order of the Secretary of the Army

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

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1434202

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).