ATP 3-12.3

Electromagnetic Warfare Techniques

JANUARY 2023

This document supersedes ATP 3-12.3, dated 16 July 2019.

Headquarters, Department of the Army

This publication is available at the Army Publishing Directorate site (https://www.armypubs.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

Army Techniques Publication
No. 3-12.3

Headquarters
Department of the Army
Washington, D.C., 30 January 2023

Electromagnetic Warfare Techniques

Contents

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

*This publication supersedes ATP 3-12.3, dated 16 July 2019.

Figures

Tables

Preface

ATP 3-12.3 complements the electromagnetic warfare tactics presented in FM 3-12. ATP 3-12.3 supersedes ATP 3-12.3, dated 16 July 2019.

The principal audience for ATP 3-12.3 is electromagnetic warfare professionals, spectrum managers, and unit leaders assigned to echelons theater army and below. Commanders and staffs of Army headquarters serving as a joint task force or multinational headquarters also use applicable joint or multinational doctrine for command and control of joint or multinational forces. Trainers and educators throughout the Army may also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of armed conflict and the rules of engagement (refer to FM 6-27). Commanders also adhere to the Army Ethic as described in ADP 6-22.

ATP 3-12.3 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. This publication is not the proponent for any Army terms. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition.

ATP 3-12.3 applies to the Active Army, Army National Guard, Army National Guard of the United States and United States Army Reserve, unless otherwise stated.

The proponent for ATP 3-12.3 is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Division, United States Army Cyber Center of Excellence. Send comments and recommendations on a Department of the Army Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-OPD (ATP 3-12.3), 416 B Street, Fort Gordon, GA 30905-5735, by e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@army.mil.

This page intentionally left blank.

Introduction

ATP 3-12.3 provides doctrinal guidance and direction to the Army for conducting electromagnetic warfare during Army operations. This publication provides a description of electromagnetic warfare roles, relationships, responsibilities, and capabilities to support Army and joint operations.

ATP 3-12.3 nests with and supports FM 3-12 and JP 3-85. Readers should be familiar with FM 3-0 and FM 6-0 to understand the fundamentals of integrating and synchronizing electromagnetic warfare with Army operations.

ATP 3-12.3 provides techniques for Army electromagnetic warfare. It describes how electromagnetic warfare supports and enables operations as well as other mission tasks and functions at each echelon.

Electromagnetic warfare integrates into operations using already established joint and Army processes such as the intelligence process, targeting, and the military decision-making process. This publication includes electromagnetic warfare staff responsibilities, contributions to the military decision-making process and targeting, and the reliance on intelligence preparation of the battlefield. It describes doctrinal techniques to address future operational challenges with current electromagnetic warfare capabilities. Due to rapidly evolving electromagnetic warfare capabilities and techniques, the Cyber Center of Excellence will review and update ATP 3-12.3 as needed to keep pace with continuously evolving threat electromagnetic warfare.

Chapter 1 provides an introduction to electromagnetic warfare, including electromagnetic attack, electromagnetic protection, and electromagnetic support.

Chapter 2 discusses electromagnetic warfare professionals and their roles and responsibilities. It discusses the relationships between staff members and their duties during the planning and execution of electromagnetic warfare.

Chapter 3 captures how electromagnetic warfare aligns with each phase of the operations process and discusses electromagnetic warfare contributions to the military decision-making process. This chapter addresses staff contributions to electromagnetic warfare planning and equipment configuration for successful employment.

Chapter 4 discusses planning, preparation, execution, and assessment considerations for electromagnetic attack. This chapter also describes jamming techniques and their characteristics and discusses electromagnetic attack in the targeting process.

Chapter 5 discusses electromagnetic protection techniques, including the integration of electromagnetic warfare and signal planning to conduct electromagnetic protection. This chapter provides radio users and staff techniques to prevent threat radio interception and detection and targeting of friendly forces.

Chapter 6 describes electromagnetic support planning and execution techniques to include synchronizing signals intelligence resources that complement electromagnetic support activities. This chapter outlines lines of bearing, cuts, fixes, establishing a direction-finding baseline, and the causes of direction-finding errors.

Appendix A describes radio frequency propagation characteristics and the bands within the electromagnetic spectrum.

Appendix B includes formulas used to determine transmission power requirements for jamming radio receivers.

Appendix C discusses friendly electromagnetic warfare equipment and associated characteristics, including ground and airborne electromagnetic warfare platforms.

Appendix D provides forms, formats, reports, and messages used to plan and execute electromagnetic warfare and spectrum management operations.

Chapter 1

The Operational Environment and Electromagnetic Warfare

This chapter provides an overview of electromagnetic warfare and discusses the importance of electromagnetic warfare during Army operations. This chapter also describes the electromagnetic warfare divisions and provides an overview of the electromagnetic environment.

OVERVIEW

1-1. Since the beginning of the 20th century, electromagnetic warfare (EW) has played an ever-increasing role in shaping the outcomes of various military conflicts around the globe. *Electromagnetic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-85). The pioneers of radio recognized the military application of the electromagnetic spectrum. In the decades that followed, state and non-state actors alike used radios to support navigation, command and control, intelligence gathering, and information operations. Radio communications are desirable targets due to their use in military operations. Commanders learned to protect their radios while seeking to exploit, degrade, or destroy threat spectrum capabilities.

1-2. Historically, EW has played significant roles in combat operations. During World War II, British forces used radio transmissions to overpower German radio receivers. The jamming missions successfully disrupted the Germans' command and control systems and navigation capabilities. Following World War II, the Army continued to invest in EW competencies until the early 1990s.

1-3. During Operation ENDURING FREEDOM in Afghanistan and Operation IRAQI FREEDOM in Iraq, the U.S. Army encountered threats to friendly bases, convoys, and dismounted Soldiers as adversaries used radio-controlled improvised explosive devices to attack ground forces. As a countermeasure to the threat, the Army acquired new electromagnetic attack capabilities to jam radio-activated triggers and defend friendly forces from explosive devices. The success of EW during these conflicts demonstrates the value of its continued use and further refinement and development of tactics, techniques, and procedures. EW is and will be increasingly vital to Army operations to defeat peer threats in support of all combat operations and across all domains. As the threat becomes more advanced and the operational environment becomes more complex, the Army will need to continue building and developing EW competencies to support decisive action and win in large-scale combat operations.

OPERATIONAL ENVIRONMENT

1-4. The operational environment encompasses all domains—air, land, maritime, space, and cyberspace. The Army uses a multidomain approach to operations, integrating joint and Army capabilities and synchronizing actions across all domains and across the strategic contexts. Understanding the operational environment is essential for Army leaders, engineers, planners, system operators, and cyber Soldiers to plan and execute effective EW.

CONGESTED ENVIRONMENT

1-5. The extensive use of the electromagnetic spectrum creates competition for bandwidth resources. All forces and supporting agencies depend on the electromagnetic spectrum for communications, information collection, and EW capabilities in support of operations in the air, land, maritime, space, and cyberspace domains.

CONTESTED ENVIRONMENT

1-6. Contested communications environments exist due to threat actions to degrade or deny the operations of spectrum-dependent devices. EW elements conduct operations to mitigate the effects of a contested environment.

1-7. Threat attacks may combine electromagnetic attack, other information warfare effects, and lethal fires to deny friendly forces the use of spectrum-dependent systems. To accomplish this goal, threat forces gather technical and combat information about their enemies. As threat forces locate and identify friendly units, threat information warfare elements establish priorities to—

- Jam communications assets.
- Deceptively enter radio networks.
- Interfere with the normal flow of U.S. and allies' communications.

1-8. During competition, commanders base their planning and decisions on a continually evolving understanding of their operational environment. Integrated EW, signals intelligence, and cyberspace capabilities collect against and analyze threat operational and tactical systems and other factors of the operational environment and civil networks. This effort builds the information that allows a commander to visualize the operational environment to a level of detail that allows centralized planning and decentralized execution.

ELECTROMAGNETIC ENVIRONMENT

1-9. The Army and potential adversaries increasingly use weapons, threat warning devices, sustainment information systems, intelligence, surveillance, reconnaissance, and communications equipment that rely on the electromagnetic spectrum to operate. The electromagnetic spectrum is a maneuver space consisting of all frequencies of electromagnetic radiation (oscillating electric and magnetic fields characterized by frequency and wavelength). The electromagnetic spectrum is organized into frequency bands based on specific physical characteristics. The electromagnetic spectrum includes radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, x-rays, and gamma rays (JP 3-85). The Army is dependent on the electromagnetic spectrum across every domain. To prevail in future conflicts and achieve positions of advantage against threat actors, Army forces will not only need to protect against threat actions, but also target threat capabilities at the right time and place to open windows of opportunity and relative advantage across all domains, particularly during large-scale combat operations.

1-10. The Army operates using the electromagnetic spectrum in all geographic regions. The *electromagnetic environment* is the resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment (JP 3-85). The electromagnetic environment is a subset of the spectrum, which might affect or is relevant to a given operation. Technological advances in the past decade caused a rapid increase in civil, commercial, and military spectrum-enabled and -dependent capabilities. This proliferation, combined with the U.S. military's reliance on the electromagnetic spectrum and the low entry costs for adversaries, creates substantial military challenges. The commander's ability to maneuver and conduct operations within the electromagnetic spectrum is vital to achieve and maintain tactical, operational, and strategic advantages. To preserve warfighting capabilities, commanders take actions to maintain freedom of action in the electromagnetic spectrum. See appendix A for detailed information on the electromagnetic spectrum.

ELECTROMAGNETIC WARFARE DIVISIONS

1-11. EW is comprised of three distinct divisions: electromagnetic attack, electromagnetic protection, and electromagnetic support. It is important to understand the commander's intent and coordinate, deconflict, and synchronize EW activities with the other staff elements to increase combat effectiveness, protect the force, and project power.

ELECTROMAGNETIC ATTACK

1-12. *Electromagnetic attack* is the division of electromagnetic 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 3-85). See chapter 4 for more information on electromagnetic attack.

ELECTROMAGNETIC PROTECTION

1-13. *Electromagnetic protection* is the division of electromagnetic 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 3-85). See chapter 5 for more information on electromagnetic protection.

ELECTROMAGNETIC SUPPORT

1-14. *Electromagnetic support* is the division of electromagnetic 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 3-85). See chapter 6 for more information on electromagnetic support.

Chapter 2

Electromagnetic Warfare Roles and Authorities

Electromagnetic warfare requires highly trained and skilled personnel. This chapter discusses electromagnetic warfare professionals and their unique and overlapping duties and responsibilities. This chapter discusses the staff members with roles and responsibilities when planning and conducting electromagnetic warfare operations.

ROLES AND RESPONSIBILITIES

2-1. EW personnel on the staff are in the cyberspace electromagnetic activities (CEMA) section at theater army through brigade echelons and consist of a cyber electromagnetic warfare officer (CEWO), electromagnetic warfare technicians, electromagnetic warfare noncommissioned officers, and spectrum managers. The CEMA section includes EW-trained personnel, personnel trained in spectrum management, and personnel trained in cyberspace operations. For more information on cyberspace-trained personnel, refer to FM 3-12. EW personnel assigned to the CEMA section are accountable to the chief of staff and the G-3 or S-3 for planning, development, integration, and synchronization of EW. Battalions have a single EW representative that is a member of the battalion staff.

2-2. EW personnel in the CEMA section plan and conduct EW across the range of military operations. EW personnel conduct CEMA with assistance from, and in coordination with, other members of the CEMA working group. FM 3-12 contains more information on the CEMA working group. EW personnel plan the employment of electromagnetic attack, frequencies for targeting, analyze the probability of frequency fratricide, and collaborate with the G-6 or S-6 to mitigate harmful effects from EW to friendly personnel, equipment, and facilities.

2-3. The CEWO disseminates key mission status information, such as cancellation of electromagnetic attack, and coordinates with other staff members within the command post to contribute to situational awareness. The CEWO coordinates with—

- The G-2 or S-2.
- The G-3 or S-3.
- The G-6 or S-6.
- The fires cell.
- The protection cell.
- Information advantage staff.
- The space support element.

- The staff judge advocate.

ECHELONS THEATER ARMY THROUGH BRIGADE

2-4. The Army assigns EW personnel to CEMA sections at theater army, corps, division, and brigade combat team. Each EW professional has specific roles and responsibilities.

CYBER ELECTROMAGNETIC WARFARE OFFICER

2-5. The CEWO's responsibilities regarding EW include—

- Integrating, coordinating, and synchronizing EW effects and activities into operations.
- Nominating EW targets for approval from the fire support coordinator and commander.
- Receiving, vetting, and processing EW targets from subordinate units.
- Developing and prioritizing effects in the electromagnetic spectrum.
- Developing and prioritizing targets with the fire support coordinator.
- Monitoring and continually assessing measures of performance and measures of effectiveness for EW operations.
- Maintaining the CEMA staff running estimate.
- Coordinating targeting and assessment collection with higher, adjacent, and subordinate organizations or units.
- Advising the commander and staff on plan modifications, based on the assessment.
- Advising the commander how EW effects can impact the operational environment.
- Providing recommendations for commander's critical information requirements.
- Drafting and transmitting the electromagnetic attack request format or other applicable theater-specific electromagnetic attack requests.
- Participating in other cells and working groups, as required, to ensure integration of EW operations.
- Deconflicting EW operations with the G-6 or S-6 spectrum manager.
- Coordinating with the CEMA working group to plan and synchronize EW operations.
- Assisting the G-2 or S-2 during intelligence preparation of the battlefield, as required.
- Providing information requirements to support planning, integration, and synchronization of EW operations.
- Exercising delegated electromagnetic attack control authority on behalf of the commander the commander.

ELECTROMAGNETIC WARFARE TECHNICIAN

2-6. The electromagnetic warfare technician—

- Serves as the EW technical and tactical subject matter expert to the CEWO and to the CEMA, targeting, and other working groups.
- Plans and coordinates EW across functional and integrating cells.
- Provides input for the integration of threat electromagnetic order of battle during intelligence preparation of the battlefield.
- Maintains and assists in the development of the CEMA staff running estimate.
- Coordinates target information and synchronizes electromagnetic attack and electromagnetic support activities with the G-2 or S-2 staff.
- Integrates EW into the targeting process, monitors EW target requests, and conducts battle damage assessment for EW.
- Recommends employment of EW resources.
- Provides technical oversight and supervision for the maintenance of EW equipment.
- Conducts, maintains, and updates an electromagnetic environment survey.
- Identifies enemy and friendly effects within the electromagnetic spectrum.
- Assists in the development and execution of standard operating procedures and battle drills.

ELECTROMAGNETIC WARFARE NONCOMMISSIONED OFFICER

2-7. The electromagnetic warfare noncommissioned officer—

- Plans, manages, and executes EW tasks.
- Manages the availability and employment of EW assets.
- Serves as senior developer and trainer for EW.
- Distributes, maintains, and consolidates EW staff products.
- Collects and maintains data for electromagnetic environment surveys.
- Coordinates and deconflicts spectrum resources with the spectrum manager.
- Operates and maintains EW tools.

SPECTRUM MANAGER

2-8. There are spectrum managers in the G-6 or S-6 staff and the CEMA section. The G-6 or S-6 spectrum manager coordinates spectrum resources that support the friendly use of the electromagnetic spectrum. The CEMA section spectrum manager deconflicts spectrum resources for EW activities and provides the EW input to the common operational picture. The CEMA section spectrum manager duties and responsibilities include—

- Leading, developing, and synchronizing the EW and electromagnetic protection plan by assessing electromagnetic attack effects on friendly force emitters.

- Mitigating harmful impact of an electromagnetic attack on friendly forces through coordination with higher and subordinate, adjacent units.
- Synchronizing with the G-2 or S-2 on the electromagnetic attack effects to support intelligence gain and loss considerations.
- Synchronizing cyberspace operations to protect radio frequency-enabled transport layers.
- Coordinating support for the protection of radio frequency-enabled military information support operations and psychological operations.
- Collaborating with staff, subordinate, and senior organizations to identify unit emitters for inclusion on the joint restricted frequency list (JRFL).
- Updating guarded frequencies to the G-6 or S-6 staff for the JRFL.
- Performing EW-related documentation and investigation of prohibitive electromagnetic interference to support the G-6 or S-6 led joint spectrum interference resolution (JSIR) program.
- Participating in the CEMA working group to deconflict spectrum requirements.
- Advising and assisting with the planning and execution of EW operations.

Note. The JRFL is a concise list of restricted frequencies and networks categorized as taboo, protected, and guarded. For more information on taboo, protected, and guarded frequencies, see chapter 3.

AUTHORITIES

2-9. When conducting electromagnetic attack and electromagnetic support, there are capabilities that require coordination across all echelons. The commander may delegate these authorities to manage, prioritize, integrate, and synchronize EW capabilities.

ELECTROMAGNETIC ATTACK CONTROL AUTHORITY

2-10. Electromagnetic attack control authority is the authority usually delegated from the joint force commander through component commanders, down to the lowest level possible having the following attributes:

- Situational awareness of the electromagnetic operating environment.
- Positive control of the electromagnetic attack capability.
- Ability to monitor and assess electromagnetic attack transmission activity for determining corrective action.

2-11. Electromagnetic attack control authority responsibilities include—

- Participating in development of, and ensuring compliance with, electromagnetic spectrum coordination measures (such as the JRFL).
- Maintaining situational awareness of all electromagnetic attack-capable systems and related operational parameters in the joint operations area.
- Assisting in resolving spectrum prioritization issues.

- Coordinating with other Service components on electromagnetic attack requirements.
- Monitoring and assessing joint force electromagnetic attack transmission activity for electromagnetic attack control authority compliance and determining corrective action when necessary.

ELECTROMAGNETIC SPECTRUM COORDINATING AUTHORITY

2-12. The joint force commander normally delegates electromagnetic spectrum coordinating authority to the joint staff J-3; however, core expertise and joint force-assigned mission will dictate actual assignment. The J-3 plans, coordinates, monitors, manages, assesses, and prioritizes execution of joint electromagnetic spectrum operations. The commander with delegated electromagnetic attack control authority will normally grant direct liaison authority to the joint electromagnetic spectrum operations cell director for execution of responsibilities that include—

- Directing the planning, development, publication, and issuance of joint electromagnetic spectrum operations guidance (such as spectrum superiority objectives or spectrum prioritization), the joint electromagnetic spectrum operations plan, and spectrum operating instructions.
- Coordinating support of joint electromagnetic spectrum operations functions across the joint staff.
- Incorporating spectrum guidance into the respective plans and orders.
- Establishing processes that integrate host-nation and other affected nations' constraints and requirements.
- Coordinating with the joint frequency management office (if not incorporated within the joint electromagnetic spectrum operations cell) to manage, prioritize, integrate, synchronize, and deconflict use of the electromagnetic spectrum.
- Developing broad policies and procedures for the coordination required among all joint spectrum users.
- Developing policy, within intelligence community guidelines, for sharing intelligence information to existing user-defined operational pictures.
- Consolidating Service component plans for operating in the electromagnetic spectrum for joint force commander approval.
- Monitoring joint force actions to assess their effects on spectrum superiority and mission objectives.

STAFF RESPONSIBILITIES FOR ELECTROMAGNETIC WARFARE

2-13. Various staff elements contribute to EW by providing unique products and guidance to the CEWO during all phases of an operation. The same staff members participate in the CEMA working group as necessary.

G-2 or S-2 Staff

2-14. The G-2 or S-2 staff advises the commander and staff on intelligence aspects of EW operations. The G-2 or S-2 staff—

- Provides the electromagnetic order of battle to support programming of unit EW systems.
- Maintains appropriate threat EW data.
- Maintains the signals intelligence (SIGINT) priorities of collection and informs the staff for situational awareness.
- Maintains situational awareness of EW assets by accounting for organic and requested capabilities on the intelligence, surveillance, and reconnaissance synchronization matrix.
- Ensures electromagnetic order of battle requirements are a part of the information collection plan.
- Determines enemy organizations' network structures, disposition, capabilities, limitations, vulnerabilities, and intentions through collection, analysis, reporting, and dissemination.
- Determines enemy EW vulnerabilities and high-payoff targets.
- Provides intelligence support to targeting operations.
- Assesses the effects of friendly EW activities on the enemy.
- Conducts intelligence gain or loss analysis for EW targets with intelligence value.
- Aids in preparation of the intelligence-related portion of the EW running estimate.
- Recommends guarded frequencies to the G-6 or S-6 spectrum manager for the JRFL.
- Provides updates to the electromagnetic order of battle.
- Participates in the CEMA working group to synchronize information collection with EW requirements and deconflict planned EW activities.
- Coordinates electromagnetic support and SIGINT operations with the CEMA section.

G-3 or S-3 Staff Responsibilities

2-15. The G-3 or S-3 staff is responsible for the overall planning, coordination, and supervision of EW activities. The G-3 or S-3 staff—

- Plans for and incorporates EW into operation plans and orders, in particular with the fire support and information advantage plans.
- Tasks EW activities to assigned and attached units.
- Exercises control over EW, including electromagnetic deception plans.
- Directs electromagnetic protection measures, such as emission control (EMCON), terrain masking, and spectrum management based on recommendations from the G-6 or S-6 staff, the CEWO, and the CEMA working group.

- Coordinates EW training requirements to maintain unit readiness.
- Issues EW tasks as part of the information collection plan. These tasks are according to the collection plan and the information requirements developed by the G-2 or S-2 staff and the requirements manager.
- Ensures, through the CEMA working group, that EW activities support the overall plan.
- Integrates electromagnetic attack in the targeting process.
- Directs tasking of electromagnetic support and electromagnetic attack assets in support of operations.

G-6 or S-6 Staff

2-16. The information systems technician, network management technician, information services technician, spectrum manager, and information security manager participate in planning EW. The G-6 or S-6 staff—

- Assists the CEWO with the preparation of electromagnetic protection policy.
- Reports enemy electromagnetic attack activity detected by friendly communications elements to the CEMA working group.
- Identifies and deconflicts electromagnetic interference.
- Issues signal operating instructions.
- Ensures network connectivity for all EW computer systems.
- Provides spectrum resources to support the unit or task force (refer to ATP 6-02.70).
- Coordinates for spectrum usage with higher echelon G-6 or S-6, J-6, and applicable host-nation and international agencies as necessary.
- Prepares the restricted frequency list and issues EMCON guidance.
- Coordinates frequency assignment and use.
- Supports the CEMA working group by assisting in the development of electromagnetic deception plans and activities that include spectrum resources.
- Coordinates with higher-echelon spectrum managers for JSIR reporting.
- Assists the CEWO in issuing guidance to the unit, including subordinate elements, regarding deconfliction and resolution of electromagnetic interference problems and processes involving EW systems.
- Participates in the CEMA working group to deconflict friendly spectrum requirements with EW activities and information collection efforts.
- Supports all subordinate unit software updates and communications security requirements.
- Compiles and distributes the JRFL (spectrum manager).
- Assists the EW section with computer maintenance and troubleshooting.

Information Advantage Staff

2-17. The information advantage staff coordinates, synchronizes, and deconflicts activities to achieve objectives in the information dimension. Typically, but not solely, these activities occur through cyberspace operations and EW. The information advantage staff—

- Ensures synchronization and deconfliction with other information advantage activities.
- Considers second- and third-order effects of EW on information advantage activities and proactively plans to enhance intended effects.
- Analyzes the information dimension to discern how it affects unit operations and to exploit opportunities to gain an advantage over threat forces.
- Assesses risk to mission and force associated with the employment of any capability, product, program or message.

Staff Judge Advocate or Representative

2-18. The staff judge advocate provides legal advice to the commander. The staff judge advocate or representative reviews proposed EW operations to ensure they comply with existing DOD policies, rules of engagement, 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.

Chapter 3

Electromagnetic Warfare Planning, Preparation, Execution, and Assessment

This chapter discusses electromagnetic warfare contributions to the military decision-making process and captures how electromagnetic warfare aligns with each phase of the operations process when supporting Army operations. This chapter addresses staff contributions to planning electromagnetic warfare and configuring equipment for successful employment.

SECTION I – ELECTROMAGNETIC WARFARE CONTRIBUTIONS TO THE MILITARY DECISION-MAKING PROCESS

3-1. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). The CEWO participates in the military decision-making process (MDMP) by planning and synchronizing EW and cyberspace operations into the overall mission objectives. Depending on the commander's intent, the scope, and complexity of the operations, the CEWO considers joint, interorganizational, and multinational dependencies and interdependencies of EW resources when participating in the MDMP.

MILITARY DECISION-MAKING PROCESS

3-2. EW planners participate throughout the MDMP. In a time-constrained environment, they follow the rapid decision-making and synchronization process. The CEWO ensures planned EW activities contribute to the operation. Throughout the MDMP, the CEWO continuously identifies risks and appropriate risk mitigation techniques.

3-3. During the MDMP, the CEWO, with assistance from the CEMA section, conducts terrain and radio wave propagation analysis relevant to friendly and threat forces within the area of operations. The analysis results contribute to staff products, such as map overlays depicting EW assets and their associated ranges of effectiveness. The staff uses the products to refine the EW portions of the plan. The CEMA section builds and staffs operation order appendixes and annexes and submits them to the G-3 or S-3 staff for dissemination. The CEWO provides electromagnetic attack information to the fires staff for inclusion in Annex D of the operation order.

3-4. The CEMA section considers policies, laws, and rules of engagement that affect EW operations when participating in the MDMP. The staff judge advocate and the CEMA working group develop the rules of engagement for commander review. Planners and the staff judge advocate clarify the rules of engagement or develop supplemental rules of engagement when necessary.

3-5. EW planners synchronize EW activities with other lethal and nonlethal capabilities to achieve desired effects. The CEWO uses predetermined formulas to calculate electromagnetic attack. For additional information on predetermined formulas and jamming calculations, see appendix B.

SECTION II – PLANNING

3-6. *Planning* is the art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about (ADP 5-0). EW planning minimizes fratricide and optimizes operational effectiveness during mission execution. The CEWO must participate throughout the MDMP. Refer to FM 3-12 for more information about EW planning and the MDMP.

ELECTROMAGNETIC WARFARE PLANNING CONSIDERATIONS

3-7. Commanders and staffs use the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time) and mission variables of mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations—METT-TC (I) to understand the environment and aid in mission planning. Commanders and staffs view all the mission variables in terms of their impact on mission accomplishment. These variables can have major impacts to operations at all levels. (Refer to FM 6-0 for a detailed description of the operational and mission variables).

PLANNING FACTORS

3-8. EW planning considerations include equipment type, configurations, logistics, availability of equipment and qualified personnel, and risks. Staff planners with the necessary expertise, and in some cases access to sensitive compartmented information facilities, are essential for planning EW and related capabilities. EW integration requires placing planners at the brigade combat team level with experience in capabilities, such as special technical operations and special access program effects.

3-9. The CEWO visualizes an operational environment and electromagnetic environment using the Electromagnetic Warfare Planning and Management Tool (EWPMT) or other simulation programs to predict the behavior of radio waves used during operations. The course of action proposed by the CEWO requires analysis to determine the capabilities and limitations of the systems. For example, manpack EW systems are lightweight and highly mobile, but also have line of sight limitations, and limited transmit power for electromagnetic attack. Vehicle-mounted systems allow for higher power output, but have line of sight limitations in dense terrain. Airborne platforms offer the best line of sight of EW systems, but are vulnerable to enemy air defenses and have limited dwell time on target. *Line of sight* is the unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another (ATP 2-01.3).

LOGISTICS CONSIDERATIONS

3-10. Units conduct scheduled and demand maintenance on EW equipment. Maintenance ensures readiness for current and future operations. The CEWO, with assistance from logistics staff, develops a standard operating procedure that includes maintenance procedures. The CEWO or representative prioritizes maintenance efforts ensuring unity of effort, as maintainers are a limited resource.

3-11. The planner considers—

- An EW capability replacement plan for potential coverage gaps and unexpected outages.
- Parts availability for maintenance to prevent non-mission capable equipment.
- Access to programming equipment or planning for new software or firmware update files.
- Power resources including:
  - Batteries.
  - Generators and fuel.
  - Shore power.
  - Vehicle or transport power sources.

3-12. Commanders allocate EW resources to support various units. When EW resources support another unit, the supported unit—

- Identifies EW requirements.
- Protects and defends EW assets.
- Provides logistical support.

HAZARDS OF ELECTROMAGNETIC RADIATION

3-13. Like other military actions, conducting EW involves risks. Throughout the planning process, the CEWO continuously identifies operational risks and appropriate risk mitigation techniques. There are three broad risk categories to consider when planning EW activities in support of mission objectives. The CEWO helps identify these risks and further aids in developing mitigating measures to reduce the risk to friendly personnel and equipment. For more information about risk management, refer to ATP 5-19. The risks include—

- Hazards of electromagnetic radiation to personnel.
- Hazards of electromagnetic radiation to fuels.
- Hazards of electromagnetic radiation to ordnance.

Hazards of Electromagnetic Radiation to Personnel

3-14. Hazards of electromagnetic radiation to personnel is the danger to personnel from the absorption of electromagnetic energy by the human body. Personnel hazards are associated with the absorption of radio frequency (RF) energy above certain power levels in certain frequency bands for certain lengths of time. Institute of Electrical and Electronics Engineers standards C95.1, C95.6, and C95.7 specify the allowable amounts of radiation and personnel exposure time to RF fields at particular intensities and frequencies.

Hazards of Electromagnetic Radiation to Fuels

3-15. Hazards of electromagnetic radiation to fuels is associated with the possibility of igniting fuel or other volatile materials through RF energy-induced arcs or sparks. It takes a certain amount of arc energy to ignite fuel. This is a significant concern when there is limited separation between EW capabilities and fuel, such as airfields, forward armament and refueling points, and refueling on-the-move locations. Fortunately, there are many operational safeguards against this problem.

Hazards of Electromagnetic Radiation to Ordnance

3-16. Hazards of electromagnetic radiation to ordnance refers to the susceptibility of electro-explosive devices to RF energy. Electro-explosive or electrically initiated devices are the control devices to detonate explosives, launch ejection seats, cut tow cables, and perform other similar functions. Modern communications and radar transmitters can produce high levels of electromagnetic energy that are potentially hazardous to ordnance. These high levels of energy can cause premature actuation of sensitive electro-explosive and electrically initiated devices.

RUNNING ESTIMATE

3-17. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander’s intent and if planned future operations are supportable (ADP 5-0). Each staff element maintains its own running estimate within its own area of expertise to help commanders develop an initial understanding of their operational environment and to maintain timely assessment as the operation progresses. The EW running estimate is a tracking tool used to maintain awareness of EW capabilities. The EW running estimate provides a consolidated list of information about cyberspace and the electromagnetic spectrum to assist the CEMA section in planning, preparing, and executing operations. EWPMT provides a dynamic EW picture of the operational environment and allows for mission simulation and tracking to aid in updating the running estimate. For more information on EWPMT, see appendix C.

3-18. The operational variables—political, military, economic, social, information, infrastructure, physical environment, and time—and the mission variables of METT-TC (I) guide development of the running estimate. The CEWO prepares and continually updates the running estimate with assistance from other members of the CEMA section.

Resources useful in developing a running estimate are the unit status report and the commanders' training assessment. Threat information is available from online databases, unit intelligence assets, and national intelligence sources. Table 3-1 is an example of an EW running estimate.

Table 3-1. Example of an electromagnetic warfare running estimate

Electromagnetic Warfare Running Estimate
1. Friendly electromagnetic warfare systems. a. System nomenclature and disposition by echelon. i. Planning, modeling, and simulation tools. ii. Organic systems. iii. Echelons above corps and joint assets. b. System capabilities. i. Frequency range. ii. Modulation type(s). iii. Maximum power output. iv. Antenna configuration and characteristics. v. Command and control details (mesh network parameters, data paths, and bandwidth requirements). c. Modeling and simulation of each system based on differing parameters and area of operations i. Differing power ratios. ii. Antenna configuration. iii. Terrain. d. Constraints and limitations associated with each system.
2. Threat electromagnetic warfare systems. a. System nomenclature and disposition by echelon. b. System capabilities. i. Frequency range. ii. Modulation type(s). iii. Maximum power output. iv. Antenna configuration and characteristics. v. Command and control details (mesh network parameters, data paths, and bandwidth requirements. c. Threat electromagnetic warfare tactics, techniques, and procedures. d. Modeling and simulation of each system, based on differing parameters and area of operations. e. Critical capabilities and vulnerabilities by system.

Table 3-1. Example of an electromagnetic warfare running estimate (cont.)

3. Threat spectrum-dependent systems. a. System nomenclature and disposition by echelon. b. System characteristics. i. Frequency ranges. ii. Bandwidth requirements. iii. Power. iv. Modulation. c. Tactics, techniques, and procedures. d. Frequency allocations. e. Cueing cycles (radar sets). f. Modeling and simulation of each system, based on differing parameters and area of operations. g. Critical capabilities and vulnerabilities by system.
4. Civil infrastructure considerations. a. Networks in the area of operations. i. SCADA. ii. Internet service providers. iii. Fiber (regional, national, and international). b. Spectrum resources and allocations (with characteristics of each). i. Wi-Fi. ii. Broadcast television. iii. Broadcast radio. iv. Satellite ground stations. c. Physical access to structures and equipment.
LEGEND: SCADA supervisory control and data acquisition VHF very high frequency

Note. Table 3-1 is only an example of a running estimate and does not include all information that may be gathered and tracked. Running estimates are situational and information will depend on the operation.

3-19. The CEWO analyzes the operation and EW employment considerations early in the MDMP. These considerations include—

- Survivability of personnel and equipment.
- The time required to build or improve the unit's electromagnetic protection posture and position electromagnetic attack and electromagnetic support capabilities.
- Ability of EW resources to achieve the desired effects.
- Reprogramming of EW assets.
- Capabilities, limitations, advantages, and disadvantages of available EW and SIGINT assets.
- Intelligence available for targeting.

SURVIVABILITY

3-20. The survivability of personnel and equipment relies on force protection and electromagnetic protection techniques. Electromagnetic protection enhances force protection efforts as another method to mitigate environmental and threat effects. The CEMA section plans the mitigation actions, and the commander decides what risk is acceptable. Risk mitigating techniques include coordinating ground or air escort and configuring EW equipment. Electromagnetic protection contributes to survivability. Antennas erected to minimum heights while maintaining communications, prevent detection and direction finding by the threat. This technique contributes to survivability. Site defense plans contribute to overall survivability. Survivability is a valuable criterion for course of action analysis during the MDMP. For more information about electromagnetic protection, see chapter 5.

TIME

3-21. The CEWO uses available time to configure and position EW assets for optimal performance. Time also affects the selection of movement techniques for a mission. The CEWO synchronizes electromagnetic attack operations with maneuver and fire to maximize effects at the appropriate time. The CEWO also plans the duration of electromagnetic attack effects based on target analysis to support survivability of EW assets.

EFFICACY

3-22. The CEWO considers which EW asset has the appropriate level of efficacy for an EW mission. Efficacy is the likelihood that an EW mission will achieve the desired effect. For example, an electromagnetic attack has a minimum transmission power threshold. Transmission power settings below the threshold have reduced levels of efficacy, or ability to achieve the desired effect. In contrast, transmission power settings above the threshold have increased levels of efficacy.

AVAILABILITY OF AIRBORNE ASSETS

3-23. Maintenance activities and other missions reduce the availability of aircraft to support EW requirements. Airborne platforms may be unavailable to support EW missions due to—

- Poor weather and limited visibility that restrict flight.
- Scheduled and demand maintenance.
- Transport missions.
- Intelligence, surveillance, and reconnaissance missions.
- Communications missions.

ELECTROMAGNETIC WARFARE REPROGRAMMING

3-24. *Electromagnetic warfare reprogramming* is the deliberate alteration or modification of electromagnetic 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 3-85). When EW or SIGINT forces observe that the threat has changed frequencies for communications or there are other changes in the electromagnetic environment, the CEWO ensures the reprogramming of EW systems or target sensing systems, to include the employment technique. EW reprogramming includes changes to self-defensive systems, offensive weapons systems, and electromagnetic support systems (JP 3-85). The change in the electromagnetic environment may also affect friendly communication systems. The CEWO informs the spectrum manager of the changes to EW requirements to coordinate the adjustment in mission parameters and may recommend friendly communications frequency changes to the G-6 or S-6. Reprograming EW equipment is the responsibility of the unit; however, units should be aware of reprogramming efforts when operating with multinational forces. Reprogramming is a national responsibility due to the effect on the electromagnetic environment. Refer to JP 3-85 for more information about reprogramming. EW reprogramming examples include—

- Changing target frequencies for jamming as well as updating restricted frequencies.
- Changing location of sensors due to environmental changes or interference.
- Installing the latest available software, firmware, and hardware for EW and SIGINT equipment.

ELECTROMAGNETIC WARFARE VISUALIZATION

3-25. The CEMA section visualizes and simulates the electromagnetic spectrum, manmade effects, and environmental impacts. The information the section gains informs friendly actions and may provide insight into possible enemy courses of action. EWPMT and other automated tools assist the CEMA section with—

- Providing input to the common operational picture.
- Displaying sensor information from EW and SIGINT assets including—
  - Detecting emitters and plotting lines of bearing.
  - Analyzing circular error probable ellipse.
- Conducting mission planning and rehearsals.
- Managing EW assets.
- Modeling and visualizing how the spectrum responds to friendly and enemy EW activities.

3-26. The CEMA section analyzes the electromagnetic spectrum using—

- Electromagnetic sensors.
- Threat system databases.
- Intelligence information.
- Operational environment factors.

3-27. EW personnel require updates as the situation changes. The tools, combined with staff interaction and the command and control system, provide the updates.

ELECTROMAGNETIC WARFARE PLATFORM CONSIDERATIONS

3-28. The employment of EW is based on specific ground-based, airborne, and functional electromagnetic attack, electromagnetic protection, and electromagnetic support considerations. The CEWO identifies EW employment considerations early in the operations process. Each consideration has certain advantages and disadvantages. The staff plans for all of these before executing EW operations.

Ground-Based Electromagnetic Warfare Considerations

3-29. Soldiers can use ground-based EW equipment when dismounted or on mobile platforms. Due to the short-range nature of tactical direction finding, electromagnetic support assets are usually located in the forward areas of the battlefield, with or near forward units.

Advantages

3-30. Ground-based EW capabilities have certain advantages. They provide direct support to maneuver units through counter radio-controlled improvised explosive device electromagnetic warfare (CREW), and communications or sensor jamming. Soldiers use ground-based EW capabilities to support continuous operations and respond quickly to the ground commander's EW requirements. However, to maximize the effectiveness of ground-based EW capabilities, maneuver units must protect EW assets from enemy ground and aviation assets. EW teams should be as survivable and mobile as the force they support. Maneuver units provide logistical support for the EW assets, and supported commanders must clearly identify EW requirements.

Limitations

3-31. Ground-based EW capabilities have certain limitations. They are vulnerable to enemy electromagnetic deception and electromagnetic attack activities. In addition, they have distance or propagation limitations against enemy electromagnetic systems. As with any spectrum-based system, units must properly program EW equipment to avoid friendly interference and compatibility issues.

Airborne Electromagnetic Warfare Considerations

3-32. While ground-based and airborne EW planning and execution are similar, they significantly differ in their employment time. Airborne EW operations happen 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.

3-33. Airborne EW requires—

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

Advantages

3-34. 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 greater mobility and flexibility and extend the range of electromagnetic attack and electromagnetic support capabilities beyond line of sight.

Limitations

3-35. Limitations associated with airborne EW capabilities include limited time on station, vulnerability to enemy electromagnetic attack, enemy air defense, electromagnetic deception techniques, and limited availability.

ELECTROMAGNETIC WARFARE CONFIGURATIONS

3-36. EW equipment requires proper configuration for successful employment. Units use EW equipment in manpack, vehicular, fixed-site, and airborne configurations. Equipment configuration includes—

- Choosing omnidirectional or directional antennas.
- The physical placement of equipment.
- Selecting power resources for EW equipment.
  - Gasoline or diesel-powered power generators.
  - Batteries for manpack and vehicular configurations.
  - Shore power for fixed EW assets.

MANPACK CONFIGURATIONS

3-37. Manpack configurations include electromagnetic attack and electromagnetic support capabilities and provide commanders the option to employ teams in areas not easily accessible by vehicle-mounted equipment. For manpack configurations, the CEWO considers—

- Weight of antennas and batteries carried by the Soldier.
- Limits to available transmit power for electromagnetic attack.
- Limits to mobility of collection teams.
- Limits to mission duration (normally 3–5 days).

VEHICLE-MOUNTED CONFIGURATIONS

3-38. Vehicle-mounted EW equipment provides electromagnetic attack and electromagnetic support capabilities during maneuver or at-the-halt. Vehicle-mounted EW configurations include—

- Mounted and dismounted capabilities.
- Jamming capabilities.
- Direction-finding capabilities for locating and targeting threat transmitters.

FIXED-SITE CONFIGURATIONS

3-39. Fixed-site EW configurations have more available transmit power than manpack and vehicular EW configurations. Fixed-site EW configurations have multiple transmitters, receivers, and antennas that enable the conduct of multiple EW activities simultaneously. A fixed site may include portable systems that require configuration and operation only at-the-halt, requiring personnel to install or construct the system.

AIRBORNE CONFIGURATIONS

3-40. Airborne EW is the coupling of EW assets to airborne platforms, such as unmanned aircraft systems, tethered balloons, and rotary- and fixed-wing aircraft. Airborne EW assets provide greater range and mobility than ground-based assets.

3-41. The synchronization of airborne EW missions requires detailed planning. The time on target for airborne EW assets coupled to rotary- and fixed-wing platforms is normally brief. Time on target for airborne EW is limited due to the flight speed of the aircraft. The short time on target is also a technique used to minimize the threat's abilities to detect the platforms using visual, direction-finding, or radar detection techniques.

3-42. Airborne EW activities require liaisons between the aircrews of the platform and the supported ground forces. Liaisons ensure—

- Situational awareness of mission support by platform.
- The supported unit is aware of platform protection tactics, techniques, and procedures to counter threat aircraft and air defense systems.

3-43. Airborne platforms are low-density, high-demand resources. CEWOs consider airborne platforms for EW, SIGINT, surveillance, and reconnaissance missions in the deep area. Airborne assets are limited by the extensive maintenance requirements for the aviation platform. If a unit has 12 airborne platforms with three on mission, nine are likely to be undergoing maintenance, returning from a mission, or in-flight to relieve an ongoing mission.

OTHER STAFF SECTIONS' CONTRIBUTIONS TO ELECTROMAGNETIC WARFARE PLANNING

3-44. The CEMA section depends on other staff sections for various products to support situational understanding, targeting, and electromagnetic protection. The G-2 or S-2, G-6 or S-6, and the staff judge advocate contribute to EW planning.

G-2 OR S-2 STAFF

3-45. EW planners rely on the G-2 or S-2 staff for all-source intelligence identified during intelligence preparation of the battlefield to assist in defining the electromagnetic operational environment. The CEWO submits requests for information to address gaps identified during intelligence preparation of the battlefield.

3-46. In most cases, the CEWO relies on the SIGINT-derived enemy electromagnetic order of battle for EW targeting. Likewise, EW assets can sometimes discover SIGINT collection opportunities due to the capabilities of EW platforms. Therefore, the G-2 or S-2 staff collaborates and coordinates with the CEWO to align EW and SIGINT assets against the commander's information requirements to achieve the best possible outcomes. SIGINT and EW resources, synchronized with the commander's scheme of maneuver, significantly enhance situational awareness while increasing the precision of the targeting process.

3-47. Useful products the G-2 or S-2 creates or assists in creating include—

- High-payoff target list.
- Electromagnetic order of battle.

G-6 OR S-6 STAFF

3-48. The CEWO uses the JRFL and friendly network architecture to plan EW and avoid electromagnetic interference. The CEWO and the G-6 or S-6 use this information to develop the unit electromagnetic protection plan. The JRFL includes—

- Taboo frequencies.
- Protected frequencies.
- Guarded frequencies.

Taboo Frequencies

3-49. Taboo frequencies are friendly frequencies that should never be deliberately jammed or interfered with by friendly forces. Usually, these include international distress, safety, and controller frequencies. They are generally long-standing frequencies. Taboo frequencies may be time-oriented, and the restrictions may be removed as the tactical situation changes. During crisis or conflict, short duration electromagnetic attack may be authorized on taboo frequencies for self-protection to provide coverage from unknown threats or threats operating outside their known frequency ranges, or for other reasons.

Protected Frequencies

3-50. Protected frequencies are friendly frequencies used for a particular operation, identified, and protected to prevent inadvertent jamming by friendly forces while executing electromagnetic attack against hostile forces. These frequencies are so critical that jamming should be restricted unless necessary or until coordination with the engaged unit is made. They are generally time-oriented and may change with the tactical situation. It is important to update protected frequencies periodically.

Guarded Frequencies

3-51. Guarded frequencies are threat frequencies currently being exploited for combat information and intelligence. A guarded frequency is time-oriented in that the list changes as the threat assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain versus the loss of the technical information. For more information about taboo, protected, and guarded frequencies, refer to JP 3-85.

STAFF JUDGE ADVOCATE

3-52. Conducting EW requires an understanding of the rules of engagement and legal authorities. The CEWO consults the staff judge advocate or legal advisor for interpretation of the standing rules of engagement. The staff judge advocate or legal advisor reviews EW activities to ensure compliance with existing DOD policies, rules of engagement, and applicable domestic and international laws, including the law of armed conflict.

3-53. When considering electromagnetic attack or electromagnetic support, the staff judge advocate or legal advisor will assist in the planning of operations and will review past operations. As part of this assistance, the staff judge advocate considers what impacts operations may have on host-nation communications and the legal implications related to those impacts. Refer to FM 6-27 for more information on rules of engagement and FM 3-12 for more information on EW authorities.

ELECTROMAGNETIC WARFARE CONTRIBUTIONS TO THE STAFF

3-54. The CEWO collaborates with, and provides information to, other staff sections to aid in planning. This information answers requests for information and aids in refining staff products.

CONTRIBUTIONS TO G-2 OR S-2 STAFF

3-55. The CEWO contributes to intelligence preparation of the battlefield and throughout the MDMP by providing input related to EW activities. Intelligence preparation of the battlefield involves systematically and continuously analyzing the mission variables of METT-TC (I) in the area of operations. Commanders and staffs use intelligence preparation of the battlefield to develop situational understanding. Some of the CEWO's input to intelligence preparation of the battlefield includes—

- Information regarding how the electromagnetic environment affects the operational environment.
- Input to likely threat courses of action by providing information on threat spectrum-dependent capabilities, tactics, techniques, and procedures.
- Input to the commander's critical information requirements, including friendly force information requirements and priority intelligence requirements.

3-56. When evaluating how the electromagnetic environment affects an operational environment, the CEWO—

- Analyzes the electromagnetic environment and identifies known or suspected threat emitters of interest and neutral emitters in the area of operations.
- Identifies facilities which may support or house enemy EW capabilities.
- Contributes to the G-2 or S-2 understanding of the enemy's use of the electromagnetic spectrum.

3-57. When describing the effects of an operational environment on EW activities, the CEWO—

- Conducts terrain analysis 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 terrain that protects communications and target acquisition systems from threat collection and direction-finding activities.
- Identifies how terrain affects line of sight, including effects on both communications and noncommunications transmitters.
- Evaluates how vegetation affects radio wave absorption and antenna height requirements.
- Locates power lines and their potential to interfere with radio waves.
- Assesses likely air and ground avenues of approach, their dangers, and potential support that EW activities could provide for them.
- Determines how weather—including visibility, cloud cover, rain, and wind—may affect ground-based and airborne EW activities and capabilities, for example, when poor weather conditions prevent airborne EW launch and recovery.
- Assists the G-2 or S-2 staff with the development of the modified combined obstacle overlay.
- Considers all other relevant aspects of an operational environment that affect EW activities, using the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time) and mission variables of METT-TC(I).

3-58. The CEWO contributes to the G-2 or S-2 staff's understanding during enemy course of action development by providing—

- Subject matter expertise on enemy EW tactics, techniques, and procedures for enemy situation template development.
- A review of named areas of interest and target areas of interest to confirm EW considerations.
- EW options to support decision points.
- EW input to the event template and event matrix.

CONTRIBUTIONS TO THE TARGETING WORKING GROUP

3-59. The targeting working group recommends priorities for targets according to its judgment and the advice of the fires cell, targeting officer, and the field artillery intelligence officer. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). The targeting working group maintains a high-payoff target list and informs the commander of targets that do not support the commander's guidance. A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60). The high-payoff target list includes the recommended priority of targets, target engagement sequence, target category, and a name or a number. The CEWO provides input to the high-payoff target list.

3-60. The CEWO recommends to the G-3 or S-3 staff and the fire support element whether to engage a target with EW. The fires support element uses the decide, detect, deliver, and assess methodology to direct friendly forces to attack the right target with the right asset at the right time. The targeting working group provides the high-payoff target list to the operations, intelligence, and fires support elements. The staff employs the high-payoff target list to understand and determine attack guidance and to refine the collection plan. This list may also indicate the commander's operational need for battle damage assessment of the specific target and the time window for collecting and reporting it (ATP 3-60).

3-61. The CEWO participates in the targeting process. After the targeting working group approves an EW target, the CEWO deconflicts the electromagnetic attack activity with the friendly use of spectrum resources. To support targeting, the CEWO—

- Matches EW resources with specific high-payoff targets and high-value targets.
- Ensures EW activities meet targeting objectives.
- Deconflicts electromagnetic attack with friendly use of the spectrum.
- Coordinates with the G-2 or S-2 staff to gain targeting information that supports electromagnetic attack.
- Manages EW missions through the command post or joint operations center and the tactical air control party for airborne electromagnetic attack.
- Exercises electromagnetic attack control authority, if delegated.
- Requests theater-level EW support.
- Informs the commander, staff, and subordinate units of current and planned locations of EW resources.

SECTION III – PREPARATION

3-62. *Preparation* is those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5-0). Preparation begins before arrival on the battlefield and continues through the redeployment phase. Preparation involves processes and activities that units perform to improve their ability to execute an operation. Preparation includes, plan refinement, rehearsals, information collection, coordination, inspections, and movement.

ELECTROMAGNETIC WARFARE PREPARATION

3-63. EW preparation ensures timely support for the commander's scheme of maneuver and includes—

- Initiating EW training that includes actual and simulated resources and environments.
- Reviewing maintenance activities to ensure that EW equipment is clean and serviceable.
- Planning, initiating, and reporting the movement of EW resources.
- Coordinating route clearance and escort requirements to mitigate risk and prevent delays during maneuver.
- Revising and refining the EW estimate, EW tasks, and EW to support the plan.
- Rehearsing the synchronization of EW and SIGINT 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 intelligence elements.

3-64. During preparation, the CEMA section—

- Synchronizes the EW running estimate with the SIGINT running estimate.
- Requests changes or exceptions to the JRFL and signal operating instructions through the G-2 or S-2 and G-6 or S-6 staff.
- Completes risk assessments and develops risk mitigation strategies.
- Leads the CEMA working group.
- Develops and rehearses battle drills and staff processes including—
    - Staffing the electromagnetic attack request format or other applicable theater-specific requests.
    - Integrating information collection activities with the G-2 or S-2 staff.

- Coordinating for external maintenance and reprogramming support for EW assets.
- Initiating electromagnetic protection procedures to counter electromagnetic interference and enemy jamming actions.
- Developing standard operating procedures.
- Establishing reporting procedures.

DECONFLICTING THE ELECTROMAGNETIC SPECTRUM

3-65. *Frequency deconfliction* is a systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions (JP 3-85). Deconflicting spectrum use requires an understanding of signal operating instructions, the JRFL, and mission requirements. The CEWO considers the distance, location, and the purpose of equipment reliant on friendly or restricted frequencies and recommends exceptions to signal operating instructions or the JRFL. Signal operating instructions contain call signs, call words, frequency assignments, signs, and countersigns for friendly forces. For more information regarding signal operating instructions and JRFL, refer to ATP 6-02.70.

3-66. Mission requirements may drive modifications to signal operating instructions and the JRFL. Modifications require staffing and approval through the G-2 or S-2 and G-6 or S-6 staff. When EW activities conflict with signal operating instructions or the JRFL, the commander decides which has priority. For signal operating instructions and JRFL deconfliction, the CEWO considers—

- The purpose of the frequency.
- Waveform characteristics.
- Location and time of use.

3-67. Due to security concerns, frequencies employed in intelligence roles may not be included in signal operating instructions. The CEWO maintains awareness of the frequencies that support SIGINT activities through coordination with the G-2 or S-2 staff.

ELECTROMAGNETIC SPECTRUM RESOURCES

3-68. The G-6 or S-6 section spectrum manager uses the electromagnetic spectrum certification process to gain the use of previously unallocated spectrum resources, which requires completing a standard frequency action format.

3-69. Host nations have spectrum usage plans that assist in spectrum management and frequency assignment. The G-6 or S-6 spectrum manager assists the CEMA section in frequency assignment for EW activities. The G-6 or S-6 spectrum manager requests frequency resources through an online database. The online database enables managers to determine the historical spectrum supportability of like systems. Spectrum managers use Department of Defense Form 1494 (*Application for Equipment Frequency Allocation*) to request frequencies. For more information about Department of Defense

Form 1494 and spectrum management operations, refer to ATP 6-02.70. See appendix C for more information on spectrum management systems.

INTEGRATION OF ELECTROMAGNETIC WARFARE AND SIGNALS INTELLIGENCE

3-70. EW and SIGINT systems have similar capabilities that are mutually beneficial. Integrated EW and SIGINT assets present an efficient, holistic approach that reduces duplication of effort, enables additional information collection, and provides flexibility in employing EW and SIGINT resources. EW and SIGINT teams collaboratively use direction-finding techniques to achieve a higher level of fidelity on the location of emitters. Combining the capabilities of EW and SIGINT sensors and spreading them throughout the area of operations locates targeted emitters more accurately.

3-71. Though EW and SIGINT are similar, there are important distinctions between them. Legal considerations distinguish EW and SIGINT activities and the authorization for each to support operations that, if not observed, can complicate and delay the execution of electromagnetic attack effects and SIGINT operations. Commanders and planners should collaborate closely with SIGINT elements and legal authorities to ensure compliance with SIGINT policy when planning EW activities.

DISTINCTIONS BETWEEN ELECTROMAGNETIC WARFARE AND SIGNALS INTELLIGENCE

3-72. Commanders have the option to employ SIGINT sensors to augment electromagnetic support activities. Electromagnetic support and SIGINT employ the same or similar capabilities. The task and purpose are the main factors when deciding to use SIGINT or electromagnetic support capabilities. SIGINT sensors perform electromagnetic support activities when used to provide immediate threat information, including threat warnings, avoidance, targeting, and jamming. When SIGINT sensors are intercepting, identifying, and locating or localizing sources of intentional and unintentional radiated electromagnetic energy for intelligence purposes, they are supporting a SIGINT mission. These distinctions are identified when answering—

- Who tasks or controls the SIGINT sensors?
- What are the sensors tasked to provide?
- What is the purpose of the task driving the employment of the sensors?

3-73. Electromagnetic support sensors provide combat information to support immediate threat recognition, targeting, and planning of future operations. Units may also transfer select data from electromagnetic support activities to the United States SIGINT System to produce foreign intelligence. The CEWO and the G-2 or S-2 staff develop a standard operating procedure for information exchange.

SECTION IV – EXECUTION

3-74. *Execution* is the act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation (ADP 5-0). Commanders focus their subordinates on executing the concept of the operation by clarifying their commander's intent and mission orders.

ELECTROMAGNETIC WARFARE EXECUTION

3-75. CEWOs routinely synchronize electromagnetic attack tasks with the other functional or integrating cells responsible for the information tasks. In this way, they ensure that electromagnetic attack efforts do not cause fratricide or unacceptable collateral damage.

3-76. During execution, the CEMA working group—

- Serves as the EW experts for the commander.
- Maintains the EW running estimate.
- Monitors EW operations and recommend adjustments.
- Recommends adjustments to the commander's critical information requirements based on the situation.
- Recommends adjustments to EW-related control measures and procedures.
- Maintains direct liaison with the fires cell and Department of Defense information network operations officer to ensure integration and deconfliction of EW operations.
- Coordinates and manages EW taskings to subordinate units or assets.
- Coordinates requests for nonorganic EW capabilities.
- Continues to assist the targeting working group in target development.
- Recommends targets for engagement by electromagnetic attack assets.
- Receives, processes, and coordinates subordinate units' requests for EW during operations.
- Receives and processes immediate support requests for suppression of enemy air defenses or EW from joint or multinational forces.
- Coordinates with the airspace control section on suppression of enemy air defenses or EW missions.
- Provides input to the overall assessment regarding effectiveness of electromagnetic attack missions.
- Maintains, updates, and distributes the status of EW assets.
- Validates and disseminates stop jamming requests.
- Coordinates and expedites JSIR reporting with the G-2 or S-2 and G-6 or S-6 for potential deconfliction.
- Exercises delegated electromagnetic warfare control authority for ground-based EW within the area of operations.

3-77. The CEWO participates in the targeting working group to identify targets and directs employment of EW assets in support of an operation. Targeting requires continuous involvement from the CEWO. After planning, the CEWO participates in the targeting board and assesses effects using measures of effectiveness. During execution the CEWO—

- Prosecutes approved EW targets.
- Evaluates the effectiveness of EW.
- Maintains situational understanding of EW activities and associated effects.
- Oversees the movement and placement of EW assets in support of operational requirements.
- Continues to identify and assess risk.
- Receives information from EW assets and disseminates to the staff—
  - Detection and location of targeted and potential enemy emitters, including enemy EW assets.
  - Indicators and warnings of enemy activity from EW.
- Maintains direct liaison with the fires cell, G-2 or S-2, and G-6 or S-6 staff to ensure integration and deconfliction of EW activities.
- Coordinates and manages EW missions tasked to subordinate units and requests for nonorganic EW support.
- Validates and disseminates stop jamming requests.
- Exercises delegated electromagnetic attack control authority.

SPECIAL CONSIDERATIONS DURING EXECUTION

3-78. Spectrum resources are congested due to friendly, neutral, and threat use; and contested due to threat activities. Spectrum resource availability also shifts during an operation. The CEWO updates any changes within the electromagnetic environment and updates the common operational picture. During execution, EW planners continually consider—

- The electromagnetic order of battle.
- Signal operating instructions.
- The JRFL.
- Anticipated or reported electromagnetic interference.
- Use of single system configurations or multiple system configurations in a layered approach to accomplish objectives.

SECTION V – ASSESSMENT

3-79. *Assessment* is the determination of the progress toward accomplishing a task, creating a condition, or achieving an objective (JP 3-0). Commanders and 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.

ELECTROMAGNETIC WARFARE ASSESSMENT

3-80. Assessment occurs throughout planning, preparation, and execution; it includes three major tasks:

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

3-81. The CEMA working group makes assessments throughout the various phases of an operation. They assess EW activities during the MDMP, intelligence preparation of the battlefield, information collection synchronization, targeting, and risk management integration.

MEASURES OF PERFORMANCE AND MEASURES OF EFFECTIVENESS

3-82. The CEWO develops the measures of performance and measures of effectiveness for evaluating EW activities during execution. Normally, the CEWO evaluates measures of performance and measures of effectiveness by analyzing data collected by both active and passive means.

3-83. Measures of effectiveness help define whether an EW capability is creating the desired effects or conditions. Example measures of effectiveness from electromagnetic attack include—

- Indications of disrupted or deactivated target radar assets.
- Indications of increased radio traffic on the radar command and control network.
- Indications of target radar power increase.
- Indications of target radar changing frequencies.

3-84. Measures of performance help evaluate whether a unit is accomplishing tasks to standard. In the context of EW, example measures of performance include—

- Whether the electromagnetic attack asset is transmitting at the planned power.
- Whether the electromagnetic attack asset is transmitting the required bandwidth.
- Whether the electromagnetic attack asset is transmitting using the correct polarization.
- Whether all assets for a given mission are synchronized.

3-85. CEWOs use caution when selecting measures of effectiveness to avoid flaws in an analysis of the EW mission. For example, the lack of enemy electromagnetic activity, such as communications or improvised explosive device initiation, does not necessarily mean it was the result of the EW mission; other factors may be the cause. A flawed measure of effectiveness might cause EW operators to conclude incorrectly that an enemy commander is not able to direct the maneuver of subordinates because of electromagnetic attack effects. The enemy commander may have an alternate means of communication.

3-86. During execution, the CEMA working group participates in combat assessments within the targeting process to determine the effectiveness of electromagnetic attack. Combat assessment consists of three elements:

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

Chapter 4
Electromagnetic Attack Techniques

Electromagnetic attack, when effectively employed, enables the commander to dominate the electromagnetic environment and supports the scheme of maneuver during Army operations. This chapter discusses planning and preparation considerations when conducting electromagnetic attack. This chapter also describes common electromagnetic attack techniques and their characteristics, and electromagnetic attack in the targeting process.

PLANNING ELECTROMAGNETIC ATTACK

4-1. Commanders use electromagnetic attack to affect threat communications and noncommunications capabilities. Electromagnetic attack may be conducted as a single action or supplement other lethal or nonlethal attacks. Dynamics in an operational environment require the CEWO to employ different electromagnetic attack techniques based on mission variables. Electromagnetic attack techniques include countermeasures and electromagnetic deception. Army operations employ offensive and defensive electromagnetic attack such as—

- Jamming adversary radar or command and control systems.
- Using antiradiation missiles to suppress adversary air defenses.
- Using electromagnetic deception to confuse adversary surveillance and reconnaissance systems.
- Employing self-propelled, towed, or stationary decoys.
- Using self-protection and force protection measures such as use of expendables (flares and active decoys).
- Employing directed-energy or infrared countermeasures.

4-2. Planning electromagnetic attack actions must be based on mission analysis and a firm understanding of the commander’s intent. Once the mission and scheme of operations (maneuver, fires, effects, and information advantage) is understood, the CEMA section, in conjunction with the staff, carefully considers—

- Interference with friendly communications.
- Intelligence gain or loss.
- Spectrum use by neutral actors.
- The persistence of effects.
- Electromagnetic signatures.
- Personnel and equipment capabilities and limitations.

- Desired offensive or defensive effects to support and accomplish mission objectives.
- Delivery method for effects—airborne, ground, or a combination of both.
- Electromagnetic order of battle to understand and validate electromagnetic attack targets.
- Priority of enemy units, systems, functions.

ELECTROMAGNETIC ATTACK EFFECTS

4-3. Electromagnetic attack denies the threat the ability to use the electromagnetic spectrum, or spectrum-dependent equipment. An electromagnetic attack may also affect personnel, decision making, or potential courses of action. Electromagnetic attack effects include denying, destroying, degrading, deceiving, delaying, diverting, neutralizing, or suppressing threat spectrum-dependent capabilities. These effects are mutually exclusive, and these terms are common when describing desired effects. For more information on effects, refer to JP 3-60.

4-4. The different electromagnetic attack systems have varying capabilities. EW personnel planning and employing the systems consider each of the system-specific parameters, the environment, and mission requirements. Each system has specific capabilities and may require ingenuity during planning to ensure mission success.

ELECTROMAGNETIC ATTACK CONSIDERATIONS

4-5. Electromagnetic attack depends on electromagnetic support and SIGINT to provide targeting information and battle damage assessment. Throughout the MDMP and the targeting process, the CEMA section coordinates and deconflicts spectrum requirements with the G-6 or S-6 spectrum manager. Refer to JP 3-85 for more information about electromagnetic attack and defensive electromagnetic attack planning.

4-6. The CEMA working group plans and rehearses spectrum deconfliction procedures. When electromagnetic attack conflicts with information collection efforts, the commander either dictates priorities or the G-3 or S-3 decides based on commander's guidance.

4-7. Threat intelligence collection activities can influence electromagnetic attack planning. A well-equipped peer threat can detect electromagnetic attack activities by employing electromagnetic support techniques to gain intelligence on U.S. force locations and intentions. Analysis of the enemy electromagnetic order of battle aids the CEWO in protecting electromagnetic attack assets. The CEWO protects electromagnetic attack assets through electromagnetic protection and risk mitigation techniques to counter the threat electromagnetic support and electromagnetic attack efforts. For more information about electromagnetic protection, see chapter 5.

Electromagnetic Warfare Persistence

4-8. Aside from antiradiation missiles, the effects of jamming are less persistent than effects achieved by lethal means. Jamming effects persist as long as the jammer is emitting within range to affect the targeted receiver or receivers. These effects last a matter of seconds or minutes, which makes the timing of such missions critical. Timing is essential when units use jamming in support of aviation or ground platforms. For example, in a mission that supports the suppression of enemy air defenses, 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 possible reaction time of threat air defenses. Because jamming may cause the threat to take unexpected actions or use other means of communication to avoid the intended effect, the CEWO uses electromagnetic support techniques to sense and validate the persistence of known threat transmissions.

Electromagnetic Pulse

4-9. An *electromagnetic pulse* is a strong burst of electromagnetic radiation caused by a nuclear explosion, energy weapon, or by natural phenomenon, that may couple with electrical or electromagnetic systems to produce damaging current and voltage surges (JP 3-85). An electromagnetic pulse creates a permanent effect and destroys equipment, rendering it useless until the threat repairs or reconstitutes the capability. Units at echelons theater army and below seeking to destroy a target using an electromagnetic pulse rely on strategic-level decisions and capabilities to achieve this effect.

Countermeasures

4-10. *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 3-85). The Army uses countermeasure techniques to mitigate threat EW sensing and attack activities. Countermeasures can be active or passive and used preemptively or reactively. Countermeasure devices and techniques include flares, chaff, radar jammers, CREW systems, and decoys. *Chaff* is radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion (JP 3-85).

Electromagnetic Deception

4-11. Deception techniques include misleading transmissions that present false indications of friendly force battle rhythms. Control and coordination are necessary to avoid confusing friendly activities with deception missions. When planning electromagnetic deception, EW planners consider activities that support the current friendly operation, as well as those that will support the deception mission, integration, and deconfliction. EW supports both military deception and tactical deception, using electromagnetic deception and scaling appropriately for the desired effect. Electromagnetic deception uses deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to a threat or to threat spectrum-dependent weapons, thereby degrading or neutralizing the threat’s combat capability.

Electromagnetic deception can increase or decrease ambiguity, affecting the situational understanding of the threat decision maker. This can indicate to a threat commander the certainty of a course of action or create sufficient confusion to disrupt proper decision-making.

4-12. EW supports information advantage activities and deception plans using electromagnetic deception techniques. The G-3 or S-3 staff plans and supervises deception missions. The information advantage staff develops deception plans. Integration of electromagnetic deception with other information advantage activities is necessary when conducting deception missions. The CEWO is responsible for the EW portion of the deception plan.

4-13. Time is a critical factor in deception planning. A deception plan intended to deceive the adversary for two or three days usually includes well-coordinated electromagnetic deception that uses as many friendly transmitters as reasonable. Regardless of the duration, the threat's ability to detect emitters is essential to the success of electromagnetic deception. Deceptive emissions require—

- A frequency that is compatible with threat receivers.
- Signals strong enough to reach threat sensors.
- Modulation techniques employed and detected by threat equipment.
- Planning and deconfliction for electromagnetic deception broadcast locations.

4-14. Each piece of spectrum-dependent equipment exhibits an electromagnetic signature. Electromagnetic deception presents realistic decoy signatures to threat sensors, potentially causing the threat to draw incorrect conclusions about friendly locations and activities. The three types of deception are—

- Simulative electromagnetic deception.
- Manipulative electromagnetic deception.
- Imitative electromagnetic deception.

Simulative Electromagnetic Deception

4-15. Simulative electromagnetic deception attempts to represent friendly notional or actual capabilities to mislead threat forces. Simulative electromagnetic techniques require extensive command and staff collaboration to present a believable deception plan. What the threat detects electronically should be consistent with other information sources. Simulative electromagnetic deception transmissions require close attention. Electromagnetic deception effects are often of short duration.

4-16. Simulative electromagnetic deception includes the use of systems that give off emissions indicative of a particular organization. Simulative electromagnetic deception also includes using emitters to imply a type or change of activity by a unit, for example, placing surveillance radars in a typical defensive array when the intent is to attack.

Manipulative Electromagnetic Deception

4-17. Manipulative electromagnetic deception uses communication or noncommunication signals to convey indicators that mislead the enemy. For example, to indicate that a unit will attack when it is actually going to withdraw, the unit might transmit false plans and requests for ammunition. Units use manipulative electromagnetic deception to mislead the enemy to misdirect their electromagnetic attack and electromagnetic support assets, while interfering less with friendly communications. Manipulative electromagnetic deception seeks to eliminate, reveal, or convey misleading indicators of friendly intentions. Success in manipulative electromagnetic deception and simulative electromagnetic deception depends on understanding how friendly transmitters appear to the threat.

Imitative Electromagnetic Deception

4-18. Imitative deception mimics threat emissions with the intent to mislead them. Imitative electromagnetic deception, if recognized by the enemy, can compromise friendly SIGINT efforts. Imitative deception normally requires approval from higher-echelon commands.

4-19. An example of imitative electromagnetic deception includes entering the adversary's communication nets by using their call signs and radio procedures and giving threat commanders instructions to initiate actions that are advantageous to friendly forces. Targets for imitative electromagnetic deception include any threat receiver and range from cryptographic systems to plain-language tactical nets. Imitative electromagnetic deception can cause a unit to be in the wrong place, to place ordnance on the wrong target, or to delay attack plans. Imitative deception presents false information to the threat and affects decision making. Imitative electromagnetic deception requires equipment capable of convincingly duplicating the emissions of enemy equipment to be effective.

PREPARING ELECTROMAGNETIC ATTACK

4-20. In preparation for electromagnetic attack, the CEWO gathers target information from electromagnetic support sensors and the electromagnetic order of battle. The information includes the location of the targeted asset, its technical characteristics, and the frequencies in use. Using location, characteristics, and frequency, the CEWO determines which assets are best to conduct an electromagnetic attack. The CEWO then calculates the power required to jam the targeted receiver. See appendix B for the formulas for calculating required jamming power. The CEWO gives guidance to subordinate units about electromagnetic attack. The guidance includes information that allows the subordinate unit to prepare for the electromagnetic attack. Electromagnetic attack guidance includes—

- Target identification.
- Target location.
- Special coordination requirements and procedures.
- Jamming technique.

- Jamming duration.
- Desired effect.
- Battle damage assessment method of delivery and prescribed format.

ELECTROMAGNETIC ATTACK REQUESTS

4-21. Unit standard operating procedures establish guidelines for drafting, processing and submitting ground and airborne electromagnetic attack requests. Units also review joint tactical air strike requests (JTAR), the electromagnetic attack request format, nonlethal effects requests, and other theater-specific formats, and incorporate them as necessary. Refer to ATP 3-09.32 more information about the JTAR. See appendix D for more information about the electromagnetic attack request format.

4-22. The objective of electromagnetic attack is to disrupt or degrade the threat's ability to receive electromagnetic signals radiating from their transmitters, or process signals from other sources, such as friendly transmissions, with confidence. CEWOs integrate electromagnetic attack into the tactical plan by coordinating with the targeting board and the CEMA working group. The target list is an output from the targeting board and specifies the targets and times of attack, regardless of the method used. When preparing for electromagnetic attack, the CEWO considers—

- The commander's intent.
- The rules of engagement.
- The location and identity of the targeted receiver and associated transmitter.
- The characteristics of the targeted receiver and associated transmitter.
- The target engagement calculations.
- The associated risk when targeting with electromagnetic attack.

4-23. The CEWO coordinates with the staff to plan electromagnetic attack. The G-2 or S-2 staff provides the electromagnetic order of battle to aid in the development of targets. The CEWO maintains the electromagnetic order of battle for future targeting efforts. The electromagnetic order of battle includes—

- Threat's unit or organization.
- Frequencies in use.
- Call signs.
- Location.
- Power of transmitters.
- Bandwidth.
- Equipment nomenclature.
- Modulation type.
- Multiplexing capability.
- Pulse duration.
- Pulse repetition frequency.
- Antenna type.
- Antenna height.

- Antenna orientation.
- Antenna gain.

4-24. The CEWO determines the minimum power required to attack the target receivers. Excessive power makes it easier for the threat to locate and attack the friendly electromagnetic attack asset. Distances between the threat transmitter and receiver and the friendly electromagnetic attack asset are critical considerations for electromagnetic attack asset placement.

4-25. Terrain is a factor because line of sight is necessary between the electromagnetic attack asset and the location of the targeted receiver. The threat may use terrain to mask transmitted signals from friendly detection and attack. Other terrain considerations include—

- Urban structures.
- Bodies of water.
- Soil composition.
- Vegetation density.

Electromagnetic Attack Platform Selection

4-26. The selection of electromagnetic attack platforms is a significant factor when preparing to conduct electromagnetic attack. Electromagnetic attack platform selection considerations include—

- Concealment characteristics.
- Power output capability.
- Availability of physical protection.
- Time available for the mission.
- Route clearance and escort requirements to conduct friendly maneuver.
- Augmented security coordination.
- Airspace coordination for airborne EW assets.

EXECUTING ELECTROMAGNETIC ATTACK

4-27. The CEWO has multiple options to choose from when executing electromagnetic attack. The CEWO prosecutes electromagnetic attack from airborne and ground-based platforms and monitors the electromagnetic attack activities during the mission. Mobile platforms consist of vehicular and dismounted configurations. Units conduct electromagnetic attack using the chosen jamming techniques. Electromagnetic support and SIGINT capabilities evaluate effectiveness of the jamming efforts to the CEWO.

Close Air Support

4-28. Close air support delivers electromagnetic attack using a variety of aerial platforms. There are two types of close air support requests—preplanned and immediate. The CEWO reviews the air tasking order when resourcing electromagnetic attack requirements. When close air support is available, the CEWO submits a request to use close air support for the electromagnetic attack mission.

4-29. The air support operations center provides the air tasking order, which has detailed information on aircraft, crews, missions, munitions, and targets. Planners submit preplanned close air support requests to support operations. The air tasking order typically covers a 24-hour duty cycle. The joint air operations command and control center establishes cut-off times to receive preplanned air support requests for inclusion in the air tasking order. Immediate air support requests arise from situations that develop outside the planning horizon of the joint air tasking cycle. It is important to understand that air assets available to satisfy immediate air support requests already exist in the published air tasking order. For more information about close air support and the air tasking order, refer to JP 3-09.3.

AIRBORNE ELECTROMAGNETIC ATTACK

4-30. Airborne electromagnetic attack delivers jamming from rotary-wing, fixed-wing, or unmanned aircraft systems. Although some of these platforms are organic to the Army, much of the airborne electromagnetic attack capability resides in other Services. Requesting airborne electromagnetic attack often requires coordination with joint forces. Effective airborne electromagnetic attack requires integrating procedures and communications between the supported unit and the airborne electromagnetic attack asset owner.

Communication With the Joint Terminal Attack Controller

4-31. Communication between the aircrew, CEWO, and the joint terminal attack controller throughout the mission is beneficial for maintaining situational understanding and for retasking an asset. Best practices include active communication between the CEWO and the aircraft that is delivering the attack.

4-32. When the CEWO cannot communicate with the aircrew or the joint terminal attack controller, the supporting aircraft continues with the airborne electromagnetic attack mission specified in the electromagnetic attack request format. A technique is to note in the electromagnetic attack request format regarding what to do in the event of a communication failure.

Canceling and Retasking Airborne Electromagnetic Attack

4-33. Changes within an operational environment and electromagnetic attack missions may make it necessary to reprioritize assets. Air platforms are in demand for other purposes such as surveillance, intelligence missions, or communications. The CEWO can request dynamic retasking of airborne electromagnetic attack assets and requests retasking with the joint terminal attack controller and the joint air operations center.

Airborne Electromagnetic Attack Cancellations at the Battalion and Brigade

4-34. Sometimes it is necessary to cancel airborne electromagnetic attack missions. CEWOs communicate cancellations to the asset owner and requestor points of contact.

Reporting cancellations ensures the most efficient use of electromagnetic attack assets and availability for other missions.

Advanced Cancellation of a Preplanned Mission

4-35. Cancellation of an airborne electromagnetic attack mission more than six hours before a scheduled flight is considered a routine cancellation. The requestor includes the reason for the cancellation. The CEWO immediately communicates a cancellation of a mission to release the airborne electromagnetic attack asset for other missions. The CEWO also notifies the fire support officer and the air liaison officer. Cancellations made during operations include direct voice communications whenever possible to ensure someone is available and ready to process the cancellation.

Short-Notice Cancellation of a Preplanned Mission

4-36. Short-notice airborne electromagnetic attack cancellations are cancellations that occur less than six hours before a preplanned mission. Short-notice cancellations require immediate action to avoid mission launches and the unnecessary employment of an asset. The CEWO informs the designated point of contact that a cancellation is coming by the most expeditious means available. Following the initial notification, the CEWO sends the official cancellation JTAR to the appropriate point of contact as soon as possible. Since the cancellation may require communications that bypass the normal chain of command, CEWOs include the process in the unit standard operating procedures and battle drills.

Immediate Cancellation of Preplanned Mission

4-37. CEWOs use immediate cancellation techniques to cancel missions within one hour of the expected execution time. CEWOs use the fastest communication means possible, such as Internet relay chat or voice communications, to distribute the necessary cancellation information. Immediately following an immediate cancellation, CEWOs contact the prescribed point of contact and provide an official cancellation using the points of contact on the JTAR and electromagnetic attack request format to ensure units receive information promptly. Effective units include this process in the unit standard operating procedures and battle drills.

Dynamic Retasking

4-38. The staff makes every effort to provide immediate electromagnetic attack in response to an urgent request, including the allocation of available airborne electromagnetic attack assets. The retasking of airborne electromagnetic attack assets fulfills requests for on-demand requirements.

4-39. The process for retasking airborne electromagnetic attack platforms varies depending on joint and Army command and control, task organization, force disposition, and unit boundaries. The requesting unit submits a request to their supporting EW representative.

4-40. If the requesting unit previously submitted a JTAR for electromagnetic attack support, the CEWO modifies the existing JTAR with a numbered change. Some units make the change using red for easier identification. If the requesting unit has not submitted a JTAR for the mission, the CEWO creates a new JTAR. The CEWO provides status updates to the requesting unit. Effective units address the processes for maintaining updated JTARs in their standard operating procedures and battle drills.

4-41. Due to the dynamic nature of an urgent requirement, there is no way to calculate the amount of time needed for coordinating the airborne electromagnetic attack. The CEWO or joint terminal attack controller notifies the appropriate EW representative and air support operations center when it is apparent that the duration of electromagnetic attack will exceed the initially anticipated time. The air support operations center notifies the airborne electromagnetic attack asset and coordinates any additional fuel requirements or determines the need to re-task another airborne electromagnetic attack asset. The air support operations center then informs the CEWO and joint terminal attack controller of what support to expect. The joint terminal attack controller or CEWO contacts the air support operations center to release airborne electromagnetic attack assets upon mission completion or cancellation.

ELECTROMAGNETIC JAMMING TECHNIQUES

4-42. CEWOs direct the use of jamming techniques to disrupt the threat's ability to effectively receive or process electromagnetic signals by overcoming the threat receiver with higher-power transmissions. Successful jamming of receivers requires an understanding of available jamming techniques.

Electromagnetic Jamming

4-43. *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, with the intent of degrading or neutralizing the enemy's combat capability (JP 3-85). CEWOs integrate electromagnetic attack techniques, including electromagnetic jamming, into operation orders and exercise technical control over EW platoons executing electromagnetic jamming.

4-44. The primary effects of jamming persist when the jammer is within range of the target and emitting. Effects of jamming may be evident in the actions of the adversary during or following the electromagnetic attack mission. Jamming techniques include—

- Standoff jamming.
- Escort jamming.
- Spot jamming.
- Barrage jamming.
- Sweep jamming.
- Follower jamming.

Standoff Jamming

4-45. Standoff jamming disrupts or degrades threat command and control systems and sensors that operate in the electromagnetic spectrum. A standoff jamming mission projects from a stationary and protected location within a friendly area of operations. Standoff jamming—

- Affords maximum protection to EW professionals and the systems they deploy from threat actions.
- Generally requires high power and large antennas to reach deep into the threat area of operations.
- Requires precise intelligence on threat frequencies and receiver locations to maximize jamming effects.
- Creates windows of opportunity for Army and joint forces to conduct maneuver.

Escort Jamming

4-46. Escort jamming uses a jamming platform that accompanies maneuver forces. Escort jamming is defensive in nature and protects maneuver forces from threat weapons systems that use RF triggers. Successful escort jamming requires precise intelligence regarding threat frequency use. Escort jamming usually does not require the same level of power or large antennas as standoff jamming. Escort jammers use similar vehicle configurations to maneuver vehicles to screen them from visual identification.

Spot Jamming

4-47. The CEWO can jam a specific frequency using a technique referred to as spot jamming. Spot jamming is the least intrusive form of electromagnetic attack, as it does not jam untargeted frequencies. The CEWO requires specific threat system characteristics to plan and execute spot jamming successfully.

Barrage Jamming

4-48. Some electromagnetic attack assets can jam more than one frequency at a time. For example, if the threat incorporates frequency hopping, which uses two or more frequencies at different times during a single transmission, barrage or sweep jamming techniques are considered. Barrage jamming is the jamming of all frequencies within a specified portion of the spectrum at the same time. Barrage jamming techniques apply less power to each jammed frequency because the power extends across the targeted frequency range. Barrage jamming generally requires the EW asset to be closer to the target receivers than sweep or spot jamming techniques. Figure 4-1 on page 4-12 illustrates spot and barrage jamming.

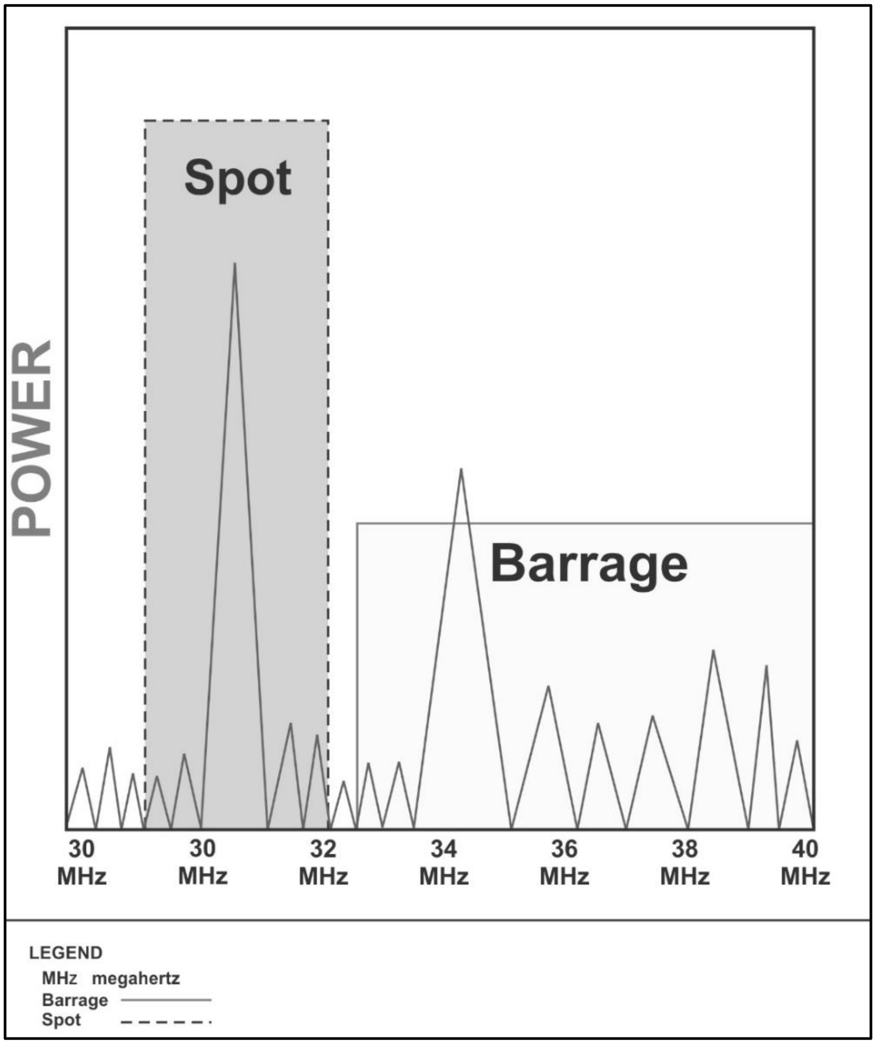


Figure 4-1. Spot and barrage jamming

Sweep Jamming

4-49. The CEWO employs sweep jamming when the electromagnetic order of battle provides a frequency range but not the specific frequency in use. Sweep jamming is the jamming of a selected portion of the electromagnetic spectrum by sweeping the known frequency range at a predetermined rate. Sweep and spot jamming use a higher level of transmitting power than barrage jamming.

Follower Jamming

4-50. Follower jamming is a form of electromagnetic attack to target receivers automatically when the system detects a threat transmission. Follower jamming is passive until a targeted transmitter emits a signal. Follower jamming uses spot, barrage, and sweep jamming techniques. EW professionals configure the jammer to attack a specific frequency or range of frequencies. The G-2 or S-2 compiles the electromagnetic order of battle and determines the frequencies employed by the threat. The CEWO ensures the proper equipment configuration to jam the prescribed frequencies. Follower jamming also jams threat frequency hopping receivers. Because the asset is not always transmitting, the follower jamming technique allows a jammer to maximize its resources against a target while minimizing the threat's ability to sense and locate the jammer.

Electromagnetic Intrusion

4-51. *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 3-85). The CEWO employs electromagnetic intrusion based on the electromagnetic order of battle identifying a specific type of emitter. Electromagnetic intrusion techniques are discrete and tailored to specific target systems, as opposed to more broad techniques such as spot, sweep, or barrage jamming. An example of electromagnetic intrusion would be radio transmissions simulating air traffic control communications and giving false instructions to a pilot.

DEFENSIVE ELECTROMAGNETIC ATTACK

4-52. Defensive electromagnetic attack degrades the threat's ability to employ weapons that use RF-activated triggers. Defensive electromagnetic attack protects friendly personnel and equipment. CREW systems implement this defensive electromagnetic attack.

4-53. Defensive electromagnetic attack uses the electromagnetic spectrum to protect personnel, facilities, capabilities, and equipment. Examples include self-protection and other protection measures such as the use of expendables (flares and active decoys), jammers, towed decoys, directed-energy infrared countermeasures, and CREW systems.

4-54. CREW systems conduct defensive electromagnetic attack to jam threat radio frequencies to prevent radio-controlled improvised explosive devices from receiving a triggering signal, thus stopping the device from detonating. Units program CREW systems with threat-specific loadsets based on various sources of intelligence, including the technical exploitation of recovered radio-controlled improvised explosive devices. The loadset configures the operational frequency range, change rate, and other attributes of the CREW system. The Army employs mounted, dismounted, and fixed CREW systems as countermeasures to radio-controlled improvised explosive devices.

ELECTROMAGNETIC ATTACK TECHNIQUES IN LARGE-SCALE COMBAT OPERATIONS

4-55. Peer threats rely on the electromagnetic spectrum for command and control, sensing and targeting, and EW. Units require electromagnetic attack capabilities during large-scale combat operations to counter threat communications and noncommunications emitters.

4-56. When jamming threat communications, the CEWO aligns EW capabilities with targets. The electromagnetic attack does not jam every possible threat communication. Figure 4-2 is an example of electromagnetic attack disrupting communications between an enemy command post and an enemy tank company. The close proximity and transmit power of the radios of the enemy tanks in a company formation allows them to maintain uninterrupted communication. The enemy command post transmissions to the company have a greater distance to travel and weaker signal at the receiving antenna, leaving the communications vulnerable to jamming. In this illustration, the enemy company can still effectively communicate within the company formation, but not with the command post.

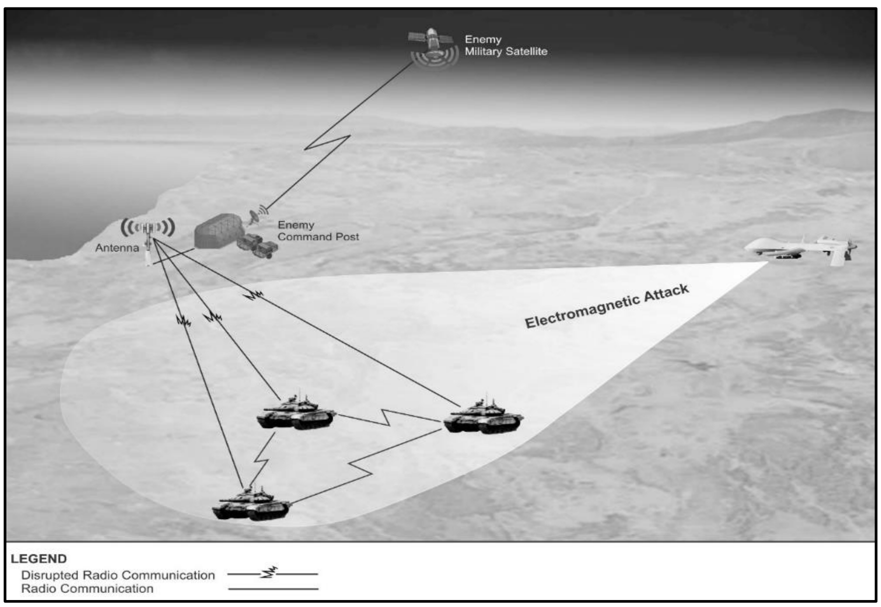


Figure 4-2. Jamming to disrupt enemy command post-to-company communications

4-57. Enemies employ multiple sensors and noncommunications emitters, such as radars, to detect and locate friendly forces during large-scale combat operations. The CEWO uses EW activities, such as electromagnetic deception, to disrupt the enemy's ability to target friendly forces. The CEWO also disrupts enemy SIGINT and electromagnetic support sensors to prevent detection, location, and exploitation of friendly transmitters.

4-58. A common misperception with electromagnetic attack is that jammers affect every emitter on the battlefield. Factors that limit jamming effectiveness include antenna type and power. EW personnel require an understanding of the characteristics of links between nodes such as frequencies in use, transmission power levels, modulation type, and available bandwidth. The electromagnetic order of battle includes these characteristics and ties them to a node. The G-2 or S-2 provides the electromagnetic order of battle to EW planners to support targeting. EW planners use the electromagnetic order of battle to assess which targets to engage with electromagnetic attack at a time and place that supports the commander's intent and scheme of maneuver. Planners then determine how to engage targets based on threat system characteristics and the electromagnetic attack capabilities of available friendly assets.

ELECTROMAGNETIC ATTACK IN THE TARGETING PROCESS

4-59. 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 decides which targets to acquire and attack. As the operation continues, the staff assesses the results.

4-60. Targeting provides an effective method to match 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 implement actions to achieve the intended effects on the targets. The CEWO integrates electromagnetic attack into targeting to achieve desired effects in support of Army operations. The CEWO considers the functions of decide, detect, deliver and assess for targeting.

DECIDE

4-61. The decide function begins the targeting cycle by establishing the focus and priorities for targeting and information collection. The decide function for EW uses threat information from the CEMA section and G-2 or S-2, including threat tactics, techniques, and procedures.

4-62. The CEWO plans the integration of EW into standard targeting products identified by the fires cell. The planning products include—

- High-payoff target list.
- Target selection standards.
- Attack guidance matrix.
- Target list worksheet.
- Annex C, Appendix 12 of the operation order.

DETECT

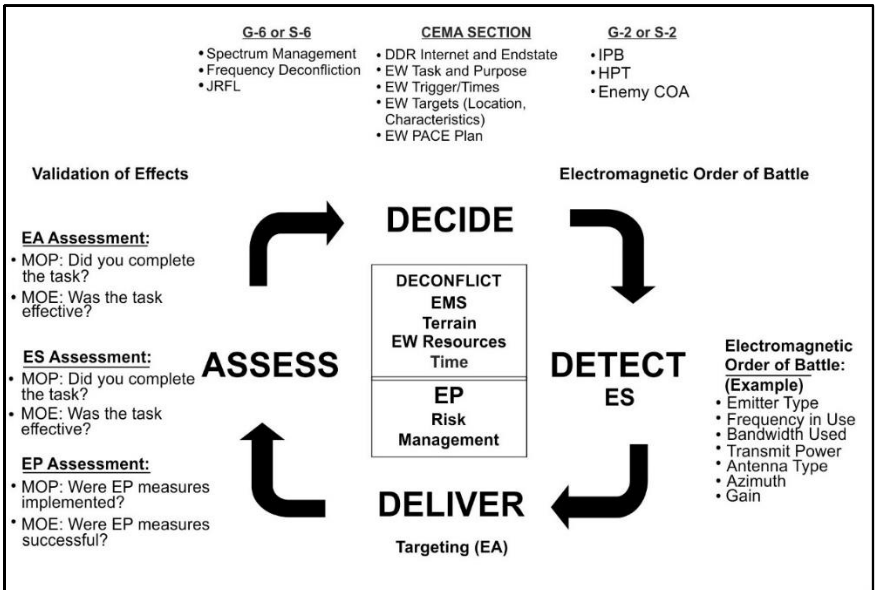
4-63. The targeting working group identifies high-payoff targets. The G-3 or S-3 tasks assets to detect the targets. The collection manager pairs assets to targets based on the collection plan. The CEWO coordinates with the collection manager to synchronize electromagnetic support and SIGINT assets to detect high-payoff targets. Electromagnetic support and SIGINT assets provide data that includes the location of transmitters and receivers, transmitter signal strength, and frequencies used by the targeted receiver to deliver lethal or nonlethal fires against the target.

DELIVER

4-64. 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. EW assets deliver electromagnetic attack and may use electromagnetic support or SIGINT resources to determine the effectiveness of the electromagnetic attack. Electromagnetic support and SIGINT assets also serve as observers when the commander directs lethal fires against enemy transmitters. Close coordination between those conducting SIGINT and electromagnetic attack is critical during the engagement. This coordination assists the CEWO in avoiding unintentional interruption of an ongoing SIGINT effort. The CEWO continually coordinates with adjacent unit CEWOs to mitigate unintended effects on friendly units.

ASSESSMENT

4-65. The targeting working group synchronizes EW with other effects. The CEWO coordinates and synchronizes joint and multinational airborne and ground-based EW capabilities. The CEWO also manages the organic EW capabilities within the main command post. Figure 4-3 on page 4-17 illustrates EW in the targeting process.



LEGEND

CEMA	cyberspace electromagnetic activities
COA	course of action
DDR	disarmament, demobilization and reintegration
EA	electromagnetic attack
EMS	electromagnetic spectrum
EP	electromagnetic protection
ES	electromagnetic support
EW	electromagnetic warfare
G-2	assistant chief of staff, intelligence
G-6	assistant chief of staff, signal
HPT	high-payoff target
IPB	intelligence preparation of the battlefield
JRFL	joint restricted frequency list
MOE	measure of effectiveness
MOP	measure of performance
PACE	primary, alternate, contingency, and emergency
S-2	battalion or brigade intelligence staff officer
S-6	battalion or brigade signal staff officer

Figure 4-3. Electromagnetic warfare in the targeting process

This page intentionally left blank.

Chapter 5
Electromagnetic Protection Techniques

The greatest threat to command and control communications at the tactical level is the enemy's use of electromagnetic warfare assets to geolocate and target friendly communications. This chapter discusses electromagnetic protection and some techniques used to overcome electromagnetic interference and jamming. Successful electromagnetic protection requires planning and execution by all members of the unit.

PLANNING ELECTROMAGNETIC PROTECTION

5-1. Electromagnetic protection is a command responsibility. Commanders ensure that all Soldiers in their units train to apply electromagnetic protection techniques. Commanders rely on the staff to mitigate electromagnetic vulnerabilities. The staff continuously measures the effectiveness of the applied electromagnetic protection techniques. Commanders' electromagnetic protection responsibilities include—

- Reading after action reviews and reports about threat jamming or deception efforts and assessing the effectiveness of electromagnetic protection.
- Ensuring the staff reports and analyzes electromagnetic interference, deception, or jamming.
- Analyzing the impact of threat efforts to affect friendly communications.
- Ensuring the unit incorporates appropriate electromagnetic protection techniques such as—
  - Changing network call signs and frequencies in accordance with signal operating instructions.
  - Using approved communications security devices.
  - Loading and using prescribed encryption keys.
  - Using planned authentication procedures.
  - Employing EMCON.

5-2. Threats invest heavily in communications jammers; positioning, navigation, and timing jammers; and offensive cyberspace capabilities to challenge friendly use of the electromagnetic spectrum. Establishing an electromagnetic protection program helps mitigate threat efforts to diminish friendly survivability.

5-3. Electromagnetic protection uses techniques such as limiting transmissions and using natural or manmade objects to mask radiated energy from traveling to undesired destinations. Electromagnetic protection is essential to prevent the threat from learning friendly behaviors and intentions in the electromagnetic spectrum.

5-4. The CEWO considers friendly communications asset characteristics, their priorities for protection, and their purpose of employment when planning electromagnetic protection. Additionally, the CEWO considers threat EW and SIGINT capabilities and their use against friendly systems. The G-6 or S-6 is the primary subject matter expert for the characteristics of friendly communications resources, while the G-2 or S-2 provides the electromagnetic order of battle. The resulting electromagnetic protection plan must balance the unit's need to communicate and operate with the level of protection needed based on the threat assessment.

STAFF ELECTROMAGNETIC PROTECTION RESPONSIBILITIES

5-5. The staff implements the electromagnetic protection plan for the commander. Staff responsibilities are—

- Planning, coordinating, and supporting the execution of electromagnetic protection activities (CEMA working group).
- Advising the commander of threat spectrum-dependent capabilities (G-2 or S-2).
- Supervising the CEMA section, including electromagnetic protection scenarios in command post exercises and field training exercises, and evaluating employment of electromagnetic protection techniques (G-3 or S-3).
- Working with the CEWO to prepare and conduct the unit electromagnetic protection training program.
- Ensuring that primary, alternate, contingency, and emergency means of communications are available to support command and control (G-6 or S-6).
- Distributing communications security materials (G-6 or S-6).
- Performing friendly frequency management and deconfliction and issuing signal operating instructions. (G-6 or S-6 spectrum manager).
- Reviewing the JRFL and updating the list of taboo, protected, and guarded frequencies (G-6 or S-6 spectrum manager).

Note. The primary, alternate, contingency, and emergency communication plan complements electromagnetic protection, as it provides redundant means of communication and designates the order in which an element will move through available communications methods until contact with the desired recipient is established.

5-6. Preventive electromagnetic protection techniques include all measures taken to avoid threat detection and threat electromagnetic attack. Electromagnetic protection seeks to mitigate threat information collection and intelligence gathering efforts. Electromagnetic communications equipment has built-in features used to mitigate threat electromagnetic attack, electromagnetic support, and SIGINT actions. Electromagnetic protection plans include the use of built-in features and user tactics, techniques, and procedures for countermeasures against threat actions.

5-7. To protect friendly combat capabilities, units—

- Regularly brief personnel on threat EW capabilities.
- Safeguard spectrum-dependent capabilities during exercises, workups, and pre-deployment training.
- Coordinate and deconflict spectrum usage.
- Conduct routine home station training on electromagnetic protection measures.
- Take appropriate actions to minimize the vulnerability of friendly receivers to threat jamming, such as reduced power, brevity of transmissions, and directional antennas.

ELECTROMAGNETIC PROTECTION CONSIDERATIONS

5-8. Electromagnetic protection is only effective when everyone in an organization understands its importance and can readily identify opportunities to implement protection activities. A solid understanding of the mission greatly aids in the establishment of the electromagnetic protection plan to support mission objectives. Electromagnetic protection includes system technical capabilities, such as frequency hopping, shielding of electronics, spectrum management, and EMCON procedures. In developing an effective electromagnetic protection plan, the CEWO and the CEMA working group should consider—

- Vulnerability analysis and assessment of friendly communications assets.
- Electromagnetic protection monitoring techniques and feedback procedures.
- Electromagnetic protection effects on friendly capabilities.

Vulnerability Analysis and Assessment

5-9. Vulnerability analysis and assessment form the basis for effective electromagnetic protection plans. EW personnel use electromagnetic support capabilities to survey and characterize the unit's electromagnetic signature. Survey results help the commander and staff visualize and understand the information the unit's electromagnetic signature might reveal to the threat. Based on the electromagnetic survey, the commander and staff determine appropriate measures to minimize electromagnetic signatures. The G-6 or S-6 is the primary subject matter expert on the characteristics of friendly communications systems, while the G-2 or S-2 provides information on the threat's electromagnetic order of battle and weapon systems.

5-10. The National Security Agency monitors communications security and provides security posture feedback to units. Its programs focus on telecommunications systems using wire and electromagnetic communications. Their programs can support and remediate the command's communications security procedures.

5-11. A red team provides an independent capability to explore alternatives in plans and operations in the context of an operational environment and from the threat's perspective. A red team aids in identifying friendly and enemy vulnerabilities and opportunities, assists in identifying areas for assessment, and provides critical reviews and analysis of plans to identify potential weaknesses and vulnerabilities. The red team, in conjunction with the CEWO and the G-2 or S-2 staff, increases understanding of the operational environment and determines what intelligence the adversary can gain.

Signature Mitigation

5-12. Armed with a complete picture of friendly electromagnetic signature and threat capabilities, the commander and staff determine electromagnetic hardening measures, electromagnetic masking techniques, spectrum management procedures, and EMCON procedures to minimize the unit's electromagnetic signature.

5-13. During planning, preparation, execution, and assessment, the CEWO reviews the unit's electromagnetic protection techniques and procedures to determine weaknesses and develops improvement plans. The command should conduct assessments and vulnerability analyses periodically to verify the effectiveness of mitigation techniques. Units should consistently practice electromagnetic protection during all training, exercises, and deployments.

Electromagnetic Protection Effects on Friendly Capabilities

5-14. The CEWO and the G-6 or S-6 present the risk assessment to the commander during the MDMP. The commander decides what level of risk is acceptable. For electromagnetic protection planning, the CEWO and G-6 or S-6 consider—

- Spectrum management.
- Electromagnetic hardening.
- Electromagnetic masking.
- EMCON.
- Electromagnetic compatibility.
- Terrain masking.
- Wartime reserve modes.

SPECTRUM MANAGEMENT OPERATIONS

5-15. *Spectrum Management Operations* are the interrelated functions of spectrum management, frequency assignment, host-nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02). Spectrum management affects a unit's ability to conduct electromagnetic protection. The G-6 or S-6 spectrum manager prepares and maintains a list of friendly frequencies and coordinates with the G-2 or S-2 who maintains the list of threat frequencies in use. Knowing the purpose of spectrum resources and their characteristics allows the spectrum manager to assist the CEWO when preparing the electromagnetic protection portion of an operation or mission.

5-16. Spectrum management also involves knowing the types and quantity of friendly emitters in the area of operations. Using frequencies employed by other friendly forces in the same area of operations may cause unintended interference, or frequency fratricide.

5-17. Units choose the optimal frequency to communicate based on mission requirements. For example, use of high frequency (HF) is desirable when communicating over land for thousands of miles. VHF, in contrast to HF, is usually ineffective at distances over 30 kilometers. The spectrum manager analyzes RF characteristics using modeling software that calculates a transmitter's intended and unintended effects on a receiver and the distance the radio wave travels. The database includes frequencies used for command and control and electromagnetic attack.

ELECTROMAGNETIC HARDENING

5-18. *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 3-85). The CEWO and G-6 or S-6 mutually develop standard operating procedures and inspect the configuration of unit equipment such as the proper grounding of communications assemblages, serviceability of cable shielding, and adequate cable connectivity. These actions protect friendly communications and noncommunications resources from threat identification, lethal and nonlethal attack, and exploitation.

ELECTROMAGNETIC MASKING

5-19. *Electromagnetic 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 electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-85). Electromagnetic masking disguises, distorts, or manipulates friendly electromagnetic radiation to conceal critical information or present false perceptions to threat commanders. Electromagnetic masking is an essential component of military deception, operations security, and signals security.

ELECTROMAGNETIC COMPATIBILITY

5-20. *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 3-85). Before units acquire EW equipment, the units conduct electromagnetic compatibility analysis to identify any potential issues, and to ensure maximum use of equipment.

EMISSION CONTROL

5-21. *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 3-85). EMCON prevents the threat discovering and attacking the locations of friendly forces with EW. When establishing EMCON best practices, it is important to understand the general categories and status criteria for EMCON levels. Based on the tactical situation or operational environment, the commander can dictate the appropriate EMCON level. During operations, commanders should consider EMCON level 3 (amber) as the baseline condition. Figure 5-1 captures the five EMCON levels and the general descriptive criteria associated with each level.

EMCON Status	Description
EMCON 5 **Green**	Describes a situation where there is no apparent hostile activity against friendly emitter operations. Operational performance of all EMS-dependent systems is monitored, and password-encryption-enabled systems are used as a layer of protection.
EMCON 4 **Yellow**	Describes an increased risk of attack after detection. Increased monitoring of all EMS activities is mandated, and all end users must make sure their systems are secure, encrypted, power levels monitored, and transmissions limited. EMS usage may be restricted to certain emitters, and rehearsals for elevated EMCON is ideal.
EMCON 3 **Amber**	Describes when a risk has been identified. Counter ECM (encryption, FH, directional antennas) on important systems is a priority, and the CEWO's alertness is increased. All unencrypted systems are disconnected.
EMCON 2 **Red**	Describes when an attack has taken place but the EMCON system is not at its highest alertness. Non-essential emitters may be taken offline, alternate methods of communication may be implemented and modifications are made to standard lower EMCON configurations (for example, power levels and antenna types).
EMCON 1 **Black**	Describes when attacks are taking place based on the use of the EMS. The most restrictive methods of EP are enforced. Any compromised systems are isolated from the rest of the network.

LEGEND

CEWO	cyber electromagnetic warfare officer	**EMS**	electromagnetic spectrum
ECM	electromagnetic countermeasures	**FH**	frequency hop
EMCON	emission control	**EP**	electromagnetic protection

Figure 5-1. Emission control status

5-22. The EMCON emitter matrix establishes the operational criteria for emitters at each EMCON level and works in conjunction with the primary, alternate, contingency, and emergency communication plan. Every emitter within the unit should be included and the corresponding criteria described. The commander, with assistance and input from the CEWO and the G-6 or S-6, decides which restrictions to place on each spectrum-dependent system, at each EMCON level. Figure 5-2 on page 5-7 demonstrates the use of the EMCON levels and shows how they escalate for the single channel ground and airborne radio system-advanced system improvement program radio.

Emitter	Emitter Criteria by EMCON level				
	EMCON 5 Green	EMCON 4 Yellow	EMCON 3 Amber	EMCON 2 Red	EMCON 1 Black
SINCGARS-ASIP	Use system as prescribed in the Army technical manual.	Must encrypt systems to use them.	Must encrypt and use in FH mode.	Must encrypt and use in FH mode. Cannot transmit above 10 watts and must use directional antennas when available.	Do not use.

LEGEND

EMCON emission control
FH frequency hop
SINCGARS-ASIP single channel ground and airborne radio system-advanced system improvement program

Figure 5-2. Emitter and system criteria by emission control level

Techniques to Control Emissions

5-23. The most basic protection from enemy EW is good radio discipline. This discipline can take the form of using minimum power, antenna masking, and minimizing transmissions.

Minimum Transmit Power

5-24. The use of minimum transmit power prevents signals from traveling beyond the intended receiving station and thereby limits the threat's ability to find and fix friendly forces. Some transmitters include adjustable transmit power settings. A technique to establish minimum transmission power is begin with the lowest power setting and gradually increasing the output power until the intended recipient can validate the successful reception of the transmitted signal.

Antenna Masking

5-25. Antenna masking allows for antenna characteristics such as power, direction, and sensitivity to be modified by the use of shielding and radar reflective camouflage netting. See paragraph 5-31 for more information on camouflage net masking.

Minimizing Transmissions

5-26. Techniques to minimize transmissions include ensuring all transmissions are necessary, preplanning messages before transmitting them, transmitting quickly and precisely, using equipment capable of data burst transmission, and alternate means of communication. Table 5-1 on page 5-8 provides details on the techniques to minimize transmissions.

Table 5-1. Techniques for minimizing transmissions and transmission times

Technique	*Description*
Ensure all transmissions are necessary	Analysis of U.S. tactical communications indicates that most communication used in training exercises is explanatory and not directive. Units use tactical radio communications to convey orders and critical information rapidly. Execution of the operation must be inherent in training, planning, ingenuity, teamwork, and established and practiced standing operating procedures. The high volume of radio communications that usually precedes a tactical operation makes the friendly force vulnerable to enemy interception, direction finding, jamming, and deception.
Note. Even when communications are secure, the intensity of radio transmissions can betray an operation, and the enemy can still disrupt the ability of U.S. forces to communicate.	
Preplan messages before transmitting them	The radio operator should know what to say before beginning a transmission. When the situation and time permit, the operator should write out the message before beginning the transmission. This minimizes the number of pauses in the transmission and decreases transmission time. It also ensures the conciseness of the message.
Transmit quickly and precisely	This is critical when the quality of communications is poor. This reduces the need to repeat a radio transmission. Unnecessary repetition increases transmission time and the enemy's opportunity to intercept U.S. transmissions and gain valuable information. When a transmission is necessary, the radio operator should speak in a clear, well-modulated voice, and use proper radiotelephone procedures.
Use equipment capable of data burst transmission	This is one of the most significant advantages of tactical satellite communications systems. Soldiers use limited time for encoded messages on a digital entry device for transmission over satellite systems.
Use an alternate means of communications	Soldiers use alternate means of communications, such as cable, wire, or messages to convey necessary directives and information.
Use brevity codes	A brevity code is a code which provides no security, but which has as its sole purpose the shortening of messages rather than the concealment of their content. Refer to ATP 1-02.1 for more information on brevity codes.

Radio Placement

5-27. The placement of transmitters and distant receivers in close proximity limits the threat's ability to jam the intended signal. The G-6 or S-6 staff ensures that antennas are more than twice the distance of their height from infrastructure such as power lines. For safety, units avoid placing antennas near sleep areas, tents, and vehicle parking areas.

5-28. The G-6 or S-6 staff manages friendly use of spectrum resources. The G-6 or S-6 staff spectrum manager provides the CEMA section spectrum manager with a database of all assigned friendly frequencies. The G-6 or S-6 staff recommends command post locations to the G-3 or S-3 staff. Variables for site selection include feasibility for Defense Information Systems Network connectivity to higher, lower, and adjacent command posts. Site selection includes electromagnetic protection considerations such as—

- Available terrain for electromagnetic masking.
- Distance between transmitters and receivers.

TERRAIN MASKING

5-29. Transmitters placed on hilltops, mountaintops, or buildings are vulnerable to threat direction-finding techniques, and jamming. Known transmitter locations allow a threat to jam the receivers, listen to transmissions, collect information such as friendly battle rhythm and duration of friendly transmissions, or to attack using lethal fires. To mitigate these vulnerabilities, CEWOs use terrain masking techniques by placing antennas on the side of the mountain, hill or building in a manner that allows the optimal friendly use of the antenna while preventing threat detection and exploitation.

5-30. Figure 5-3 illustrates friendly use of terrain masking. In this example, friendly forces avoid detection by threat direction-finding sensors. This technique applies to any emitter, to include radars and directional antennas, focusing on placing the emitters where they are least detectable.

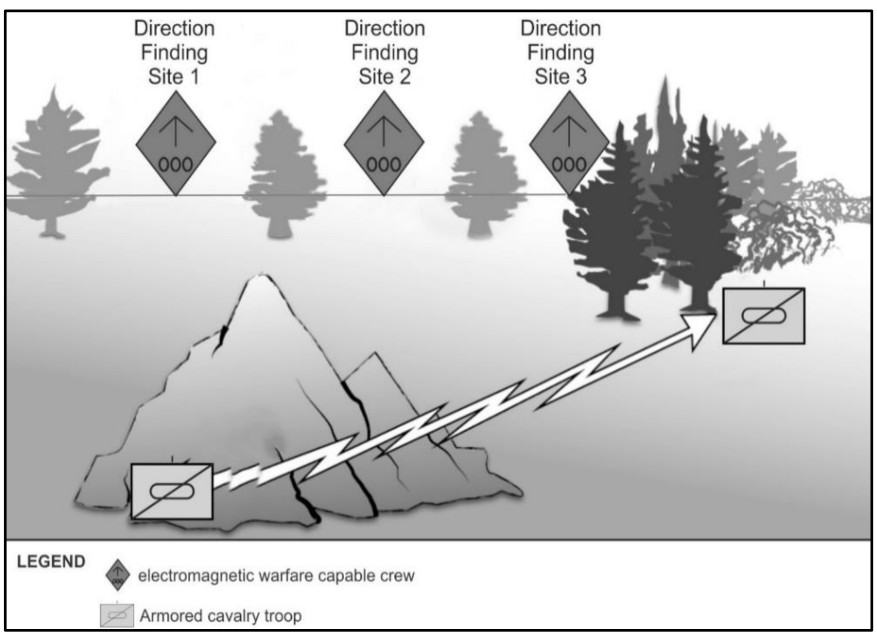


Figure 5-3. Friendly use of terrain masking

CAMOUFLAGE NET MASKING

5-31. Units use camouflage material to cover communications assemblages and their power generators. It is difficult to conceal most communications systems. Radar reflective camouflage netting is an effective means of blocking stray electromagnetic radiation from directional antennas. Camouflage netting placed to the sides and back of a line of sight or satellite communications antenna ensures only the main beam of the antenna radiates. Since the main beam is directional, it is much harder for the threat to detect; the threat would need to be directly in the transmission path.

WARTIME RESERVE MODES

5-32. *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 3-85). Threats search for information that reveals friendly EW vulnerabilities, such as technical articles, magazines, news programs, and web pages that are available on the Internet. The Army prevents public access to wartime reserve modes.

ELECTROMAGNETIC INTERFERENCE

5-33. *Electromagnetic interference* is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. (JP 3-85) Electromagnetic interference prevents successful transmissions. Units must recognize and mitigate electromagnetic interference to use the electromagnetic spectrum to communicate.

5-34. Electromagnetic protection is a preventive measure or countermeasure used to mitigate intentional and unintentional electromagnetic interference. Electromagnetic interference is a concern during planning and execution. A lack of consideration of electromagnetic protection actions creates vulnerabilities to friendly use of the electromagnetic spectrum. Electromagnetic interference does not always require action.

MITIGATION

5-35. Electromagnetic interference requires action when it negatively affects operations by interfering with friendly use of the electromagnetic spectrum. Units incorporate techniques to minimize, reduce, or eliminate prohibitive electromagnetic interference. Techniques to resolve electromagnetic interference include—

- Changing friendly frequencies as prescribed in the signal operating instructions or operation order.
- Implementing terrain masking techniques.
- Using directional antennas.
- Relocating transmitters and receivers.

5-36. The cause of electromagnetic interference can be internal or external. If the electromagnetic interference remains after grounding or disconnecting the antenna, the disturbance is most likely internal and caused by a radio malfunction. Users should contact maintenance personnel for repairs or replace the faulty equipment. Operators can eliminate or substantially reduce the electromagnetic interference or suspected jamming by grounding the radio equipment or disconnecting the receiving antenna. If measures to eliminate the radio as the source of the disturbance are unsuccessful, the interference is most likely electromagnetic jamming.

5-37. Causes of unintentional electromagnetic interference include—

- Friendly and threat use of the same frequencies.
- Other electronic or electric and electromechanical equipment.
- Atmospheric conditions.
- Malfunction of the radio.
- A combination of any of the above.

5-38. Unintentional electromagnetic interference normally travels a short distance; a search of the immediate area may reveal its source. Moving the receiving antenna a short distance may cause noticeable variations in the strength of the interfering signal. Conversely, little or no variation may indicate threat jamming. Regardless of the source, users should take appropriate actions to reduce the effect of electromagnetic interference on friendly communications.

ELECTROMAGNETIC INTERFERENCE BATTLE DRILL

5-39. Some prohibitive electromagnetic interference has a measurable, operational impact. Units execute battle drills to address prohibitive electromagnetic interference, which helps isolate the cause of interference and dispel erroneous assumptions about its cause. For example, knowing that CREW devices are jammers may lead to a hasty assumption that a CREW device impairs the use of combat net radios when operator error or faulty equipment is the cause of the electromagnetic interference. The uninformed assumption that CREW systems are the problem leads to an unnecessary loss of confidence in EW equipment. Lack of confidence in equipment can lead to reluctance to prosecute EW and can negatively impact operations. Proper analysis uses sensors and indicators that identify interfering frequencies, transmission power levels, transmitter strength, and receiver sensitivity.

5-40. Normally, the G-6 or S-6 spectrum manager submits JSIR reports to resolve interference. When appropriate, the staff disseminates the mitigating steps to subordinate units as lessons learned and best practices to avoid future interference. A well-constructed electromagnetic interference battle drill guides units to respond to electromagnetic interference in a consistent, methodical manner. Table 5-2 is an example of an electromagnetic interference troubleshooting battle drill.

***Note*.** Validated lessons learned and best practices are available on the Cyber Lessons and Best Practices Website.

Table 5-2. Electromagnetic interference troubleshooting battle drill

Signal	*Description*
1	Follow equipment troubleshooting steps (verify frequency, cable and antenna connections, communications security). If electromagnetic interference continues, follow remaining steps.
2	Determine start and stop times or duration of electromagnetic interference.
3	Identify electromagnetic interference 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 a joint spectrum interference resolution report through the G-6 or S-6 spectrum manager.
LEGEND	
G-6	assistant chief of staff, signal
S-6	battalion or brigade signal staff officer

JAMMING

5-41. Communications are key at all levels of operations. Threat jamming techniques may prevent commanders from communicating with subordinate units. The lack of communications can negatively affect operations, affect the outcome of battle, and result in possible loss of life. Communications operators must be able to recognize, overcome, and report jamming activities.

RECOGNIZING ELECTROMAGNETIC JAMMING

5-42. Radio operations require that radio operators can recognize potential characteristics of electromagnetic jamming. Recognizing electromagnetic jamming is not always easy; the threat uses diverse forms of jamming. Radio operators require awareness of the possibility of jamming. Training and field experience are invaluable opportunities for operators' ability to distinguish jamming from unintentional electromagnetic interference.

Obvious Jamming

5-43. Obvious jamming is usually easy to detect. When experiencing jamming, it is essential to recognize and overcome the incident. Table 5-3 on page 5-13 lists some common jamming signals.

Table 5-3. Common jamming signals

Signal	*Description*
Random Noise	It is indiscriminate in amplitude and frequency. It is similar to normal background noise. Random noise degrades all types of signals. Operators often mistake it for receiver or atmospheric noise and fail to take appropriate electromagnetic protection actions.
Stepped Tones	Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Single-channel amplitude modulation or frequency modulation use stepped tones for voice circuits.
Spark	Spark is one of the most effective jamming signals. Spark uses short intensity and high intensity; they repeat at a rapid rate. This signal is effective in disrupting all types of radio communications.
Gulls	Generated by a quick rise and slow fall of a variable radio frequency and are similar to the cry of a seagull. It produces a nuisance effect and is very effective against voice radio communications.
Random Pulse	Pulses of varying amplitude, duration, and rate are generated and transmitted. They disrupt teletypewriter, radar, and all types of data transmission systems.
Wobbler	A single frequency modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.
Recorded Sounds	Any audible sound, especially of a variable nature, distracts radio operators and disrupts communications. Music, screams, applause, whistles, machinery noise, and laughter are examples of recorded sounds.

Table 5-3. Common jamming signals (cont.)

Signal	*Description*
Preamble Jamming	A broadcasted tone over the operating frequency of secure radio nets resembles the synchronization preamble of the speech security equipment. Preamble jamming results in all radios being locked in the receive mode. It is especially effective when employed against radio networks using speech security devices.

Subtle Jamming

5-44. The threat can use powerful, unmodulated or noise-modulated jamming signals. Modulation is the process of adding information to an RF signal or carrier by varying its amplitude, frequency, or phase. A lack of noise characterizes unmodulated jamming signals. Noise-modulated jamming signals are characterized by noticeable audible noise. Subtle jamming is ambiguous when there is no sound heard from the receivers. Although everything appears normal to the radio operator, the receiver cannot receive an incoming friendly signal. Users may assume their radios are malfunctioning, instead of recognizing the subtle jamming.

OVERCOMING JAMMING

5-45. Threat jamming requires friendly action. The following paragraphs address the actions to take for detected threat jamming. Users continue normal operations after overcoming jamming or jamming ceases and submit or update the JSIR report. The unit submits a JSIR report regardless of overcoming the jamming or electromagnetic interference. For more information about JSIR reporting, see appendix D.

Continue to Operate

5-46. Threat electromagnetic attack usually involves jamming followed by a brief listening period. Operator activity during the listening period indicates how effective the jamming has been. If friendly communications continue as normal, the threat assumes the jamming is not effective. However, if the threat senses the radio traffic stops, they assume the jamming is effective. Because the threat is monitoring friendly operations, friendly operators continue to use the communications equipment to prevent the threat's assessment of the desired effect.

Improve the Signal-to-Jamming Ratio

5-47. The signal-to-jamming ratio is the relative strength of the desired signal to the jamming signal at the receiver. Signal refers to the desired signal received. Jamming refers to the jamming received. It is best to have a signal-to-jamming ratio in which the desired signal is stronger than the jamming. In this situation, the jamming signal cannot significantly degrade the desired signal. Improving the signal-to-jamming ratio enables successful communications. To improve the signal-to-jamming ratio, operators and signal leaders consider the following courses of action:

- Increase the transmitter power output.
- Adjust, change, or relocate the antenna.
- Establish a retransmission station.
- Use an alternate route for communications.
- Change frequencies.

Increase the Transmitter Power Output

5-48. When the threat successfully jams, operators use the available reserve power on the distant transmitter to overpower jamming. The operator then submits a JSIR report.

Adjust, Change, or Relocate the Antenna

5-49. When jamming occurs, the radio operator ensures optimal antenna positioning to receive the desired signal. Methods that apply to a specific radio set are in the appropriate operator's technical manual. Depending on the antenna, adjustment methods include antenna reorientation, changing the antenna polarization, and installing a different antenna with a longer range.

Note. Distant and local stations require the same antenna polarization. Operators polarize antennas in the horizontal or vertical planes. See appendix A.

Establish a Retransmission Station

5-50. A retransmission station reduces the distance between transmitters and intended receivers. This technique improves the signal-to-jamming ratio.

Use an Alternate Route for Communications

5-51. Threat jamming seeks to prevent friendly forces from communicating with another radio station. When degraded radio communications occur between two radio stations, operators implement the primary, alternate, contingency, and emergency communication plan and use another frequency or communication method. An example of an alternate communication method is changing from a terrestrial line of sight transmission path to satellite communications. Refer to FM 6-02 for more information about primary, alternate, contingency, and emergency communication planning.

5-52. Units provide network diagrams that illustrate friendly radio stations, alternate routes for communications, and the associated terrain. Radio operators use this information to make route adjustments to improve communications.

Change Frequencies

5-53. Commanders may direct units to change to an alternate frequency to overcome threat jamming. If a prescribed frequency change does not occur smoothly, the threat may discover what is happening, and try to disrupt or degrade communications on the new frequency. All radio operators require knowledge of when they are to switch to an alternate frequency. Procedures that describe the conditions and plans to change frequencies are included in the operation order, signal operating instructions, or standard operating procedures.

5-54. Through CEMA, units have an opportunity to develop deception plans before changing frequencies. Preplanned and well-coordinated actions are required for dummy stations to continue to operate on the jammed frequency to mask the change to an alternate frequency.

REPORTING JAMMING

5-55. Units report suspected jamming and any unidentified or unintentional electromagnetic interference that disrupts the ability of U.S. forces to communicate. Units report suspected jamming or interference, even if the radio operator can overcome the effects of the jamming or interference. Units use the information in the JSIR report to locate, mitigate, or destroy the threat jamming equipment or take other action to benefit U.S. forces.

> ***Note.*** Army units use the JSIR format to describe and report electromagnetic interference for intentional and unintentional interference to friendly communications. Refer to CJCSM 3320.02E for additional information regarding the JSIR Program.

REMEDIAL ELECTROMAGNETIC PROTECTION TECHNIQUES

5-56. Remedial electromagnetic protection techniques that help reduce the effectiveness of threat jamming efforts are—

- Identification of threat jamming signals.
- Determination of the electromagnetic interference as being obvious or subtle jamming.
- Recognition of jamming causing electromagnetic interference by—
  - Determining if the electromagnetic interference is internal or external to the radio.
  - Determining if the electromagnetic interference is deliberate or unintentional.
- Reporting jamming and other electromagnetic interference incidents.
- Overcoming jamming and electromagnetic interference by adhering to the following techniques—
  - Continue to operate.
  - Diagnose the root cause of electromagnetic interference.
  - Improve the signal-to-jamming ratio.
  - Adjust the receiver settings.
  - Increase the transmitter power output.
  - Adjust or change the antenna.

- Establish a retransmission station.
- Relocate the antenna.
- Use an alternate route for communications.
- Change the frequencies.
- Acquire another satellite or retransmission station.
- Install firmware and software updates.
- Use enhancements to tactical radio ancillary equipment and communications security devices.

THREAT ELECTROMAGNETIC ATTACK ON FRIENDLY COMMUNICATIONS NODES

5-57. Threats may attack or exploit friendly communications nodes that support operations. They have developed equipment and techniques to contest friendly spectrum use. Friendly units use electromagnetic protection measures to counter threat EW and exploitation actions against friendly communications nodes and links.

5-58. Threat attacks on friendly communications nodes can disrupt or destroy information, intelligence gathering efforts, and communications that support weapons systems. Threat forces expend considerable resources gathering intelligence about U.S. forces. Goals or effects may include—

- Jam friendly communications.
- Enter friendly radio networks.
- Collect information and intelligence about friendly forces.

EQUIPMENT AND COMMUNICATIONS ENHANCEMENTS

5-59. Some communications equipment has embedded capabilities to prevent jamming, location, or listening by threat forces. Operators use these embedded capabilities when supporting operations.

FREQUENCY HOPPING MODE

5-60. Frequency hopping helps mitigate the effects of threat jamming, and in keeping friendly location data from threat forces. Some peer threats with advanced EW equipment can jam radios that use frequency hopping techniques. Single-channel transmissions are vulnerable to jamming by unsophisticated transmitters, so units use frequency hopping mode but remain vulnerable to threat direction finding and electromagnetic attack efforts.

ADAPTIVE ANTENNA TECHNIQUES

5-61. Adaptive antenna techniques result in more survivable communications. These techniques typically link with spread spectrum waveforms to combine frequency hopping with pseudo-noise coding. Pseudo-noise coding is a technique to make spread spectrum waveforms and frequency hopping mode appear to be background RF noise to an unintended receiver. Spread spectrum is a form of wireless communication in which the frequency of the transmitted signal varies deliberately and uses more bandwidth than the signal would normally, making it less susceptible to interference.

FREQUENCY HOP MULTIPLEXER

5-62. The frequency hop multiplexer and vehicular whip antennas enhance very high frequency (VHF) communications. The frequency hop multiplexer is an antenna multiplexer used with a single-channel ground and an airborne radio system in stationary and mobile operations. The frequency hop multiplexer allows multiple radios to transmit and receive through one VHF antenna while operating in the frequency hopping mode, single-channel mode, or both. Using one antenna reduces the visual and electromagnetic profiles of command posts and reduces emplacement and displacement times.

Chapter 6

Electromagnetic Support Techniques

This chapter describes electromagnetic support planning and execution techniques to include synchronizing signals intelligence resources that complement electromagnetic support activities. This chapter outlines lines of bearing, cuts, fixes, establishing a direction-finding baseline, and what causes direction-finding errors.

PLANNING ELECTROMAGNETIC SUPPORT

6-1. Threat forces use the electromagnetic spectrum to give orders, monitor and manage operations, detect aircraft using radar, and conduct direction finding. Collection against and location of threat transmitters aids in the development of situational understanding and assists with targeting. Electromagnetic support uses direction-finding techniques to find threat transmitters. Once located, the commander can direct lethal or nonlethal fires.

ELECTROMAGNETIC SUPPORT CONSIDERATIONS

6-2. The task and purpose of the mission determine whether a SIGINT or EW asset is appropriate for a given mission. Electromagnetic support assets conduct immediate threat recognition, targeting, future operations planning, and other tactical actions such as threat geolocation for avoidance.

6-3. When the threat employs electromagnetic security measures, the CEWO may require assistance from SIGINT elements to understand the nature of the emissions. *Electromagnetic security* is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of noncommunications electromagnetic radiations (e.g., radar) (JP 3-85).

PREPARING ELECTROMAGNETIC SUPPORT

6-4. The CEMA section uses electromagnetic support assets to scan the electromagnetic environment for transmissions and illustrates the results in a manner that the commander and staff can understand. Units develop an electromagnetic environment survey using airborne, ground, and maritime platforms. The G-2 or S-2 assists the CEMA section by developing and disseminating the electromagnetic order of battle (refer to FM 2-0). EW platoons conduct the electromagnetic environment survey. The electromagnetic environment survey aids the CEWO in understanding friendly, threat, and neutral spectrum use; the nature, limitations, and sources of electromagnetic interference in an operational environment; and planning the employment of electromagnetic support equipment. The CEMA section submits requests for information to address information gaps to the G-2 or S-2 staff.

ELECTROMAGNETIC ENVIRONMENT SURVEY

6-5. The electromagnetic environment survey provides input, and the CEMA section enters the information into automated tools to maintain a current picture of the electromagnetic environment. Like weather reports for aircraft pilots, the electromagnetic environment survey informs the CEWO about the activities and conditions of the electromagnetic environment, enabling the CEWO to choose optimal courses of action for EW.

6-6. Electromagnetic environment surveys begin with the enemy electromagnetic order of battle. The electromagnetic order of battle provides the CEWO with an initial overview of threat spectrum-dependent capabilities derived from intelligence preparation of the battlefield. The electromagnetic order of battle assists the CEWO in making EW plans that exploit adversary vulnerabilities while preserving friendly capabilities.

EXECUTING ELECTROMAGNETIC SUPPORT

6-7. Electromagnetic support gathers information about friendly and threat electromagnetic emissions to support the commander's situational awareness and decision making. Understanding friendly electromagnetic signatures and threat capabilities and locations helps commanders plan electromagnetic protection and EMCON measures to protect friendly personnel and systems. The information gathered through electromagnetic support enables threat recognition and supports current operations, targeting, protection, and future operations planning. Some information gathered during electromagnetic support may simultaneously feed into intelligence channels for further processing into intelligence products.

6-8. Comparing detected electromagnetic signatures with the electromagnetic order of battle can assist in determining whether SIGINT activities have already characterized the signal. This information informs development of protection plans. EW personnel should refer unknown or uncharacterized signatures to the G-2 or S-2 for analysis.

6-9. The CEWO and the G-2 or S-2 mutually develop standard operating procedures and battle drills to integrate and synchronize electromagnetic support and SIGINT activities. Integration techniques take advantage of similar equipment capabilities and synchronize EW and SIGINT resources to increase flexibility. SIGINT teams pass targeting information to EW teams. The SIGINT direction-finding equipment complements geolocation efforts and transitions a line of bearing into a cut or a fix for targeting. Integration facilitates immediate sharing of information and reduces delays in targeting.

ELECTROMAGNETIC RECONNAISSANCE

6-10. *Electromagnetic reconnaissance* is the detection, location, identification, and evaluation of foreign electromagnetic radiations (JP 3-85). EW personnel conduct electromagnetic reconnaissance to understand the types of threat emissions. The information obtained from electromagnetic reconnaissance helps shape the operational environment by providing the commander with situational awareness to support decision-making. Information from electromagnetic reconnaissance can lead to the implementation or modification of electromagnetic protection measures or dictate electromagnetic attack actions.

THREAT WARNING

6-11. Threat warning enables the commander and staff to quickly identify immediate risks to friendly forces and implement appropriate countermeasures. EW personnel employ sensors to detect, intercept, identify, and locate threat electromagnetic signatures and provide early warning of imminent or potential hostile activities. EW personnel coordinate with the G-2 or S-2 before nominating a detected emitter for targeting. Commanders may need to accept risk, balancing the value of continued SIGINT collection on a target emitter versus the tactical utility of eliminating the threat capability. Threat warning contributes to intelligence preparation of the battlefield and helps characterize threat communications and noncommunications emitters.

DIRECTION FINDING

6-12. Direction-finding activities provide lines of bearing, cuts, and fixes to locate transmitters. When EW teams conduct direction finding, they use available electromagnetic support assets. The CEMA section coordinates support from the G-2 or S-2 for SIGINT resources to sense transmitters, collect information, and geolocate specified emitters of interest. The CEMA section shares the information collected from electromagnetic support assets during direction-finding activities with the G-2 or S-2 to aid in ongoing intelligence preparation of the battlefield. In addition, the CEMA section can provide direction-finding information to the targeting board to aid in targeting requirements.

Line of Bearing

6-13. A line of bearing is a single approximate azimuth from a sensor providing the approximate direction to the transmitter. Figure 6-1 illustrates a line of bearing approximate direction.

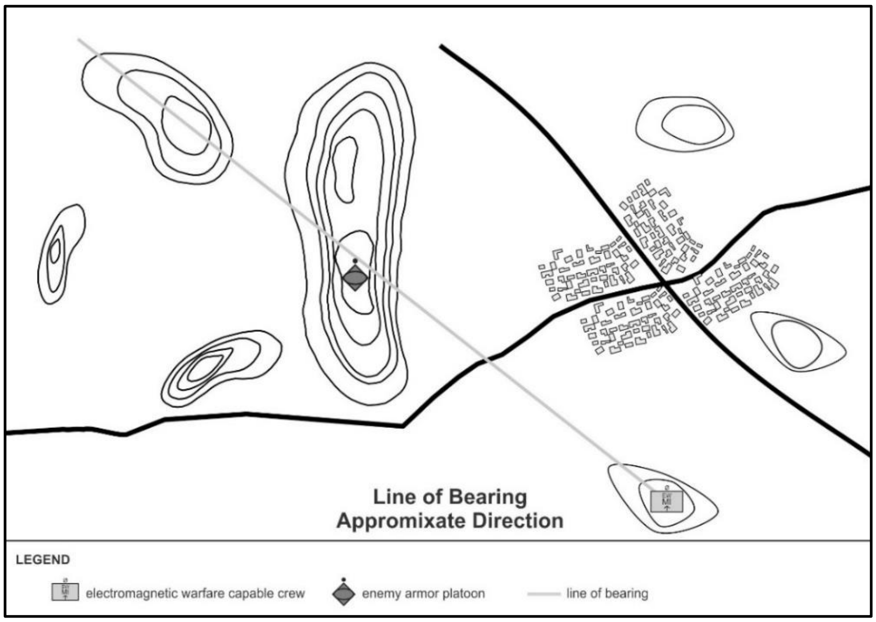


Figure 6-1. Example of a line of bearing approximate direction

Cut

6-14. A cut uses two approximate lines of bearing to calculate the general location of a transmitter by determining where two lines of bearing intersect. Figure 6-2 illustrates a cut general location.

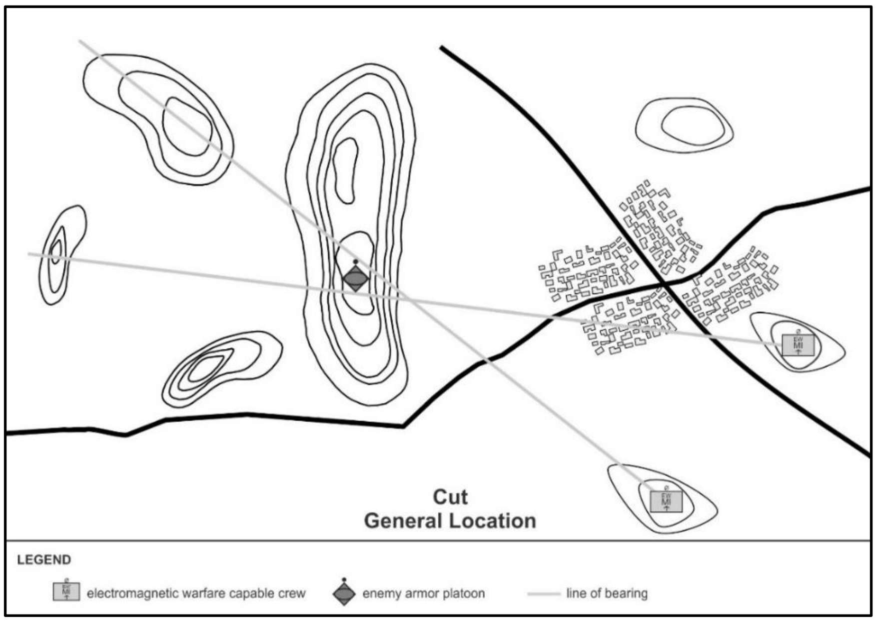


Figure 6-2. Example of a cut general location

Fix

6-15. Figure 6-3 illustrates a fix, which provides a more precise location. A fix uses three or more approximate lines of bearing to determine a location by triangulation. A cut or fix may use approximate azimuths from one sensor receiving the signal multiple times from different locations, or from different sensors.

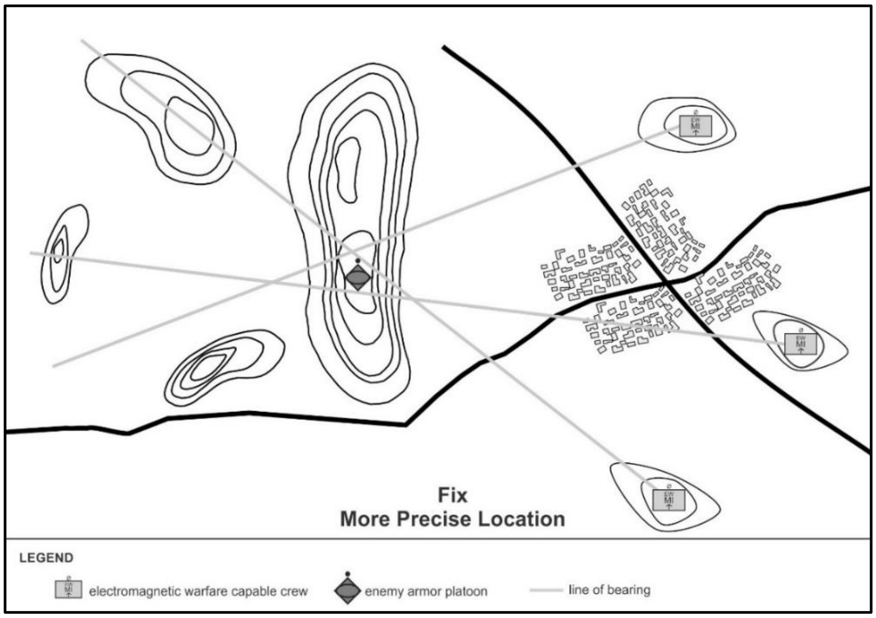


Figure 6-3. Example of a fix more precise location

Direction-Finding Baselines

6-16. A ground-based direction-finding baseline is that imaginary line or axis along which the direction-finding equipment of a direction-finding network deploy. A direction-finding network consists of three or more individual sites. The establishment of a direction-finding baseline is a matter of positioning the equipment so that good bearing angles for triangulation within the target area are possible. Triangulation is the intersection of bearings at the target area.

6-17. EW personnel ensure that each direction-finding site has an unobstructed path between the direction-finding antenna and any point in the target area. Often, the tactical situation precludes a clear path. EW personnel plan tactical direction-finding baselines to ensure masked or hidden portions of the target area are still visible to at least three sites. There are two types of baseline configurations used to establish a ground-based direction-finding network—concave and convex.

Concave Baseline

6-18. Direction-finding networks use concave baselines when the expected target location will be in a compact, narrow but deep frontal area. Concave baselines offer satisfactory bearings at longer ranges, and excellent triangulation at short ranges. Figure 6-4 illustrates a concave baseline.

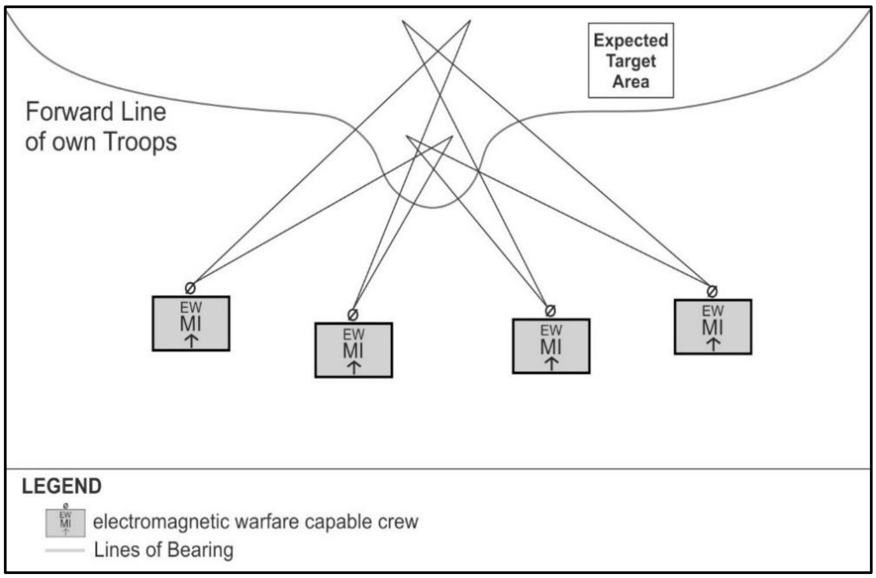


Figure 6-4. Concave baseline

Convex Baselines

6-19. Convex direction-finding baselines provide reasonable azimuth angles over a wide front. Convex baselines will satisfy the average tactical or strategic situation. Figure 6-5 on page 6-8 illustrates a convex baseline.

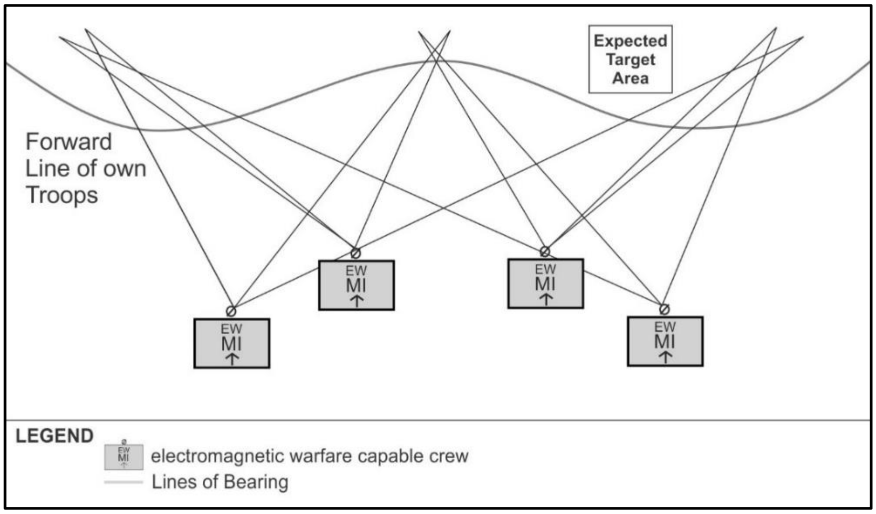


Figure 6-5. Convex baseline

Baseline Distance

6-20. The baseline distance is a straight-line distance that separates the two outermost direction-finding sites. As a rule of thumb, the depth at which a direction-finding network can effectively locate enemy transmitters is equal to the total distance of the baseline joining the two outermost direction-finding sites. This distance extends from the center of the imaginary baseline to the target area. For example, if the direction-finding baseline is 80 kilometers in length, the net fix location capability is 80 kilometers in depth.

6-21. Establishing a tactical direction-finding baseline is dependent on the mission variables of METT-TC (I). Tactical commanders determine areas available for siting direction finding equipment within their area of operations. The CEWO dictates the baseline configuration employed in most situations. Figure 6-6 on page 6-9 illustrates baseline distance.

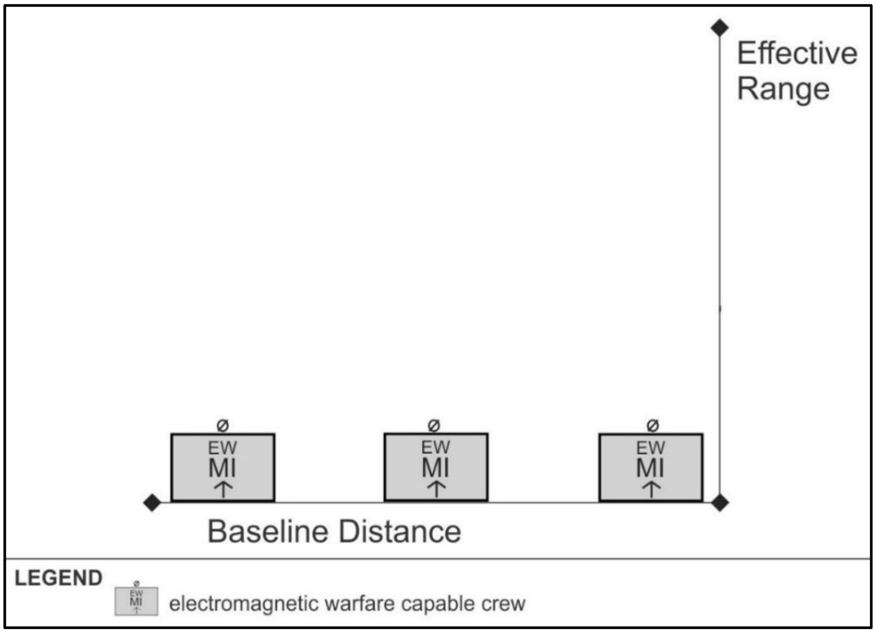


Figure 6-6. Baseline distance

Probabilities and Errors

6-22. The reception of a line of bearing on a target signal by a direction-finding receiver does not always determine the exact azimuth to the transmitter. Because of weather and terrain effects on radio signals, the angle of the target signal varies upon arrival.

6-23. For direction-finding missions, the further the receiver is from the transmitter, the greater the error associated with the intercept angle. When the CEWO plots lines of bearing of three or more receiving stations on a map, there is a triangular area of overlap where the lines of bearing intersect to form a fix. A circle drawn with a radius that covers all the points of the triangle represents the location of the transmitter. The circle is the circular error probability. Because there is circular error probability, the precise location of the transmitter cannot be certain. Figure 6-7 on page 6-10 illustrates circle error probability.

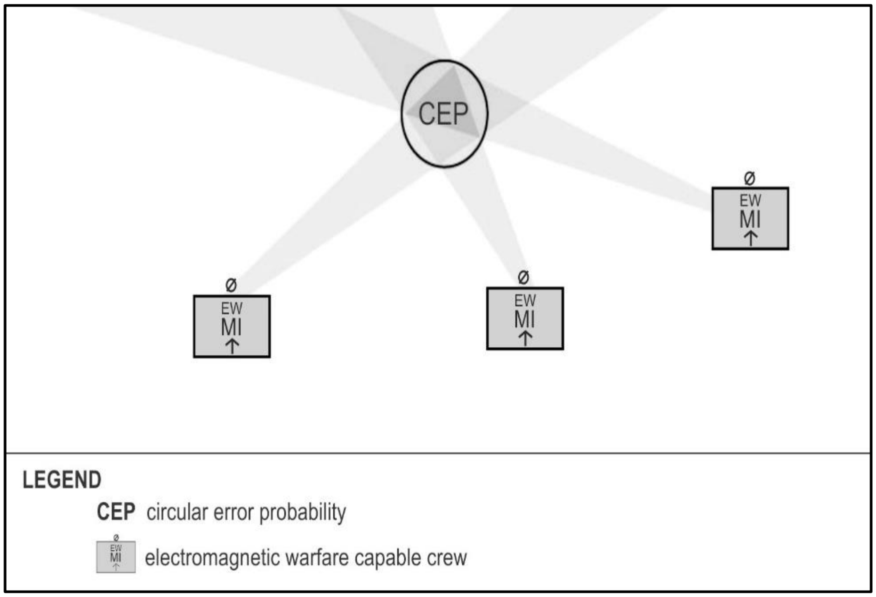


Figure 6-7. Circular error probability

6-24. The EW platoon leader minimizes the circular error probability of a fix by using multiple lines of bearing of the same signal and plotting the angles to determine a more precise location. The more lines of bearing used to obtain a fix, the smaller the circular error probability.

ERRORS AFFECTING INTERCEPT ANGLES

6-25. When conducting direction-finding activities, the EW platoon may encounter various signal errors that affect intercept angles. Understanding that these signal errors exist and being able to identify certain characteristics may minimize how much the signals are affected. The signal errors that should be considered are—

- Source error.
- Path error.
- Polarization error.
- Site error.
- Instrument error.

Source Error

6-26. A source error is a disruption of radio waves introduced near the targeted transmitter. The type of directional antenna used or the terrain conditions at the antenna site may cause this type of error. If the direction-finding equipment is farther than 15 kilometers from the transmitting antenna, the size of the source error is usually small. If the direction finding equipment is closer than 15 kilometers, the source error causes an inaccurate line of bearing.

Path Error

6-27. Deviations in frequency and phase between the transmitter and direction-finding system are path error. Important sources of path error include—

- Scatter.
- Refraction.
- Reflection.
- Reradiation.

Scatter

6-28. A small portion of the radio wave entering the ionosphere is scattered instead of bending and returning to the Earth's surface. A scattered wave projects in any direction, returning to the Earth at random angles. The scatter phenomenon accounts for signals sporadically received in skip zone regions. An error caused by scattering has a greater impact on strategic direction-finding sites. An error caused by scatter has little impact on tactical direction finding sites.

Refraction

6-29. Refraction occurs when waves bend or refract from their normal path as they pass from one medium to another. For example, the velocity of a radio wave over salt water is greater than its velocity over land or fresh water. Figure 6-8 on page 6-12 illustrates the false azimuth that results from the change in a radio wave's direction when it crosses a coastline at an oblique angle. Refraction error is evident when either a direction-finding site or the transmitting antenna is near the coast. This effect also varies with the transmission frequency.

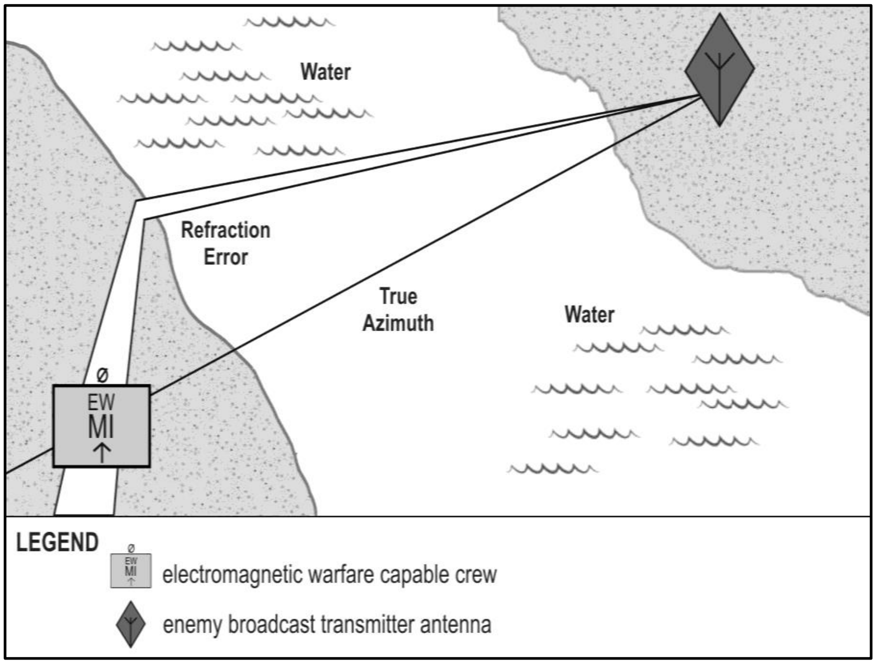


Figure 6-8. False azimuth indicated by refraction error

Reflection

6-30. Reflection occurs when radio waves strike and reflect off an artificial or natural surface. Figure 6-9 on page 6-13 illustrates the reflection of a radio wave. The degree of reflection is not measurable, as it depends upon the obstruction and the frequency of the transmitted wave. Generally, direction-finding errors are greatest from reflection when the reflecting media are located near either the transmitter or the direction-finding equipment. Reflection error affects both strategic and tactical direction-finding systems.

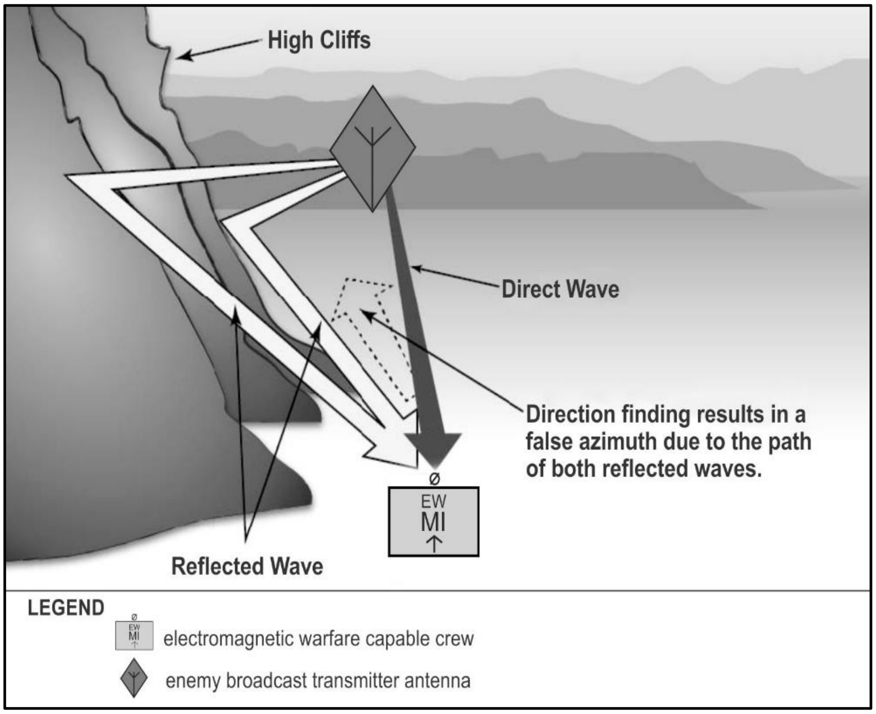


Figure 6-9. Reflection of a radio wave

Reradiation

6-31. Reradiation occurs when a wave strikes a metallic object that resonates at the wave's frequency. Abnormally polarized, reradiated signals make it difficult for direction-finding equipment to determine accurate lines of bearing. Reradiation error occurs near the direction-finding site. Barbed wire, trucks, tanks, other combat vehicles, and metal buildings can cause a reradiation error. It is essential to consider obstacles when selecting direction-finding sites.

Polarization Error

6-32. Polarization error occurs when a direction-finding antenna receives an undesired voltage induced by a component of a radio wave. This undesired voltage blurs the bearing and makes an azimuth reading difficult to determine. For example, a direction-finding antenna, such as a vertical loop, receives vertically polarized radio waves. If the received wave is abnormally polarized, the voltage induced by the two components may combine. The azimuth reading on the signal is difficult, if not impossible, to determine. The polarization error effect depends on the direction-finding antenna's ability to discriminate between the vertically polarized wave and the horizontally polarized wave of the received signal. Polarization error is common in most direction-finding activities. For more information about polarization error, see appendix A.

Site Error

6-33. Site error occurs in the immediate vicinity of the direction-finding site. The proper orientation of the antenna is critical to accurate direction finding; therefore, at each new location, the operator orients the antenna to a known reference point, such as true north. Adapting the antenna reference point produces an accurate measurement of the arrival angle of the wavefront. Obstructions near direction-finding sites contribute to site error. The closer the obstruction is to the direction-finding site, the greater its adverse effect on the accuracy of the site's lines of bearing.

Instrument Error

6-34. Poor maintenance and improper calibration of direction-finding equipment can result in instrument error. Direction-finding equipment requires calibrations and adjustments at regular intervals. Maintenance, calibrations, and equipment adjustments improve direction-finding performance. These procedures are available in associated direction-finding equipment technical manuals.

Appendix A

The Electromagnetic Spectrum

Electromagnetic warfare professionals must understand radio wave propagation, the electromagnetic spectrum, and the electromagnetic environment to achieve desired effects. This appendix describes the fundamentals of the electromagnetic spectrum and radio wave propagation.

RADIO WAVE BANDS AND CHARACTERISTICS

A-1. Frequency is an essential consideration in radio wave propagation. Table A-1 shows the frequency ranges of each band.

Table A-1. Radio wave bands and frequencies

Radio Wave Band	*Frequency*	*Frequency in megahertz*
ELF	3–30 hertz	Only a small portion of the band is useful for communications.
VLF	3–300 kHz	Below .03 MHz
LF	30–300 kHz	.03–.3 MHz
MF	300 kilohertz–3 MHz	.3–3 MHz
HF	3–30 MHz	3–30 MHz
VHF	30–300 MHz	30–300 MHz
UHF	300 MHz –3 GHz	300–3,000 MHz
SHF	3–30 GHz	3,000–30,000 MHz
EHF	30–300 GHz	30,000–300,000 MHz

Legend:

EHF	extremely high frequency	MF	medium frequency
ELF	extremely low frequency	MHz	megahertz
GHz	gigahertz	SHF	super high frequency
HF	high frequency	UHF	ultrahigh frequency
kHz	kilohertz	VHF	very high frequency
LF	low frequency		

EXTREMELY LOW FREQUENCY

A-2. Generally, extremely low frequency waves occur accidentally or naturally. This frequency is the white noise and electrical hum encountered in almost all circuits, resulting from the interaction of solar wind and atmospheric charges. Extremely low frequency is effective for subsurface communications.

VERY LOW FREQUENCY

A-3. Very low frequency signals are compatible with the Earth-ionosphere waveguide and propagate over great distances with low attenuation and excellent stability. Earth-ionosphere waveguide is a phenomenon that allows some radio waves to propagate in the space between the ground and the boundary of the ionosphere. During magnetic storms, very low frequency signals may constitute the only source of radio communications over great distances. Operators do not use very low frequency for great distances over land because of the long wavelength and requirement for large antennas. Magnetic storms have little effect on these transmissions because of the efficiency of the Earth-ionosphere waveguide. However, interference from atmospheric noise may be troublesome. Applications include navigation, time signals, submarine communications, and certain aircraft.

LOW FREQUENCY

A-4. As frequency increases to the low frequency band and diffraction decreases, there is greater attenuation with distance, and the range for a given power output rapidly drops. Using more efficient antennas for transmitting offsets the drop in power and increases range. Low frequency signals are most stable within ground wave distance of the transmitter. A wider bandwidth permits pulsed signals at 100 kilohertz. The pulsed signals allow separation of the stable ground wave pulse from the variable skywave pulse up to 1,500 kilometers (932 miles), and up to 2,000 kilometers (1,243 miles) for overwater paths. Loran systems use the low frequency band, which is useful for radio direction finding.

MEDIUM FREQUENCY

A-5. Medium frequency ground waves provide dependable service, but long-distance communications require increased transmit power. This range varies from about 645 kilometers (400 miles) at the lower portion of the band to about 24 kilometers (15 miles) at the upper end for a transmitted signal of 1 kilowatt. Achievable distance depends on—

- Transmitter power level.
- Antenna efficiency.
- The nature of the terrain between the transmitting and receiving stations.

A-6. Elevating the antenna may allow transmission of direct waves. Direct wave propagation may improve the quality of the transmission. At the band’s lower frequencies, skywaves are available both day and night. As the frequency increases, ionospheric absorption increases to a maximum at about 1,400 kilohertz. At higher frequencies, the absorption decreases, permitting increased use of skywaves. Since the ionosphere changes with the hour, season, and sunspot cycle, the reliability of skywave signals is variable. By careful selection of frequency, ranges of as much as 12,875 kilometers (8,000 miles) with 1 kilowatt of transmitted power are possible, using multi-hop signals. However, the frequency selection is critical. If the frequency is too high, the signals penetrate the ionosphere and are lost in space; if it is too low, signals are too weak. In general, skywave reception is equally good by day or night. Lower frequencies are best for the night.

HIGH FREQUENCY

A-7. The ground wave range of HF signals is limited to about 5 kilometers (3 miles), but the antenna’s elevation may increase the direct wave distance of transmission. Additionally, the height of the antenna has a substantial effect on skywave transmissions. By day, this may be 10–30 megahertz; at night, it may drop to the 8–10 megahertz range. Army forces use HF radios for beyond line of sight communication.

VERY HIGH FREQUENCY

A-8. VHF communication uses the direct wave, or direct wave plus a ground reflected wave. Although some wave interference between direct and ground-reflected waves is present, elevating the antenna to increase the distance at which direct waves can be used results in increased reception distances. Diffraction in the VHF range is much less than with lower frequencies, but most evident when signals cross sharp mountain peaks or ridges. Under suitable conditions, ionospheric reflections are sufficiently strong to be useful, but generally, they are unavailable. There is little interference from atmospheric noise in this band. Reasonably efficient directional antennas are possible with VHF. Uses include terrestrial line of sight, ground-to-air, air-to-air, land, and maritime-mobile communications. Most tactical radios operate over VHF range.

ULTRAHIGH FREQUENCY

A-9. Skywaves are absent in the ultrahigh frequency band since the ionosphere lacks enough density to refract the waves, which instead pass through the ionosphere into space. Ground waves and ground-reflected waves are usable, although there is some wave interference. Diffraction is negligible, but the radio horizon extends about 15 percent beyond the visible horizon, due to refraction. Reception of ultrahigh frequency (UHF) signals is virtually free from fading and interference by atmospheric noise. This band is widely used for ship-to-ship and ship-to-shore communication. Army forces use UHF for narrowband (single-channel) tactical satellite, some radars, and terrestrial-line of sight communication.

SUPER HIGH FREQUENCY

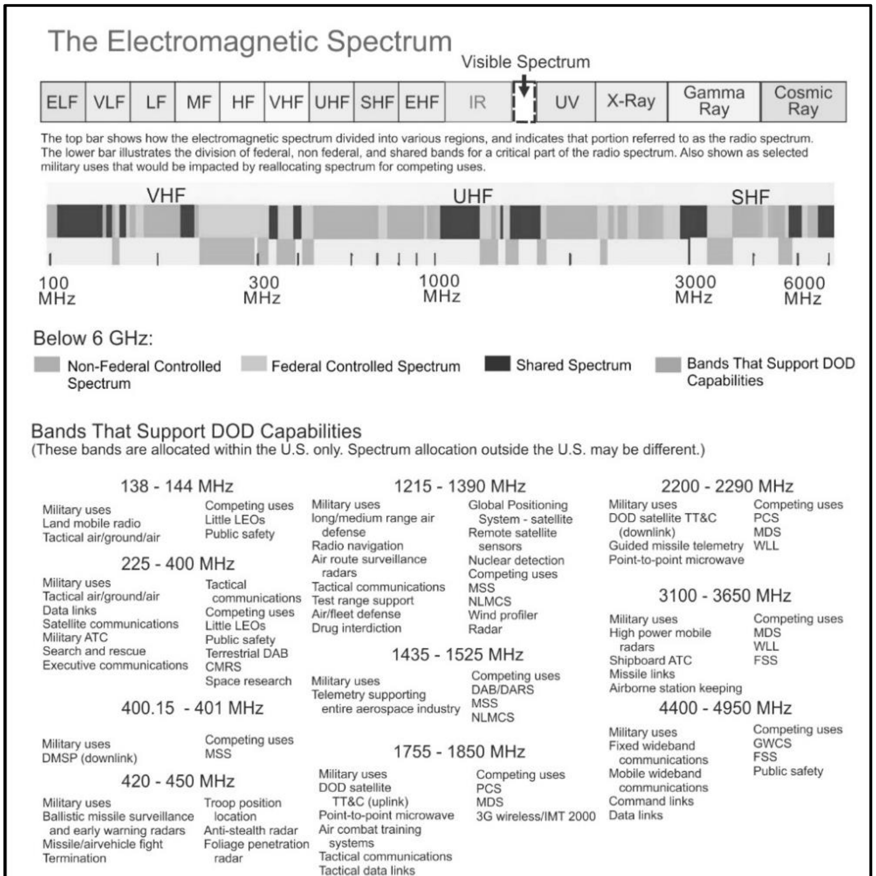
A-10. In the super high frequency band, also known as the microwave or centimeter-wave band, skywaves are absent. Transmission is entirely by direct and ground-reflected waves. Diffraction and interference due to atmospheric noise are virtually nonexistent. Transmission in the super-high frequency band is similar to that of ultrahigh frequency, but the effects of using shorter waves is greater. Reflection by clouds, water droplets, and dust particles increases, causing greater scattering, increasing wave interference and fading. The super-high frequency range is used for terrestrial-line of sight radios, radar, and wideband satellite communications.

EXTREMELY HIGH FREQUENCY

A-11. Extremely high frequency is the highest radio frequency range. Compared to terrestrial radio signals in lower ranges, extremely high frequency is even more prone to atmospheric attenuation than super high frequency. Protected satellite communications use extremely high frequency.

REGULATION OF FREQUENCY USE

A-12. While the characteristics of various frequencies are important to the selection of the most suitable one for any given purpose, there are additional considerations. Confusion and extensive interference would result if every user had complete freedom of selection. The allocation of various frequency bands to particular uses is a matter of international agreement. Within the United States, the Federal Communications Commission authorizes the use of specific frequencies. Figure A-1 on page A-5 displays the frequencies supporting DOD capabilities, federally controlled frequencies, and shared spectrum.



LEGEND

ATC	air traffic control	LF	low frequency
CMRS	commercial mobile radio service	MDS	multipoint distribution system
DAB	digital audio broadcast - terrestrial	MF	medium frequency
DARS	digital audio radio service - satellite	MHz	megahertz
DOD	Department of Defense	MSS	mobile satellite service
DMSP	Defense Meteorological Satellite Program	NLMCS	new land mobile communications service
EHF	extremely high frequency	PCS	personal communications service
ELF	extremely low frequency	SHF	super high frequency
FSS	fixed satellite service	TT&C	telemetry, tracking and commanding
GHz	gigahertz	UHF	ultrahigh frequency
GWCS	general wireless communications service	UV	ultraviolent
HF	high frequency	VHF	very high frequency
IMT 2000	third generation mobile telephony	VLF	very low frequency
IR	infrared	WLL	wireless local loop
Little LEO	low earth orbit		

Figure A-1. Department of Defense use of the electromagnetic spectrum

EARTH'S ATMOSPHERE

A-13. The Earth's atmosphere encompasses numerous layers, three of which are key to this discussion: the troposphere, the stratosphere, and the ionosphere. The troposphere and ionosphere play a crucial role in long-range radio communications. Table A-2 summarizes the characteristics and features of the three layers.

Table A-2. Atmospheric layers, elevation, characteristics, and their effects on radio waves

Atmospheric Layer	*Elevation in Kilometers(km) and Miles (mi)*	*Characteristics*	*Effects on Radio Frequencies*
Ionosphere	50–600 km 31–373 mi	Electrically charged set of layers with large amounts of free electrons.	• Excellent refraction of medium frequency and high frequency signals. • Primary medium for skywaves.
Stratosphere	15–50 km 9–31 mi	The only isothermal region of the atmosphere.	No effect.
Troposphere	10–15 km 6–9 mi	• Sustains life. • Lowest region of the atmosphere. • Temperatures decreases with increasing altitude.	• Primarily acts to absorb radio waves. • Small amounts of refraction possible, but unpredictable.
Legend: km kilometers mi miles			

TROPOSPHERE

A-14. The troposphere is that portion of the Earth's atmosphere extending from the surface of the Earth to an elevation of approximately 10–15 kilometers (6–9 miles). This region of the atmosphere greatly influences electromagnetic emissions—a direct result of the ever-changing conditions, such as temperature and moisture content, within this layer. This region is where most weather activities occur; it also contains the mixture of life-sustaining gases.

STRATOSPHERE

A-15. The stratosphere is located between the troposphere and the ionosphere about 15–50 kilometers (9–31 miles) above the Earth's surface. The stratosphere and the isothermal region are synonymous. The isothermal region, by definition, maintains a nearly constant temperature. The stratosphere has little, if any, effect on radio waves, which travel through this layer to reach the ionosphere.

IONOSPHERE

A-16. The ionosphere is a region of numerous positive and negative ions and unattached electrons. The extent of ionization depends upon the kinds of atoms present, the density of the atmosphere, the position relative to the Sun (time of day and season), solar flares, magnetic storms, and nuclear detonations, all impacting ionization. After sunset, ions and electrons recombine faster than they are separated, decreasing the ionization of the atmosphere. Table A-3 on page A-8 illustrates the differences in the three major regions of the Earth's atmosphere.

Table A-3. Ionospheric layers and effects on radio waves

Ionosphere Layer	*Elevation*	*Features*	*Effects on Radio Frequencies*
F	145–400 km 90–249 mi (F2: 145–200 km) (F2: 90–124 mi) (F1: 240–400 km) (F1: 149–249 mi)	• Very positively ionized with large amounts of free electrons. • During the day, separates into the F1 and F2 layers. • At night, F layer decreases in ionization and increases in altitude.	• Primary means of refracting medium frequency and high frequency signals in skywave propagation. • At night, slightly erratic behavior, but much greater communications distances.
E	100–200 km 62–124 mi	• Positively ionized with varying amounts of free electrons. • Condition changes with temperature, angle of the sun, magnetic fields, and time of day.	• Erratic behavior. • Sometimes refracts radio waves in the medium frequency, high frequency, and very high frequency bands.
D	50–100 km 31–62 mi	• Layer closest to the Earth. • Negatively ionized with relatively little free electrons. • Exists only during the day.	• Primarily acts to absorb HF radio waves. • Layer may refract low frequency and very low frequency, but unpredictable.
Legend: HF high frequency km kilometers mi Miles			

A-17. In the ionosphere, air density is so low that oxygen exists mainly as separate atoms, rather than as combined oxygen molecules, as it does nearer to the Earth's surface. The F layer is where the energy level is low, and ionization from solar radiation is intense. Above this level, the ionization decreases because of the lack of atoms to be ionized. Below this level, it decreases because the ionizing agent of the appropriate energy is already absorbed. During daylight, two levels of maximum ionization are present—the F2 layer, at about 200 kilometers (125 miles) above the Earth's surface, and the F1 layer, at about 145 kilometers (90 miles). At night, these combine to form a single F layer. The D layer disappears at night due to low ionization. Figure A-2 on page A-9 illustrates the composition of the ionosphere during the day and then during the night.

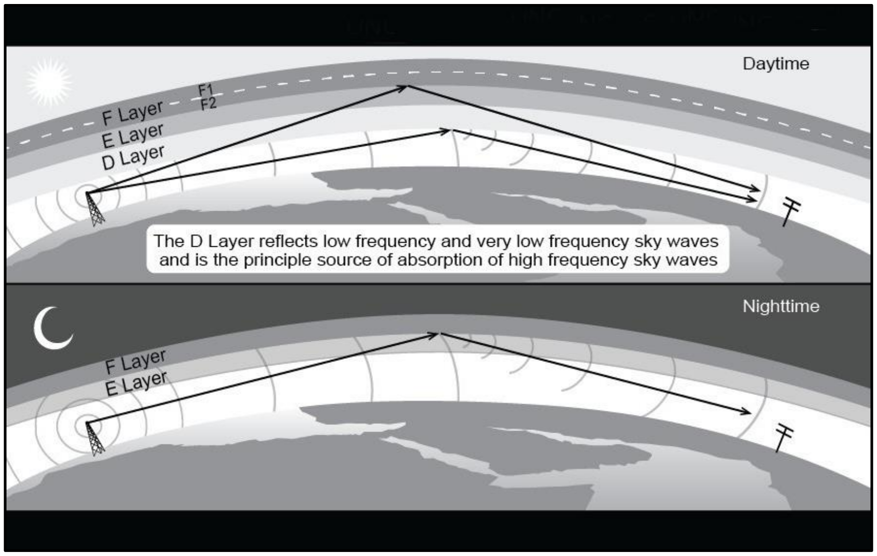


Figure A-2. The ionosphere—daytime and nighttime composition

A-18. The ion—a key characteristic of the atmosphere—affects radio waves. Since an atom normally has an equal number of negatively charged electrons and positively charged protons, it is electrically neutral. An ion is an atom or a group of atoms that become electrically charged, either positively or negatively, by the loss or gain of one or more electrons.

A-19. Loss of electrons may occur in a variety of ways. In the atmosphere, ions form due to the collision of atoms with rapidly moving particles, or due to the effects of cosmic rays or ultraviolet light. In the lower atmosphere, recombination soon occurs, leaving a small percentage of ions. However, in the thin atmosphere far above the Earth's surface atoms are widely separated, and many ions may be present.

BANDS OF THE ELECTROMAGNETIC SPECTRUM

A-20. The electromagnetic spectrum encompasses the entire range of electromagnetic radiation frequencies. The frequency range suitable for radio transmission extends from 10 kilohertz–300,000 megahertz. This portion of the spectrum has several bands, as shown in figure A-3. Below the RF spectrum, and overlapping it, is the audio frequency band, extending from 20–20,000 hertz. Above the RF spectrum are infrared, the optical (visible) spectrum (light in its various colors), ultraviolet rays, x-rays, and gamma rays. Figure A-3 on page A-10 illustrates the electromagnetic spectrum and communication bands. Within the RF range, from 1–40 gigahertz (1,000–40,000 megahertz), between the ultrahigh frequency and extremely high frequency are additional bands, defined as—

- L band: 1–2 gigahertz—Global Positioning System, Inmarsat, and Iridium.
- S band: 2–4 gigahertz—some radar.

- C band: 4–8 gigahertz—terrestrial line of sight, some radar, and wideband satellite communications.
- X band: 8-12 gigahertz—terrestrial line of sight, some radar, and wideband satellite communications.
- Ku band: 12–18 gigahertz—wideband satellite communications; protected satellite communications uplink.
- K band: 18–27 gigahertz—short-range radar.
- Ka band: 27–40 gigahertz— protected satellite communications downlink; close-range targeting radar.

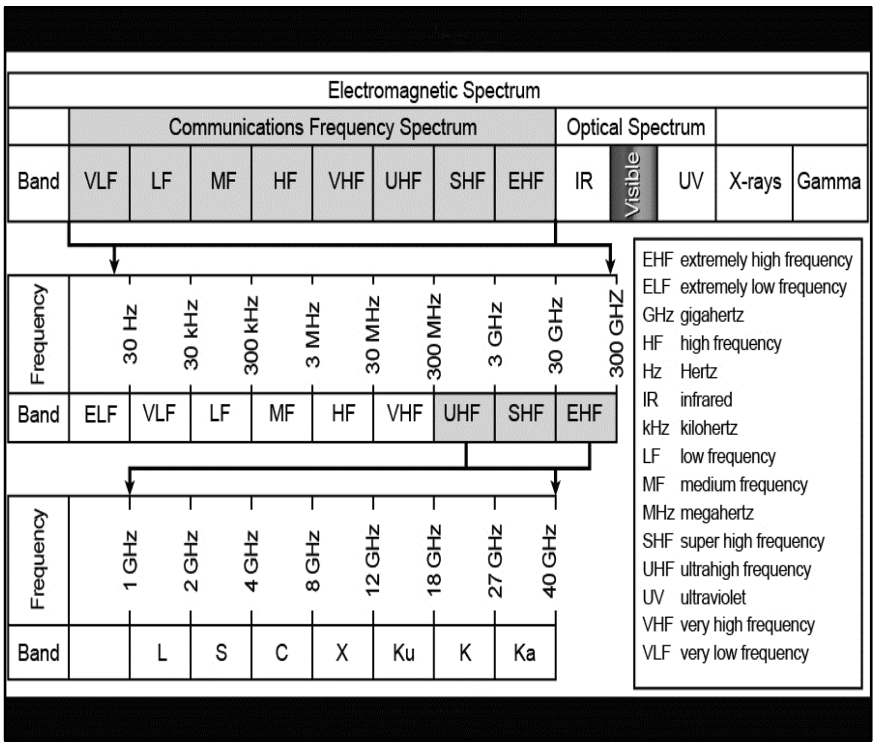


Figure A-3. The electromagnetic spectrum and communication bands

A-21. Modern communications systems use frequencies between extremely low frequency and extremely high frequency. Typical frequency ranges for modern communications include—

- Voice (push-to-talk) radios use HF through ultrahigh frequency range.
- Cordless telephones use VHF range.
- Television broadcast (Channels 2 through 13) uses VHF range.
- Frequency modulation (FM) radio broadcast uses VHF range.

- Television broadcast (Channels 14 through 69) use ultrahigh frequency range.
- Cellular phones use L and S bands.
- Satellite communications use C, X, Ku, and Ka bands between ultrahigh frequency and extremely high frequency ranges.

RADIO WAVES

A-22. Radio waves are one form of electromagnetic radiation. Radio waves form the foundation of radio communications. Applications for use include fixed and mobile radio communication, broadcasting, communications satellites, radar and radio navigation systems, and wireless computer networks.

RADIO WAVE TERMINOLOGY

A-23. Understanding radio wave theory requires understanding common terms. Radio wave terms include—

- Cycle.
- Frequency.
- Wavelength.
- Phase.
- Amplitude.
- Modulation.

Cycle

A-24. One cycle is a complete sequence of values, from wave crest to wave crest or from zero amplitude to zero amplitude. The distance traveled by the energy during one cycle is the wavelength, usually expressed in metric units (such as meters or centimeters).

Frequency

A-25. Frequency is the number of cycles per second expressed in hertz. The entire pattern of a wave, before repeating, is one cycle. One thousand hertz equals one kilohertz (kHz), 1 million hertz equals one megahertz (MHz), and 1 billion hertz equals one gigahertz (GHz). The radio frequency spectrum ranges from 3 kilohertz–300 gigahertz.

Wavelength

A-26. The wavelength is the distance a wave takes to complete one cycle. Wavelength also measures the distance from any one point of a wave to the same point on the next wave, such as crest to crest or trough to trough. Wavelengths are measured in metric units. The longer the wavelength, the better a wave reacts to propagation properties.

Phase

A-27. The phase of a wave is the amount the cycle progresses from a specified origin. For most purposes, phase is expressed in circular measure; 360 degrees is considered a complete cycle. Generally, the origin is not important, the principal interest being the phase relative to that of some other wave. Thus, two waves with crests one-quarter cycle apart are 90 degrees out of phase. If the crest of one wave (+) occurs at the trough (-) of another, the two are 180 degrees out of phase.

Amplitude

A-28. The amplitude of a wave is the distance measured from the centerline, or resting point, to the top of the crest or the bottom of the trough. The larger the amplitude the more energy a wave carries. Figure A-4 illustrates two cycles of a sine wave, depicting frequency, cycle, wavelength, and amplitude.

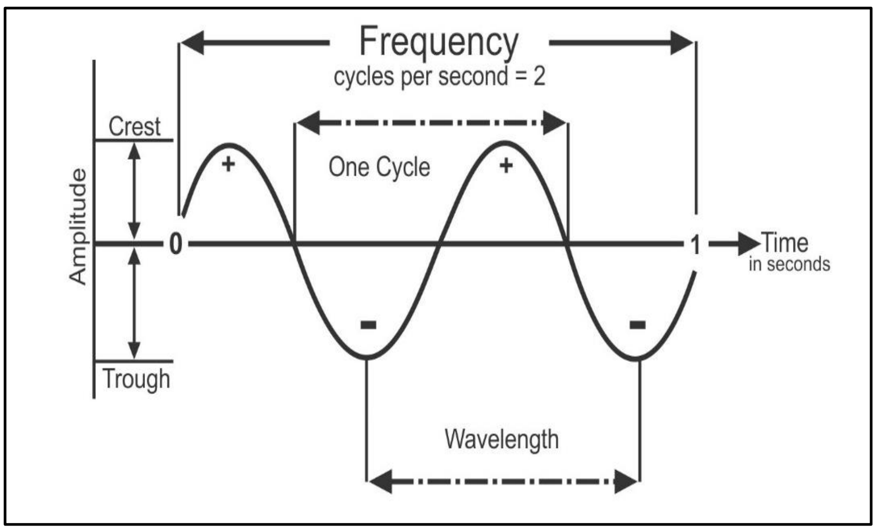


Figure A-4. Elements of a radio wave

Modulation

A-29. Modulation is a process that alters one or more properties of a waveform to convey information. Modulation techniques can be either analog or digital.

MODULATION TECHNIQUES

A-30. There is a variety of modulation techniques available for radio communication. Each of the techniques have some characteristics that make them useful in certain circumstances and in certain frequency ranges.

Continuous Wave

A-31. Continuous wave refers to a signal transmitted at a constant frequency and amplitude. Continuous waves are only audible at the extremely low and very low frequency ranges, when they may produce an audible high-pitched hum in a receiver. Applications for continuous wave include radio direction finding and Morse code communications. Any of several types of modulation may be used.

Amplitude Modulation

A-32. In amplitude modulation, the amplitude of the carrier wave alters according to the amplitude of a modulating wave, usually of audio frequency, as shown in figure A-5. The receiver demodulates the signal by removing the carrier wave and converting it to its original form. This form of modulation is widely used in voice radio, as in the standard broadcast band of commercial broadcasting.

Frequency Modulation

A-33. In frequency modulation, the frequency changes according to the frequency of the modulating signal, as shown in figure A-5. Tactical radios most commonly use frequency modulation.

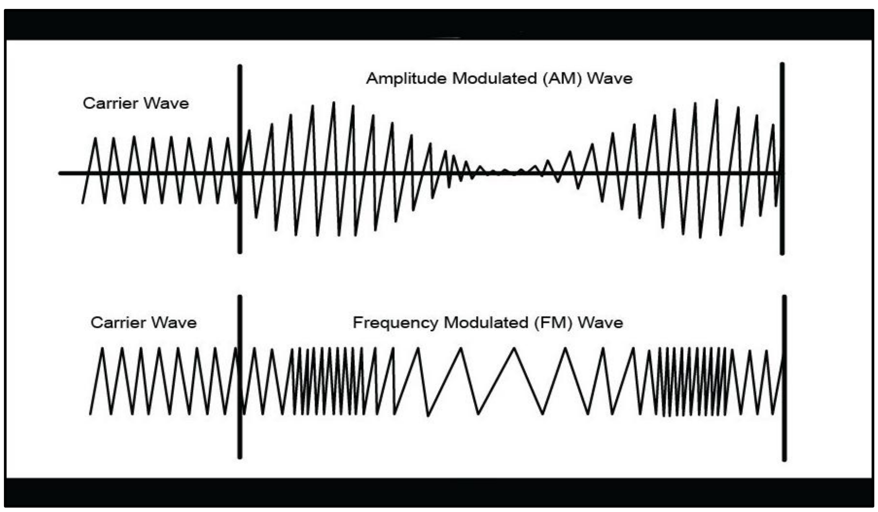


Figure A-5. Amplitude modulation and frequency modulation

Pulse Modulation

A-34. Pulse modulation is somewhat different from other forms. There is no impressed modulating wave. In this form of transmission, the transmitter uses short bursts of the carrier wave, separated by relatively long periods of silence, during which there is no transmission (see figure A-6 on page A-14). Some radio navigation aids use this transmission type including radar and radio navigation such as loran navigation.

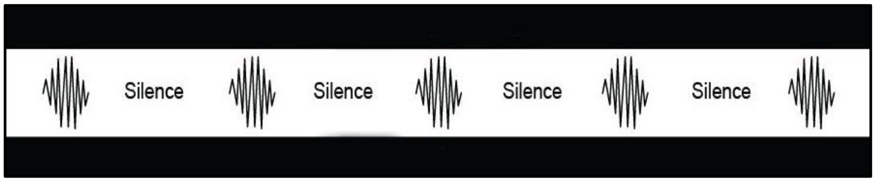


Figure A-6. Pulse modulation

Phase-Shift Keying

A-35. Phase shift keying modulates the analog carrier wave with a digital signal, where the phase of the carrier wave shifts between two or more values. There are multiple phase shift keying methods used in radio communications. The simplest method utilized is a bi-phase method (0 degrees and 180 degrees), where 0-degree phase equals a binary 0 and 180-degree phase equals a binary 1.

RADIO WAVE PROPAGATION

A-36. Radio waves travel through space at light speed—approximately 300,000,000 meters per second (186,000 miles per second). The following is a conversion formula for wavelength and frequency. If the frequency in hertz is known and a conversion to wavelength is desired, apply—

$$\text{Wavelength (meters)} = \frac{300{,}000{,}000}{\text{frequency (hertz)}}$$

A-37. If wavelength (in meters) is known and a conversion to frequency (hertz) is desired, apply—

$$\text{Frequency (hertz)} = \frac{300{,}000{,}000}{\text{wavelength (meters)}}$$

A-38. Radio wave propagation extends or transmits electromagnetic energy through space. Wavelength, frequency, and polarization are essential elements of the actual wave and affect radio wave propagation. The simplest form of propagation is through the space wave. The wave radiates from the transmitter and continues through space until it reaches the receiver. The Earth’s curved surface, while appearing to be flat over a short distance, limits the effective line of sight range.

A-39. Users determine the total limiting distance by assuming an Earth with a radius four-thirds its proper radius. Such an Earth would have a larger circumference and, hence, a longer distance to the horizon. Increasing the height of either the transmitting or the receiving antenna extends line of sight range, effectively extending the horizon. Given the height of two antennas (in feet), the line of sight distance can be calculated by

$$\text{LOS distance (miles)} = 1.41 \times \sqrt{\text{(height 1 [feet])}} + 1.41 \times \sqrt{\text{(height 2 [feet])}}$$

identifying the square root of the known height, multiplying the result by 1.41, and adding the sums together to obtain the line of sight distance in miles. The following formula can also be applied using kilometers and meters:

A-40. This line of sight distance formula does not include terrain or address free-space path loss, which involves the loss of signal strength along an unobstructed line of sight path (see paragraph A-72).

A-41. Figure A-7 gives an approximation of the line of sight transmission range without any mathematical calculations. Using a straightedge on the chart, aligned with the elevations of the transmitting and receiving antennas, allows a user to determine the transmission range.

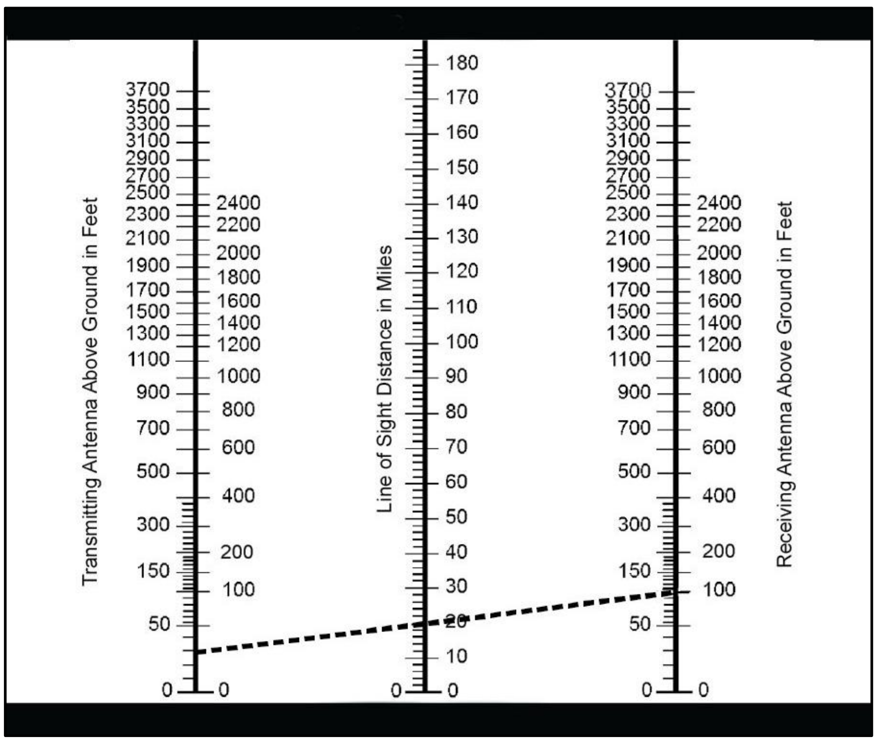


Figure A-7. Antenna heights and line of sight distances

A-42. Radio waves tend to travel in straight lines unless acted upon by some force. Radio waves tend to reflect off sharply defined objects. The higher the frequency, the greater the tendency of signals to reflect off objects. A refracted wave bounces off the ionosphere at the same angle at which it arrives, meaning the angle of incidence is equal to the angle of arrival. Radio waves can also encounter other obstructions or objects that will scatter, diffract, or reflect the signal. Substantial energy losses limit the distance of travel when the Earth reflects the waves. This energy is lost in the form of heat dissipated into the Earth’s crust. Factors that affect radio wave propagation include—

- Wavelength.
- Polarization.
- Physical obstructions.
- Space, land, air, and water.
- Weather.

POLARIZATION

A-43. Radio waves produce both an electric field and magnetic field, which are always perpendicular. The direction of the E field of a radio wave relative to the ground determines the polarization of the wave (see figure A-8). Polarization can be linear—vertical or horizontal—or nonlinear (circular or elliptical). Thus, if the component field is vertical, the wave is vertically polarized, and if horizontal, it is horizontally polarized.

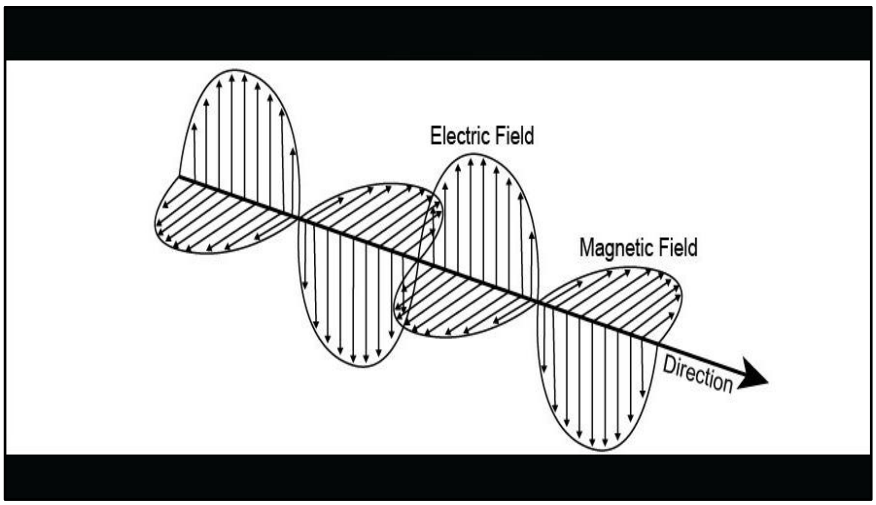


Figure A-8. Electric and magnetic fields of a radio wave

A-44. To illustrate vertical wave polarization, imagine a rope lying reasonably straight on the ground. If one raises and lowers the loose end of the rope with a violent up and down motion, a series of undulating waves will travel along the rope. The movement of the waves will be vertical to the ground, or vertically polarized. If the same rope had a similar movement applied horizontally, the waves would be in a horizontal plane, or horizontally polarized.

A-45. If one uses a whip or other vertically oriented transmitting antenna to propagate radio waves, the transmitted wave is vertically polarized. Vertically polarized waves travel along the surface of the Earth. The waves travel vertically because the Earth short-circuits any horizontal component. If the transmitting antenna is horizontal relative to the Earth's surface, the transmitted wave is horizontally polarized. Circular and elliptical polarization adopt characteristics of both vertical and horizontal polarization, resulting in a circularly polarized or hybrid waveform. Figure A-9 shows waves traveling in space polarized in any desired direction.

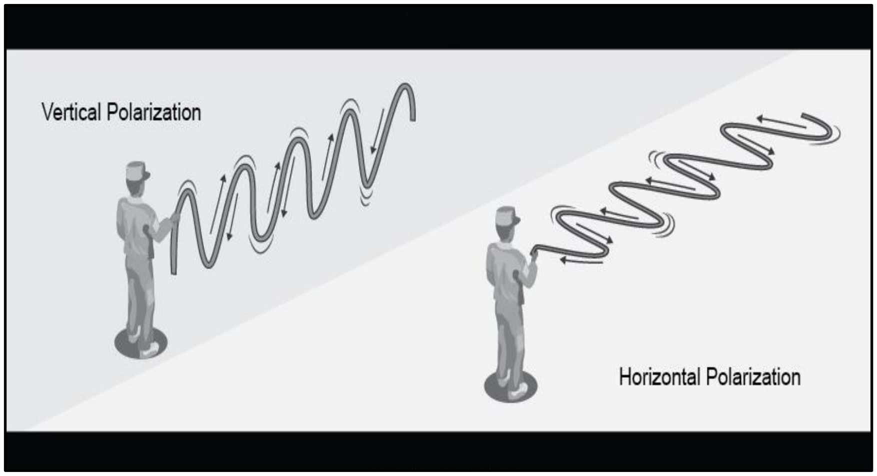


Figure A-9. Vertical and horizontal polarization

A-46. Some antennas also apply a circular polarization in which the E field rotates the RF signal circularly, either to the right or to left of the axis of propagation. Instead of transmitting in just one plane, a circularly polarized antenna transmits in both planes at once, with a 90-degree phase shift between the two planes. The signal, in this case, would look like a corkscrew as opposed to a wave. Circular polarization occurs in two variations—right-hand (clockwise) or left-hand (counterclockwise) circular polarization. Circular polarization reduces the probability of multipath interference. If the two plane waves have different amplitudes or the phase difference is other than 90 degrees, the polarization is elliptical (see figure A-10 on page A-18).

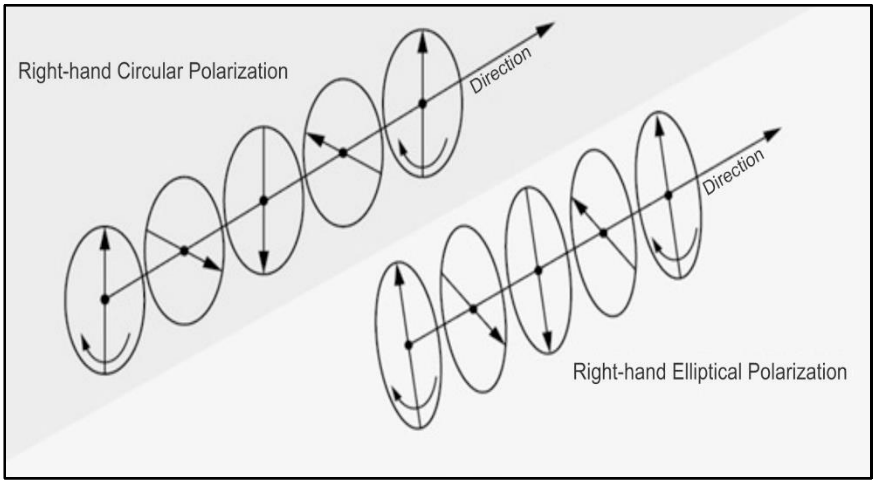


Figure A-10. Right-hand circular and elliptical polarization

A-47. Polarization is sometimes predictable based on an antenna's geometry. An antenna's linear polarization is generally along the direction (as viewed from the receiving location) of the antenna's currents. Antennas with horizontal elements, such as television broadcast, use horizontal polarization. Even when the antenna system is vertically orientated, such as an array of horizontal dipole antennas, the polarization is in the horizontal direction, corresponding to the current flow. It is best for a receiving antenna to match the polarization of the transmitted wave for optimum reception.

A-48. When a vertically polarized antenna tries to communicate with a horizontally polarized antenna (called cross-polarization), and vice versa, there can be as much as a 30-decibel loss in signal strength—a factor of 1,000. A horizontally aligned signal will not align with a vertically aligned antenna, so a considerable amount of the transmitted wave will simply bypass the receiving station.

REFLECTION

A-49. Reflection involves a change in the direction of waves when a wave bounces off a barrier. When radio waves strike a surface, the surface reflects them in the same manner as light waves. The Earth's surface reflects all radio waves. The strength of the reflected wave depends on the angle of incidence (the angle between the incident ray and the horizontal surface), type of polarization, frequency, reflecting properties of the surface, and divergence of the reflected ray. Lower frequencies penetrate the Earth's surface more than higher ones. At very low frequencies, radios receive signals below the surface of the sea. The wavefront of a radio wave is an expanding spherical surface, all the points of which are in the same phase. A phase change occurs when a wave reflects from the surface of the Earth. The amount of the change varies with the conductivity of the Earth (such as soil composition and moisture content) and the polarization of the wave, reaching a maximum of 180 degrees for a horizontally polarized wave reflected from seawater (considered to have infinite conductivity).

A-50. Figure A-11 shows a planar wavefront reflected from a smooth surface. As in the reflection of light, the angle of incidence equals the angle of reflection. However, the incident wavefront, A–A1, is reversed by the reflecting surface and appears at B–B1—180 degrees out of phase. The reversal in reflection occurs because point X of the incident wave reaches the reflecting surface before point Y and reflects to point X1 during the time it takes for point Y, on the wavefront, to move to the point of reflection, which is Y1.

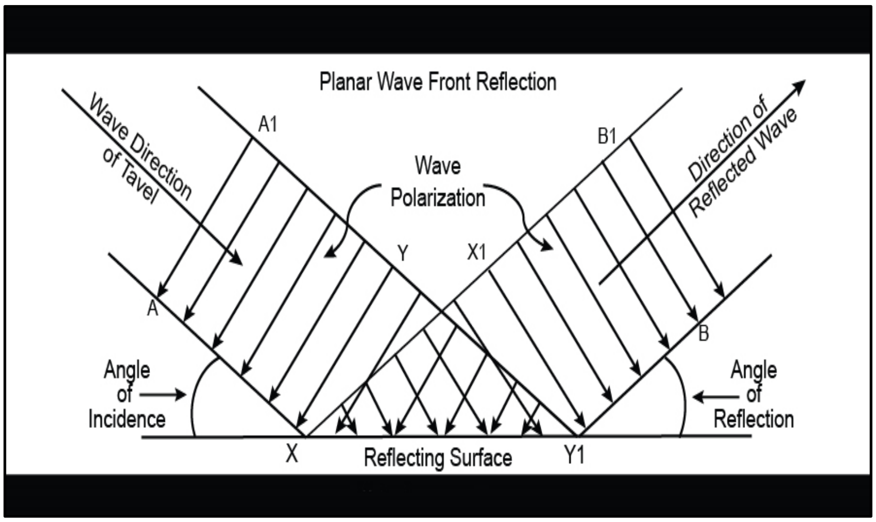


Figure A-11. Planar wavefront reflection

A-51. When a reflected wave and a direct wave arrive at a receiver, the total signal is the vector sum of the two. If the signals are in phase, they reinforce each other, producing a stronger signal. If there is a phase difference, the signals tend to cancel each other, the cancellation being complete if the phase difference is 180 degrees and the two signals have the same amplitude. This interaction of waves is wave interference.

A-52. At lower frequencies, there is no practical solution to counter interference caused in this way. For frequencies in the VHF range (30–300 megahertz) and higher, the operator can improve the condition by elevating the antenna if the wave is vertically polarized. Operators reduce interference at higher frequencies by using directional antennas to avoid reflection.

A-53. Various reflecting surfaces occur in the atmosphere. In higher frequency ranges, reflections occur from the rain. At the highest radio frequencies, reflections are possible from clouds, particularly rain clouds. Reflections may even occur at a sharply defined boundary surface between air masses, as when warm, moist air flows over cold, dry air. When such a surface is roughly parallel to the surface of the Earth, radio waves may travel for greater distances than normal. The principal source of reflection in the atmosphere is the ionosphere (see paragraphs A-92 through A-104).

REFRACTION

A-54. Refraction involves a change in the direction of waves as a wave passes from one medium to another. Refraction of radio waves is like that of light waves. The direction of travel changes as a signal passes from air of one density to that of a different density. The principal cause of refraction in the atmosphere is the difference in temperature and pressure occurring at various elevations and within different air masses.

A-55. Although refraction occurs at all frequencies, below 30 megahertz the effect is small in comparison with ionospheric effects, diffraction, and absorption. At higher frequencies, refraction in the lower layer of the atmosphere extends the radio horizon to a distance about 15 percent greater than the visible horizon. The effect is the same as if the radius of the Earth was about one-third greater than it is and there was no refraction.

A-56. Sometimes the lower portion of the atmosphere becomes stratified. This stratification results in nonstandard temperature and moisture changes with height. A horizontal radio duct forms if there is a marked temperature inversion or a sharp decrease in water vapor content with increased height. Super-refraction is when HF radio waves travel horizontally within the duct and refract while remaining within the duct, following the curvature of the Earth over great distances (see figure A-12). Operators achieve maximum range when both transmitting and receiving antennas are within the duct. The frequency range affected by ducts varies from about 200 megahertz to more than 1,000 megahertz.

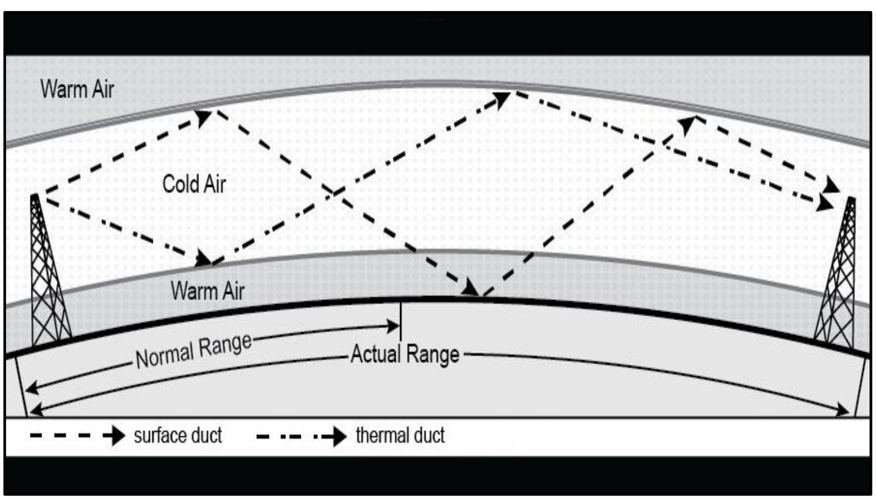


Figure A-12. Super-refraction ducts

A-57. At night, surface ducts may occur over land due to cooling of the surface. At sea, surface ducts about 15 meters (50 feet) thick may occur at any time in the trade wind belt—easterly surface winds found in the tropics near the equator. Surface ducts of 30 meters (100 feet) or more in thickness may extend from land out to sea when warm air from the land flows over the cooler ocean surface. Elevated ducts from about a meter (a few feet) to more than 300 meters (1,000 feet) in thickness may occur at elevations between 300 meters (1,000 feet) to about 457 meters (1,500 feet) because of the settling of a large air mass. Large air masses frequently occur in Southern California and certain areas of the Pacific Ocean.

A-58. Bending in the horizontal plane occurs when a ground wave crosses a coast at an oblique angle because of a marked difference in the conducting and reflecting properties of the land and water over which the wave travels. The effect is the coastal refraction or land effect.

DIFFRACTION

A-59. Radio wave diffraction refers to distortion when a wave encounters an obstacle. Diffraction causes a wave to change direction as it passes around a barrier or through an opening. When a radio wave encounters an obstacle, its energy reflects or absorbs, causing a shadow beyond the obstacle; however, some energy does enter the shadow area because of diffraction.

A-60. From the edge of the obstacle, energy radiates into the shadow area and outside of the area. The latter interacts with energy from other parts of the wavefront, producing alternate bands in which the secondary emission reinforces, or tends to cancel, the energy of the primary emission. The practical effect of an obstacle is significantly reduced signal strength in the shadow area, and a disturbed pattern for a short distance outside the shadow area, as illustrated in figure A-13.

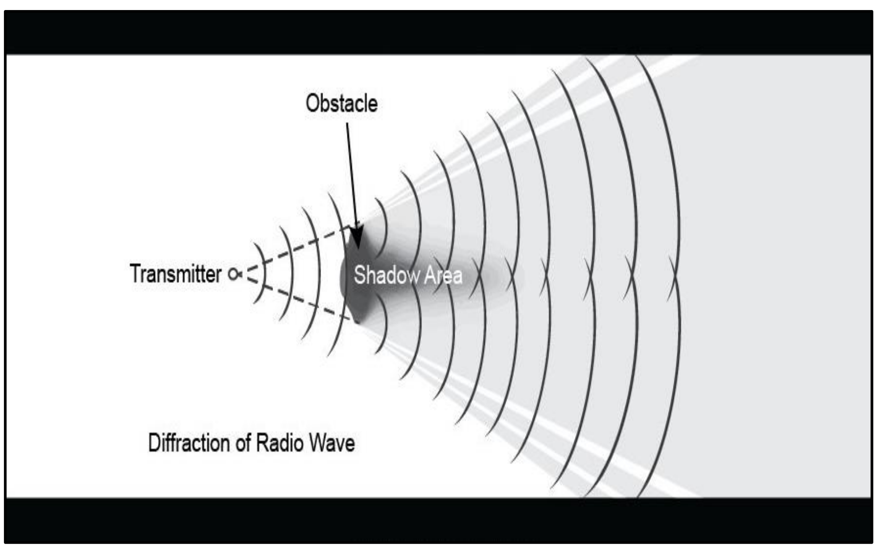


Figure A-13. Diffraction of radio waves around a solid object

A-61. The amount of diffraction is inversely proportional to the frequency, being greatest in the lowest frequency ranges. The lower the frequency, or the longer the wavelength, the greater the diffraction. Thus, radio waves diffract more than light or sound waves. In VHF and UHF communications, line of sight creates a shadow area beyond significant terrain features. In contrast, HF signals will diffract enough to leave a usable signal in the shadow area as shown in figure A-14.

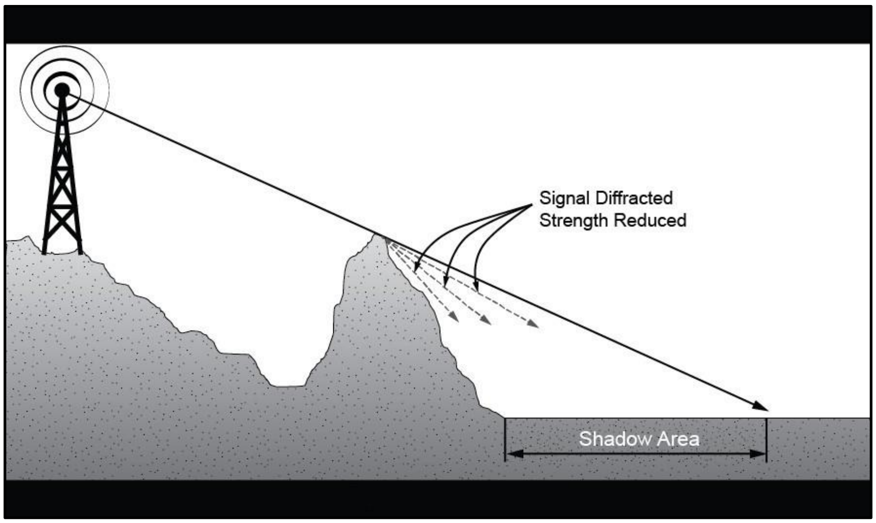


Figure A-14. Diffraction of radio waves around a terrain feature

ABSORPTION AND SCATTERING

A-62. The amplitude of a radio wave expanding outward through space varies inversely with distance, weakening with increased distance. The decrease of strength with the distance of a radio wave is attenuation.

A-63. A wave traveling along the Earth's surface loses a certain amount of energy due to absorption Because of this absorption, the remainder of the wavefront tilts downward, resulting in further absorption. Attenuation is greater over a surface that is a poor conductor. Relatively little absorption occurs over seawater, which is an excellent conductor at low frequencies. As a result, low frequency ground waves travel great distances over water.

A-64. Weather also affects the absorption rates of radio waves. Heavy rainfall can cause excessive absorption and may reduce the transmitting and receiving range of frequencies at VHF and above. Attenuation due to fog is determined by the quantity of water per unit volume and by the size of droplets. Fog is of minor importance for frequencies below 2 gigahertz but can cause serious attenuation at frequencies above 2 gigahertz. Extreme cold will cause radio signals to fade or even cease. Vegetation, such as a jungle environment, also increases absorption and shortens the range of transmissions.

A-65. A skywave (see paragraph A-79) suffers an attenuation loss in its encounter with the ionosphere. The amount depends upon the height and composition of the ionosphere as well as the frequency of the radio wave. Maximum ionospheric absorption occurs at about 1,400 kilohertz.

A-66. In general, atmospheric absorption increases with frequency. It is a problem only in the super-high frequency and extremely high frequency ranges. At these frequencies, attenuation increases by scattering due to reflection by oxygen, water vapor, water droplets, and rain in the atmosphere.

NOISE

A-67. Unwanted signals in a receiver are interference. The intentional production of such interference to obstruct communication is jamming. Unintentional interference is noise.

A-68. Noise may originate within the receiver. A humming sound is usually the result of induction from neighboring circuits carrying alternating current. Poor contacts or faulty components within the receiver cause irregular crackling or sizzling sounds. Stray currents in normal components cause some noise which sets the ultimate limit of sensitivity that used by a receiver. The noise is the same at any frequency.

A-69. Noise originating outside the receiver may be either manmade or natural. Manmade noises originate in electrical appliances, motor and generator brushes, ignition systems, and other sources of sparks that transmit electromagnetic signals picked up by the receiving antenna.

A-70. Atmospheric noise, atmospherics, or static are the discharge of static electricity in the atmosphere and cause natural noise. A thunderstorm is an example of a cause for natural noise. An exposed surface may acquire a more substantial charge of static electricity. Friction from water or solid particles that blow against a surface causes static. Water droplets striking a surface cause positive and negative charge—one part of the droplet requires a positive charge and the other a negative charge. These charges transfer to the surface of the water.

A-71. The charge tends to gather at points and ridges of the conducting surface. When it accumulates enough to overcome the insulating properties of the atmosphere, it discharges into the atmosphere. Under suitable conditions, discharge becomes visible. Atmospheric noise occurs to some extent at all frequencies but decreases as frequency increases. Above about 30-megahertz, atmospheric noise is not generally a problem.

FREE-SPACE PATH LOSS

A-72. Usually, the major loss of energy is due to the spreading of a wavefront as it travels away from the transmitter. As the distance increases, the wavefront spreads, like the beam of a flashlight. The amount of energy contained within any area of the wavefront decreases as the distance increases. The free-space path loss calculation excludes environmental effects.

A-73. The amount of energy lost between a transmitter and a receiver is measured in decibels. The following are typical calculation rules:

- Distance in kilometers multiplied by 10 results in the loss of 20 decibels.
- Distance in kilometers doubled results in the loss of 6 decibels.

MULTIPATH INTERFERENCE

A-74. Multipath interference is a phenomenon whereby a wave from a single source travels to a receiver by two or more paths and, provided the wave remains coherent, two or more components of the wave interfere with each other. The waves travel along a different path and arrive at the receiver out of phase with each other, as shown in figure A-15. Multipath fading interferes with the desired signal in amplitude and phase.

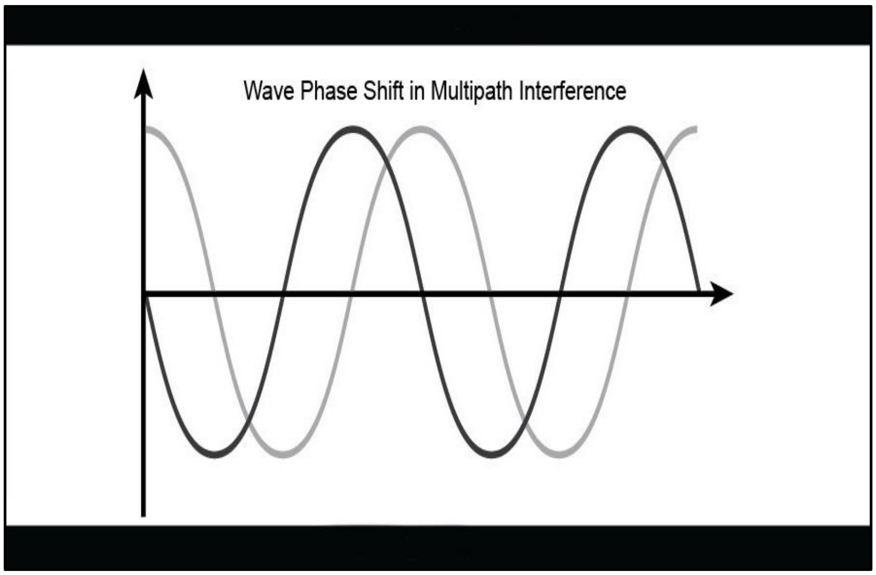


Figure A-15. Phase shift in multipath interference

GROUND WAVE

A-75. The wave that travels along the surface of the Earth is a ground wave. Ground wave propagation is the result of electrical characteristics of the Earth and diffraction of the waves along the curvature of the Earth. The strength of the ground wave at the receiver depends on the power output and frequency of the transmitter, the shape and conductivity of Earth along the transmission path, and local weather conditions.

Direct Wave

A-76. A direct wave is a radio wave that travels directly from the transmitting antenna to the receiving antenna, as depicted in figure A-16 on page A-25. This part of the wave is limited to line of sight distance between the transmitting and receiving antennas, plus the small distance added by atmospheric refraction and diffraction of the wave along the Earth's curvature. Operators can extend this distance by increasing the height of the transmitting or receiving antenna, or both.

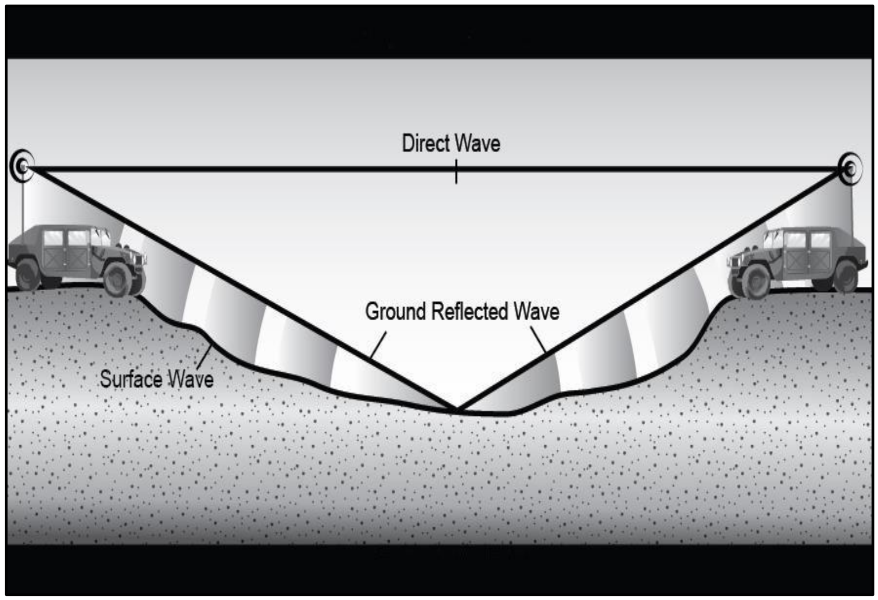


Figure A-16. Possible routes for ground waves

Ground Reflected Wave

A-77. A ground reflected wave is a radio wave that reaches the receiving antenna after reflecting from Earth's surface. Cancellation of the radio signal can occur when the ground reflected component and the direct wave component arrive at the receiving antenna simultaneously and are 180 degrees out of phase with each other.

Surface Wave

A-78. The conductivity and dielectric constant of the Earth affect the component of a ground wave, which is a surface wave. When both the transmitting and receiving antennas are on, or close to the ground, the direct and ground-reflected components of the wave tend to cancel out, and the resulting field intensity is principally that of the surface wave. However, the surface wave component also affects waves above the Earth's surface. The effect extends to considerable heights, diminishing in field strength with increased height. Because the ground absorbs part of its energy, the electric intensity of the surface wave attenuates at a greater rate. This attenuation depends on the relative conductivity of the surface over which the wave travels (see table A-4 on page A-26).

Table A-4. Propagation characteristics of terrain

Surface Type	*Relative Conductivity*	*Dielectric Constant*
Seawater	Good	80
Large bodies of fresh water	Fair	80
Wet soil	Fair	30
Flat, loamy soil	Fair	15
Dry, rocky terrain	Poor	7
Desert	Poor	4
Jungle	Unusable	Unusable

SKYWAVE

A-79. A skywave is a wave reaching a receiver by way of the ionosphere. When a radio wave encounters a particle with an electric charge, the particle vibrates. The vibrating particle absorbs electromagnetic energy from the radio wave, which it then radiates. The net effect is a change of polarization and an alteration of the path of the wave.

A-80. The higher the frequency, the greater the ionization density required to refract radio waves back to the Earth's surface. The F layer of the ionosphere refracts the higher frequencies because it is the most highly ionized. The E layer's varying ionization creates erratic behavior, refracting medium frequency, HF, and the lower radio waves. The D layer of the ionosphere, which is the least ionized, primarily absorbs radio waves; small amounts of refraction are possible but unpredictable.

A-81. At any given time and for each ionized region, there is an upper-frequency limit at which radio waves transmitted vertically are refracted back to Earth. This limit is the critical frequency. Radio waves directed vertically at frequencies higher than the critical frequency pass through the ionized layer out into space (see ray 1 in figure A-17). Generally, operators direct radio waves used in communications toward the ionosphere, at an oblique angle called the angle of incidence.

A-82. Radio waves at frequencies above the critical frequency refract back to Earth if transmitted at angles of incidence smaller than the critical angle. At the critical angle, and at all angles larger than the critical angle, if the frequency is higher than the critical frequency, the radio waves will pass through the ionosphere. At frequencies greater than about 30 megahertz, virtually all the energy penetrates through the ionosphere. As the frequency increases, the required angle decreases.

A-83. Figure A-17 on page A-27 shows ray 1 entering the ionosphere at an angle that alters the wave and allows it to pass into space. As the horizontal angle decreases, ray 2 refracts back toward the Earth. As the angle decreases further, such as with ray 3, the wave returns to Earth at a greater distance from the transmitter.

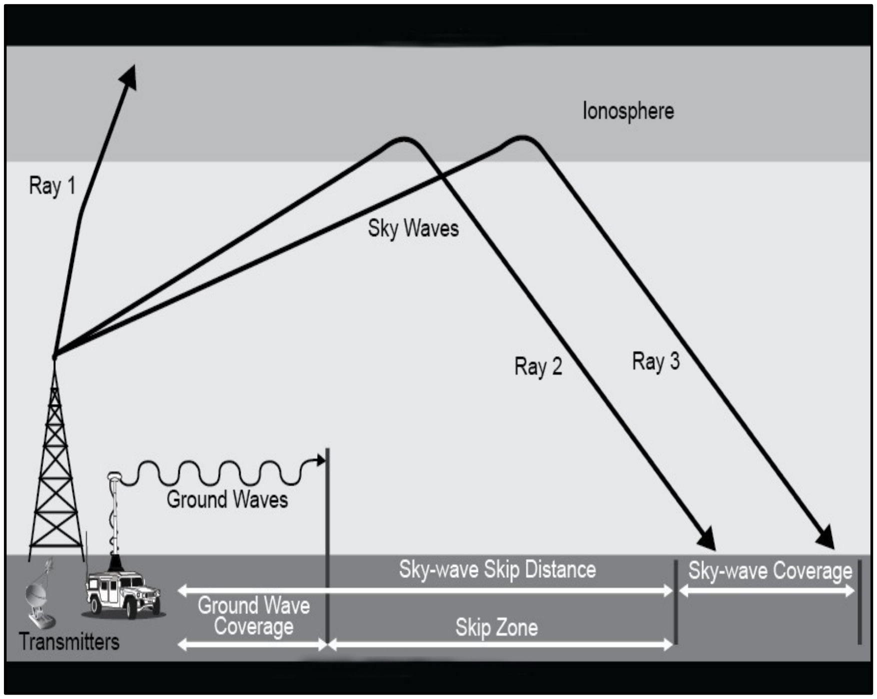


Figure A-17. Relationship between skip zone, skip distance, and ground wave

A-84. At angles greater than the critical angle, the wave passes through the ionosphere, continuing into space. The skip distance is the minimum distance from the transmitter and receiver. A skip zone is the area where the ground wave extends out for less distance that the skywave.

A-85. A near-vertical transmission path is a near-vertical incidence skywave. A near-vertical incidence skywave usually uses frequencies less than 10 megahertz and can operate on the lower sideband or the upper sideband for voice and data communications. This skywave provides reliable communication ranging from 50–400 kilometers (30–250 miles) by directing energy at 60–90 degrees, which—provided the frequency or power is not too high—refracts back toward the Earth's surface. This near-vertical angle of transmission reduces the skip zone and can overcome terrain features hampering short distance and beyond line of sight communications.

A-86. The antenna height in relation to the operating frequency affects the angle at which transmitted radio waves strike the ionosphere. Operators control this angle of incidence to achieve the desired area of coverage. Lowering the antenna height will increase the angle of transmission and provide a broad and even signal pattern within a region the size of a typical corps' area of operations. Raising the antenna height lowers the angle of incidence. Lowering the angle of incidence produces a skip zone (see figure

A-17). In a corps-sized area of operations, the skip zone is not a desirable condition. However, low angles of incidence make long-distance communications possible.

A-87. At any given receiver, there is a maximum usable frequency for skywave communication. Acceptable reception occurs between the maximum usable and lowest usable frequencies. Within usable frequency range, the operator can use the optimum frequency for best reception results. The frequency used cannot be too near the maximum usable frequency, because this frequency fluctuates with changes of intensity within the ionosphere. During magnetic storms, the ionosphere density decreases. The maximum usable frequency decreases, and the lowest usable frequency increases. Radio blackout occurs when there are no usable frequencies.

A-88. Skywave signals reaching a given receiver may arrive by any of several paths, as shown in figure A-18. A signal having a single reflection is a one-hop signal. A signal that undergoes two reflections with a ground reflection between is called a two-hop signal, and so forth. A multi-hop signal undergoes several reflections. The layers at which the reflections occur are one hop E, two hop F, and so forth.

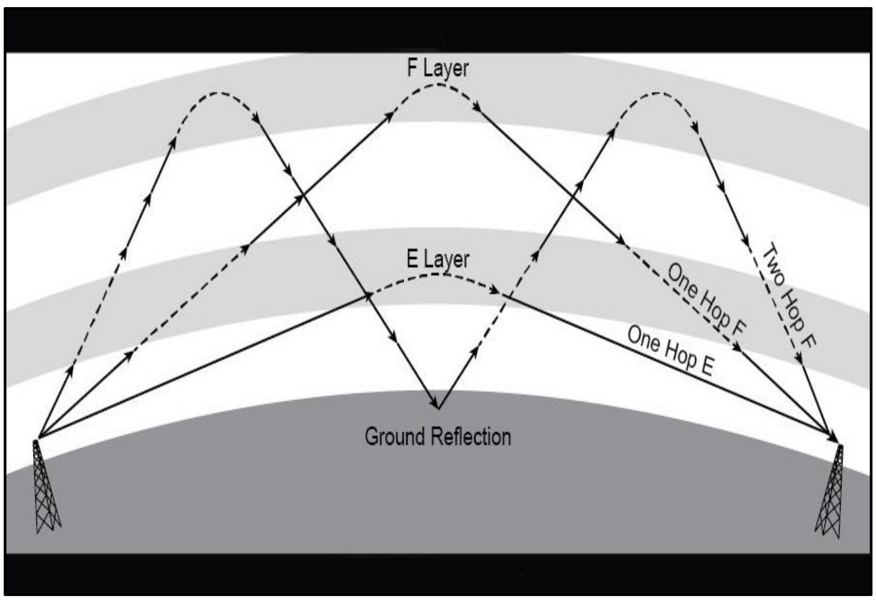


Figure A-18. Skywave paths

A-89. Because of the different paths and phase changes occurring at each reflection, the various signals arriving at a receiver have different phase relationships. Since the density of the ionosphere continually fluctuates, the strength and phase relationships of the various signals may undergo an almost continuous change. The various signals may reinforce each other at one moment and cancel each other the next, resulting in fluctuations in the strength of the total signal received. This phenomenon is a result of the interaction of components within a single reflected wave or reduced strength due to changes in the reflecting surface. Ionospheric changes are associated with fluctuations in the radiation received from the Sun, since this is the principal cause of ionization. Signals from the F layer are particularly erratic because of the rapidly fluctuating conditions within the layer itself.

A-90. The maximum distance for a usable, one-hop E signal during the daytime is about 2,400 kilometers (1,500 miles). At this distance, the signal leaves the transmitter in approximately a horizontal direction. At night, the E layer decreases and becomes relatively useless for radio transmission. A one-hop F signal can extend out to 4,000 kilometers (2,500 miles). At lower frequency ranges, ground waves extend out for great distances.

A-91. Polarization error occurs when skywave polarization changes during reflection from the ionosphere, accompanied by an alteration in the direction of travel of the wave. Night effect occurs near sunrise and sunset, when rapid changes occur in the ionosphere, reception becomes erratic, and polarization error is at maximum.

A-92. During daylight hours, the ionosphere is subject to the maximum ultraviolet output from the Sun, bringing the D, E, F1, and F2 layers to their highest reflection potential for higher frequencies.

A-93. At night, the composition of the ionospheric layers change—the D layer disappears, the E layer decreases in strength, and the F1 and F2 layers combine. The higher frequencies are more likely to penetrate the ionosphere, so operators use lower frequencies during the night.

A-94. The one exception to the rule concerns operations conducted during the summer. Due to the proximity of the Sun to the Earth and the more prolonged exposure of the ionosphere during this season, operators can use higher frequencies during the day and night. However, one must remember that the actual number of layers, their heights above the Earth, and the relative intensity of ionization present will vary.

Maximum Usable Frequency

A-95. The maximum usable frequency is the highest frequency at which a radio wave will return to Earth at a given distance when using a given ionized layer and a transmitting antenna with a fixed angle of radiation. The maximum usable frequency is always higher than the critical frequency because the angle of incidence is less than 90 degrees. As the distance between the transmitter and receiver increases, the maximum usable frequency will also increase. At certain frequencies, radio waves lose some energy through absorption by the D layer and a portion of the E layer.

A-96. The total frequency absorption is less, and communication becomes more satisfactory, as operators use higher frequencies—up to the maximum usable frequency. The absorption rate is greatest for frequencies ranging from 500 kilohertz–2 megahertz during the day. At night, the absorption rate decreases for all frequencies. Table A-5 on page A-30 outlines the general guidance on transmission angles (in degrees) for day and night communications.

Table A-5. Transmission angle and distance

Transmit Angle (degrees)	***Distance to F Layer***			
	Daytime		***Nighttime***	
	Kilometers	***Miles***	***Kilometers***	***Miles***
0	3,220	2,000	4,508	2,800
5	2,415	1,500	3,703	2,300
10	1,932	1,200	2,898	1,800
15	1,450	900	2,254	1,400
20	1,127	700	1,771	1,100
25	966	600	1,610	1,000
30	725	450	1,328	825
70	153	95	290	180
80	80	50	145	90
90	0	0	0	0

LOWEST USABLE FREQUENCY

A-97. As the frequency of transmission over any skywave path decreases, atmospheric noise becomes greater and results in an unacceptable signal-to-noise ratio. The frequency above the point that has too much noise for use is the lowest usable frequency. Frequencies lower than the lowest usable frequency are too weak for communications. The lowest usable frequency also depends on the power output of the transmitter and the transmission distance. When transmission power decreases, the rate of refraction increases. Waves below the lowest usable frequency refract back to the Earth at a shorter distance, as indicated in figure A-19 on page A-31. When the lowest usable frequency is greater than the maximum usable frequency, skywave communications are not possible.

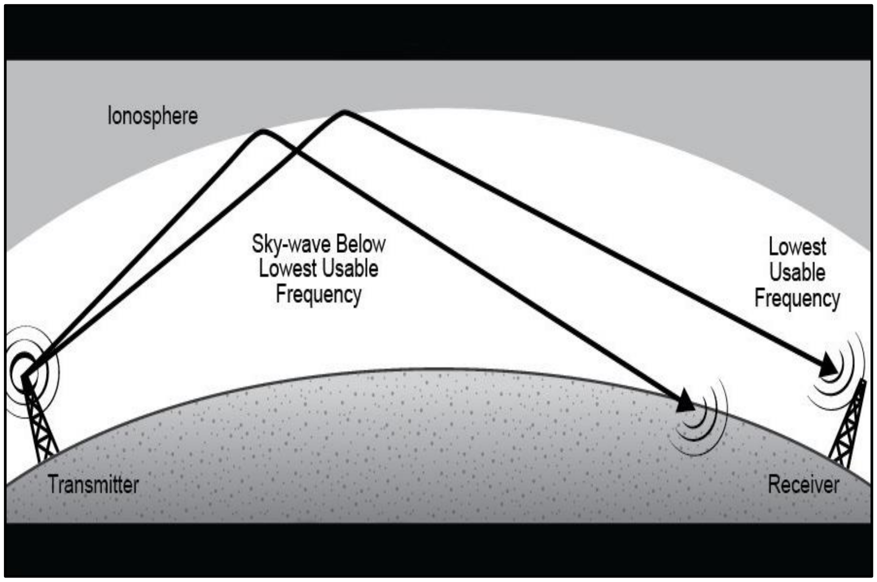


Figure A-19. Refraction of frequency below the lowest usable frequency

REGULAR IONOSPHERIC ACTIVITY

A-98. When planning a communications link, there are regular and irregular ionospheric activities for consideration. Some variations affect or degrade communications and cannot be mitigated. Regular ionospheric activities include—

- Diurnal variations.
- Seasonal changes.
- 11-year sunspot cycle.
- 27-day sunspot cycle.

Diurnal Variations

A-99. Daily daytime and nighttime changes occur in the composition and number of ionospheric layers. Skip distance varies and absorption increases during the day, therefore—

- During the day, operators use higher frequencies when ion density of the F2 layer is greater, and frequencies suffer less absorption while passing through the D layer.
- At night, operators use lower frequencies when the D layer disappears.

Seasonal Changes

A-100. As the position of the Sun moves from one hemisphere to the other with corresponding seasonal changes, the maximum ion density in the D, E, and F1 layers shift accordingly. Each change is relatively greater during the summer, raising the virtual height of the ionosphere's F2 layer considerably in summer. During winter, the ion density decreases (peaking at noon) and the virtual height of the F2 layer decreases.

Twenty-Seven-Day Sunspot Cycle

A-101. This cycle is another sunspot variation resulting from the rotation of the sun on its axis. As the number of sunspots changes from day to day, with solar rotation, the formation of new spots, or the disappearance of old ones on the visible part of the sun, absorption in the D layer also changes. Similar changes occur in the E-layer critical frequency. These variations exhibit wide geographic ranges. Although fluctuations in F2 layer critical frequencies from day to day are higher than for any other layer, these fluctuations are not generally of a worldwide character. Because of the variability of the F2 layer, precise predictions of its critical frequencies are not possible for individual days. However, long-term trends and geographical distribution can be projected in advance.

IRREGULAR IONOSPHERIC ACTIVITY

A-102. Irregular ionospheric activity is not accurately predictable. Irregular ionospheric activities include sporadic E, sudden ionospheric disturbance (Dellinger fade), and ionospheric storms.

Sporadic E

A-103. An excessively ionized E layer obscures reflections returning from the higher layers. This phenomenon causes unexpected propagation of a signal hundreds of miles beyond the normal range. This effect, called sporadic E, frequently occurs during the day and night. However, there is a seasonal pattern, peaking during the summer in both hemispheres with a much smaller peak in winter. An occurrence of sporadic E is not usually simultaneous at all stations. Operators use lower frequencies to achieve short-hop communications under these conditions.

Ionospheric Storms

A-104. Ionospheric storms usually accompany magnetic disturbances about 18 hours after a sudden ionospheric disturbance, can last for several hours—up to a couple of days—and may extend over a large portion of the Earth. The critical frequencies are much lower than normal because of a decrease in ion density and the virtual heights of the layers much greater so that maximum usable frequencies are much lower than normal. It is often necessary to lower the working frequency to maintain communications during one of these storms. There is also increased absorption of radio waves during storms. Ionospheric storms are most severe at higher latitudes and decrease in intensity toward the equator.

Appendix B
Jamming Calculations

This appendix discusses jamming formula symbols, the minimum jammer power output, and the maximum jammer distance.

FORMULA SYMBOLS

B-1. EW professionals use jamming formulas to determine the jamming power output and jammer distance to a target. This information enables EW personnel to understand the technical aspects of jamming and establishes the basis for advising the commander on jamming mission characteristics and effects. Mathematical formulas use the symbols in table B-1. Each symbol identifies a unit of measurement used for accurate calculations.

Table B-1. 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 modulation jammer tuning accuracy factor.
N	Terrain and ground factors: 5 = Very rugged terrain (rocky, mountainous 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. Technical intelligence publications and manuals contain friendly equipment and threat system specifications. The G-2 or S-2 provides the electromagnetic order of battle for threat systems. It is necessary to estimate the electromagnetic order of battle when no information is available.

FORMULA 1—MINIMUM JAMMER POWER OUTPUT

B-3. When the difference between Ht and Hj is less than 10 meters, they are considered 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 antenna. Figure B-1 illustrates 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

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

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

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

$$Pj = 10 \text{ x } (1)^2 \text{ x } (1.88)^4$$

$$Pj = 10 \text{ x } 12.46$$

$$Pj = 124.60 \text{ or } 125 \text{ watts}$$

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.

LEGEND
FM frequency modulation
LPA log periodic array

Figure B-1. Example minimum jammer power output calculations

FORMULA 2—MAXIMUM JAMMER DISTANCE

B-4. This formula is determine the maximum distance of jamming using a whip antenna from the target receiver. For the log periodic array antenna, the Pj factor is doubled. Figure B-2 on page B-3 shows the maximum jammer distance 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

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

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

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

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

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

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

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.

LEGEND

FM frequency modulation
LPA log periodic array

Figure B-2. Example maximum jammer distance calculation

This page intentionally left blank.

Appendix C

Electromagnetic Warfare Equipment and Systems

Units use program of record systems and available joint electromagnetic warfare resources to support the commander's intent. This appendix includes characteristics of Army and joint equipment that is useful in electromagnetic warfare planning.

ARMY

C-1. The Army is currently increasing its EW capabilities. It maintains several EW systems in its inventory. When requested, the Army provides these capabilities to formations at echelons corps and below.

ELECTROMAGNETIC WARFARE PLANNING AND MANAGEMENT TOOL

C-2. The CEWO uses the EWPMT to visualize and model the behavior of the electromagnetic spectrum in the area of operations before executing an EW mission. The CEWO also shares the view of the electromagnetic environment with the staff. The CEWO uses the EWPMT in conjunction with the electromagnetic order of battle provided by the G-2 or S-2 staff to analyze likely threat EW courses of action. The EWPMT provides an automated platform that enables the CEWO to—

- Provide input to the common operational picture.
- Display sensor information from deployed EW and SIGINT assets including—
  - Detected emitters.
  - Plotted lines of bearing.
  - Analysis of circular error probable ellipse.
- Conduct mission planning and rehearsals.
- Manage EW assets.
- Model and visualize how the electromagnetic environment will respond to friendly and enemy EW activities.

C-3. The CEMA section coordinates with the G-6 or S-6 network management technician for network configurations such as the specified Internet protocol address and computer name. The network management technician ensures the EWPMT has connectivity with the data distribution service. The data distribution service facilitates near real-time data sharing. The connectivity to the data distribution service allows the EWPMT to integrate with other command post information systems to publish and subscribe to the organization's common operational picture and assist in achieving greater situational understanding. Map data for the EWPMT is available from the National Geospatial-Intelligence Agency.

C-4. The EWPMT provides situational awareness tools to enable the CEWO or spectrum manager's planning, execution, and understanding of the battlespace. Knowing what is taking place in the electromagnetic spectrum around the unit's area of operations can give Soldiers the initiative and allow actions inside the threat decision cycle. The EWPMT's comprehensive spectrum situational awareness view automatically creates and updates from tactical data and operational situational awareness data received from intelligence cells, mission command information systems, and other external sources. This data may be real-time, (such as symbol data or ongoing target engagements), near real-time (such as logistic reports and some forms of intelligence data) or non-real-time (such as civil infrastructure or facility database). Normally, situational awareness data is received digitally and automatically populates the situational awareness view, but the EWPMT operator can also enter situational awareness data manually.

C-5. The EWPMT situational awareness view provides a comprehensive view of the electromagnetic operational environment, including—

- Enemy units and symbols—emitter information, such as range and lines of bearing, including actual locations of units through intelligence analysis.
- Map data (images, raster background, and so forth).
- Friendly units and symbols—
  - Emitter information, such as range and lines of bearing.
  - Status information from the squad level through division and joint commands.
  - EW frequency fratricide predictions from planned and active electromagnetic attack activities.
  - Detailed unit status for organic EW assets in the area of operations.
- Allied and neutral units—
  - Symbols and emitter information.
  - EW frequency fratricide predictions from planned or active electromagnetic attack activities.
- Control graphics—
  - EW threats categorized as planned, actively or previously engaged, suspect, and others, with effectivity predictions against those targets for planned and active EW operations.
  - Military and civil infrastructure such as facilities, bridges, and key terrain features.
  - Significant events such as civil unrest, bombings, arson, and riots.
- Spot reports, including enemy sightings and other relevant information.
- Weather information.

Counter Radio-Controlled Improvised Explosive Device Electromagnetic Warfare Systems

C-6. Although the Army has the largest inventory, all U.S. ground forces use CREW systems to prevent improvised explosive device detonation by RF energy. These forces maintain mounted, dismounted, and fixed-site CREW capabilities to protect personnel and equipment. As technology improves, the capabilities of some systems have progressed beyond mere jamming to information collection and direction finding. The systems currently in use by U.S. forces and multinational partners include—

- Mounted—
  - AN/VLQ-12 Duke V2/V3 (Army).
  - Symphony (coalition).
  - EGON Active/Reactive Counter-IED System (special operations forces).
- Dismounted—
  - AN/PLT-5 THOR II (explosive ordnance disposal).
  - Guardian H3 (North Atlantic Treaty Organization).
  - MODI (conventional and non-conventional).

C-7. Jammers may function in an active or reactive mode. Active mode means the jammer continuously emits a signal to block a preprogrammed frequency. Active mode is effective against multiple low-power signals but is vulnerable to threat 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 vulnerable to direction finding and are excellent against high-power signals.

Aircraft Survivability Equipment

C-8. Aircraft survivability equipment aims to reduce aircraft vulnerability, thus allowing aircrews to accomplish their immediate missions and survive. Army aviation maintains a suite of aircraft survivability equipment that provides electromagnetic protection against threat spectrum-enabled weapon systems (detection, tracking, and targeting). This protection can include RF warning and countermeasures systems, common missile warning systems, information requirement countermeasures systems, and laser detection and countermeasure systems.

Intelligence Systems

C-9. The intelligence community operates and maintains systems capable of providing electromagnetic support information. Usually, the information is collected, consolidated as data, and further analyzed to become SIGINT, but the additional capability can also provide combat information for electromagnetic support purposes. The systems and operators must use the correct authorities and procedures when conducting SIGINT or electromagnetic support, without confusing classifications or missions.

Guardrail Common Sensor

C-10. The Guardrail Common Sensor is a corps-level, airborne SIGINT collection and locating system. It provides tactical commanders with near real-time targeting information. Key features include—

- Integrated communications intelligence and electromagnetic intelligence reporting.
- Enhanced signal classification and recognition.
- Near real-time direction finding.

C-11. The Guardrail Common Sensor shares technology with the ground-based common sensor, airborne reconnaissance-low, and other joint systems.

Prophet Enhanced

C-12. Prophet Enhanced is a ground-based tactical SIGINT and electromagnetic support sensor system. This system contributes to force protection, target development, and situational awareness through SIGINT support to units.

SPECTRUM TOOLS

C-13. The G-6 or S-6 spectrum manager assists the CEMA section in frequency assignment for EW activities. The G-6 or S-6 spectrum manager requests frequency resources through Spectrum XXI or by liaising with the combatant command or the host-nation spectrum authorities.

C-14. The End-to-End Supportability System is a web application that facilitates warfighter deployment and communications by providing worldwide visibility of host-nation supportability of spectrum-dependent devices. The End-to-End Supportability System automates the distribution of host-nation coordination requests, allowing combatant command submission for host-nation supportability and reducing time requirements for managing the host-nation spectrum authorization process. The design of the database provides informed decision making concerning frequency bands. It enables managers to determine the historical spectrum supportability of similar systems.

NAVY

C-15. The Navy's primary airborne EW platform is the EA-18G Growler. The Navy also maintains both surface and subsurface EW shipboard systems for offensive and defensive missions to support the fleet.

C-16. The EA-18G Growler's general capabilities include—

- Suppression of enemy air defenses. The EA-18G Growler counters enemy air defenses using both reactive and preemptive jamming techniques.
- Standoff and escort jamming.
- Integrated air and ground airborne electromagnetic attack.

- 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.

C-17. The EA-18G Growler's airborne electromagnetic attack capabilities are—

- Effectiveness against any surface-to-air threat.
- Ability to sense and locate threats.
- Uninterrupted communications during jamming operations.

AIR FORCE

C-18. The Air Force has two primary EW platforms:

- EC-130H Compass Call.
- RC-135V/W Rivet Joint.

EC-130H COMPASS CALL

C-19. The EC-130H Compass Call is an airborne tactical EW system. The EC-130H delivers degrade and disrupt effects on threat communications systems and radars used to support threat air, ground, and maritime operations, and many modern commercial communications systems a threat might employ.

RC-135V/W RIVET JOINT

C-20. The RC-135V/W Rivet Joint is a combatant command-level surveillance asset that responds to strategic taskings. The RC-135V/W Rivet Joint is equipped with information gathering equipment that enables monitoring of threat electromagnetic activity. The aircraft has secure communications using HF, VHF and UHF radios and satellite communications.

MARINE CORPS

C-21. The Marine Corps uses a variety of EW systems and supporting systems to execute their tactical EW missions. Like the other Services, equipment and techniques change based on threat and technology.

AN/ULQ-19(V)2 ELECTRONIC ATTACK SET

C-22. The AN/ULQ-19(V)2 electronic attack set allows operators to conduct spot or sweep jamming of single-channel voice or data signals operating in the standard military frequency range of 20–79.975 megahertz from selected mobile platforms—for example, high mobility multipurpose wheeled vehicles, mobile electromagnetic warfare support system, and helicopters. When employed as a tactical, general purpose, low-VHF jamming system, the AN/ULQ-19(V)2 has a 250-watt RF linear amplifier that produces a nominal 200 watts effective radiated power using a standard omnidirectional whip antenna. To conduct jamming, the system must operate with an unobstructed signal line of sight to the targeted communications transceiver.

AN/MLQ-36 Mobile Electronic Warfare Support System

C-23. The AN/MLQ-36 Mobile Electronic Warfare Support System provides a multifunctional capability that provides limited armor protection for SIGINT and EW operators. This equipment can provide SIGINT and EW support to highly mobile military operations in urban terrain where maneuver and armor protection are critical. The AN/MLQ-36 consists of a signals intercept system, a radio direction finding system, an electromagnetic attack system, a secure communications system, and an intercom system installed in a logistic variant of the light armored vehicle. The AN/MLQ-36A Mobile Electromagnetic Warfare Support System product improvement program is an advanced SIGINT and EW system integrated into a light armored vehicle.

C-24. The Mobile Electromagnetic Warfare Support System product improvement program provides a total replacement of the EW mission equipment in the AN/MLQ-36 Mobile Electromagnetic Warfare Support System. The Mobile Electromagnetic Warfare Support System product improvement program provides the ability to detect and evaluate enemy communications emissions, detect, and categorize enemy noncommunications emissions, determine lines of bearing, and degrade enemy tactical radio communications during expeditionary operations. When mission-configured and working cooperatively with other Mobile Electromagnetic Warfare Support System product improvement program platforms, the common suite of equipment can also provide precision location of battlefield emitters. The system has an automated tasking and reporting data link available to other Marine air-ground task force assets such as the AN/TSQ-130 technical control and analysis center product improvement program. The Mobile Electromagnetic Warfare Support System product improvement program and its future enhancements will provide the capability to exploit new and sophisticated enemy electromagnetic emissions and conduct electromagnetic attack in support of existing and planned national, theater, fleet, and Marine air-ground task force SIGINT and EW operations.

Appendix D
Forms, Reports, and Messages

Electromagnetic warfare professionals use several different forms, reports, and messages in the performance of their duties. The common forms and formats are included in this appendix.

ELECTROMAGNETIC ATTACK REQUEST FORMAT

D-1. Electromagnetic attack requests fall within three operational categories: preplanned, preplanned on-call, and immediate. The CEWO enters requests for electromagnetic attack effects through the targeting working group using the electromagnetic attack request format (see table D-1 on page D-2). Requesting preplanned electromagnetic attack support is similar to requesting close air support. Requests for electromagnetic attack effects use Department of Defense Form 1972 (*Joint Tactical Air Strike Request*) (see paragraph D-2) with specific electromagnetic attack effects requests attached in an electromagnetic attack request format.

Table D-1. Electromagnetic attack request format

<table>
<tr><td colspan="2">Requesting Major Support Command:</td></tr>
<tr><td colspan="2">Requesting Unit:</td></tr>
<tr><td colspan="2">Contact information: This person will be responsible to verify approved request before the mission starts and to relay the information to the executing unit.</td></tr>
<tr><td colspan="2">Joint Tactical Air Strike Request Number: Enter the joint tactical air strike request number for submission with the electromagnetic attack request format.</td></tr>
<tr><td colspan="2">Concept of Operations: Describe the concept of operations. This will include the objective, forces used, timeline of the mission, and coordination efforts required for mission success. Relate the impact of mission success to specific objectives for the integrated tasking order.</td></tr>
<tr><td colspan="2">Electromagnetic Attack Concept of Operations: Define the desired effect(s) and timeline.</td></tr>
<tr><td colspan="2">CEASE BUZZER Procedures: This will be in accordance with theater special instructions. Provide frequency to communicate between the jamming control authority and electromagnetic attack asset. VHF and UHF are the primary means to talk to a supporting aircraft. If unable to establish communications, consider using another asset to relay information. Some aircraft may be internet relay chat capable.</td></tr>
<tr><td colspan="2">Friendly Frequency Use for Operation:</td></tr>
<tr><td>Target Communication System(s) to be Jammed or Denied:</td><td>Target requested—list the type and frequency, if known.
Intelligence assessment (required—do not copy and paste frequencies from one day to the next without intelligence validation assessment).
Target location in latitude and longitude or military grid reference system.</td></tr>
<tr><td colspan="2">Jamming date-time group(s): from and to, in Zulu Time (preferred):</td></tr>
<tr><td colspan="2">Type of Electromagnetic Attack Requested: preplanned and scheduled; on-call:</td></tr>
<tr><td colspan="2">LEGEND:
VHF very high frequency
UHF ultrahigh frequency</td></tr>
</table>

JOINT TACTICAL AIR STRIKE REQUEST

D-2. CEWOs use Department of Defense Form 1972 to request airborne electromagnetic attack. The JTAR specifies the effects desired using airborne and space-based platforms (see figure D-1 on page D-3). The CEWO's completion of the JTAR is critical to helping air planners in the combat air operations center select the aircraft and payload to support the JTAR.

D-3. To ensure the air component achieves the effects desired by the ground component, the JTAR must clearly describe desired effects in detail. Most organizations require the submission of a JTAR and an electromagnetic attack request format together. The JTAR and electromagnetic attack request format complement each other. Once filled with operational information, the Department of Defense Form 1972 becomes classified SECRET. This sample is unclassified.

JOINT TACTICAL AIR STRIKE REQUEST — See Joint Pub 3-09.3 for preparation instructions.

SECTION - MISSION REQUEST — DATE

1. UNIT CALLED: Chieftan | THIS IS: Gator 01 | REQUEST NUMBER: 1A9501-A | SENT: TIME 1615, BY MAJ Smith

2. PREPLANNED: [A] PRECEDENCE 4 | [ ] PRIORITY II; IMMEDIATE: [C] PRIORITY ____ | RECEIVED: TIME 1615, BY SrA Ford

3. TARGET IS NUMBER OF
[A] PERS IN OPEN 20-30 | [B] PERS DUG IN ____ | [C] WPNS/MG/RR/AT ____ | [D] MORTARS, ARTY ____
[E] AAA ADA ____ | [F] RKTS MISSILE ____ | [G] ARMOR 3x BTR in a line | [H] VEHICLES 4 Stationary
[I] BLDGS 2 | [J] BRIDGES ____ | [K] PILLBOX, BUNKERS ____ | [L] SUPPLIES, EQUIP ____
[M] CENTER (CP, COM) ____ | [N] AREA ____ | [O] ROUTE ____ | [P] MOVING N E S W ____
[Q] REMARKS ____

4. TARGET LOCATION IS
[A] 11SUG8005 (COORDINATES) | [B] ____ (COORDINATES) | [C] ____ (COORDINATES) | [D] ____ (COORDINATES)
[E] TGT ELEV 10 | [F] SHEET NO. 2857 II | [G] SERIES V795S | [H] CHART NO ____
CHECKED BY: Ssgt INTEL

5. TARGET TIME/DATE: [A] ASAP ____ [B] NLT 1600 [C] AT ____ [D] TO ____

6. DESIRED ORD/RESULTS: [A] ORDINANCE LGB/Guns; [B] DESTROY ____ [C] NEUTRALIZE X [D] HARASS/INTERDICT ____

7. FINAL CONTROL: [A] FAC/RABFAC II [B] CALL SIGN GATOR 20 [C] FREQ ORANGE 17; [D] CONT PT JACKS

8. REMARKS

SAMPLE

SECTION II - COORDINATION

9. NSFS: 4XTLAMFLA1SS | 10. ARTY | 11. AIO/G-2/G-3

12. REQUEST. [X] APPROVED [ ] DISAPPROVED | 13. BY: MAJ Hughes | 14. REASON FOR DISAPPROVAL

15. RESTRICTIVE FIRE/AIR PLAN: [A] IS NOT IN EFFECT [B] NUMBER | 16. IS IN EFFECT: [A] (FROM TIME) ____ [B] (TO TIME) ____

17. LOCATION: [A] ____ (FROM COORDINATES) [B] ____ (TO COORDINATES) | 18. WIDTH (METERS) | 19. ALTITUDE/VERTEX: [A] ____ (MAXIMUM/VERTEX) [B] ____ (MINIMUM)

SECTION III - MISSION DATA

20. MISSION MUMBER 3031/3022	21. CALL SIGN Razor 51/52 Venom 16/17	22. NO. AND TYPE AIRCRAFT (2) AV-8B (2) AH-1Z	23. ORDANCE SCL 1/3
24. EST/ACT TAKEOFF 1424	25. EST TOT 1438	26. CONT PT (COORDS) Breaker	27. INITIAL CONTACT
28. FAC/FAC(A)/TAC(A) CALL SIGN/ FREQ	29. AIRSPACE COORDINATION AREA	30. TGT DESCRIPTION	31. TGT COORD/ELEV

32. BATTLE DAMAGE ASSESSMENT (BDA) REPORT (USMTF INFLTREP)
LINE 1/CALL SIGN Razor 51/52 | LINE 4/LOCATION 18SUG8005
LINE 2/MSN NUMBER 3021/3022 | LINE 5/TOT 1454
LINE 3/REQ NUMBER 1A9501-A | LINE 6/RESULTS Neutralize/Destroy
REMARKS ____
*TRANSMIT AS APPROPRIATE

DD FORM 1972, MAY 2019 — PREVIOUS EDITION MAY BE USED. — Reset — Adobe Professional 7.0

Figure D-1. Sample joint tactical air strike request

JOINT SPECTRUM INTERFERENCE RESOLUTION

D-4. Operators report electromagnetic interference using the JSIR-Online Portal. The JSIR-Online Portal is located on the SECRET Internet Protocol Router Network. Unit standard operating procedures may also require JSIR approval from the chain of command using the JSIR format in figure D-2.

Sharing information contained in the completed JSIR report helps the unit build situational understanding of the threat and aids in the development of mitigation procedures. The report preparer provides a copy of the completed form to the CEWO, spectrum manager, and G-6 or S-6 staff.

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 enough 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 and frequency/frequencies).
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 additional 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 D-2. Joint spectrum interference resolution report instructions

STOP JAMMING MESSAGE

D-5. To stop jamming, the CEWO submits a stop jamming message as illustrated in figure D-3.

STOP JAMMING MESSAGE

GENERAL INSTRUCTIONS: Use to terminate a jamming task conducted by an electromagnetic 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 D-3. Stop jamming message instructions

ELECTROMAGNETIC WARFARE FREQUENCY DECONFLICTION MESSAGE

D-6. The CEWO completes an EW frequency deconfliction message to identify and categorize frequencies to be utilized by friendly forces, and to prevent frequency fratricide (see figure D-4 on page D-6).

ELECTROMAGNETIC WARFARE FREQUENCY DECONFLICTION MESSAGE [EWDECONFLICT]

REPORT NUMBER: E010 {USMTF # F402}

GENERAL INSTRUCTIONS: Use to promulgate a list of protected, guarded, and taboo frequencies to ensure friendly force use of the frequency spectrum without adverse impact from friendly electromagnetic attack.

Reference: ATP 3-12.3

LINE 1 – DATE AND TIME ____________	(DTG)
LINE 2 – UNIT ____________	(Unit making report)
LINE 3 – TYPE____________	(TABOO, PROTECT, or GUARD)
LINE 4 – STATUS ____________	(Restricted status of frequency: NEW, CHANGE, CANCEL, or RENEW)
LINE 5 – FREQUENCY____________	(Frequency/frequencies)
LINE 6 – ON TIME ____________	(Start DTG of frequency restriction)
LINE 7 – OFF TIME ____________	(End DTG of frequency restriction)
LINE 8 – LOCATION ____________	(UTM or six-digit grid coordinate with MGRS grid zone designator)

**Repeat lines 3 through 8 as a group to accommodate multiple reports. Assign sequential line numbers to succeeding iterations; for example, first iteration 3 through 8; second iteration 3a through 8a; and so on.

LINE 9 – NARRATIVE ____________	(Free text for additional information required for clarification of report)
LINE 10 – AUTHENTICATION	(Report authentication)

LEGEND

DTG	date-time group
MGRS	military grid reference system
UTM	universal transverse mercator

Figure D-4. Electromagnetic warfare frequency deconfliction message instructions

ELECTROMAGNETIC WARFARE MISSION SUMMARY

D-7. The CEWO maintains a record of EW missions. The record is the EW mission summary (see figure D-5 beginning on page D-7).

ELECTROMAGNETIC WARFARE MISSION SUMMARY [EWMSNSUM]

REPORT NUMBER: E015 {USMTF # G424}

GENERAL INSTRUCTIONS: Use to summarize significant EW missions and the status of offensive EW assets.

Reference: ATP 3-12.3

LINE 1 – DATE AND TIME ________	(DTG)
LINE 2 – UNIT________	(Unit making report)
LINE 3 – FROM________	(Beginning DTG Zulu of period summarized)
LINE 4 – THROUGH________	Ending DTG Zulu of period summarized)
LINE 5 – COUNTRY________	(Nationality of the target emitter of concern)
LINE 6 – LOCATION________	(UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 7 – EMITTER ________	(Emitter call sign and name or nomenclature)
LINE 8 – FUNCTION________	(Primary function of target)
LINE 9 – NOTATION ________	(Notation or sorting code)
LINE 10 – SIGNAL________	(Type of signal of target emitter)
LINE 11 – ON TIME________	(DTG that planned EA activity was initiated)
LINE 12 – OFF TIME________	(DTG that planned EA activity was terminated)
LINE 13 – PRIORITY________	(Relative importance of EA mission)
LINE 14 – TYPE ________	(Type of EA used against the emitter)
LINE 15 – PRIMARY FREQUENCY________	(Primary frequency of EA target signal)
LINE 16 – SECONDARY FREQUENCY________	(Secondary frequency of EA target signal)
LINE 17 – LOW FREQUENCY________	(Lower frequency limit of target equipment class)
LINE 18 – HIGH FREQUENCY________	(Upper frequency limit of target equipment class)
LINE 19 – BANDWITH________	(Target frequency bandwidth expressed in MHz)
LINE 20 – PULSE REPETITION________	(Pulse repetition interval or frequency)
LINE 21 – SYSTEM USED ________	(Name/nomenclature of EW asset used to perform the task)
LINE 22 – OPERATIONAL ________	(Number of units that can perform primary EW mission)
LINE 23 – NONOPERATIONAL________	(Number of units that cannot perform primary EW mission)
LINE 24 – DESTROYED ________	(Number of units that were destroyed in combat)
LINE 25 – CHAFF________	(Type of chaff)
LINE 26– LOWER FREQUENCY________	(Lower frequency of a range of frequencies that was blanked by chaff or the lower EA frequency)
LINE 27 – UPPER FREQUENCY________	(Upper frequency of a range of frequencies that was blanked by chaff or the lower EA frequency)
LINE 28 – LOW LEVEL ________	(Lower altitude in hundreds of feet of airspace that was blanked by chaff)
LINE 29 – UPPER LEVEL________	(Upper altitude in hundreds of feet of airspace that was blanked by chaff)
LINE 30 – TECHNIQUE________	(EA technique employed)

LEGEND

DTG	date-time group	MGRS	military grid reference system
EA	electromagnetic attack	MHz	megahertz
EW	electromagnetic warfare	UTM	universal transverse mercator

Figure D-5. Electromagnetic warfare mission summary

LINE 31 – COUNTRY________	(Country in which chaff was employed)
LINE 32 – ON TIME ________	(DTG that the chaff drop was initiated)
LINE 33 – OFF TIME________	(DTG that the chaff drop was terminated)
LINE 34 – START LOCATION________	(Start location of the chaff drop in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 35 – STOP LOCATION________	(Stop location of the chaff drop in UTM or six-digit grid coordinate with grid zone designator)
LINE 36 – NARRATIVE ________	(Free text for additional information required for clarification of report)
LINE 37 – AUTHENTICATION________	(Report authentication)

LEGEND

DTG	date-time group	MGRS	military grid reference system
EA	electromagnetic attack	MHz	megahertz
EW	electromagnetic warfare	UTM	universal transverse mercator

Figure D-5. Electromagnetic warfare mission summary (continued)

ELECTROMAGNETIC WARFARE TASKING MESSAGE

D-8. The CEWO uses the EW tasking message format to task an EW asset to provide a requested effect (see figure D-6 beginning on page D-9).

ELECTROMAGNETIC WARFARE REQUESTING/TASKING MESSAGE [EWRTM]

REPORT NUMBER: E020 {USMTF # A426}

GENERAL INSTRUCTIONS: Use (1) to task component commanders to perform EW operations to support the overall EW plan, (2) to support component EW operations, and (3) to request EW support from sources outside their commands.

Reference: ATP 3-12.3

LINE 1 – DATE AND TIME ______	(DTG)
LINE 2 – UNIT______	(Unit making report)
LINE 3 – EA ______	(Electromagnetic Activity)
LINE 4 – TASKED______	(Designator of tasked unit if the JOC is tasking the unit)
LINE 5 – COUNTRY______	(Nationality of the target emitter of concern)
LINE 6 – LOCATION______	(UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 7 – EMITTER______	(Emitter call sign and name or nomenclature)
LINE 8 – FUNCTION ______	(Primary function of target)
LINE 9 – NOTATION______	(Notation or sorting code)
LINE 10 – SIGNAL ______	(Type of signal of target emitter)
LINE 11 – ON TIME______	(DTG that planned EA activity was initiated)
LINE 12 – OFF TIME ______	(DTG that planned EA activity will be terminated)
LINE 13 – PRIORITY______	(Relative importance of EA mission)
LINE 14 – TYPE ______	(Type of EA and technique used against the emitter)
LINE 15 – PRIMARY FREQUENCY______	(Primary frequency of EA target signal)
LINE 16 – SECONDARY FREQUENCY______	(Secondary frequency of EA target signal)
LINE 17 – LOW FREQUENCY______	(Lower frequency limit of target class)
LINE 18 – HIGH FREQUENCY______	(Upper frequency limit of target class)
LINE 19 – BANDWITH______	(Target frequency bandwidth expressed in MHz)
LINE 20 – PULSE REPETITION ______	(Pulse repetition interval or frequency)
LINE 21 – ES ______	(Electromagnetic support)
LINE 22 – COUNTRY______	(Nationality of the target emitter of concern)
LINE 23 – LOCATION ______	(Emitter location described in UTM or six-digit grid coordinate with MGRS grid zone designator)
LINE 24 – EMITTER ______	(Emitter call sign and name or nomenclature)
LINE 25 – FUNCTION______	(Primary function of target)
LINE 26 – NOTATION______	(Notation or sorting code)
LINE 27 – SIGNAL ______	(Type of signal of target emitter)
LINE 28 – PRIMARY FREQUENCY______	(Primary frequency of ES target signal)
LINE 29 – SECONDARY FREQUENCY______	(Secondary frequency of ES target signal)
LINE 30 – LOW FREQUENCY______	(Lower frequency limit of target equipment class)

Legend:

DTG	date-time group	MGRS	military grid reference system
EA	electromagnetic attack	MHz	megahertz
EW	electromagnetic warfare	UTM	universal transverse mercator
JOC	joint operations center		

Figure D-6. Electromagnetic warfare tasking message

LINE 31 – HIGH FREQUENCY__________	(Upper frequency limit of target class)
LINE 32 – BANDWITH__________	(Target frequency bandwidth expressed in MHz)
LINE 33 – PULSE REPETITION__________	(Pulse repetition interval or frequency)
LINE 34 – ON TIME __________	DTG that planned ES activity was initiated
LINE 35 – OFF TIME __________	DTG that planned ES activity was terminated
LINE 36 – ESSENTIAL __________	(EEI category indicator)
LINE 37 – PRIORITY__________	(Relative importance of ES mission)
LINE 38 – CHAFF__________	(Type of chaff)
LINE 39 – LOWER FREQUENCY__________	(Lower frequency of a range of frequencies that is to be blanked by chaff or the Lower EA frequency)
LINE 40 – UPPER FREQUENCY__________	(Upper frequency of a range of frequencies that is to be blanked by chaff or the Upper EA frequency)
LINE 41 – LOW LEVEL__________	(Lower altitude in hundreds of feet of airspace to be blanked by chaff)
LINE 42 – UPPER LEVEL __________	(Upper altitude in hundreds of feet of airspace to be blanked by chaff)
LINE 43 – TECHNIQUE __________	(EA technique to be employed)
LINE 44 – COUNTRY__________	(Country in which chaff is to be employed)
LINE 45 – ON TIME __________	(DTG that the planned chaff drop will be initiated)
LINE 46 – OFF TIME __________	(DTG that the planned chaff drop will terminate)
LINE 47 – START LOCATION __________	(Start location of the chaff drop in UTM or six-digit grid coordinate with grid zone designator)
LINE 48 – STOP LOCATION __________	(stop location of the chaff drop in UTM or six-digit grid coordinate with grid zone designator)
LINE 49 – NARRATIVE __________	(free text for additional information required for report clarification)
LINE 50 – AUTHENTICATION __________	(Report authentication)

Legend:

DTG	date-time group	MGRS	military grid reference system
EA	electromagnetic attack	MHz	megahertz
EW	electromagnetic warfare	UTM	universal transverse mercator
JOC	joint operations center		

Figure D-6. Electromagnetic warfare tasking message (continued)

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. ATP 3-12.3 is not the proponent for any Army terms. The proponent publication for joint and Army terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP Army doctrine publication

ATP Army techniques publication

CEMA cyberspace electromagnetic activities

CEWO cyber electromagnetic warfare officer

CJCSI Chairman of the Joint Chiefs of Staff instruction

CJCSM Chairman of the Joint Chiefs of Staff manual

CREW counter radio-controlled improvised explosive device electromagnetic warfare

EMCON emission control

EW electromagnetic warfare

EWPMT Electromagnetic Warfare Planning and Management Tool

FM field manual; frequency modulation

G-2 assistant chief of staff, intelligence

G-3 assistant chief of staff, operations

G-6 assistant chief of staff, signal

HF high frequency

IEEE Institute of Electrical and Electronics Engineers

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

JTAR joint tactical airstrike request

MDMP military decision-making process

METT-TC (I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations
RF	radio frequency
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
SIGINT	signals intelligence
UHF	ultrahigh frequency
VHF	very high frequency

SECTION II – TERMS

assessment

The determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. (JP 3-0)

chaff

Radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes. (JP 3-85)

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 3-85)

electromagnetic attack

Division of electromagnetic 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 3-85)

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 3-85)

electromagnetic environment

The resulting product of the power and time distribution, in various frequency ranges, of the radiated or conducted electromagnetic emission levels encountered by a military force, system, or platform when performing its assigned mission in its intended operational environment. (JP 3-85)

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 3-85)

electromagnetic 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 electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-85)

electromagnetic interference

Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. (JP 3-85)

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 3-85)

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, with the intent of degrading or neutralizing the enemy's combat capability. (JP 3-85)

electromagnetic protection

Division of electromagnetic 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 3-85)

electromagnetic pulse

A strong burst of electromagnetic radiation caused by a nuclear explosion, energy weapon, or by natural phenomenon, that may couple with electrical or electronic systems to produce damaging current and voltage surges. (JP 3-85)

electromagnetic reconnaissance

The detection, location, identification, and evaluation of foreign electromagnetic radiations. (JP 3-85)

electromagnetic 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 3-85)

electromagnetic support

A division of electromagnetic 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 3-85)

electromagnetic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. (JP 3-85)

electromagnetic warfare reprogramming

The deliberate alteration or modification of electromagnetic 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 3-85)

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. Also called **EMCON**. (JP 3-85)

execution

The act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation (ADP 5-0)

frequency deconfliction

A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. (JP 3-85)

high-payoff target

A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. (JP 3-60)

line of sight

The unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another. (ATP 2-01.3)

military decision-making process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. Also called **MDMP.** (ADP 5-0)

preparation

Those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5-0)

planning

The art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about (ADP 5-0)

spectrum management operations

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

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

targeting

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

wartime reserve modes

Characteristics and operating procedures of sensor, communications, navigation aids, threat recognition, weapons, and countermeasures systems that will contribute to military effectiveness if unknown to or misunderstood by opposing commanders before they are used, but could be exploited or neutralized if known in advance. (JP 3-85)

This page intentionally left blank.

References

All websites accessed on 08 September 2022.

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. November 2022.

FM 1-02.1. *Operational Terms*. 9 March 2021.

FM 1-02.2. *Military Symbols*. 18 May 2022.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/doctrine.

Chairman of the Joint Chiefs of Staff publications are available online: https://www.jcs.mil/library/

CJCSM 3320.02E. *Joint Spectrum Interference Resolution (JSIR) Procedures*. 20 May 2022.

JP 3-0. *Joint Campaigns and Operations*. 18 June 2022.

JP 3-09.3. *Close Air Support*. 10 June 2019.

JP 3-60. *Joint Targeting*. 28 September 2018.

JP 3-85. *Joint Electromagnetic Spectrum Operations.* 22 May 2020.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-22. *Army Leadership and the Profession*. 31 July 2019.

ATP 1-02.1/MCRP 3-30B.1/NTTP 6-02.1/AFTTP 3-2.5. *Multi-Service Tactics, Techniques, and Procedures for Multi-Service Brevity Codes*. 28 May 2020.

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 01 March 2019.

ATP 3-09.32/MCRP 3-31.6/NTTP 3-09.2/AFTTP 3-2.6. *Multi-Service Tactics, Techniques, and Procedures for the Joint Application of Firepower (JFIRE)*. 18 October 2019.

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

ATP 5-19. *Risk Management*. 9 November 2021.

ATP 6-02.70. *Techniques for Spectrum Management Operations.* 16 October 2019.

FM 2-0. *Intelligence*. 6 July 2018.

FM 3-0. *Operations*. 1 October 2022

FM 3-12. *Cyberspace Operations and Electromagnetic Warfare*. 24 August 2021.

FM 6-0. *Commander and Staff Organization and Operations*. 16 May 2022.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.

OTHER PUBLICATIONS

Unless otherwise indicated, Institute of Electrical and Electronics Engineers publications are available on the IEEE Standards Association Website: https://standards.ieee.org.

IEEE C95.1-2019/Cor 2-2020 – *IEEE Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz – Corrigenda 2*. 24 September 2020.

IEEE C95.6-2002 – *IEEE Standard for Safety Levels with Respect to Human Exposure to Electromagnetic Fields, 0-3 kHz*. 23 October 2002.

IEEE C95.7-2014 – *IEEE Recommended Practice for Radio Frequency Safety Programs, 3 kHz to 300 GHz*. 8 August 2014.

WEBSITES

End-to-End Supportability System Website. https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/host-nation-spectrum-worldwide-database-online-hnswdo. (Copy and paste link into browser address bar.) (Requires DOD-approved certificate login and user account registration.)

Cyber Lessons and Best Practices Website. https://lwn.army.mil/web/cll/home. (Requires DOD-approved certificate login required.)

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, Department of the Army forms are available on the Army Publishing Directorate Website: https://armypubs.army.mil.

Department of the Army Form 2028. *Recommended Changes to Publications and Blank Forms.*

Unless otherwise indicated, Department of Defense forms are available online: https://www.esd.whs.mil/Directives/forms/.

Department of Defense Form 1494. *Application for Equipment Frequency Allocation*.

Department of Defense Form 1972. *Joint Tactical Air Strike Request.*

RECOMMENDED READINGS

CJCSI 3320.02F. *Joint Spectrum Interference Resolution*. 8 March 2013.

CJCSM 3320.01C. *Joint Electromagnetic Spectrum Management Operations in the Electromagnetic Operational Environment*. 14 December 2012, Directive current as of 5 February 2019.

This page intentionally left blank.

Index

Entries are by paragraph number.

Entries are by paragraph number.

ATP 3-12.3

30 January 2023

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2302300

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

This page intentionally left blank.

PIN: 205422-000