

CHAPTER 1

Overview

As the modern battlespace has become more sophisticated, military operations are executed in an increasingly complex electromagnetic environment. While military forces use the electromagnetic spectrum to detect and identify enemy forces and to perform communications, surveillance, and weapons systems operations, both military forces and civilians use the electromagnetic spectrum for communications, navigation, information gathering, processing, storing, and reporting. This overlapping usage of the electromagnetic spectrum complicates the military's use of its electronic equipment and the military's gathering and security of military information.

Successful military operations now greatly depend on control of the electromagnetic spectrum. The force that can deprive the enemy the use of the electromagnetic spectrum, exploit the enemy's use of the electromagnetic spectrum to obtain information for its own purposes, and control the electromagnetic spectrum will have an important advantage. During a conflict, all commanders attempt to dominate the electromagnetic spectrum by targeting, exploiting, disrupting, degrading, deceiving, damaging, or destroying their opponent's electronic systems that support their military operations. Electronic warfare (EW) includes "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy." (Joint Publication [JP] 1-02) Electronic warfare is an important part of a military commander's arsenal of weapons. It allows a commander to provide electronic warfare support (ES), electronic attack (EA), and electronic protection (EP).

ELECTRONIC WARFARE SUPPORT

Electronic warfare support (ES) is the "division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations." (JP 1-02) The ES intelligence collection effort—

- Is used in peace, crisis, and war, which contributes to the building of an EW/intelligence database for planning and operations.

- Provides an all weather, day/night, long-range information gathering capability.
- Exploits an enemy's electromagnetic emissions and may provide information on enemy capabilities and intentions.
- Is covert and passive.
- Is a nonintrusive method of intelligence collection.

Electronic warfare support systems provide immediate threat recognition and are a source of information for immediate decisions involving electronic attack, electronic protection, avoidance, targeting, and other tactical employments of forces. Electronic warfare support systems collect data and produce information or intelligence that can be used to—

- Corroborate other sources of information or intelligence.
- Direct EA operations.
- Initiate self-protection measures.
- Task weapon systems for physical destruction.
- Support EP efforts.
- Create or modify EW databases.
- Support information operations (IO) activities.

Electronic warfare support data can be used to produce signals intelligence (SIGINT), provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. Electronic warfare support and SIGINT both involve searching for, intercepting, identifying, and locating sources of intentional or unintentional radiated electromagnetic energy. The primary differences between the two are the detected information's intended use, the degree of analytical effort expended, the detail of information provided, and the timelines required. Electronic warfare support is conducted for immediate threat recognition and provides information required for immediate tactical decisions. Signals intelligence is used to gain information concerning the enemy, usually in response to an intelligence requirement. See MCWP 2-15.2, *Signals Intelligence*, for more information.

ELECTRONIC ATTACK

Electronic attack (EA) is “that division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires.” (JP 1-02)

Some common types of EA are spot, barrage, and sweep electromagnetic jamming. Electronic attack also includes various electromagnetic deception techniques such as false target or duplicate target generation.

Directed energy is “an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles.” (JP 1-02) A directed-energy weapon is a system that uses “directed energy primarily as a direct means to damage or destroy an enemy’s equipment, facilities, and personnel.” (JP 1-02)

Antiradiation weapons are weapons that use radiated energy emitted from the target as their mechanism for guiding onto a targeted emitter (e.g., high speed antiradiation missile system [HARM]).

ELECTRONIC PROTECTION

Electronic protection (EP) is “that division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.” (JP 1-02) In combat, electronic protection includes, but is not limited to, the application of good training and sound procedures for countering enemy electronic attack. United States forces (operators, users, and planners) must understand the enemy threat and the vulnerability of our electronic equipment to enemy EA efforts and ensure that appropriate actions are taken to safeguard our equipment from attack. To protect US forces, electronic protection must minimize an enemy’s opportunity for successful ES and EA operations against US forces; therefore, it is necessary to—

- Regularly brief the EW threat to force personnel.
- Provide training on appropriate EP responses.
- Ensure that electronic system capabilities are safeguarded during exercises, workups, and pre-crisis training.

The technical aspects of EP must be considered when equipment acquisition programs are initiated. Equipment should be designed to limit inherent vulnerabilities. Additionally, these programs must be reviewed when EA vulnerabilities are detected.

Electronic protection measures include the selection of a scheme of maneuver that will minimize friendly electronic emissions that the enemy can intercept or disrupt using his ES and EA capabilities. Electronic protection can be accomplished through numerous methods; for example, a simple scheme of

maneuver that can be executed with few or no emissions, by imposing radio silence or emission control (EMCON) procedures, by selecting avenues of approach that interposes terrain between friendly transmitters and enemy intercept stations. Electronic protection also includes measures to minimize the vulnerability of friendly receivers to enemy jamming; for example, reduced power, brevity of transmissions, and directional antennas.

SPECTRUM MANAGEMENT

Spectrum management plays a key role in the successful planning and execution of electronic warfare. Spectrum management includes “planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective of spectrum management is to enable electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference.” (JP 1-02) Electronic warfare staff personnel have a major role to perform in the dynamic management of the electromagnetic spectrum during operations. Electronic warfare management activities are coordinated and deconflicted through the electronic warfare coordination cell (EWCC). The EWCC’s primary mechanism for spectrum management is the restricted frequency list (RFL), which identifies friendly and enemy frequencies that cannot be jammed for various reasons. For further guidance on electromagnetic spectrum use, see Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3320.01, *Electromagnetic Spectrum Use in Joint Military Operations*. For specific guidance on reporting and controlling electromagnetic interference, see CJCSI 3320.02A, *Joint Spectrum Interference Resolution (JSIR)*.