



ELECTROMAGNETIC WARFARE DIVISIONS

Last Updated: 30 July 2019

Electromagnetic warfare (EW) consists of three divisions: electromagnetic attack–(EA), electromagnetic warfare support (ES), and electromagnetic protection (EP). All three contribute to operational success across all domains. Capabilities inherent to the EW divisions can be used for both offensive and defensive purposes and are coordinated through electromagnetic battle management (EMBM).

Electromagnetic Attack

“EA is the division of EW involving the use of electromagnetic (EM) energy, directed energy (DE), or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy operational capability”. EA prevents or reduces an enemy’s use of the electromagnetic spectrum (EMS) through denial, degradation, disruption, deception, and destruction for offensive or defensive purposes.

- ✦ **Offensive EA** is generally employed at the request and onset of friendly force engagement of the enemy and, in many cases, suppress a threat for a limited period. Examples include active applications such as EM jamming, meaconing and intrusion; expendable decoys; anti-radiation missiles; directed energy (DE) and high-energy weapons including lasers, radio-frequency weapons, high-power microwave, and electromagnetic pulse (EMP); delivery of electromagnetic cyberspace attacks; and navigation warfare.
- ✦ **Defensive EA** activities use the EMS to protect personnel, facilities, capabilities, and equipment. Examples include employing self-protection and force protection measures such as flares, chaff, low-observable technologies, towed decoys, protection jammers, and DE infrared (IR) countermeasures.

Electromagnetic Warfare Support

“ES is the division of EW involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of threat recognition, targeting, planning, and conduct of future operations” ([JP 3-85](#)). Commanders, aircrews, and operators use ES to provide near real time information to supplement information from other intelligence sources. Additionally, ES information can be correlated with other [intelligence, surveillance, and reconnaissance](#) (ISR) information to provide a more accurate picture of the [electromagnetic operational environment](#) and therefore a better understanding of the battlespace. This information can be developed into an electromagnetic order of battle (EOB) for situational awareness and may be used to develop new countermeasures. Development of these countermeasures is supported by updates to the Electronic Warfare Integrated Reprogramming (EWIR) database. The EWIR process enables reprogramming of EW systems to provide operational commanders with a timely and accurate means to respond to changes in the EMS and maintain the capability to effectively detect, classify, and counter enemy threats. The relationship between ES and [signals intelligence](#) (SIGINT), which includes [electromagnetic intelligence](#) and [communications intelligence](#), is close because they share common functions of search, interception, identification, location, and exploitation of electromagnetic radiation. The distinction lies in the type and use of information, and who has tasking authority. ES resources are tasked by or under direct control of operational commanders. The operational commander may have authority to task national SIGINT assets to provide ES or may have direct [operational control](#) over tactical resources capable of providing ES. In either case, ES is distinguished by the fact that the operational commander determines aspects of resource configuration required to provide ES that meets immediate operational requirements. SIGINT is tasked by national authorities. The passive nature of ES allows it to be effectively employed during peacetime.

Electromagnetic Protection

“EP includes the actions taken to protect personnel, facilities, and equipment from any effects of friendly, neutral, or enemy use of the EMS, as well as naturally-occurring phenomena that degrade, neutralize, or destroy friendly combat capability” ([JP 3-85](#)). Examples of EP include frequency agility, changing pulse repetition frequency, emission control (EMCON), and EM hardening (to include EMP hardening). Integration of EP and other security measures can prevent enemy detection, denial, disruption, deception, degradation or destruction. Friendly force reliance on advanced technology demands comprehensive EP safeguards and considerations.

¹⁷ For the reason these terms have been changed from “electronic” to “electromagnetic,” see “Note on the Terms ‘Electronic’ vs. ‘Electromagnetic’” in, [“Introduction to Electromagnetic Spectrum Operations,”](#) this publication.

Proper frequency management is a key element in preventing adverse effects (e.g., jamming friendly forces) from friendly actions. Much of the success of EP occurs during the design and acquisition of equipment. EMCON is a passive application of EP.

EW Effects

EW involves the use of EM energy and DE to control the EMS or to attack the enemy. Military forces depend on the EMS for applications that include: intelligence; communication; positioning, navigation, and timing; sensing; [command and control](#) (C2); attack; ranging; data transmission; and information and storage. Control of the EMS is critical to the success of military operations.

EW has offensive and defensive aspects that work in a “move-countermove” fashion. Often, these aspects are used simultaneously and synergistically. In the same way air, space, and cyberspace superiority allows friendly forces the freedom from attack, freedom to maneuver, and freedom to attack, the properly coordinated use of EW allows friendly forces to use the EMS. As an example, the offensive denial of a C2 network by EM jamming disrupts the adversary’s ability to control forces that would otherwise engage a friendly strike force. The proper use of EP allows friendly radar and communications to continue operating in the presence of enemy jamming. The proper employment of EW involves various applications of control to achieve **detection, denial, deception, disruption, degradation, exploitation, protection, and destruction.**

Detection

Detection is identification of potential enemy EM²⁰ emissions through use of ES measures ([JP 3-85](#)). It involves assessing the electromagnetic environment (EME) to include radar and radio frequencies; electro-optics and lasers; and the IR spectrums using active and passive means. It is the first step in EW because effective mapping of the EME is essential to develop an accurate EOB. The EOB is

RC-135 V/W RIVET JOINT



The Rivet Joint provides electromagnetic warfare support to detect, identify, locate and disseminate enemy integrated air defense system structure.

²⁰ For the reason these terms have been changed from “electronic” to “electromagnetic,” see “Note on the Terms ‘Electronic’ vs. ‘Electromagnetic’” in, [“Introduction to Electromagnetic Spectrum Operations,”](#) this publication.

critical for EW decision making and for using the EMS to meet mission objectives. The various means of detection include on-board receivers; space-based systems; unmanned aircraft; [human intelligence](#); and other ISR systems. Detection supports all divisions of EW and enables the avoidance of known hostile systems. When avoidance is not possible, it may become necessary to deny, deceive, disrupt, degrade, or destroy the enemy's electromagnetic systems or capabilities.

Denial

Denial is defined as the prevention of access to or use of systems or services

([JP 3-85](#)). In an EW context, it is the prevention of an adversary from using EMS-dependent systems (e.g., communications equipment, radar) by affecting a particular portion of the EMS in a specific geographical area for a specific period. Denial involves controlling the information an enemy or

adversary receives, preventing the acquisition of accurate information about friendly forces. Denial is accomplished through EA; expendable countermeasures; destructive measures; network applications; tactics, techniques, and procedures; and EMCON.

Deception

Deception is measures designed to mislead the adversary by manipulation, distortion, or falsification of evidence to induce the adversary to react in a manner prejudicial to the adversary's interests ([JP 3-85](#)). Through the use of the EMS, EW manipulates the decision-making loop of the opposition, making it difficult to distinguish between reality and the perception of reality. If an adversary relies on EM sensors to gather intelligence, deceptive information can be channeled into these systems to mislead and confuse. Deception efforts should simulate as many adversary information sources as possible to create the desired effects. Multi-sensor deception can increase the adversary's confidence about the "plausibility" of the deception story.

Deception efforts are coordinated with the military deception officer and considered during development of a deception plan, the information operations plan, and the overall operations or campaign plans. Operational security is critical to an effective deception

EC-130H Compass Call



The Compass Call employs electromagnetic attack to disrupt or deny enemy C2

plan.

EM deception as it applies to EW is the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of EM energy in a manner intended to convey misleading information to an enemy or to enemy EM-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. There are three types of EM deception: manipulative, simulative, and imitative.

Counter Communications System



The Counter Communications System employs electromagnetic attack to disrupt or deny enemy satellite communications.

★ **Manipulative.** EM

deception involves an action to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces. EM manipulation may involve low observable technology used to reduce radar returns, simulation of threat signatures from nonlethal platforms, and communication and non-communication signals used to splinter displays or convey threat activity. Manipulative electromagnetic deception can be used to cause the enemy to misdirect ES and EA assets and, therefore, cause fewer problems with friendly communications. In this application it is an EP technique.

★ **Simulative.** EM deception is action to simulate friendly, notional, or actual capabilities to mislead hostile forces. Simulative EM may involve using airborne expendables to simulate false targets or transmitting deceptive EA techniques to mask the true location of a target.

★ **Imitative.** EM deception introduces EM energy into enemy systems that imitate enemy emissions. Any enemy receiver can be the target of imitative EM deception. This might be used to screen friendly operations through the use of repeater jamming techniques.

In general, EW deception planning determines how to use EM means to mislead the adversary and create an advantage for friendly forces.

Disruption

Disruption is to interrupt the operation of adversary EMS-dependent systems (JP 3-85). Effective disruption limits adversary capabilities by degrading or interfering with the adversary's use of the EMS to limit the enemy's combat capabilities.

Disruption is achieved by using EM jamming, EM deception, EM intrusion, and physical attack. These will enhance attacks against hostile forces and act as a force multiplier.

Degradation

Degradation is to reduce the effectiveness or efficiency of adversary EMS-dependent systems (JP 3-85). Employing EM jamming, EM deception, and EM intrusion is intended to degrade adversary systems thus confusing or delaying actions of adversary operators.

Exploitation

Exploitation is taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes (JP 3-85). In the context of EW, it entails using adversary EM radiation for friendly advantage. EM energy may provide tactical, operational, and strategic situational awareness of the EMOE, and is used to develop an EOB. Data transmissions produce EM energy for exploitation by signals intelligence provide targeting for EM or destructive attacks, and develop awareness of operational trends.

Protection

Protection is the preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given

Miniature Air-Launched Decoy (MALD)



The MALD and MALD-Jammer variant can achieve a variety of effects employing electromagnetic attack.

operational area ([JP 3-85](#)). This includes ensuring that EW activities do not electromagnetically destroy or degrade friendly intelligence sensors; communications systems; positioning, navigation, and timing capabilities; and other EMS-dependent systems and capabilities. Protection is achieved by component hardening, EMCON, EMS management and deconfliction, and other means to counterattack and defeat adversary attempts to control the EMS.

Destruction

Destruction is to make the condition of a target so damaged that it can neither function as intended nor be restored to a usable condition ([JP 3-85](#)). When used in the EW context, destruction is the use of EA to eliminate targeted adversary personnel, facilities, or equipment. Target tracking radars and C2 nodes may be high value targets because their destruction seriously hampers an adversary's effectiveness. Destruction requires determining the exact location of the target. This location may be determined through the effective application of ES measures. Adversary EM systems can be destroyed by a variety of weapons and techniques ranging from bombardment with conventional munitions, high-speed antiradiation missiles, intense radiation, and high-energy particle beam overloading. Destruction of EM capabilities has the most sustained effects and may be the best means of denying adversary use of the EMS. The duration of the destructive effects depends on an adversary's reconstitution capability.
