



CURTIS E. LEMAY CENTER

FOR DOCTRINE DEVELOPMENT AND EDUCATION



ANNEX 3-51 ELECTRONIC WARFARE

INTRODUCTION TO ELECTRONIC WARFARE

Last Updated: 10 Oct 2014

Electronic Warfare (EW) is waged to secure and maintain freedom of action in the electromagnetic spectrum (EMS). Military forces rely heavily on the EMS to sense, communicate, strike, and dominate offensively and defensively across all warfighting domains. EW is essential for protecting friendly operations and denying adversary operations within the EMS.

The term EW refers to military action involving the use of electromagnetic (EM) and directed energy (DE) to control the EMS or to attack the enemy. This is not limited to radio or radar frequencies but includes infrared (IR), visible, ultraviolet, and any other free-space electromagnetic radiation. EW is critical to air, space, and cyberspace forces gaining freedom of action within contested environments.

EW consist of three divisions: electronic attack (EA), electronic warfare support (ES), and electronic protection (EP). All three contribute to the success of air, space, and cyberspace operations. Proper employment of EW capabilities produces the effects of detection, denial, deception, disruption, degradation, exploitation, destruction, and protection. Capabilities inherent to the EW divisions can be used for both offensive and defensive purposes and are coordinated through electromagnetic battle management (EMBM).

EW operations have developed over time to exploit the opportunities and vulnerabilities inherent in the physics of EM energy. The principal activities used in EW include the following: countermeasures, EMBM, EM compatibility; EM deception; EM hardening, EM interference resolution, EM intrusion, EM jamming, electromagnetic pulse (EMP), EMS control, electronic intelligence collection, electronic masking, electronic probing, electronic reconnaissance, electronics security, EW reprogramming, emission control, joint electromagnetic spectrum operations (JEMSO), joint electromagnetic spectrum management operations (JEMSMO), low-observability/stealth, meaconing, navigation warfare (NAVWAR), precision geolocation, and wartime reserve modes.

Employed across the range of military operations (ROMO), EW can enhance the ability of operational commanders to achieve an advantage over adversaries. Commanders rely on the EMS for intelligence; communication; positioning, navigation, and timing (PNT); sensing; command and control (C2); attack; ranging; data transmission; and information and storage. Therefore, control of the EMS is essential to the success of

military operations and is applicable at all levels of conflict. EW considerations must be fully integrated into operations in order to be effective.

Additionally, the scope of these operations is global and extends from the earth's surface into space. **Unfettered access to selected portions of the EMS is critical for weapon system**

effectiveness and protection of critical assets. EW is a force multiplier that

can create effects throughout ROMO. When EW actions are properly integrated with other military capabilities, synergistic effects may be achieved, losses are minimized, and effectiveness is enhanced.

Friendly forces must prepare to operate in highly contested and nonpermissive [electromagnetic environments](#) (EME) and understand EW's potential to increase force effectiveness. This may be aggravated by both intentional and unintentional emissions from friendly, neutral, and enemy forces, as well as the natural environment. EM interference is caused by EMP; hazards of EM radiation to personnel, ordnance, and volatile materials; and natural phenomena effects of sunspots, lightning, and precipitation static. For example, clouds, sun glint, ground reflections, moisture, and dust can degrade performance of systems operating in the IR and optical frequencies. Atmospheric conditions can distort radar signals causing track errors, extending the detection ranges or creating "holes" in radar coverage. Rain and frozen precipitation also affects microwave transmissions by attenuating and scattering the signal. Even disturbances on the sun and in the upper atmosphere can create radio frequency interference (RFI) in radars and satellite links, impact high-frequency radio and satellite communications (SATCOM), and degrade Global Positioning System (GPS) accuracy. Planners using forecasts of terrestrial and space environmental conditions can exploit or mitigate these effects to their advantage over an adversary.

Air Force electronic warfare operations embody the art and science of employing military capabilities to achieve objectives through control of the EMS. EW exploits weaknesses in an adversary's ability to operate and applies force against the adversary's offensive, defensive, and supporting capabilities across the EMS. An effective EW strategy requires an integrated mix of passive, disruptive, and destructive

Freedom of action within the electromagnetic spectrum (EMS)



Air Force Joint Terminal Attack Controllers rely on access to the EMS to communicate with aircrews

systems to protect friendly weapon systems, components, and communications-electronics systems from the enemy's threat systems.

Electronic warfare is intimately tied to advances in technology. Technology enabled the utilization of the EMS to communicate through radios as a practical standard in the early 1900s, and developed in aviation to enable navigation in all conditions. The advent of radar and its proven effectiveness early in World War II started the “move–countermove” developments of radar, sensors, jammers, and countermeasures. Shortly after the development of radar, chaff was developed as a countermeasure. Concurrently, airborne jammers were developed to minimize the effectiveness of radar. The cold war witnessed the development of radar with effective electronic protection. Further EA developments were designed to defeat these protective measures. Conflicts in Vietnam and the Middle East provided deadly reminders of the necessity for effective EW against advanced threats and of the intense effort required to counter these threats. Current technology has given rise to new enemy capabilities, which includes the use of microwave and millimeter wave technologies, lasers, electro-optics, digital signal processing, and programmable and adaptable modes of operation. It also includes the use of IR, visible, and ultraviolet frequencies and that part of the electromagnetic spectrum where [directed energy](#) (DE) weapons might function. More recently EW responded to emerging threats by countering improvised explosive devices (IED). Anticipating future technological developments is vital for EW and the survivability of friendly forces.

Electronic Warfare in Information and Cyberspace Operations

EW's relationship to [Information Operations](#) (IO) is as an [information-related capability](#) (IRC). IO does not “own” individual capabilities but rather employs IRCs in an integrated manner to create effects contributing towards a specified end-state. EW creates effects throughout the ROMO, and across all domains. Therefore, those planning and executing EW operations must be aware of the intent of other IRCs such as [military deception](#) (MILDEC), [military information support operations](#) (MISO) and [operations security](#) (OPSEC) to lessen the chance of compromise. While IO's primary focus is on the cognitive dimension of the information environment and EW's primary focus is to achieve objectives across the physical domains. EW's integration with other IRCs through IO is vital to ensure the capabilities complement rather than conflict with each other.

Cyberspace operations require both wired and wireless links to transport information. Any wireless link requires access to the EMS and therefore requires coordination and synchronization between EW and Air Force information network operations in order to maximize and potentially achieve synergistic effects. For more on [electronic warfare's role in cyberspace operations](#) see JP 3-13.1, *Electronic Warfare*.

Directed Energy in Electronic Warfare

Directed energy (DE) is an umbrella term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic

particles. [Directed-energy warfare](#) (DEW) is military action involving the use of DE weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the EMS through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and to retain friendly use of the EMS. Applications of DE include: laser, radio frequency, and particle beam. DE can be applied to conduct EA, ES, or EP. For example, a laser designed to blind or disrupt optical sensors is EA. A warning receiver designed to detect and analyze a laser signal is ES. A visor or goggle designed to filter out the harmful wavelength of laser light is EP.

Operational Requirements

The level of EW involvement will always depend on the specific requirements of the mission. Electronic warfare is task oriented. Operational objectives, the tactical situation, the effectiveness and availability of combat systems, and the prevailing domestic and international political climate determine the appropriate application of EW capabilities. EW planning is not just the automatic addition of a specific jamming pod or escort package for a mission. Each task may require a specific EW response in order to achieve a desired objective. Commanders and their staffs must consider the threat and assets available to support EW objectives.

Intelligence, Surveillance, and Reconnaissance

A critical enabler of successful military operations is a thorough knowledge of enemy capabilities derived from near-real-time information, focused for the operational commander, as well as long term operational, scientific, and technical intelligence information gathered over a period of time. Knowledge of the enemy's projected military capabilities is required to avoid surprise. Accurate intelligence is needed to gauge the intent of an adversary, and this intelligence must be transmitted to the users in a timely manner.

Commanders must know their own EW capabilities and those of potential adversaries. Each year, new technology weapons systems are fielded in increasing numbers. Adversaries recognize US potential vulnerabilities of EMS dependent systems. Seeking to take advantage of this fact, some potential adversaries are organized to attack our critical weapons systems control functions and associated communications nodes. Many countries have been purchasing modern and capable weapons systems from a variety of sources. In addition, terrorists may acquire highly sophisticated and dangerous weapons. To counter these possibilities, commanders and their staff must become well versed in the development and employment of weapons systems and the EW capabilities of all possible adversaries.

Numerous intelligence, surveillance and reconnaissance systems and methods are used to collect the data needed to build the various electronic databases required to effectively employ EW. Advanced processing and exploitation systems, with man-in-the-loop management and oversight, transform the data into usable intelligence, while survivable communications grids bring the intelligence to the operational user. As in all

military operations, defining and managing intelligence requirements are critical to EW. Since many collection methods require EMS access, ISR must be coordinated, deconflicted, and synchronized with other EW operations through EMBM and joint [electromagnetic spectrum management operations](#) (JEMSMO) processes.
