INTRODUCTION TO ELECTROMAGNETIC WARFARE

Last Updated: 30 July 2019

Electromagnetic warfare (EW)[8] is waged to secure and maintain freedom of action in the electromagnetic spectrum (EMS). Military forces and other entities are dependent 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) energy and directed energy (DE) to control the EMS or to attack the enemy**" (Joint Publication [JP] 3-85, *Joint Electromagnetic Spectrum Operations*). This is not limited to radio or radar frequencies but includes infrared (IR), visible, ultraviolet, and any other free-space electromagnetic radiation such as wireless cyberspace applications. EW is critical in gaining freedom of action within contested and congested environments.

EW consists of three divisions: electromagnetic attack[9] (EA), electromagnetic warfare support[10] (ES), and electromagnetic protection[11] (EP). All three contribute to operational success across the operational environment. Proper employment of EW capabilities produces the effects of detection, denial, deception, disruption, degradation, exploitation, destruction, and protection. Capabilities inherent in 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, EM intelligence collection, EM masking, EM probing, EM reconnaissance, EM security, EW reprogramming, emission control,

[8] 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.

[9] Ibid.

[10] Ibid.

[11] Ibid.

low-observability and stealth, meaconing, navigation warfare, precision geolocation, and wartime reserve modes. Joint doctrine provides collective terms encompassing the EW operations described above with spectrum management. These terms are joint EMS operations and joint electromagnetic spectrum management operations (JEMSMO). For more information on these terms.

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; 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 should be fully integrated into operations in order to be effective. Additionally, the scope of these operations is global and extends from below 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 capabilities, synergistic effects may be achieved, minimizing losses and enhancing effectiveness.

Freedom of action within the electromagnetic spectrum

Air Force joint terminal attack controllers rely on access to the EMS to communicate with aircrews.

Air Force electromagnetic 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 systems to protect friendly weapon systems, components, and communications systems from the enemy's threat systems.

Electromagnetic warfare is tied closely 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 EP. 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 EMS where DE weapons might function. More recently, EW responded to emerging threats by countering improvised explosive devices and satellite communications. Anticipating future technological developments is vital for EW and the survivability of friendly forces.

Electromagnetic 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. Therefore, those planning and executing EW operations should be aware of the intent of other IRCs such as military deception, military information support operations and operations security to lessen the chance of compromise. 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 electromagnetic warfare's role in cyberspace operations see JP 3-85.

Directed Energy in Electromagnetic Warfare

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 is military action involving the use of DE weapons, devices, and countermeasures to incapacitate, cause direct damage or destruction of enemy equipment, facilities, and personnel, and/or to determine, exploit, reduce, or prevent hostile use of the EMS through damage, destruction, and disruption" (JP 3-85). 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. EW 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 create a desired effect. Commanders and their staffs must consider the threat and assets available to support EW objectives.

Intelligence, Surveillance, and Reconnaissance (ISR)

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. Intelligence, surveillance, and reconnaissance are critical force multipliers when applying lethal and nonlethal effects of airborne, space, and cyberspace EW.

Exploitation of the EMS

Most modern military systems, from support systems to weapons systems, exploit the electromagnetic operational environment (EMOE) to function optimally by sensing the EME and/or using EM energy to communicate through it. Sensing systems support intelligence collections, situational awareness, targeting, etc. EMS sensors can be active (e.g., air-to-air radars, laser target designators) or passive (e.g., radar warning receivers, IR weapons seekers). Communications systems support Air Force C2, weapons control links, information dissemination, etc.

Commanders should know their own EW capabilities and those of potential adversaries. New technologically advanced weapons systems are being fielded in increasing numbers. Adversaries recognize potential vulnerabilities of US EMS-dependent systems. Seeking to take advantage of this fact, some potential adversaries have 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 staffs must become well versed in the development and employment of weapons systems and the EW capabilities, to include navigation warfare, of all possible adversaries. Numerous

ISR systems and methods are used to collect the data needed to build the various electromagnetic 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 operations should be coordinated, deconflicted, and synchronized with EW operations through EMBM and JEMSMO processes.
