

CATALOG OF DOCTRINE TOPICS

Introduction to Electronic Warfare Operations

Electronic Warfare Divisions

Electronic Warfare Effects

Electronic Warfare Organization

Planning Electronic Warfare Operations

Electronic Warfare Employment



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.



ANNEX 3-51 ELECTRONIC WARFARE

ELECTRONIC WARFARE DIVISIONS

Last Updated: 10 Oct 2014

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. Capabilities inherent to the EW divisions can be used for both offensive and defensive purposes and are coordinated through [electromagnetic battle management](#) (EMBM).

Electronic Attack

EA is the division of EW involving the use of electromagnetic (EM), 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). It can be accomplished through detection, denial, disruption, deception, and destruction. EA includes lethal attack with assets like high-speed antiradiation missiles (HARMs); active applications such as decoys (flares or chaff), EM jamming, and expendable miniature jamming decoys; and employs EM or DE weapons (lasers, radio frequency weapons, particle beams, etc.).

EM jamming and the [suppression of enemy air defenses](#) (SEAD) are applications of EA:

- ★ **Electromagnetic Jamming.** EM jamming is the deliberate radiation, reradiation, or reflection of EM energy for the purpose of preventing or reducing an enemy's effective use of the EMS, with the intent of degrading or neutralizing the enemy's combat capability. Early Air Force EW efforts were primarily directed toward electronically jamming hostile radars to hide the number and location of friendly aircraft and to degrade the accuracy of radar-controlled weapons. Currently, jamming enemy sensor systems can limit enemy access to information on friendly force movements and composition and cause confusion. Jamming can degrade the enemy's decision making and implementation process when applied against command and control systems. An adversary heavily dependent on centralized control and execution for force employment presents an opportunity for EA.
- ★ **Suppression of Enemy Air Defenses.** SEAD is that activity which neutralizes, destroys, or temporarily degrades surface-based enemy air defenses by

destructive and/or disruptive means. The goal of SEAD operations is to provide a favorable situation in which friendly tactical forces can perform their missions effectively without interference from enemy air defenses. In Air Force doctrine, SEAD is not part of EW, but it is a broad term that may include the use of EW. In Air Force doctrine, SEAD is part of the counterair framework and directly contributes to offensive counterair and obtaining air superiority. This may involve using EM radiation to neutralize, degrade, disrupt, delay, or destroy elements of an enemy's [integrated air defense system](#) (IADS). During hostilities, enemy IADS will probably challenge friendly air operations. EW systems tasked to perform SEAD may be employed to locate and degrade, disrupt, neutralize, or destroy airborne and ground-based emitters. Typically, SEAD targets include radars for early warning/ground-controlled intercept (EW/GCI), acquisition (ACQ), surface-to-air missiles (SAMs), and antiaircraft artillery (AAA). Many Air Force functions can be enhanced with the employment of SEAD operations.

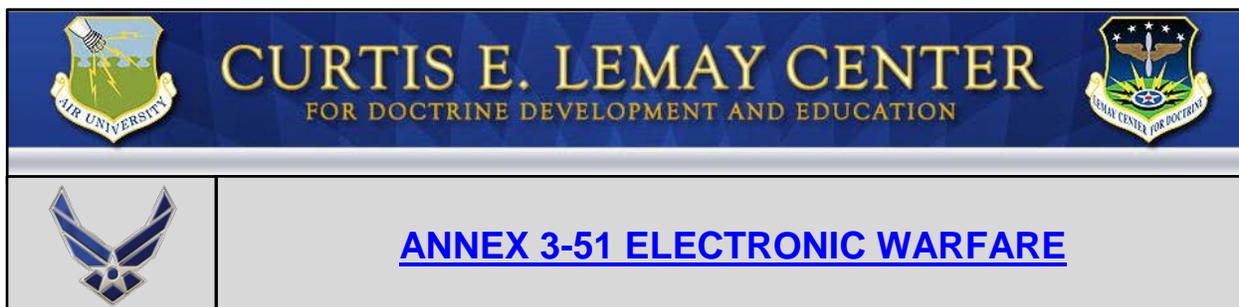
Electronic Warfare Support

ES responds to taskings to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of threat recognition. 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 electronic order of battle for situational awareness and may be used to develop new countermeasures. The relationship between ES and [signals intelligence](#) (SIGINT), which includes [electronic intelligence](#) (ELINT) and [communications intelligence](#) (COMINT), is closely related 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.¹

¹ See [Joint Publication 3-13.1, Electronic Warfare](#), and Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.03C, *Joint Electronic Warfare Policy*, for a more in-depth discussion of the relationship and distinctions between ES and SIGINT.

Electronic 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. Examples of EP include frequency agility, changing pulse repetition frequency, emission control (EMCON), and low observable technologies. Integration of EP and other security measures can prevent enemy detection, denial, disruption, deception, or destruction. Friendly force reliance on advanced technology demands comprehensive EP safeguards and considerations. Proper frequency management is a key element in preventing adverse effects (i.e., jamming friendly forces) by friendly forces. Much of the success of EP occurs during the design and acquisition of equipment. EMCON and low observable technologies are passive applications of EP.



ELECTRONIC WARFARE EFFECTS

Last Updated: 10 Oct 2014

Electronic Warfare (EW) involves the use of electromagnetic energy (EM) and directed energy (DE) to control the **electromagnetic spectrum (EMS)** or the attack the enemy. Military forces depend on the EMS for applications that include: intelligence; communication; positioning, navigation, and timing (PNT); sensing; **command and control (C2)**; attack; ranging; data transmission; and information and storage. Control of the EMS, while denying the adversary the same, is critical to the success of military operations.

Control

To control is to dominate the EMS, directly or indirectly, so that friendly forces may exploit or attack the adversary and protect themselves from exploitation or attack. Control is accomplished through applications of **electronic attack (EA)**, **electronic warfare support (ES)**, and **electronic protection (EP)**. EA limits adversary use of the EMS; EP secures use of the EMS for friendly forces; and ES enables commanders' ability to identify and monitor actions in the EMS throughout the operational environment.

While control of the EMS through the proper application of EW is advantageous, when improperly used without coordination may result in EM interference or EM fratricide, and consequently unintended effects like disruption of friendly cyberspace/information networks. Additionally, an ill-timed jamming package may highlight an otherwise unseen force or deny the use of a frequency by friendly forces. An incorrect or wrongly interpreted radar warning receiver (RWR) indication may cause an inappropriate action to be taken. **Electromagnetic battle management (EMBM)** ensures effective control of the **electromagnetic operational environment (EMOE)**. EMBM is the dynamic monitoring, assessing, planning and directing of joint electromagnetic spectrum operations (JEMSO) in support of the commander's scheme of maneuver. EMBM will proactively harness multiple platforms and diverse capabilities into a networked and cohesive sensor/decision/target/engagement system, as well as protect friendly use of the EMS while strategically denying benefits to the adversary.¹

¹ For additional information JEMSO and joint electromagnetic spectrum management operations (JEMSMO) see [JP 3-13.1, Electronic Warfare](#), and [JP 6-01, Joint Electromagnetic Spectrum 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 that air superiority allows friendly forces the freedom from attack, freedom to maneuver, and freedom to attack, the proper coordinated use of EW allows friendly forces to use the EMS. As examples, 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.

EW is not limited to manned airborne application; it is also applied from land, sea, space, and cyberspace. 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 EM emissions through use of ES measures. It involves assessing the electromagnetic environment (EME) to include radar/radio frequency, electro-optics/laser, and the infrared (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 electronic order of battle (EOB). The EOB is 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 (UA), [human intelligence](#) (HUMINT), and other [intelligence, surveillance, and reconnaissance](#) (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, or destroy the enemy’s electronic systems.

EC-130H Compass Call



The Compass Call employs electronic attack to disrupt or deny enemy command and control communications

Denial

Denial is defined as the prevention of access to or use of systems or services. 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 of time. Denial involves controlling the information an enemy or adversary receives, preventing the acquisition of accurate information about friendly forces. Denial is accomplished through EA techniques (degradation, disruption, or deception); expendable countermeasures; destructive measures; network applications; tactics, techniques, and procedures (TTP); and/or emission control (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. 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 must stimulate as many adversary information sources as possible to achieve the desired objective. Multisensor 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 an overall deception plan, IO plan, and the overall operations or campaign plans. Operational security is critical to an effective deception plan.

EM deception as it applies to EW is the deliberate radiation, reradiation, 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. Deception jammers/transmitters can place false targets on the enemy radar's scope, or cause the enemy radar to assess incorrect target speed, range, or azimuth. Such jammers/transmitters operate by receiving the pulse of energy from the radar, amplifying it, delaying or multiplying it, and reradiating the altered signal back to the enemy's transmitting radar.

There are three types of EM deception: manipulative, simulative, and imitative.

- ★ **Manipulative** EM deception involves an action to eliminate revealing or to convey misleading EM telltale indicators that may be used by hostile forces. An example of this is to mislead the enemy by transmitting a simulated unique system signature from a nonlethal platform, thereby allowing the enemy sensors to receive and catalog those systems as actual threats in the area. Low observable technology is a passive form of manipulative EM deception. By passively manipulating or denying the threat radar from receiving proper return pulses, it alters the perceived size or presence of an air vehicle. EM deception can use communication or non-communication signals to convey indicators that

mislead the enemy. It can also cause the enemy to splinter their intelligence and EW efforts to the point that they will lose their effectiveness. 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. Examples of simulative EM detection include the use of chaff to simulate false targets so that the enemy has the impression of a larger strike package or the use of a jammer to transmit a deceptive technique that misleads an adversary's target tracking radar so that it cannot find the true location of its target.

Miniature Air-Launched Decoy (MALD)



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

★ **Imitative** EM deception introduces EM energy into enemy systems that imitate enemy emissions. Any enemy receiver can be the target of imitative electromagnetic deception. This might be used to screen friendly operations. An example is the use of a repeater jamming technique that imitates enemy radar pulses. These pulses, when received by the tracking radar, input incorrect target information into the enemy's system.

Other examples include deception involving manipulation of IR signatures; radar deception consisting of reradiation of signals through the use of reflectors, transponders, or repeaters; and optical deception by manipulation of the optical region of the EMS through the use of aerosols, mists, etc. These techniques may be employed

individually or in combination. 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. 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 destruction. 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. Employing EM jamming, EM deception, and/or EM intrusion is intended to degrade adversary systems thus confusing or delaying actions of adversary operators.

Exploitation

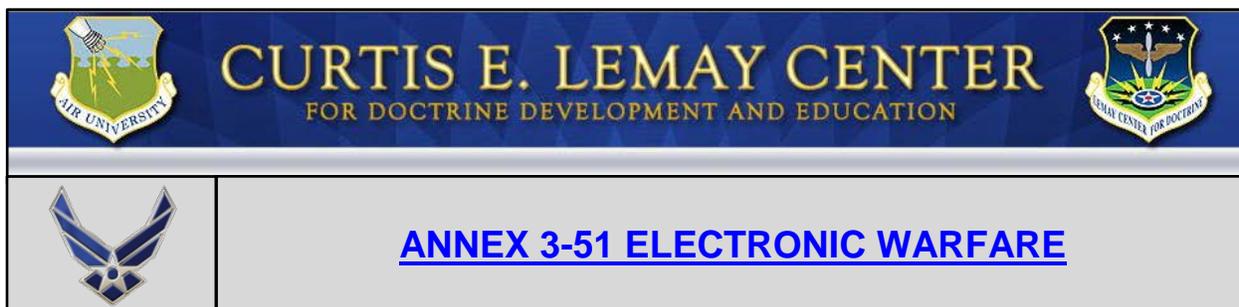
Exploitation is using adversary EM radiation for friendly advantage. EM energy may provide tactical, operational, and strategic situational awareness of the EMOE, and is used to develop an EOB. Additionally, EM energy is used to identify, recognize, characterize, locate, and track EM radiation sources to support current and future operations. Data transmissions produce EM energy for exploitation by [signals intelligence](#) (SIGINT), 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 operational area. 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. Spectrum management and EW work collaboratively to accomplish active EMS deconfliction, which includes the capabilities to detect, characterize, geolocate, and mitigate EMI that affects operations. Additionally, structures such as a [joint force commander's electronic warfare staff](#) (JCEWS) or the [Commander, Air Force Forces](#), (COMAFFOR) [electronic warfare coordination cell](#) (EWCC) enhance operational-level EP through coordination and integration of EW into the overall scheme of maneuver.

Destruction

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 to 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' capability to reconstitute. An example of EW application of destruction would be the use of a high-speed antiradiation missile (HARM) against enemy radars.



ELECTRONIC WARFARE ORGANIZATION

Last Updated: 10 Oct 2014

[Electronic warfare](#) (EW) forces are task organized on the doctrinal tenet of centralized control and decentralized execution. Air Force EW is normally controlled at the component level and executed at the lowest level providing responsiveness to the [Commander, Air Force Forces](#) (COMAFFOR). Appropriate expertise should be available at all levels of [command and control](#) (C2) where EW coordination, planning, and execution occur.

When required, the COMAFFOR may form an electronic warfare coordination cell (EWCC). The EWCC plans, manages, and assesses air component EW operations and also ensures effective coordination and synchronization with other joint force components. The EWCC is responsible for ensuring control and access to the [electromagnetic spectrum](#) (EMS) through coordination of [electronic attack](#) (EA), [electronic warfare support](#) (ES) and [electronic protection](#) (EP). Synchronization of EW activities occurs through [electromagnetic battle management](#) (EMBM) to enable freedom of action.

The EWCC is normally organized into plans and operations divisions led by experienced electronic warfare officers. EW uses EM energy and [directed energy](#) (DE) to control the EMS and create effects contributing to objectives associated with a variety of mission types that include but is not limited to: counterair; counterland; cyberspace operations; information operations; and intelligence, surveillance, and reconnaissance (ISR). Therefore, to promote unity of effort and prevent electromagnetic (EM) fratricide, the EWCC should integrate across [air operations center](#) (AOC) divisions.¹

EW and COMAFFOR Headquarters Organization

The COMAFFOR headquarters is usually comprised of normal staff directorates, A-1 through A-6, as well as a special staff. The core of the EW function is located in the A-3 as part of the AOC and its IO cell. The entire IO operation must be integrated with A-2/3/5/6. The EW personnel will provide these functions:

¹ For more on EW organization and processes within the Air Operations Center see [JP 3-13.1, *Electronic Warfare*](#); and [AFTTP 3-3.AOC, *Operational Employment Air Operations Center*](#).

Intelligence Surveillance and Reconnaissance (A-2)

- ✦ Provide to the ISR staff the A-2 related EW objectives, intent, and plans.
- ✦ Coordinate EW ISR support from JFC fusion centers, major command (MAJCOM) ISR staffs, theater intelligence agencies, national intelligence agencies, and coalition ISR sources.

Operations/Plans (A-3/A-5)

- ✦ Organize the operational EW aspects of the headquarters staff.
- ✦ Coordinate operational EW issues with the JFC and component staffs. Typical issues would include:
 - ✦ ✦ Rules of engagement for EW air component forces.
 - ✦ ✦ Assist in unit [beddown](#) requirements for EW forces.
 - ✦ ✦ EW development requirements for ATO and airspace control order (ACO).
 - ✦ ✦ Requirements for additional EW forces/capabilities.
 - ✦ ✦ Requirements for force protection.
- ✦ Identify essential elements of information (EEI) to A-2.
- ✦ Apprise the ISR team chief of EW capabilities and limitations of all components and the potential effects on operations.
- ✦ Assist ISR team chief with EW ISR support requirements of subordinate units.
- ✦ Develop and coordinate the EW plan and integrate it into the IO plan that accomplishes the JFC's objectives.
- ✦ Identify Service-specific EW training requirements and coordinate joint training with other components.
- ✦ Advise COMAFFOR on concepts of EW employment, force planning, and management of EW resources for which he has [operational control](#) (OPCON) and/or [tactical control](#) (TACON) or has established supported/supporting relationships.
- ✦ Provide information on the number and location of all EW air assets.

Communications and Information (A-6)

- ✦ Coordinate for the A-3 to ensure that frequency allocations and assignments meet technical parameters under host-nation agreements.
- ✦ Deconflict frequencies and coordinate the joint restricted frequency list (JRFL) with J-6.
- ✦ Provide communications-electronics operating instructions for air component forces.
- ✦ Plan, coordinate, and monitor EW related communications security (COMSEC) procedures and assets.

Joint and Multinational Operations

EW is an integral part of joint and multinational operations. Planning and execution of [multinational force](#) (MNF) EW is made more difficult because of security issues, different cryptographic equipment, differences in the level of training of involved forces, and language barriers. An increasing dependence on the EMS requires close coordination between all joint force and MNFs, in addition to other organizations that may be impacted like civil air traffic control facilities and civil defense activities.

Joint force and Service component EW capabilities are employed in supported and supporting roles. For example, Air Force ES capabilities may be employed to identify and locate a surface-to-air threat which subsequently may be targeted and engaged by Army surface-to-surface fires as a [suppression of enemy air defense](#) (SEAD) mission in order to establish a degree of [air superiority](#) for [close air support](#). To promote the effectiveness of joint EW actions, air component EW personnel should be familiar with joint force commander's and other Service/functional component EW organization and be prepared to directly coordinate. See [JP 3-13.1, Electronic Warfare](#), for a discussion of the joint and Service component EW organization.



PLANNING ELECTRONIC WARFARE OPERATIONS

Last Updated: 10 Oct 2014

The employment of [electronic warfare](#) (EW) capabilities to affect an adversary can provide significant advantages. EW objectives must be clearly established, support overall national and military objectives, and include identifiable indicators of success.

The [Commander, Air Force Forces](#), (COMAFFOR)¹ exploits the capabilities of airpower operations through a cohesive [joint air operations plan](#) (JAOP) and [tasking cycle](#). The COMAFFOR should clearly define EW objectives and ensure that assets supporting these objectives are properly employed and integrated throughout operations.

Air component centralized planning for EW normally occurs at the air operations center (AOC).² The AOC formulates plans and coordinates air component EW activities based on the JFC's guidance. It receives, assembles, analyzes, processes, and disseminates all source intelligence required for EW planning. EW planners are responsible for ensuring freedom of action is gained and maintained within the electromagnetic spectrum (EMS). To accomplish this, EW planners should participate in all phases of JOPPA and the joint air tasking cycle.

Employing [electronic attack](#) (EA), [electronic warfare support](#) (ES), and [electronic protection](#) (EP), EW creates effects throughout the operational environment to include all physical domains and the [information environment](#) (which includes [cyberspace](#)). The cross domain implications of EW operations require centralized planning and decentralized execution. For joint operations, EW planners must coordinate EW efforts at the JFC level in order to minimize unintended effects.

¹ A note on terminology in Air Force doctrine: **The Air Force prefers—and in fact, plans and trains—to employ in the joint fight through a commander, Air Force forces (COMAFFOR) who is normally also dual-hatted as a joint force air component commander (JFACC)**; when involved in multinational operations, the JFACC may become a combined force air component commander (CFACC). However, to simplify nomenclature in doctrine, Air Force doctrine documents simply use the term "COMAFFOR" with the assumption that, unless stated otherwise, the COMAFFOR is dual-hatted as the JFACC and perhaps CFACC. Air Force doctrine recognizes that the two responsibilities are different and should be executed through different staffs. Similarly, Air Force doctrine recognizes that the air operations center (AOC), in joint or combined operations is correctly known as a joint AOC (JAOC) or combined AOC (CAOC). However, doctrine simply uses the term "AOC."

² See [AFTTP 3-3.AOC, Operational Employment, Air Operations Center](#), for additional information on AOC EW planning and organization.

EW planning requires a broad understanding of adversary and friendly capabilities and tactics. Employment of EW assets must be closely integrated into the commander's overall planning effort. This planning requires a multidiscipline approach with expertise from functional mission areas to include but not limited to: air, space, ground, intelligence, logistics, weather, and information/cyberspace.

EW planning responsibilities include:

- ★ Provide EW coordination and planning expertise to the COMAFFOR.
- ★ Integrate EW capabilities into [deliberate](#) and [crisis action planning](#).
- ★ Prepare EW inputs for operation plans and orders.
- ★ Develop and recommend EW task to support the COMAFFOR's [course of action](#).
- ★ Plan, coordinate, and assess EA requirements.
- ★ Identify EW [shortfalls](#) and provide advice on requests for forces and joint urgent operational needs statements.
- ★ Develop an EW strategy and an operations plan that state how the COMAFFOR plans to exploit EW capabilities to support the JFC's objectives.
- ★ Integrate EW capabilities into the joint air tasking cycle.
- ★ Make EW [air apportionment](#) recommendations.
- ★ Prioritize EW effects and targets based on the COMAFFOR's objectives and available assets.
- ★ Identify requirements for [intelligence, surveillance and reconnaissance](#) (ISR) support operations, including assistance to the AOC ISR division in planning the collection and dissemination of ES information.
- ★ Represent EW within the IO cell to formulate and recommend to the joint targeting coordination board targets to support the campaign or operations plan.³
- ★ Coordinate the EW portion of the special instructions (SPINS) and [rules of engagement](#) (ROE).
- ★ Plan, coordinate, integrate, and deconflict EW in current and future operations taking in consideration lethal and nonlethal capabilities (e.g., IO, cyberspace, space, special operations, and special technical operations) within the [joint operational area](#) or [theater](#).

³ See [AFTTP 3-3.AOC, Operational Employment, Air Operations Center](#), for additional information on AOC EW planning and organization.

- ★ Coordinate EW support requests from other [Service/functional components](#) according to the JFC's priorities.
- ★ Monitor and adapt execution of EW plans in current operations.
- ★ Provide oversight and coordination of EW [measures of effectiveness](#).
- ★ Respond to subordinate unit requests for enemy EW sites' operational status, availability of friendly EW support as required and tasked by the [air tasking order](#) (ATO).
- ★ Develop a joint EW strategy.
- ★ Task, plan, coordinate, and allocate the joint EW capabilities/forces made available to the JFACC by direction of the JFC.
- ★ Perform [assessment](#) of joint EW operations at the [operational](#) and [tactical](#) levels.
- ★ Provide integrated EA, ES, and EP for the JFC.
 - ★ ★ Identify JFACC requirements.
 - ★ ★ Integrate and synchronize use of air assets.
 - ★ ★ Task theater ES assets to satisfy JFC requirements.
- ★ Function as the [electronic warfare control authority](#) (EWCA), as directed by the JFC.

EW Mission Integration

Since EW activity may create effects throughout the entire EMS, EW planning must include comprehensive [EMS management](#) to safely integrate with other EMS aspects of joint and multinational operations. EW can cause effects beyond the intended primary effect and, therefore, should be integrated with other military and IO core elements in accordance with the Law of Armed Conflict (LOAC) and applicable rules of engagement (ROE) to achieve the overall objectives and negate or mitigate undesired indirect effects.

Since information systems are increasingly networked and as EW power capacity increases, potentially disrupting or damaging even closed electronic systems, the requirement to integrate, synchronize and deconflict EW with other elements of friendly operations has become even more critical than in the past. EW personnel should be aware of direct effects and plan for indirect effects when accomplishing "traditional" EW activity, as well as planning and implementing EW activity to integrate with other IO and cyberspace elements to directly achieve the commander's objectives.

EW jammers vary in effective range, power, and modulation. EM radiations can be aimed and focused, but do not stop at definitive geographic boundaries or discrete altitudes. Therefore, theater EMS (frequency) interface deconfliction procedures, like employment of the [joint restricted frequency list](#) (JRFL) are necessary to minimize interference and degradation of friendly efforts.

Intelligence Surveillance and Reconnaissance Support

Accurate and timely Intelligence Surveillance and Reconnaissance (ISR) is the foundation for effective EW planning and employment. ISR supports EW through several functions. First, constant analysis by various scientific and technical centers guards against hostile technical surprise. Second, [indications and warning](#) (I&W) centers provide tactical and strategic warning to friendly forces. Third, ISR continually monitors threat systems to support reprogramming of all systems. Fourth, intelligence supports mission planning.

Specifically, ISR supports EW by providing technical threat descriptions and tailored threat environment descriptions. EW planning requires parametric and employment data, modeling and simulation tools, and mission planning tools to prioritize targets and defense tasks. ISR assets are required to support both offensive and defensive EW planning. To be of value, these assets must provide timely intelligence and be responsive to the commander's needs. Intelligence support includes establishing and maintaining comprehensive support databases as well as looking at scientific and technical intelligence and general military intelligence capabilities. Clearly defined intelligence requirements are necessary to ensure resulting intelligence information meets the needs of EW planners and decision makers are not overloaded with excessive or meaningless data.

Logistics Support

Readiness and sustainability of electronic assets are directly related to the quality of logistics planning. EW logistics programs should be developed in balance with modernization efforts and the operating capability each category of resources provides. Emphasis must be on total effectiveness to maximize EW capabilities.



ANNEX 3-51 ELECTRONIC WARFARE

ELECTRONIC WARFARE EMPLOYMENT

Last Updated: 10 Oct 2014

The employment of [electronic warfare](#) (EW) capabilities is vital throughout all [phases of an operation](#): shape, deter, seize initiative, dominate, stabilize, and enable civil authority. During the shape and deter phases, [electronic warfare support](#) (ES) assets contribute to the overall understanding of the [operational environment](#). A commander may employ EW to implement favorable [joint intelligence preparation of the operational environment](#) without prematurely crossing the threshold to conflict. The potential to employ nondestructive and nonlethal capabilities make EW assets vital to the preparation of the operational environment and [mission analysis](#).

Using all aspects of EW, air component forces may set the conditions for combat, and prosecute the attack once combat is underway. The ability to achieve an objective through nondestructive means may allow a more rapid transition from seizing the initiative and dominate phases to support operations in the stabilization phase. From stabilization to enabling civil authority, EW can foster restorative operations by offering options such as force protection through ES to monitor subversive elements, [electronic attack](#) (EA) to counter radio controlled improvised explosive devices (RCIEDs), or broadcasting messages supporting [military information support operations](#) (MISO) and/or civil defense to assist civil authorities.

B1-B Lancer



B1-B Lancers dispensing chaff and flares

EW Support to the COMAFFOR

The COMAFFOR provides unity of command and unity of effort for Air Force EW operations. The COMAFFOR normally exercises [operational control](#) (OPCON) over assigned and attached US Air Force EW forces. EW personnel support the COMAFFOR by accomplishing the following:

- ★ Make recommendations on the proper employment of EW capabilities and forces.
- ★ Develop a daily EW battle rhythm that supports EW planning and operations requirements.
- ★ Accomplish specified and implied EW tasks.
- ★ Represent EW within the information operations (IO) cell.
- ★ Maintain current assessment of the EW resources available (to include number, type, and status of EW assets) and analyze what resources are necessary to accomplish operational objectives.
- ★ Develop, coordinate and integrate operations to achieve EW effects based on JFC's objectives.
- ★ Predict effects of friendly and enemy EW activity on joint and multinational operations.
- ★ Plan, coordinate, execute, and assess EP (e.g., frequency management, emission control (EMCON), EW reprogramming).
- ★ Assist in frequency management. This includes deconflicting frequency requirements and assignments.
- ★ Coordinate and monitor EW reprogramming by identifying where EW reprogramming decisions and reprogramming actions affect operations.
- ★ Conduct reachback to organizations supporting air component EW operations.
- ★ Provide EW liaison to other Service and functional components of joint and multinational forces
- ★ Prepare an EW estimate of the situation to support the JFC's estimate.
- ★ Function as the EW integrator for counterair operations, strategic attack, the overall [air interdiction](#) effort, [space support](#), and theater airborne reconnaissance and surveillance.

- ✦ Coordinate EW support for [combat search and rescue](#).
- ✦ Provide [EMS database](#) and communications network support.
- ✦ Conduct joint EW training of components for joint force components, in joint operations planning for which the COMAFFOR has or may be assigned primary responsibility, or for which the air component's facilities and capabilities are suitable.

EA-18G Growler



The EA-18G Growler is a joint EW weapon system that conducts EM jamming, and employs high-speed anti-radiation missiles.

EW Employment Considerations

In contested environments, the density and potential lethality of the adversary air defense systems may challenge mission effectiveness and the survivability of air friendly forces. At the tactical level, mission planning tries to strike the appropriate balance between mission accomplishment and risks. Thorough planning at the operational level gives tactical commanders the proper tools to allow them to strike that balance. **The decision to employ EW should be based not only on overall joint campaign or operation objectives, but also on the risks of possible adversary responses and other potential effects on the campaign or operation. A properly constructed force package that includes EW enhances the probability of mission effectiveness and survival of friendly forces.**

The application of EW can prevent an adversary's use of the EMS for employment of improvised explosive devices (IEDs), specifically remotely-controlled IEDs (RCIEDs). Employing electronic attack, EW can deny or degrade the adversary's ability to use the EMS to detonate IEDs. EW can also enable friendly use the EMS to pre-detonate RCIEDs at a time of our choosing. Similarly, EW can disrupt adversary communications by disrupting an adversary's ability to use the EMS, interfering with their ability to react to friendly activity in a timely manner.

Recent increases in power supply capacities in EW systems (especially DE systems) provide capabilities for disruption or damage to many physical targets. This provides additional options in lethal/destructive attack and may enable friendly forces while causing significantly less collateral damage. New EM systems can target humans with both lethal and nonlethal effects, in some cases with debilitating but non-damaging effects.
