As with other applications of electromagnetic warfare (EW), airborne electromagnetic warfare considerations are split into the three divisions of electromagnetic attack (EA), electromagnetic warfare support (ES), and electromagnetic protection (EP). Specifically within the air domain, on a fundamental level of electromagnetic spectrum (EMS)-aided air warfare, an analogy of the adversary’s use of the EMS can be split into three categories: “swords,” “shields,” and “spies.” As a “sword,” the enemy uses the EMS via wireless communication, radars, or EMS-aided munitions, for offensive attacks to find, fix, track, target, engage, and assess action against friendly forces. Friendly EA, supported by ES (and other intelligence sources), aims to counter this. As a “shield,” the enemy utilizes counter-EMS systems such as radar, communication, and navigational jammers, to halt friendly freedom of maneuver in the EMS to complete an engagement. Friendly EP, supported by ES (and other intelligence sources), aims to counter this. Finally, as a “spy” the enemy uses the EMS via passive detection capabilities to detect and collect on friendly assets. Friendly EP, supported by ES (and other intelligence sources), also aims to counter this.

Airborne Electromagnetic Attack

Airborne EA aims to counter the enemy’s ability to use the EMS to attack friendly forces, and is split into two categories: offensive EA and defensive EA (commonly referred to as self-protection jamming). Offensive airborne EA capabilities, also referred to as “off-board EA” by protected entities, are generally employed by one air asset to protect other specific assets, or an entire strike package, depending on mission requirements. Defensive airborne EA, also referred to as “onboard EA,” by protected entities, or “electromagnetic countermeasures (ECM),” are generally employed by an air asset to protect the friendly assets. There may be instances where offensive EA can be used to protect friendly assets, or where defensive EA can be employed to support off-board assets, but planners and staffs should possess or request documentation that such employment can produce desired effects, before building plans that use EA in such a fashion.

Airborne Offensive EA

Historically, the Air Force supports the joint force requests for offensive airborne EA to
either protect surface forces or other air forces. In supporting ground or maritime forces, the aim of offensive EA in a supporting asset role, is to disrupt, deceive, degrade, destroy, or deny any adversary in a manner that benefits ongoing surface operations. This includes, but is not limited to communication equipment. There may be instances where offensive EA aircraft are the supported asset to affect targets in the land and maritime domains.

In addition to historical uses of airborne EA, the Air Force realizes the advantages of fighting as a truly multi-domain force. Airborne EA can also be used to provide effects in support of offensive and defensive counterspace operations. For instance, by attacking ground stations with EA, aircraft may negate an enemy’s ability to control their satellites and deliver space effects, to include enemy offensive counterspace attacks. Anti-radiation missiles passively hone in on radiation sources and may be used to strike ground-based space surveillance radars, missile warning radars, or satellite control stations. Successful counterspace operations will mitigate the enemy’s use of space capabilities to support their fielded forces in all domains.

In supporting joint forces in all domains, offensive airborne EA focuses on any EMS node or pathway that can be used by the adversary to engage friendly forces. This includes, but is not limited to, enemy communications and enemy radars. Examples of offensive airborne EA include:

- **Anti-Radiation Missiles (ARMs).** ARMss have sensors onboard the munition to passively home onto electromagnetic (EM) radiation of enemy systems, in order to affect them in a manner that is advantageous to friendly forces. Generally, ARMss cannot be employed in a manner that can "save" aircraft that are already being actively engaged; the inbound enemy munition will most likely impact the engaged aircraft prior to ARM impact, so effective utilization of ARMss requires proactive employment. For example, enemy knowledge of the presence of ARMss in the battlespace may serve as a deterrent.

- **Electromagnetic Intrusion.** EM intrusion is the intentional insertion of EM energy into transmission paths in any manner, with the objective of deceiving operators or causing confusion.

- **Electromagnetic Jamming.** EM jamming is the deliberate radiation, re-radiation, 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. Specifically it is the intentional transmission of EM energy into a targeted RF receiver in order to prevent its proper function. Early Air Force efforts were primarily directed toward electromagnetically 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, terrestrial and satellite communications links, and other devices that rely on the EMS can limit enemy access to information on friendly force movements and composition and cause confusion. Jamming can degrade the enemy’s decision-making and employment when applied against command and control (C2) systems. An adversary
heavily dependent on centralized control and execution for force employment presents an opportunity for EA.

- **Air-launched decoys** are systems intended to deceive or disrupt enemy evaluation of the air domain. Air-launched decoys can re-radiate or jam enemy EMS emissions.

- **Meaconing.** Meaconing consists of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause aircraft or surface stations to obtain inaccurate bearings.

- **Electromagnetic pulse (EMP)** is a short pulse of rapidly changing electric and magnetic fields. This pulse can potentially interfere with the operation or electrical and electronic equipment or cause widespread damage to infrastructure. EMP is one of a nuclear device’s effects and depending on the altitude of detonation and the yield of a nuclear device, EMP’s effects can extend hundreds of kilometers from the blast site. EMP can also be delivered via non-nuclear means, producing temporary effects or system destruction. These effects can be delivered via conventional and non-conventional means. The portion of the EMS most vulnerable to EMP is the radio spectrum. Hardening of communications systems and planning for communication system protection is vital when EMP is likely. Finally, EMP is very powerful type of EM radiation, which may be employed as a weapon, from a strong electromagnetic pulse that can be produced by a nuclear explosion or generated conventionally to produce damaging current and voltage surges.

- **Directed energy (DE) systems** are systems (e.g., lasers and radio frequency weapons, high-power microwaves (HPMs), EMP weapons that use DE [concentrated EM energy and atomic or subatomic particles]) to incapacitate, damage, or destroy enemy equipment, facilities, and/or personnel. Lasers are devices that emit light through a process of optical amplification based on the stimulated emission of EM radiation with sufficient energy to affect adversary systems, while radio frequency (RF) weapons employ EM radiation to damage equipment or harm personnel. HPMs are weapon systems utilizing high-power microwave RF. DE capabilities can be hosted in an offensive EA system as well as in a defensive EA and self-protection (DEA/SP) system.

### Airborne Defensive Electromagnetic Attack / Self-Protection

Airborne DEA/SP activities use the EMS for self-protection of an aircraft. There may be DEA/SP capabilities that can provide survival benefits for other aircraft (e.g., chaff corridors or self-protection jammers that counter EMS-dependent systems in an overwhelming manner), but generally airborne DEA/SP equipment is developed to only provide protection of the host aircraft. Airborne DEA/SP may include radar warning receivers, jammers, chaff, flares, lasers, DE, towed decoys, and low-observable technologies. The desired effect is to counter enemy EMS-dependent equipment for friendly protection.

- **Low observable technologies** increase assets’ ability to operate in the physical
domains by reducing the possibility of their detection and exploitation by adversaries through the EMS.

- **Chaff** are radar confusion reflectors, consisting of thin, narrow metallic strips of various lengths and frequency responses, which are used to reflect echoes for confusion purposes.

- **Flares** are infrared or ultraviolet generating sources ejected from aircraft to mislead infrared or ultraviolet-sensitive or -seeking targeting systems.

- **Directed energy weapons** are weapons or systems (e.g., laser turrets) that use directed energy to incapacitate, damage, or destroy enemy equipment, facilities, or personnel.

**Airborne Electromagnetic Warfare Support**

ES assets and capabilities collect, detect, intercept, identify, and locate sources of intentional and unintentional radiated EM energy. The purpose of airborne ES missions is to intercept, identify, and locate adversary electromagnetic and communication emissions to provide threat warning to friendly forces in all domains. The information gathered during ES operations is used for threat avoidance, EA, and targeting. ES platforms such as the RC-135V/W Rivet Joint and the EP-3E Aries II are tasked by an operational commander to provide combat support to friendly forces for an operationally-defined period. Supported mission areas include, but are not limited to, the following:

- **Joint Intelligence Preparation of the Operational Environment (JIPOE).** JIPOE is necessary to collect and correlate EMS reflections to build information on the target nation's weapons systems and overall order of battle. ES operations should begin as early as possible to build an accurate tactical picture prior to any counterair, counterland, countersea, counterspace, or counter-EMS operations.

- **Counterair.** ES supports offensive and defensive operations to attain and maintain control of the air. Threats to air operations are identified through electromagnetic means and disseminated to C2 and strikers before adversary weapons can be employed. Suppression of enemy air defenses (SEAD) operations rely on the rapid location and dissemination of threat data to enable accurate and timely deployment of ARMs and other EA methods.

- **Counterland.** ES supports airpower operations against enemy land forces by monitoring enemy reactions and providing imminent threat warning (ITW) to friendly forces in close proximity. Airborne ES platforms responds to real-time requests for enemy information using tactical communication methods. This allows decision makers to make target determinations for air interdiction or engagement by tactical ground units.

- **Countersea.** Airborne ES is necessary to ensure awareness of the electromagnetic
environment (EME) in a wider collection area as opposed to a region-specific focus. In addition to threat warning and identification, airborne ES produces intelligence on enemy surface and subsurface vessels, maritime patrol, harbor tracking activity, and surface C2.

**Counterspace.** ES supports offensive and defensive operations to attain and maintain control of space. Threats to space operations may be identified through electromagnetic means and disseminated to C2 and strike assets before adversary weapons can be employed. Integrated employment of multi-domain capabilities through coordinated detection, identification, engagement, and assessment of enemy forces is necessary to defeat enemy attacks and protect friendly forces.

**Combat Search and Rescue (CSAR).** ES platforms support CSAR operations by collecting and passing information on enemy activity and status of isolated personnel (IP) as required to the Joint Personnel Recovery Center (JPRC), CSAR task force, and other relevant players. During execution, threat warning to rescue forces and identification of enemy activity near the IP is a vital requirement.

**Non-Kinetic Operations.** Operations that rely on actions designed to create effects without the direct use of destructive force are often referred to as “non-kinetic” operations. This can encompass much of EW, as well as information, space, cyberspace, and special technical operations. Making such operations effective often hinges upon airborne ES platforms’ ability to provide the most accurate data pertaining to enemy EM reflections. Employing effective EA techniques is not possible without accurate identification and characterization of the EME. A critical component of planning and executing effective non-kinetic actions is providing measures of effectiveness (MOE). MOEs are used to assess changes in system behavior or capability that are tied to measuring the attainment of an end state, achievement of an objective, or creation of a desired effect. Airborne ES is necessary for identifying information relevant to an MOE and disseminating it to the non-kinetic package commander for further analysis or action. Effective EA can also support ES operations by influencing enemy activity to achieve collection of desired EM information. However, consequence management must be considered when employing EA for ES operations so as not to encourage undesired reactions from the enemy. Having an airborne EA asset act as the airborne non-kinetic package commander may be beneficial in ensuring proper mission management and coordination with non-airborne assets.

There are several planning and execution factors that should be taken into account to employ effective airborne EA. Crews should plan orbits that best meet the requirements of the mission. Proximity to friendly forces is crucial to maintain two-way coordination, but proximity to enemy forces must enable freedom of movement without provoking engagement. Threats with long effective engagement ranges may prove consequential when calculating collection effectiveness from greater standoff distances. The ability to provide imminent threat warning (ITW) quickly and accurately depends on management of orbit placement as it pertains to sensor effectiveness. Effective ITW may warrant additional ES or EA platforms, airborne and non-airborne, in order to increase
opportunity for cross-cueing and cooperative geolocation. Dissemination methods (e.g., tactical reports (TACREPs), situation reports (SITREPs), ITW, combat advisory broadcasts) should be solidified during planning to guarantee rapid and accurate sharing of information. Finally, MOE can come from multiple ES sources in multiple domains. Careful planning is needed to task EM sensors at the right time and place to verify expected outcomes during operations. This is also true for counterland, counterair, countersea, counterspace, and counter-EMS operations when providing information on EM reflections to calculate battle damage indications.

- **Tactical Reports (TACREPs) / Situation Reports (SITREPs)** are situational updates and intelligence summaries that provide adversary-based signals intelligence (SIGINT) updates with location and identification amplification to support units in all domains prior to ingress.

- **Imminent Threat Warning (ITW)** is near real time threat reporting of SIGINT-derived intelligence to provide indications and warnings to friendly forces after ingress that are within, or transitioning to, adversarial threats.

- **Cooperative geolocation** is the real-time cross-cueing with assets across all domains to provide accelerated identification and location of adversary threats.

- **Utilizing EA to support ES (or Jam-to-Exploit)** is a planning-intensive operational capability to provide EA effects on specific adversary EMS capabilities, to drive the adversary to different assets that are more readily accessible to ES assets.

**Airborne Electromagnetic Protection**

EP is a friendly EMS-dependent system’s mode of operation, or use of EMS or physical properties, to preserve itself from adversary EW, thereby allowing the system to continue operating. Ensuring EMS-dependent equipment is immune to environmental effects or other friendly EMS-dependent systems is also the goal of EP. EP is not force protection. The use of flare rejection logic on an infrared (IR) missile (i.e., allowing the IR missile to continue to function despite an adversary’s use of flares) is EP. The flare rejection technique ensures friendly use of the EMS to track the intended target despite the adversary's DEA/SP actions (i.e., the flare). Although defensive EA actions and EP both protect personnel, facilities, capabilities, and equipment, EP protects from the effects of EA (friendly or adversary) or EM interference, while DEA/SP is used primarily to protect against lethal attacks by denying adversary use of the EMS to target, guide, or trigger weapons.

Examples of EP include frequency agility, changing pulse repetition frequency, emission control (EMCON), and EM hardening (to include electromagnetic pulse 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. 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.