EW Glossary of Terms

Electromagnetic Warfare Fundamentals

EW (Electromagnetic Warfare): The use of the electromagnetic spectrum – radio waves, infrared, microwaves, and more – to sense, protect, and attack. EW is divided into three core pillars: Electronic Attack (EA), Electronic Protection (EP), and Electronic Support (ES).

EA (Electronic Attack): The offensive arm of EW. EA uses electromagnetic energy to disrupt, degrade, or destroy enemy equipment and capabilities. This includes jamming enemy radars, spoofing GPS signals, or using directed energy weapons.

EP (Electronic Protection): Measures taken to protect friendly forces and systems from the effects of EW – both enemy attacks and friendly interference. EP includes things like frequency hopping, low-probability-of-intercept radars, and hardening electronics against jamming.

ES (Electronic Support): The intelligence-gathering arm of EW. ES involves passively listening to and analyzing electromagnetic emissions to detect, identify, and locate threats. ES feeds information to both EA and EP.

ECM (Electronic Countermeasures): Specific actions taken to degrade or neutralize enemy use of the electromagnetic spectrum. ECM encompasses jamming, deception, and other active interference techniques and is a subset of Electronic Attack.

ECCM (Electronic Counter-Countermeasures): Techniques used to maintain effective use of the electromagnetic spectrum despite enemy ECM efforts. Essentially the defensive response to jamming or deception – for example, designing a radar that can "burn through" jamming or switch frequencies to avoid interference.

Spectrum Operations

EMSO/EMO (Electromagnetic Spectrum Operations): The coordinated military activities to exploit, attack, protect, and manage the electromagnetic spectrum. EMSO is the overarching operational concept that unifies EW, spectrum management, and cyber operations involving the spectrum.

Spectrum Management: Coordinating and controlling the use of the electromagnetic spectrum (radio waves, microwaves, etc.) to maximize effectiveness while minimizing interference between friendly systems.

EMBM (Electromagnetic Battle Management): Real-time coordination and deconfliction of electromagnetic spectrum use during military operations. EMBM ensures that friendly jammers don't interfere with friendly communications, and that spectrum resources are allocated where they're needed most.

EMCON (Emissions Control): Deliberate restrictions placed on the use of electromagnetic emissions – radios, radars, active jammers – to reduce the chance of detection or interference. EMCON is a key tactic for maintaining the element of surprise or protecting a unit's location.

High Energy Lasers: Directed energy weapons that use concentrated light beams to damage sensors, disable equipment, or destroy targets. Unlike science fiction, modern military lasers typically target sensors or equipment rather than people.

Electronic Attack Systems

Airborne Electronic Attack: Aircraft-based systems that jam, deceive, or disrupt enemy electronic systems (like radars and communications). Think of specialized military aircraft that can block or confuse enemy signals from the air.

RF Electromagnetic Warfare: Using radio frequency energy to detect, disrupt, or protect electronic systems. This includes jamming enemy communications or protecting friendly signals from interference.

High-Power Microwaves (HPM): Weapons that emit powerful microwave energy to damage or disable electronic systems. They can essentially "fry" enemy electronics without causing physical destruction, making them useful for disabling vehicles, computers, or communications equipment.

DRFM (Digital Radio Frequency Memory): A technology that captures an incoming radar signal and retransmits a modified version of it, creating false or misleading returns on the enemy radar screen. DRFM is the engine behind many modern electronic deception and jamming systems.

Intelligence Collection

SIGINT (Signals Intelligence): The broad category of intelligence derived from intercepting and analyzing electronic signals. SIGINT encompasses COMINT (communications), ELINT (electronic emissions), and FISINT (foreign instrumentation signals).

COMINT (Communications Intelligence): Collecting and analyzing intercepted communications between people or electronic systems. This involves monitoring enemy phone calls, radio transmissions, or digital messages.

ELINT (Electronic Intelligence): Gathering information from non-communication electronic signals, primarily from radar systems. This helps identify what types of radars enemies are using and where they're located.

GEOINT (Geospatial Intelligence): Collecting and analyzing images and geospatial information to identify, measure, and analyze physical features and activities on Earth. This includes satellite imagery, aerial photography, and mapping data used to support targeting and situational awareness.

Cyber Operations

Offensive Cyber Operations (OCO): Activities that project power through cyberspace to disrupt, deny, degrade, or destroy enemy computer systems or information. OCO can range from disabling a radar network to corrupting an adversary's logistics database.

Defensive Cyber Operations (DCO): Protecting friendly networks and systems from cyber attacks, including monitoring for intrusions, building secure systems, and responding to breaches. DCO is the cyber equivalent of electronic protection.

CNO (Computer Network Operations): The broader category of military operations involving computer networks, encompassing both offensive and defensive cyber activities as well as network exploitation for intelligence collection.

Communications & Sensing

Radar: Systems that use radio waves to detect objects, determine their range, angle, and velocity. Military radars can track aircraft, ships, vehicles, and even artillery shells or missiles.

ISR (Intelligence, Surveillance, and Reconnaissance): The integrated capability to collect and process information about adversaries and the environment. ISR systems – satellites, aircraft, sensors, and networks – feed commanders the situational awareness they need to make decisions.

IFF (Identification Friend or Foe): A system that uses electronic transponders to distinguish friendly forces from adversaries on radar and other sensor displays. IFF prevents fratricide by automatically tagging friendly platforms with a recognizable electronic signature.

ESM (Electronic Support Measures): Passive systems that detect, intercept, identify, and locate sources of electromagnetic energy – without transmitting anything themselves. ESM gives platforms situational awareness of the electronic environment around them.

C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance): The integrated framework of systems and processes that enables commanders to direct forces and manage information across an operation. C4ISR ties together communications, computing, intelligence, and sensors into a unified operational picture.

Navigation & Avionics

GNSS (Global Navigation Satellite System): The family of satellite-based navigation systems that provide positioning, navigation, and timing data worldwide. GPS (United States) is the most well-known, but GNSS also includes Russia's GLONASS, Europe's Galileo, and China's BeiDou.

GPS (Global Positioning System): The United States' satellite-based navigation system, providing precise positioning and timing data to military and civilian users worldwide. GPS is a component of the broader GNSS family.

NAVWAR (Navigation Warfare): Military operations specifically focused on controlling the use of navigation systems in a conflict. NAVWAR includes jamming or spoofing enemy GPS, protecting friendly navigation signals, and ensuring forces can navigate accurately even in a denied environment.

Navigation Warfare/PNT (Positioning, Navigation, and Timing): Activities focused on denying enemy use of navigation systems (like GPS) while ensuring friendly forces can navigate accurately. PNT capabilities are foundational to modern military operations – nearly every precision weapon and coordinated maneuver depends on them.

Modeling and Simulation (M&S): Computer programs that create virtual environments to test tactics, train personnel, or predict outcomes of electronic warfare operations before real-world deployment. M&S is essential for developing and refining EW systems without costly live testing.

Common Electronic Warfare Acronyms

AEA: Airborne Electronic Attack
AESA: Active Electronically Scanned Array
AWACS: Airborne Warning and Control System
C2: Command and Control
C4I: Command, Control, Communications, Computers, and Intelligence
C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCD: Camouflage, Concealment, and Deception
CM: Countermeasures
CNO: Computer Network Operations
COMINT: Communications Intelligence
CONOPS: Concept of Operations
DCO: Defensive Cyber Operations
DECM: Defensive Electronic Countermeasures
DEW: Directed Energy Weapon
DOTMLPF-P: Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
DRFM: Digital Radio Frequency Memory
DSP: Digital Signal Processing
EA: Electronic Attack
EA-POD: Electronic Attack Pod
EA/EW: Electronic Attack/Electronic Warfare Aircraft (like EA-18G Growler)
ECM: Electronic Countermeasures
ECCM: Electronic Counter-Countermeasures
ELINT: Electronic Intelligence
EMBM: Electromagnetic Battle Management
EMCON: Emissions Control
EMS: Electromagnetic Spectrum
EMSO: Electromagnetic Spectrum Operations
EOB: Electronic Order of Battle
EP: Electronic Protection
ES: Electronic Support
ESM: Electronic Support Measures
EW: Electromagnetic Warfare
GEOINT: Geospatial Intelligence
GNSS: Global Navigation Satellite System
GPS: Global Positioning System

HEL: High Energy Laser
HITL: Hardware in the Loop
HPM: High-Power Microwave
IFF: Identification Friend or Foe
IR: Infrared
IRCM: Infrared Countermeasures
ISR: Intelligence, Surveillance, and Reconnaissance
JAMMER: Device that deliberately blocks, interferes with, or disrupts signals
M&S: Modeling and Simulation
MAWS: Missile Approach Warning System
MDO: Multi-Domain Operations
NATO: North Atlantic Treaty Organization
NAVWAR: Navigation Warfare
NEWEG: New Electronic Warfare Environment Generator
OCO: Offensive Cyber Operations
OECM: Offensive Electronic Countermeasures
PESA: Passive Electronically Scanned Array
PNT: Positioning, Navigation, and Timing
RCS: Radar Cross Section
RF: Radio Frequency
RWR: Radar Warning Receiver
SIGINT: Signals Intelligence
UAV/UAS: Unmanned Aerial Vehicle/System
UAV/UCAV: Unmanned Aerial Vehicle/Unmanned Combat Aerial Vehicle