Electromagnetic Spectrum Operations for Military Service Members

A Comprehensive Familiarization Brief

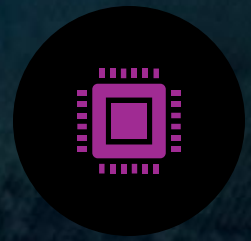
This training material was developed with advice and guidance from USW(R&E) / Gina Tyrrell

Electromagnetic Spectrum Operations

THE ELECTROMAGNETIC SPECTRUM (EMS) IS THE ESSENTIAL LINK CONNECTING ALL OPERATIONAL DOMAINS AND ENABLING MODERN MILITARY OPERATIONS

EVERY MILITARY FUNCTION DEPENDS ON THE SPECTRUM: COMMUNICATIONS, NAVIGATION, SENSING, INTELLIGENCE, AND WEAPON SYSTEMS

UNDERSTANDING EMS IS NO LONGER JUST FOR SPECIALISTS—IT IS CRITICAL FOR EVERY SERVICE MEMBER'S MISSION SUCCESS AND SURVIVAL

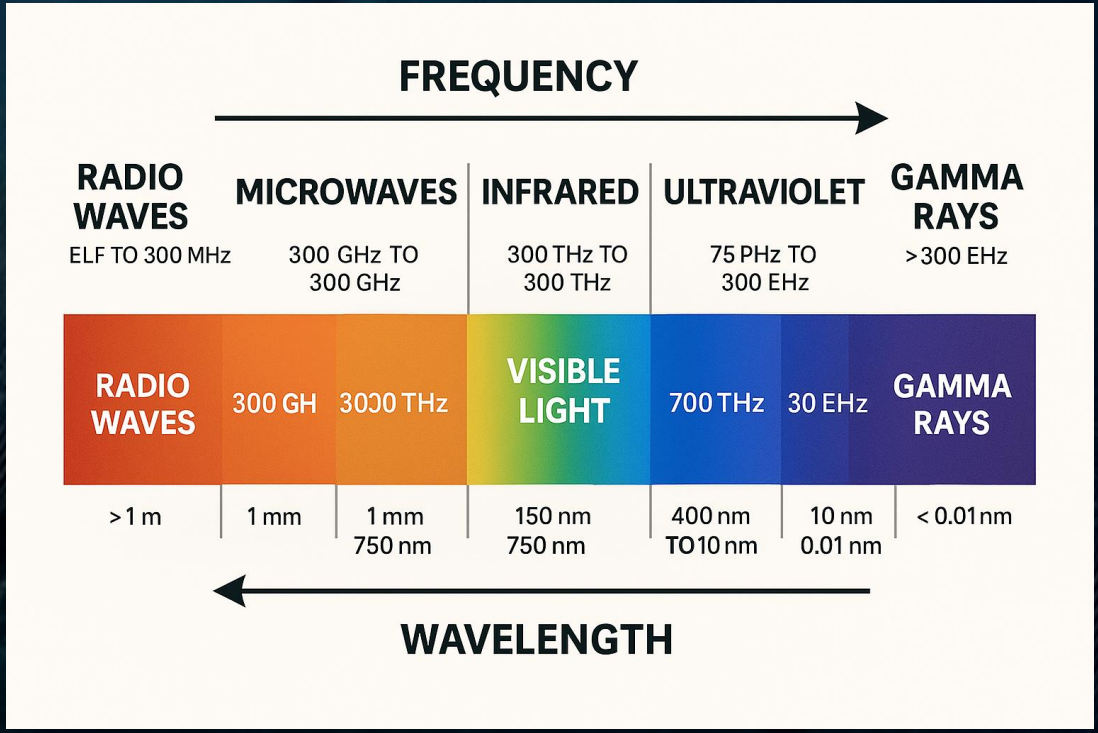


THIS BRIEFING PROVIDES FOUNDATIONAL KNOWLEDGE TO OPERATE EFFECTIVELY IN CONGESTED AND CONTESTED ELECTROMAGNETIC ENVIRONMENTS

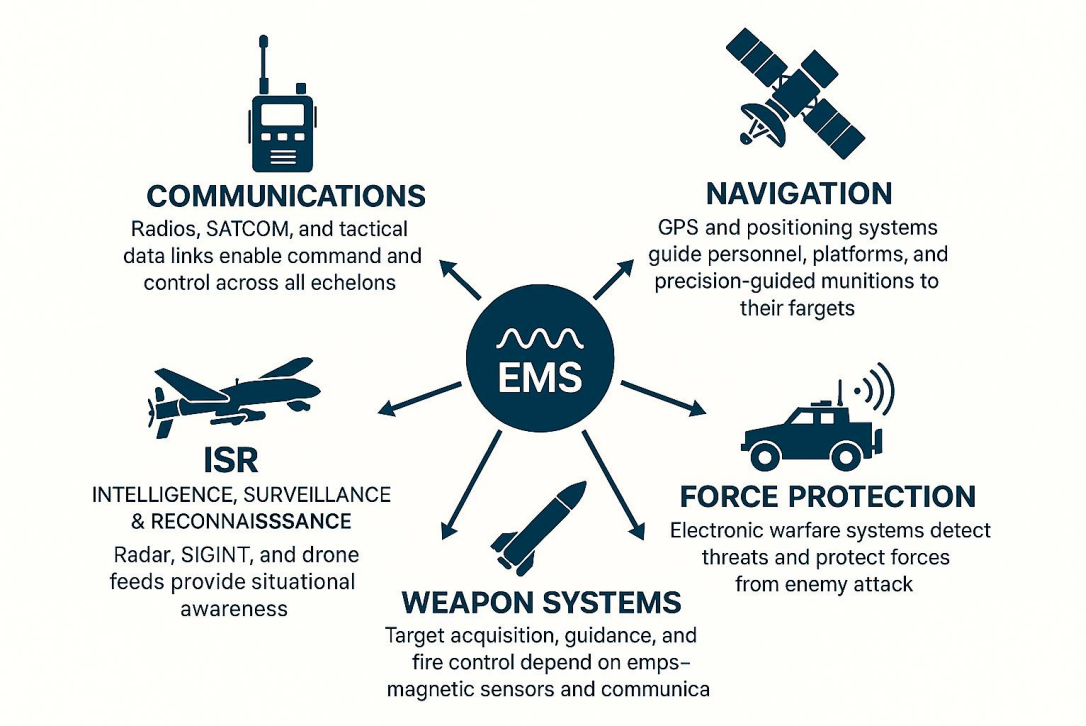
GOAL: BUILD AWARENESS OF WHY EMS MATTERS AND HOW YOUR ACTIONS IMPACT ELECTROMAGNETIC SECURITY

What is the Electromagnetic Spectrum?

- EMS covers frequencies from extremely low frequency (ELF) to gamma rays
- Electromagnetic radiation moves at the speed of light and carries information and energy
- Spectrum includes radio waves, microwaves, infrared, visible light, ultraviolet, Xray, and gamma rays
- Military mainly uses radio frequency (RF) 3 kHz to 300 GHz for communications, radar, and navigation
- Think of EMS as an invisible highway where all wireless information travels
- Key measurement units: Frequency (Hertz/MHz/GHz), Power (Watts/dBm), and Wavelength (meters)



Why the Electromagnetic Spectrum is Critical to Military Operations



- Communications: Radios, SATCOM, and tactical data links enable command and control across all echelons
- Navigation: GPS and positioning systems guide personnel, platforms, and precision guided munitions to their targets
- Intelligence, Surveillance & Reconnaissance (ISR): Radar, SIGINT, and drone feeds provide situational awareness
- Weapon Systems: Target acquisition, guidance, and fire control depend on electromagnetic sensors and communications
- Force Protection: Electronic warfare systems detect threats and protect forces from enemy attack
- Without EMS access, modern forces cannot effectively communicate, navigate, sense, or strike

Military Equipment Operating in the Electromagnetic Spectrum

- Communications: SINCGARS, MBITR radios, Harris radios, SATCOM terminals on various bands
- Navigation Systems: GPS receivers (L1: 1575.42 MHz, L2: 1227.60 MHz), DAGR, and position location systems
- ISR: ground and airborne radar, SIGINT/ELINT platforms, and UAV data links.
- Battle Command: JBCP (2.45-8 GHz), Blue Force Tracker (BFT), and tactical internet systems for situational awareness
- Electronic Warfare: Jamming systems, radar warning receivers (RWR), and countermeasure equipment across all domains
- Personal Devices: smartphones and smartwatches emit detectable RF signatures

How Military Communications Systems Work

- Radios convert voice/data to EM waves transmitted at set frequencies
- SINCGARS frequency hopping changes frequency 100 times per second to avoid detection/jamming
- Higher transmission power extends range but increases detection risk.
- Propagation affected by terrain, weather, time, and obstacles.
- Encryption protects content but does not hide electromagnetic signatures
- Antennas and power settings impact electromagnetic footprint and vulnerability

Where Your Military Systems Operate in the Spectrum

HF/VHF (1.6-88 MHz): SINCGARS, tactical radios for voice communications

UHF (225-512 MHz): MBITR, aircraft communications, and data links.

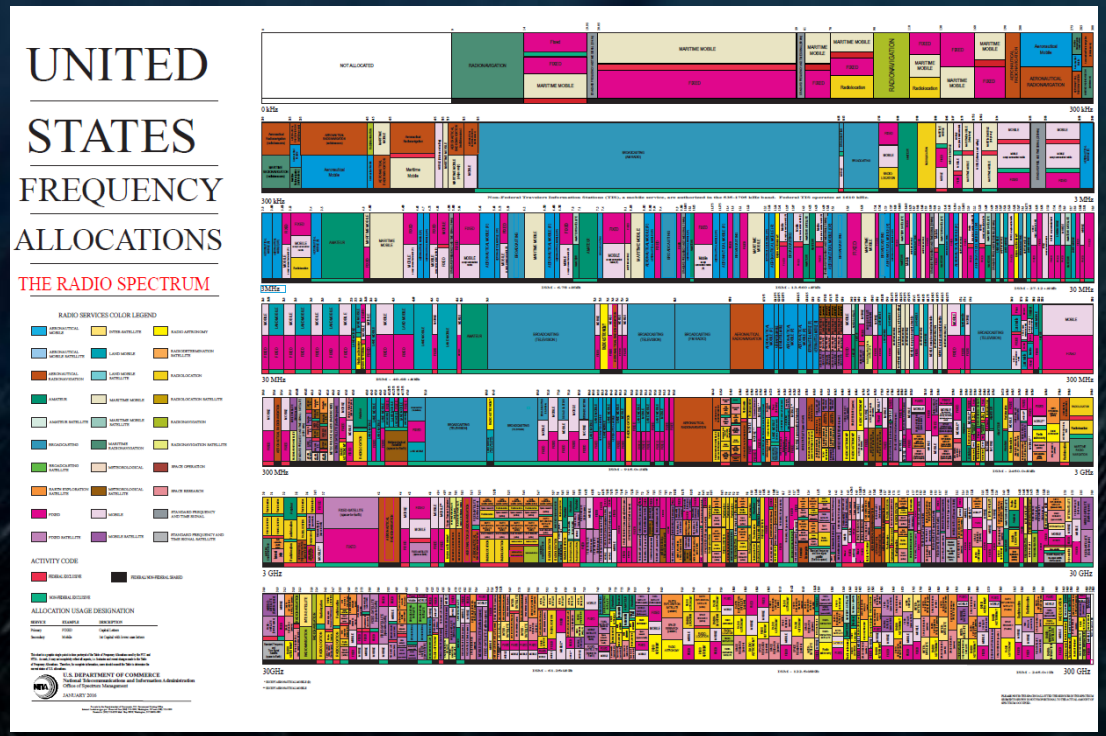
L-Band (1-2 GHz): GPS navigation, UAV control, and identification systems

S-Band (2-4 GHz): JBCP, SATCOM, Bluetooth, WiFi, 5G LTE cellular.

X-Band (8-12 GHz): fire control radars, precision targeting, SATCOM downlinks

Ku/Ka Bands (12-40 GHz): wideband SATCOM, Starlink, high-data-rate communications

The Congested Electromagnetic Environment: A Crowded Spectrum



- EMS is crowded with military and growing civilian users (5G, WiFi, IoT devices)
- Civilian spectrum demands pressure military frequency allocations
- Dense transmitter concentrations risk self-jamming and interference
- Coalition operations require close coordination to reduce interference and safeguard capability

The Contested Electromagnetic Environment: Enemy Threats

- Near peers (Russia, China) and regional powers (Iran, North Korea) possess advanced EW capabilities.
- Enemy jamming and spoofing challenge U.S. spectrum dominance.
- Russian EW disrupts Ukrainian GPS, comms, and targets emitters with lethal fires
- Allies must assume adversaries contest EMS use, risking loss of comms, navigation, and precision fires

Emerging NextG Technology: Opportunities and Risks

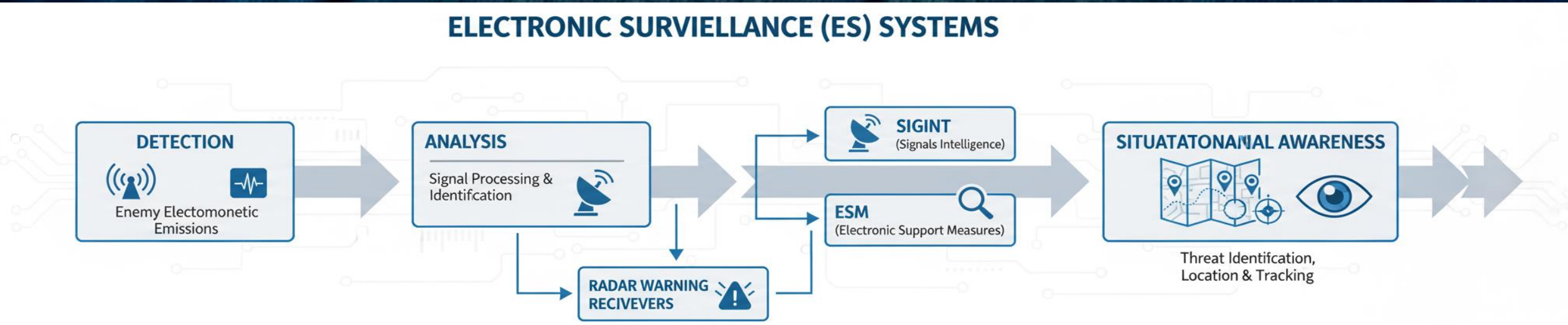
- The Double-edged Sword of Next Generation Networks
- 5G capabilities: Higher data rates, lower latency, and massive device connectivity compared to 4G/LTE
- Military applications: Enhanced C2, high bandwidth ISR, autonomous systems coordination, AR/VR training, and smart logistics
- Interference risks: 5G operates in frequency bands (3.5 GHz, 26 GHz) adjacent to military radar, SATCOM, and weather systems
- GPS vulnerability: Commercial 5G deployments near GPS frequencies (1.5 - 1.6 GHz) risk interference with military navigation
- Security concerns: 5G supply chain vulnerabilities, especially equipment from adversary nations, create cyber and EW risks
- Antijamming challenges: Military 5G systems require enhanced security and resilience features not present in commercial networks

Understanding Electronic Warfare

- Electronic Warfare: Military action using electromagnetic energy to control the spectrum or attack the enemy
  - Electronic Support (ES): Detect, identify, locate, and analyze enemy electromagnetic emissions for threat warning and targeting
  - Electronic Attack (EA): Use electromagnetic energy to disrupt, degrade, deceive, deny, or destroy enemy combat capability
  - Electronic Protection (EP): Actions taken to protect personnel, facilities, and equipment from friendly or enemy electromagnetic effects
- Dual nature: EW is both offensive (disrupting enemy systems) and defensive (protecting friendly systems from enemy interference)
- Integration: All three EW pillars work together to gain and maintain electromagnetic advantage required for mission success

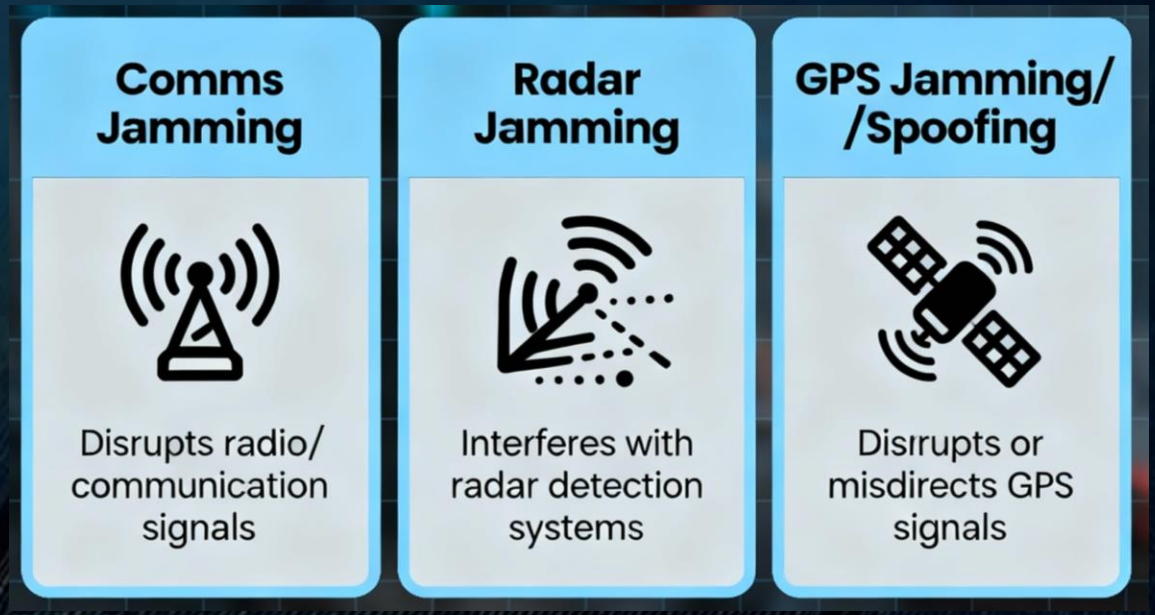
Electronic Support (ES): Finding and Tracking the Enemy

- ES systems: Passively detect and analyze enemy electromagnetic emissions without transmitting themselves
- Capabilities: Search, intercept, identify, locate, and characterize enemy radars, communications, and electronic systems
- Immediate threat warning: Radar warning receivers (RWR) alert aircrews to missile threats and targeting radars
- Supports targeting: Electronic surveillance measures (ESM) locate enemy emitters for attack by friendly fires
- Feeds intelligence: SIGINT systems collect enemy communications and radar signatures for analysis and database updates
- Foundation: ES is the foundation of situational awareness in the electromagnetic environment—knowing what the enemy is doing



Electronic Attack (EA): Disrupting and Defeating Enemy Systems

- Uses electromagnetic or directed energy weapons to attack enemy personnel, facilities, or equipment
- Jamming: Transmit high-power noise or deceptive signals to prevent enemy receivers from detecting intended signals
- Types of effects: Deny (prevent use), Degrade (reduce effectiveness), Deceive (false information), Disrupt (interrupt flow), Destroy (hard kill)
- Communications jamming: Blocks enemy tactical radios, cellular networks, SATCOM, and data links
- Radar jamming: Masks friendly platforms from detection or injects false targets into enemy radar displays
- GPS jamming/spoofing: Denies enemy navigation capability or causes weapons to miss targets by providing false position data



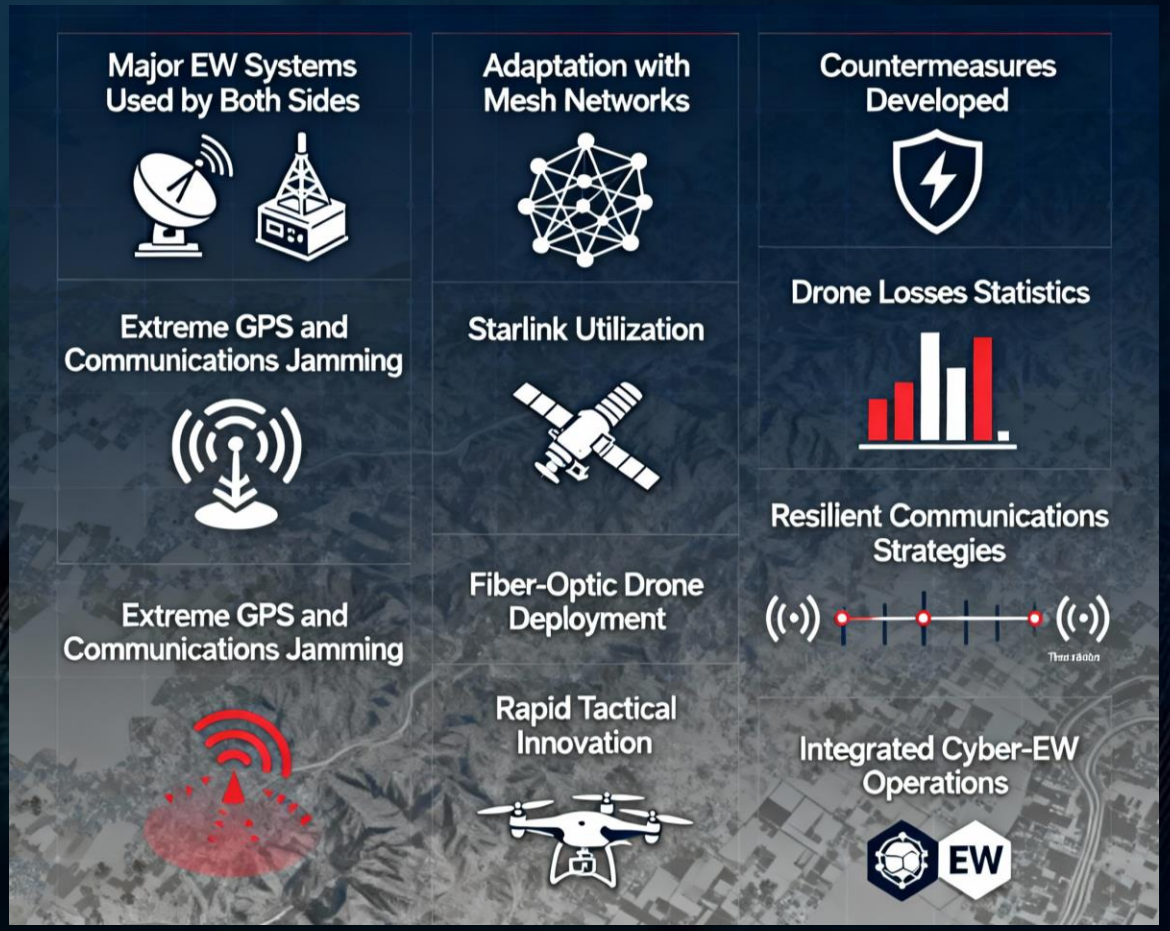
Electronic Protection (EP): Defending Friendly Systems

- Technical measures: Frequency agility (frequency hopping), spread spectrum, directional antennas, power management
- Operational measures: Emission control (EMCON), frequency management, spectrum deconfliction, and coordination
- SINCGARS advantage: Frequency hopping at 100 hops per second makes it extremely difficult for enemy to jam or intercept
- Receiver protection: Hardening, filtering, and antijam features prevent enemy EA from disrupting friendly receivers
- Mission assurance: EP ensures friendly forces can use the spectrum even when under electronic attack—maintaining communications and sensors

Protects friendly forces from enemy electronic attack and from unintentional electromagnetic interference

Russia Ukraine War: Electronic Warfare Lessons Learned

- Scale of EW: Largest use of electronic warfare in modern conflict—both sides extensively employ EW across the battlefield
- Russian GPS/GNSS jamming: Disrupts Ukrainian drone operations, precision munitions, and Blue Force Tracking systems
- Communications jamming: Russian systems deny Ukrainian tactical communications, forcing use of less secure alternatives
- Electronic warfare targeting: Detecting enemy emitters and using their electromagnetic signatures for lethal targeting
- Contested environment: Neither side achieved electromagnetic superiority—contested EMS prevented air superiority and affected all ground operations
- **Key lesson: Assume your electromagnetic emissions will be detected, targeted, and jammed in near-peer conflict**



How Electronic Warfare Affects Your Mission

- Communications disruption: Jammed radios prevent coordination, calling for fire support, or requesting MEDEVAC
- Navigation degradation: GPS jamming or spoofing causes position errors, mission delays, and potential fratricide from BFT failure
- ISR denial: Jammed UAV links blind commanders to enemy activity and prevent reconnaissance of objectives
- Weapon system failures: Precision guided munitions miss targets, electronically fused artillery becomes ineffective
- Force protection compromise: Enemy locates your position by detecting your transmissions and targets you with indirect fires
- Loss of situational awareness: Degraded communications and data links create information gaps that lead to poor decisions

Direct Impact on Operations

Every Transmission Reveals Your Position

- All emitters detectable: Every device that transmits—radio, GPS, cell phone, WiFi, Bluetooth—creates a detectable electromagnetic signature
- Detection capability: Enemy electronic support systems can detect your transmissions from long distances and use them to locate you
- Signature reveals: Your location, unit type, size, activity level, and operational patterns
- Real-world example: 2014 Ukraine—Russian forces targeted Ukrainian artillery battalion using app data from soldiers' personal smartphones
- Power/duration factor: Higher power and longer transmissions = greater detection probability and vulnerability to enemy targeting
- Personal devices danger: Personal electronic devices (phones, smartwatches, fitness trackers) continuously transmit and betray your position

Emission Control (EMCON): Managing Your Electromagnetic Footprint

- Balancing Communications Needs Against Signature
- EMCON level protocols are service-specific.
- In general, F EMCON levels from most permissive to most restrictive based on threat assessment
- Tradeoff: Leaders balance communications needs against signature management—more restrictive EMCON reduces capability but increases survivability

Level	Typical Description	Purpose
Alpha	Maximum silence (no intentional emissions)	Most restrictive, avoid all detection
Bravo	Limited emissions, essential equipment only	Some sensors/mission gear allowed
Charlie	Mission-essential emissions	Moderate restrictions, key systems active
Delta	Normal operations, minimal restriction	Least restrictive, routine ops

EMCON Best Practices: Reducing Your Vulnerability

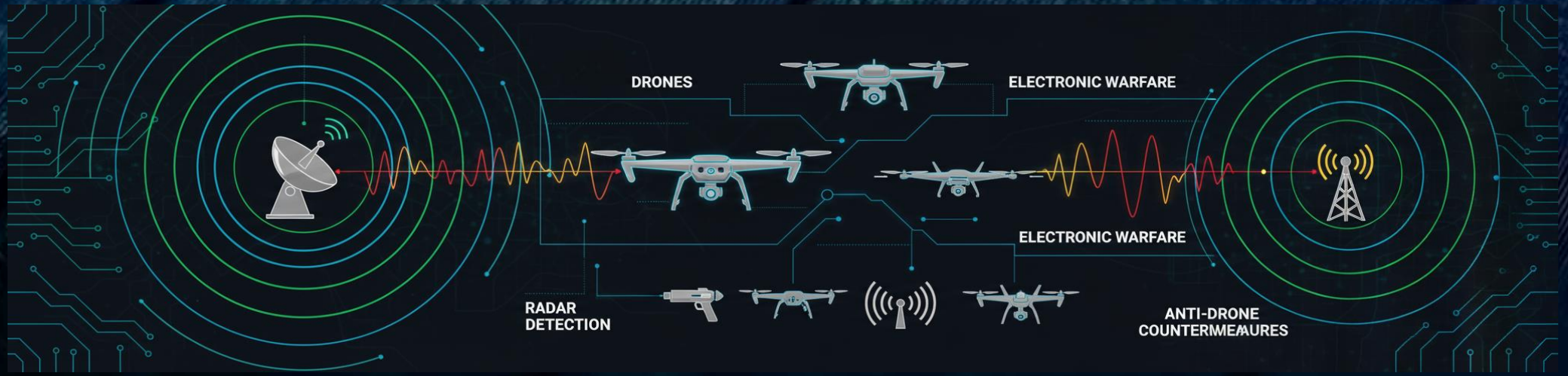
- Minimum power: Use lowest power setting necessary for communications—reduces detection range and extends radio battery life
- Directional antennas: Employ when possible—focuses signal toward intended receiver and away from enemy sensors
- Terrain masking: Position behind hills or buildings to shield transmissions from enemy direction-finding systems
- Transmission brevity: Limit transmission duration—keep radio calls brief using proper brevity codes and prowords
- Vary patterns: Vary transmission times and patterns—unpredictable emission schedules complicate enemy collection and targeting
- Lower antennas: Minimize antenna height—lower antennas reduce detection range while maintaining local communications capability

Tactical Techniques for Emission Control

Counter Unmanned Aircraft Systems and Electronic Warfare

- Threat proliferation: Commercial drones modified for ISR, attack, and resupply create new battlefield threats
- Detection methods: Radar, radio frequency sensors, electrooptical/infrared cameras identify and track hostile drones
- Electronic warfare defeat: RF jammers disrupt drone control links and GPS navigation, causing loss of control or crash
- GPS spoofing: Inject false position data to redirect drones away from protected areas or force-controlled landing
- Layered defense: Combine detection sensors, electronic attack, and kinetic effects (nets, lasers, projectiles)
- Integration challenge: CUAS systems must coordinate with air defense networks to avoid fratricide of friendly aircraft

Defeating the Proliferating Drone Threat



Directed Energy Weapons: The Future of Electronic Warfare

- Directed Energy Weapons use focused electromagnetic energy (lasers) or high-power microwaves to defeat threats
- High Energy Lasers (HEL): Engage drones, rockets, mortars, and aircraft at speed of light with unlimited magazine depth
- High-power Microwave (HPM): Generate electromagnetic pulses that damage or destroy electronic components in enemy systems
- Advantages: Precision effects, low cost per shot (cents vs. thousands for missiles), rapid engagement, no logistical tail
- Current limitations: Weather dependent (fog/rain affects lasers), line-of-sight only, require significant electrical power
- Fielding timeline: Army expects first directed energy systems of record in FY26; Navy and Air Force conducting operational tests

Cognitive Radio and Software Defined Radio: Adaptive Communications

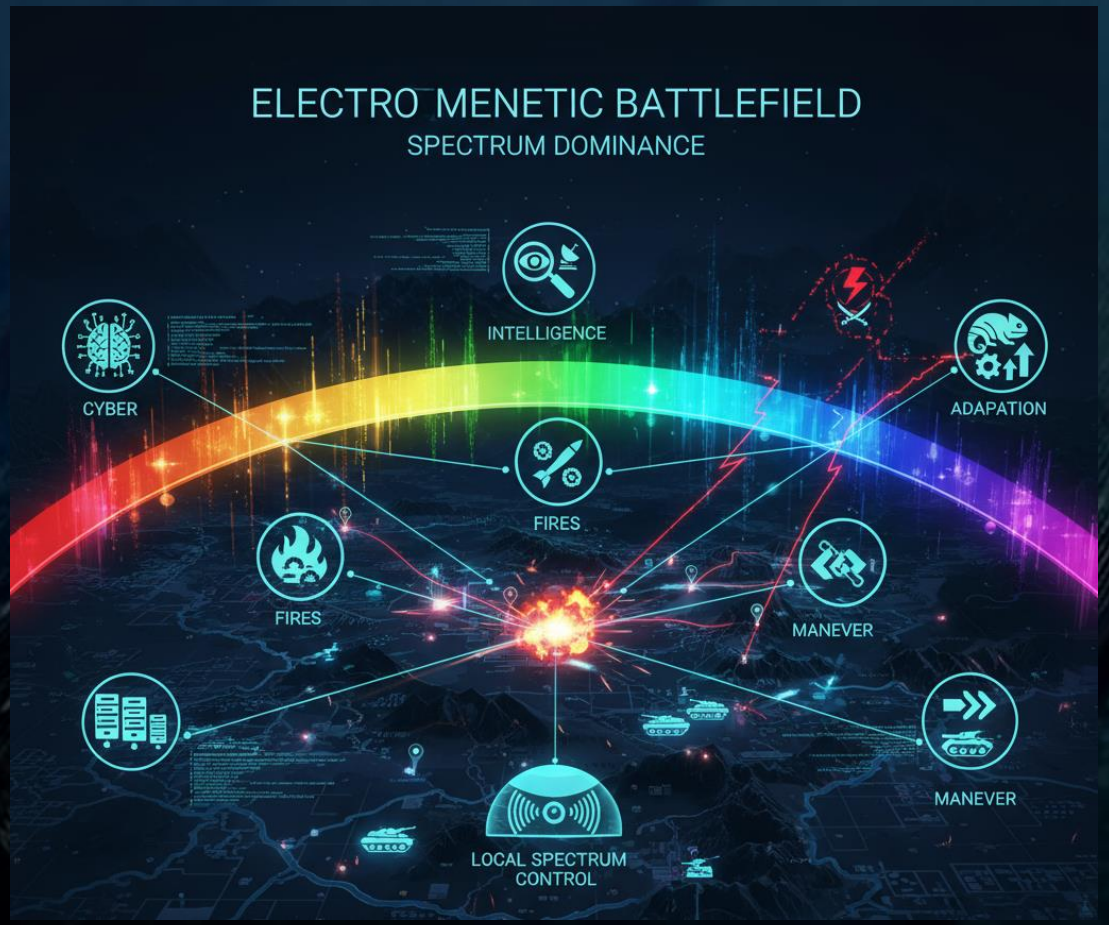
Next Generation Communications Technology

- Software Defined Radio (SDR): Radio functions implemented in software on programmable hardware rather than fixed circuits
- Flexibility advantage: Waveforms and frequencies can be changed through software updates rather than hardware replacement
- Cognitive Radio: SDR enhanced with environmental awareness and ability to dynamically adapt operating parameters
- Dynamic spectrum management: Automatically scans for available channels and switches frequencies to avoid interference and jamming
- Electronic warfare resistance: Frequency hopping protocols and transmission security features protect against interception
- Future capability: Future military radios will sense the electromagnetic environment and automatically adapt to maintain reliable communications

Key Takeaways for Service Members

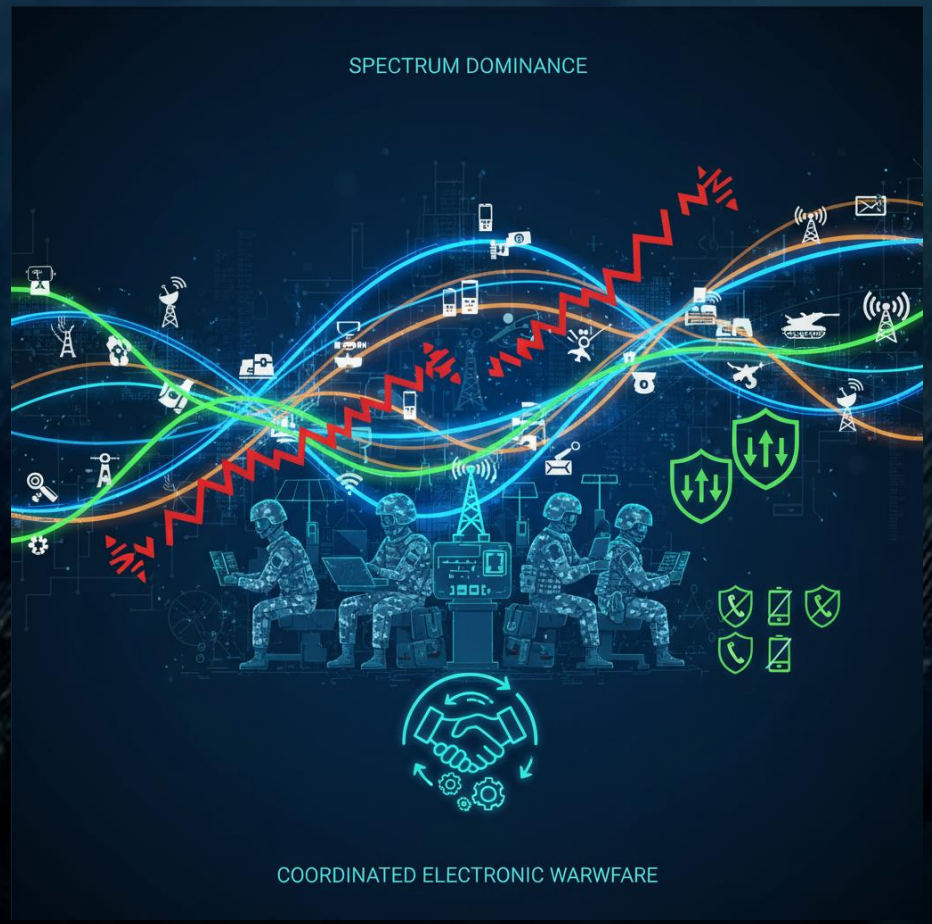
- Contested domain: The electromagnetic spectrum is a contested warfighting domain—expect enemy electronic warfare in future conflicts
- Signature matters: Your electromagnetic signature matters—every transmission is a potential liability that can reveal your position to the enemy
- Manage emissions: Use EMCON procedures, minimum power, directional antennas, and brevity to reduce vulnerability
- No personal devices: Leave personal devices behind—smartphones and smart devices continuously transmit and compromise operational security
- Everyone's responsibility: Electromagnetic discipline is everyone's responsibility—your actions directly impact mission success and unit survivability

The Strategic Importance of EMS Superiority



- Operational dependency: Modern military operations are impossible without access to the electromagnetic spectrum
- Adversary investment: Near peer competitors have invested heavily in electronic warfare to deny U.S. forces spectrum access
- Local superiority goal: Electromagnetic local superiority—controlling the spectrum in specific time and place to accomplish the mission
- Integration requirement: EMS operations must be synchronized with cyber, intelligence, fires, and maneuver
- Continuous adaptation: Electronic warfare is a dynamic cat and mouse game requiring constant innovation
- Future warfare: Victory in future conflicts will depend on our ability to operate effectively in congested and contested electromagnetic environments

Summary



- Mastering the electromagnetic spectrum is everyone’s responsibility; your discipline and knowledge in this domain directly impact mission success and the safety of your team on the battlefield
- Electromagnetic environment will be crowded with civilian and military systems and contested by adversaries capable of detecting, jamming, or targeting your emissions. Success demands constant awareness and strict electromagnetic security
- Every transmission exposes a signature vulnerable to enemy exploitation. Control your emissions, avoid personal devices, know your unit’s EMCON and PACE plans, and always train for disrupted spectrum operations—the future of warfare relies on it

Resources and Further Learning

- Joint Publication 313.1: Electronic Warfare (latest edition) for detailed EW doctrine and procedures
- Air Force Doctrine Publication 385: Electromagnetic Spectrum Operations for comprehensive EMSO concepts
- ATP 312.3: Electronic Warfare Techniques for tactical procedures and employment guidance
- Unit plans: Study your unit's specific EMCON and PACE plans and practice implementing them
- Training ranges: Participate in Electronic Warfare Training Range exercises to experience jamming and practice countermeasures
- Contact information: Questions? Contact your unit Electronic Warfare Officer, S6/G6 communications staff, or Spectrum Manager