CHAPTER XI

ELECTRONIC WARFARE

A. DESCRIPTION

Electronic Warfare (EW) encompasses the capability to disrupt or degrade an enemy's defenses throughout the areas and times—and across the entire electronic, infrared (IR), and visual spectrums—required to permit the deployment and employment of U.S. and allied combat systems. Electronic Warfare includes capabilities for deceiving, disrupting, or destroying enemy surveillance, command and control (C^2), and weapon systems/sensors (e.g., early warning, acquisition, and targeting functions) associated with the enemy's integrated air/area defense network. EW also includes the critical capabilities of recognizing attempts by hostile systems to track or engage U.S. or friendly forces, automatically initiating the appropriate countermeasures or defensive response, and protecting friendly systems through redundancy and hardening.

B. OPERATIONAL CAPABILITY ELEMENTS

The strategic goal of EW is to control and exploit the electromagnetic spectrum for maximum effectiveness of U.S. military operations—that is, to deny, disrupt, degrade, deceive, or exploit enemy use of the full electromagnetic spectrum while ensuring its use by friendly or joint forces. Successful attainment of this goal necessarily confers a superior capability on U.S. military and friendly forces to survive in their execution of all required combat, conflict operations, and missions. EW has three principal and integral operational capability elements (OCEs): electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). Each element provides a range of benefits to participants in joint organizations and operations, and can be executed in the absence of a greater command and control warfare (C^2W) or information operations (IO) strategy. Figure XI–1 depicts these principal elements as they contribute to joint operations.

Electronic attack involves the defensive or offensive protection of U.S. forces and platforms against hostile weapon, sensor, and C^3 systems. In its traditional form (*self-protection*), EA consists of a warning receiver to warn of impending weapon attack (*attack warning*), expendable countermeasures, and a jamming system working in concert to prevent sensor-guided weapons from hitting their target. The defensive protection aspects of attack warning and platform self-protection are strongly synergistic with the defensive measures and goals described in the Protection of Space Assets JWCO (Chapter XIV). More recent technology further expands the boundaries of electronic attack by engaging sophisticated, long-range target acquisition sensors—such as airborne and space-based surveillance/synthetic aperture radars, and the increasingly modern communications supporting all phases of the enemy attack or defense—thereby becoming a key, integral element of battlespace dominance. Therefore, EW and its EA element play a prominent, vital role in the new, "leveraged" concept of full-dimensional protection, as described in the Chairman of the Joint Chiefs of Staff's *Joint Vision 2010*.

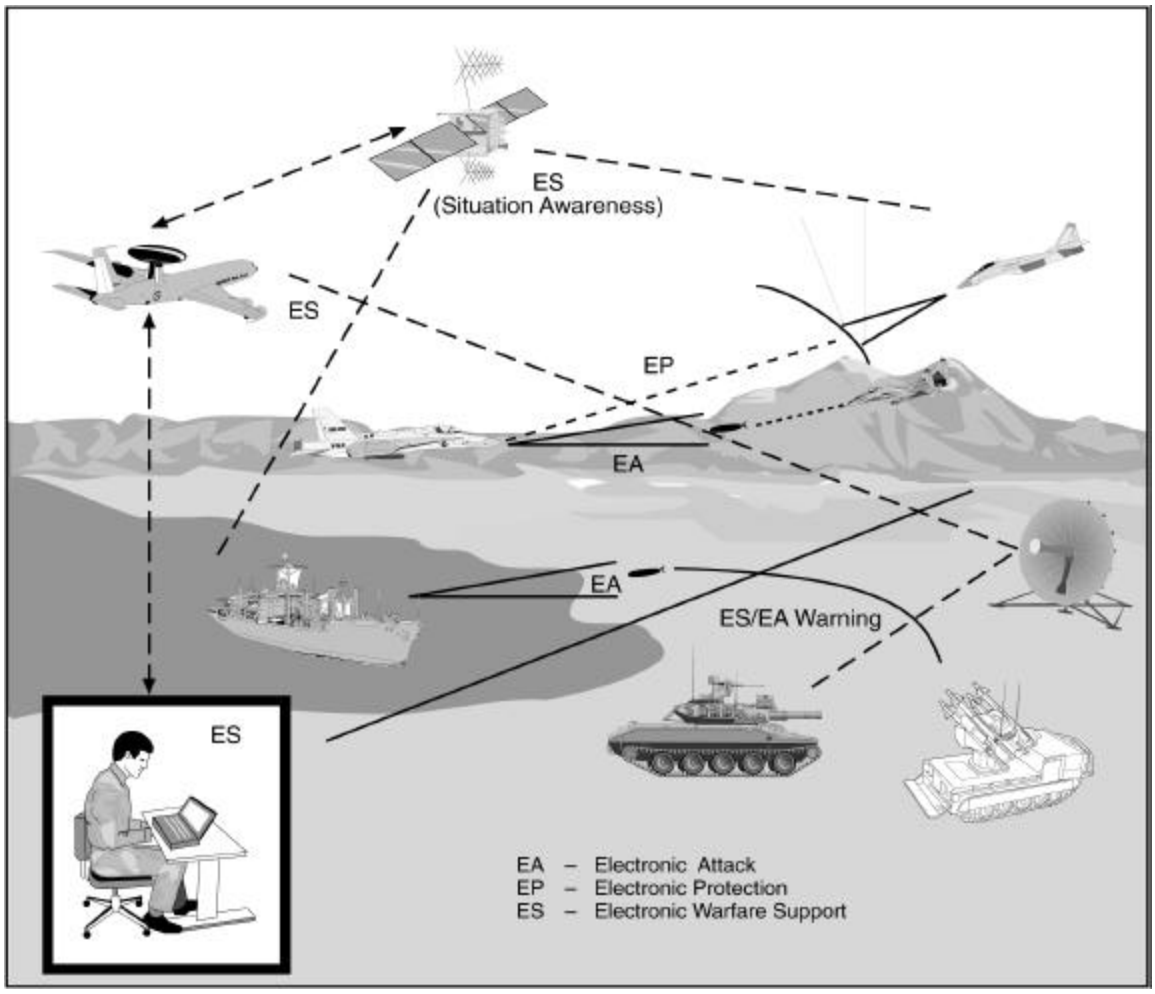


Figure XI–1. Concept—Electronic Warfare

One critical aspect of electronic attack is the ability to deny an opponent the reliable use of his own command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) systems—thereby permitting U.S. platforms and forces to operate freely throughout the battlespace with minimal loss to hostile weapons. Such freedom is gained due to confusion, analysis, and decision delays induced and propagated within the enemy's C^4ISR infrastructure regarding the location(s), structure, and intent of joint forces. This EA strategy is an enabling capability for operations requiring penetration of hostile territory (e.g., suppression of enemy air defense (SEAD), close air support (CAS), counter-C^3, and precision attack on any fixed or mobile target). Thus, again, electronic attack plays a prominent role in the *Joint Vision 2010* concept of dominant maneuver by virtue of aiding the control of operational tempo, and EA is synergistic with the Information Superiority JWCO (Chapter IV).

Electronic protection supports the development of design features and employment techniques that allow U.S. forces to enjoy the benefits of accurate electronic sensors and systems, both offensive and defensive—despite an environment that includes hostile jamming, deception activity, and enemy weapon targeting that, itself, depends on detecting, recognizing, and determining the location of U.S. emitters. EP allows operational users to initiate and prosecute a mission without degradation from opposing EW or from conventional or directed-energy weapons cued or targeted by hostile sensors. Successes in EP techniques translate into effective targeting

by joint combatants and reliable communications, surveillance, and electronic support sensors—corresponding to the JWCOs of Precision Fires (Chapter V) and Information Superiority (Chapter IV).

Electronic warfare support is the EW element that gathers, consolidates, and employs information from hostile or potentially hostile electronic sensors and C^3 systems. ES is critical to developing a comprehensive picture of the battlespace and a reliable indication of hostile force movement and intentions. ES allows force avoidance, efficient engagement, and electronic deception—EA—of enemy sensors, weapons, and communications systems. The classic definition of ES recognizes its functionality from the joint operational commander level down to the "single-seat" cockpit combatant. With increasingly sophisticated, worldwide, modern weapon systems, the pressures for ever-increasing ES fidelity are blurring the older distinctions between the classic radar warning receiver (attack warning) and the longer range electronic support measures (ESM) systems. Therefore, in the future, all joint combatants/platforms can be integrated into the battlespace picture via the contributions of their ES systems. ES enables a wide range of operational options that contribute to virtually every combat and peacekeeping mission. Hence, ES is strongly synergistic with the JWCOs of Information Superiority (Chapter IV), Precision Fires (Chapter V), Combat Identification (Chapter VI), Protection of Space Assets (Chapter XIV), and the associated concept of precision engagement presented in *Joint Vision 2010* (Reference 4).

C. FUNCTIONAL CAPABILITIES

Table XI–1 depicts the relationships between operational capability elements and functional capabilities for the EA and ES components of EW. Because electronic protection capabilities are generally specific to a sensor or C^3 system, the EP component is not addressed further in this section.[1] From a basic technology perspective, refer to the *Defense Technology Area* Plan (DTAP), Chapter VII, Sensors, Electronics, and Battlespace Environment; and Chapter X, Weapons (EW Mission Support) (Reference 3). Note that in next year's edition of the DTAP (FY01), the reporting/oversight of all EW technology moves from the Weapons panel/chapter to the reorganized Sensors, Electronics, and EW (SEEW) panel/chapter. DTAP EW DTOs have already been renumbered in accordance with this new panel (i.e., SE.xx).

D. CURRENT CAPABILITIES, DEFICIENCIES, AND BARRIERS

Current EW capabilities are generally the result of extensive, detailed concentration on the capabilities of the former Soviet Union. However, in the intervening 10 years since its breakup, a more complex, evolving, worldwide threat environment has emerged—one that threatens the continued viability of these current EW techniques, yet possesses clear, global military technology trends that allow identification of the most prominent deficiencies and barriers to joint EW operations of the future. Table XI–2 provides a top-level summary of capabilities, limitations, and key technologies to overcome current limitations and to provide those capabilities.

[1]For example, protecting operational usage of GPS is dealt with, in part, by the Navigation Warfare ACTD.

Table XI–1. Functional Capabilities Needed—Electronic Warfare

Functional Capabilities	Operational Capability Elements									
	Electronic Attack						Electronic Protection	Electronic Warfare Support		
	Attack Warning	Aircraft Protection	Ship Protection	Land Combat Vehicle Protection	C² Attack	Lethal SEAD		Signal Collection	Emitter ID/Location	Battlespace Awareness
1. Real-Time Threat Detection, ID, and Geolocation	●	●	●	●	●	●	Not addressed in this Joint Warfighting S&T Plan	●	●	●
2. Missile Approach Warning	●	●	●	●		●				●
3. Modular, Programmable EW Receiver/Processor	●	○	○	○	●	●		●	●	●
4. Sensor/Data Fusion, Electronic Intelligence	●	●	●	●	●	○		●	●	●
5. Decoy Terminal Threat Weapons		●	●	●		●				
6. UAV EW Employment	○	●	●	●	●	●		●	●	●
7. Robust, Multispectral EA of Simultaneous Threats		●	●	●		●				
8. Broadband, Coherent, Surgical RF Countermeasures		●	●	●	●	○				
9. Second-Generation Directed IRCM		●	●	●						
10. Laser-Based IRCM		●	●	●						
11. Counter IADS Surveillance, Acquisition, and C²		●	●	●	●	○		○	○	○

● Strong Support ○ Moderate Support

Table XI–2. Goals, Limitations, and Technologies—Electronic Warfare

Goal	Functional Capabilities	Limitations	Key Technologies
Operational Capability Element: Electronic Attack—Platform Protection			
>99% combined probability of no hostile weapon launches or misses	*Attack Warning* 1. Real-time RF threat detection, ID, and geolocation 2. Missile approach warning 3. Modular, programmable EW receiver/processor 4. Sensor/data fusion, electronic intelligence	1. Slow, inaccurate, and ambiguous threat ID, and bearing resolution 2. Limited probability of intercept in dense, high-signal, high-clutter environment 3. Simultaneous, overlapping signals 4. Incomplete/uncorrelated a priori database information 5. Unpredictable emitter mode changes, and tracking thereof	1. Advanced signal ID and detection algorithms 2. Distributed/parallel COTS multiprocessors 3. High-sensitivity, multiband detectors 4. Directional apertures 5. Digital and channelized receivers 6. Low-false-alarm, high-sensitivity missile warning, with accurate "time-to-go" 7. Real-time techniques for correlation/fusion of all-source information/data
	Expendable/Decoy Countermeasures 5. Decoy terminal threat weapons 6. UAV employment 7. Robust, multispectral EA of simultaneous threats	Item 1 above, plus: 6. Unmatched/incoherent spectral content and output profile/signatures 7. Tight packaging constraints 8. High cost of integrating multispectral capability(s) 9. Inaccurate ejection timing, leading to rapid stores depletion	Items 1, 3, 5, & 6 above, plus: 8. Enhanced IR flare materials 9. Kinematic/aerodynamic techniques 10. Digital RF memories (DRFMs) 11. VHSIC/application-specific ICs (ASICs) 12. MMIC/microwave power module (MPM) amplifier technologies 13. Cooperative DIRCM/ laser-based IRCM EA techniques (item15 below) 14. Signature modification/control and location masking techniques (e.g., chaff, smoke, aerosols)

Table XI–2. Goals, Limitations, and Technologies—Electronic Warfare (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Operational Capability Element: Electronic Attack—Platform Protection (continued)			
	Coherent Jamming Item 7 above, plus: 8. Broadband, coherent, surgical RFCM 9. Second-generation directed IRCM (DIRCM) 10. Laser-based IRCM 11. Counter IADS surveillance, acquisition, and C^2	Items 1, 2, 3, 5, 6, 7, & 8 above, plus: 10. High retrofit costs 11. Nonintegrated approach to EA of multispectral/multimode threats	Items 1, 3, 4, 5, 10, 11, 12, 13, & 14 above, plus: 15. Affordable, compact laser (min. 2 W/20 kHz, mid IR) 16. Coherent, doppler, monopulse, and false target CM techniques
Operational Capability Element: Electronic Attack—C^2W and SEAD			
Exploit, disrupt, deceive modern integrated defense system/ network	*Complex C^2 Signal Identification* Items 1, 3, 4, & 6 above	Items 1, 2, 3, 5, 7, & 10 above, plus: 12. Insufficient low-noise signal intercept and decoding techniques 13. Inability to track/jam in real time	Items 1, 2, 4, 5, 7, & 11 above, plus: 17. Negative signal-to-noise signal and code ID/tracking algorithms 18. Parallel signal channel tracking and algorithm techniques 19. Near-real-time code-breaking techniques
	Nonfratricidal C^2 Jamming Items 6, 8, & 11 above	Items 1, 2, 3, 5, 7, 10, & 13 above, plus: 14. Nonlinear power amplification 15. Imprecise coding/ signal demodulation 16. Poor beam/radiation control	Items 2, 5, 10, 11, 17, & 19 above, plus: 20. High-efficiency, linear, solid-state amplifiers (HF, VHF, UHF) 21. C^2-frequency MPMs 22. Efficient HF, VHF, UHF antenna designs (e.g., high-temperature, superconductivity arrays)
	Lethal SEAD Items 1, 3, 4, 5, 6, 7, 8, & 11 above	Items 1, 3, 4, 5, 6, 7, & 8 above, plus: 17. Affordability of UAV decoys 18. Affordable, compact RF support jamming (stand-off/ stand-in) techniques	Items 1, 2, 4, 5, 10, 11, & 12 above, plus: 23. Frequency/bandwidth aperture function control techniques (EA vs. ES) 24. Large-extent phased arrays
Operational Capability Element: Electronic Protection (Not considered in this document)			
Operational Capability Element: Electronic Warfare Support			
> 99% probability of signal intercept, detection, ID, and location across EM spectrum, mission, and battlespace	*High-Fidelity Signal Recognition and Tracking* Items 1, 2, & 3 above (item 2 in mission/platform context of missile warning sensor (MWS) contributions to battlespace awareness/situation assessment)	Items 1, 2, 3, 4, 5, 10, & 12 above, plus: 19. Insufficient processing time and "power" 20. Little interoperability between operational/service systems	Items 1, 2, 3, 4, 5, 6, 7, 11, 17, 18, & 19 above, plus: 25. Sub-1-degree aperture/beamforming systems 26. Rapid (e.g., GHz), high-fidelity (e.g., 10-14 bit) analog-to-digital conversion hardware/processing 27. Software-reconfigurable/"open" architectures

Table XI–2. Goals, Limitations, and Technologies—Electronic Warfare (continued)

Goal	Functional Capabilities	Limitations	Key Technologies
Operational Capability Element: Electronic Warfare Support (continued)			
	All-Source Data Integration/Fusion Item 4 above	Items 1, 2, 3, 4, 5, 15, & 19 above, plus: 21. Inability to deal with missing, incomplete, and corrupted data	Items 1, 2, 4, 5, 7, & 27 above, plus: 28. Expert systems and algorithms (knowledge-based information representation and computer "reasoning" techniques that allow manipulation of sensor, text, and archival/library data in one process)
	Hostile Battlespace Signal Intercept/ Collection Items 6 & 11 above	22. Vulnerability of conventional manned platforms	Items 1, 2, 5, 7, 11, 19, 26, & 27 above, plus: 29. UAV payloads 30. Wideband datalinking

The threat of passively guided weapons has increased dramatically over the past decade. Today, infrared-guided weapons pose a serious and growing threat to U.S. forces and platforms in the air, on land, and at sea. Inexpensive, portable missiles can be launched with ease and effectiveness against all airborne combatants. The threat of longer range infrared guided antiship missiles is equally great, and formidable in both at-sea and littoral scenarios. Land combat vehicles are similarly threatened by frontal and top-attack munitions guided by infrared and multispectral seekers. *Protection against infrared guided weapons is the highest priority need in electronic attack* and is an important deficiency that constrains the efficient execution of joint operations.

The technology barriers to resolutions of these EA deficiencies include inadequate detection range and angular resolution on attack warning systems to eject decoys or initiate jamming; insufficient power, low efficiency, and unacceptable size, weight, and cost of laser devices that could be used in countermeasure systems; and insufficient output power and excessive size, weight, and cost of high-power microwave systems for self-protection of platforms. Of particular concern in the high-power microwave arena is the integration of this weapons-level EW effect into operational concepts of Joint Forces—so as to avoid or mitigate the possible, self-inflicted, mission-degrading effects of electronics fratricide and platform "suicide." Each of these barriers is being addressed with ongoing technology demonstration programs.

As a second area of high EA priority, the rapid development and adoption of new communications technology has created deficiencies in the ability of U.S. forces to exploit and selectively disrupt modern signals. Cellular and personal communications systems used by civilians and hostile forces, and high-capacity digital, multichannel networks associated with distributed information systems, pose particularly difficult technical challenges. The ability to detect, analyze, exploit, and disrupt these signals is fundamental to the conduct of joint operations against an opponent with modern communications equipment and sensors. In the context of EA, jamming transmitters and antennas used against C^3 signals require improvements in precise modulation selection and modulator control, linearity, efficiency, output power, and directivity.

Electronic protection measures are generally specific to a sensor or C^3 system. EP measures entail the tailoring of generic protection technology and techniques (again, as treated in the

respective DTAP chapters) to satisfy the electronic protection requirements of a specific system in order to ameliorate the effects of hostile jamming, deception, targeting, or directed-energy attack. Although included as an element of EW, these efforts are an integral part of the sensor or C^3 development program (e.g., GPS). As stated previously and noted in Table XI–2, further EP details are omitted from this section.

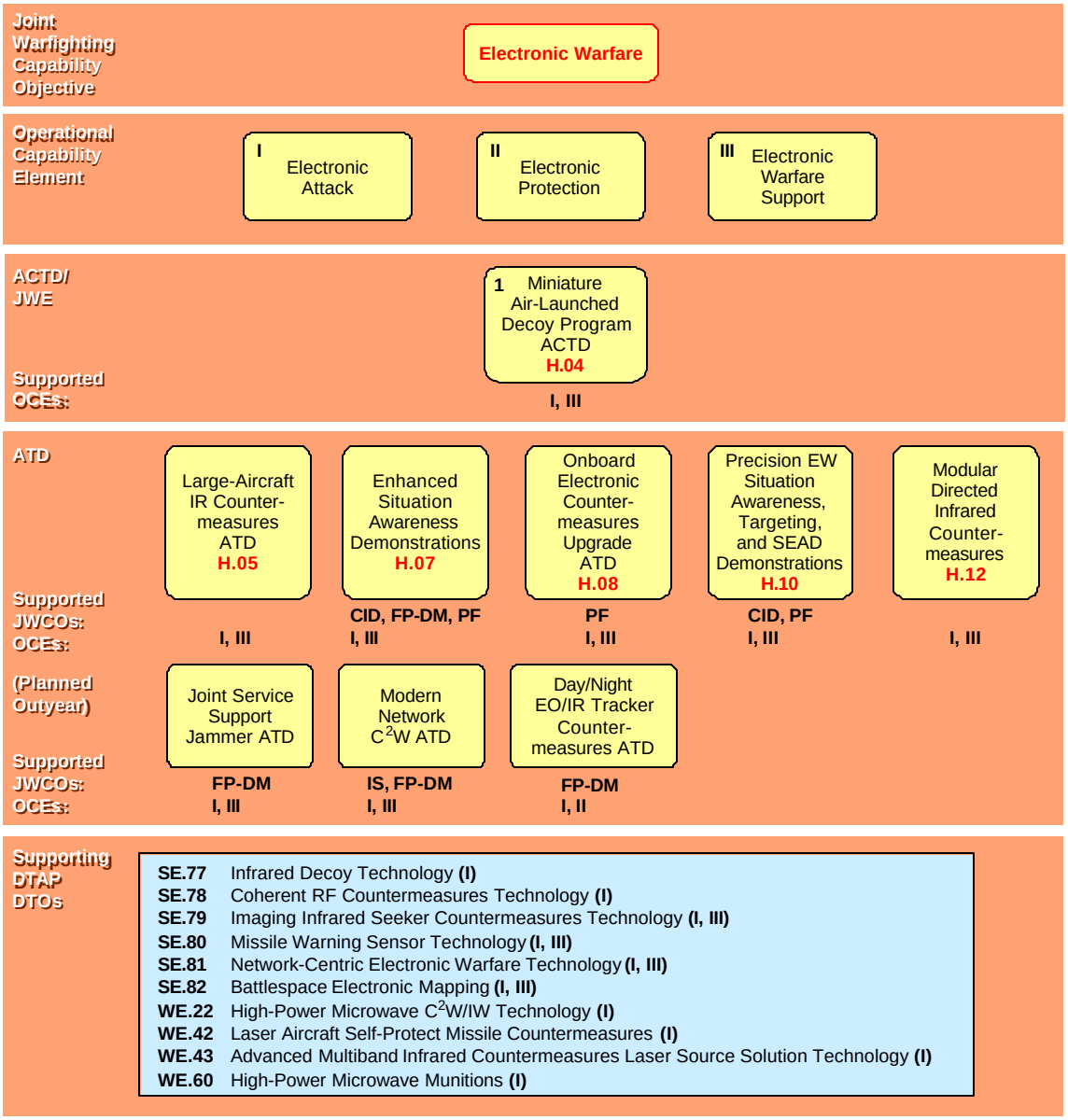
Electronic support is the activity that gathers timely information on hostile force composition, status, and intentions by intercepting and analyzing the signals from hostile electronic systems and integrating this information with that from our own forces and electronic systems—whether at the joint command, at-sea battlegroup, or single-seat cockpit/battlefield soldier level. The composition and characteristics of C^3 systems are changing rapidly as low-cost, high-performance digital technology becomes universally available. The proliferation of this technology has also encouraged the widespread availability of cellular and personal communications devices that are highly mobile and resistant to conventional electronic attacks. Optical fiber networks, coupled with increasingly more powerful computers, constitute the basis for powerful information systems that support sophisticated military C^3 functions as easily as civilian applications. These advances in processing and communications technology facilitate and encourage the acquisition of customized, unique C^3 systems in the military forces of many small countries. This diversity and unpredictability constitutes a formidable challenge to ES organizations that must support operational users with services and products in any conceivable location and situation.

As advanced knowledge of threat system parameters—necessary for attack warning and countermeasure waveform development—becomes more difficult to obtain, EW receivers on tactical aircraft, ships, and land combatants will have to assume some of the burden formerly assigned to dedicated special signal collection receivers (i.e., the "blurring" regarding ES as discussed in Section B above). This will be necessary to accumulate detailed information on classes of emitters, as well as individual emitters, and to support the development of generic system recognition algorithms.

The ability to fuse different forms of information from multiple sources is an important capability in an environment of mixed-media signals. Algorithms that can analyze and consolidate information from different sensors and databases can produce a product that is more complete and informative than the sequential examination of the individual contributions. In time-critical situations, algorithms using expert system techniques and artificial intelligence principles can represent and manipulate knowledge faster and more exhaustively than is possible using human analysts.

The technology deficiencies in electronic warfare include incomplete development of technologies suitable for unmanned aerial vehicles (UAVs) used for signal collection/ES missions (and linkages/extrapolations of this technology to broadband RF support EA countermeasures from UAV platforms); inadequate processing subsystems and algorithms for detection, identification, and analysis of new communications waveforms; unacceptable performance in signal collection against mixed-media networks containing fiber optic and other transmission media; and inadequate performance and excessive cost to acquire and maintain warning and signal collection capabilities in tactical EW receivers. Finally, current capabilities in the representation of data, automated sensor product analyses, and machine reasoning capabilities are insufficient to perform timely and complete sensor product and data fusion.

Figure XI–2 illustrates how technology developments support technical demonstrations that contribute to OCEs in Electronic Warfare. Table XI–3 correlates the technical demonstrations with the OCEs that they support.



PF: Precision Force; CID: Combat ID; FP-DM: Force Projection/Dominant Maneuver; IS: Information Superiority

Figure XI–2. Technology to Capability—Electronic Warfare

Table XI–3. Demonstration Support—Electronic Warfare

Demonstration	Operational Capability Elements			Service/ Agency	DTO	Type of Demonstration	
	Electronic Attack	Electronic Protection	Electronic Warfare Support			ACTD	ATD
Miniature Air-Launched Decoy Program ACTD	●	Not addressed in this Joint Warfighting S&T Plan	○	DARPA, Air Force	H.04	X	
Large-Aircraft Infrared Countermeasures ATD	●		●	Air Force	H.05		X
Enhanced Situation Awareness Demonstrations	○		●	Air Force	H.07		X
Onboard Electronic Countermeasures Upgrade ATD	●		○	Air Force	H.08		X
Precision EW Situation Awareness, Targeting, and SEAD Demonstrations	○		●	Army, Air Force	H.10		X
Modular Directed Infrared Countermeasures	●		○	Army, Navy	H.12		X
Infrared Decoy Technology	●			Navy, Air Force	SE.77		
Coherent RF Countermeasures Technology	●			Army, Navy, Air Force	SE.78		
Imaging Infrared Seeker Countermeasures Technology	●		○	Army, Navy, Air Force	SE.79		
Missile Warning Sensor Technology	○		●	Army, Navy, Air Force	SE.80		
Network-Centric Electronic Warfare Technology	●		●	Navy	SE.81		
Battlespace Electronic Mapping	○		●	Army, Navy	SE.82		
High-Power Microwave C^{2}W/IW Technology	●			Air Force	WE.22		
Laser Aircraft Self-Protect Missile Countermeasures	●			Air Force	WE.42		
Advanced Multiband Infrared Countermeasures Laser Source Solution Technology	●			Air Force	WE.43		
High-Power Microwave Munitions	●			Air Force	WE.60		
Joint Service Support Jammer ATD	●		●	Air Force, Navy	(Planned)		X
Day/Night EO/IR Tracker Countermeasures ATD	●		●	Air Force	(Planned)		X
Modern Network C^{2}W	●		●	Air Force, Army	(Planned)		X

● Strong Support ○ Moderate Support

E. TECHNOLOGY PLAN

The technology plan incorporates cooperative and synergistic DTO projects being conducted by the Army, Air Force, Navy, and DARPA. Below is a list of the efforts by DTO:

- *H.04, Miniature Air-Launched Decoy (MALD) Program ACTD,* pursues the development of an affordable, air-launched decoy "stimulant" for application in the lethal suppression of enemy air defense (SEAD) mission.
- *H.05, Large-Aircraft Infrared Countermeasures ATD,* is an effort to develop and demonstrate the necessary technologies to achieve the advanced, closed-loop IRCM capability for the self-protection of large aircraft.

- *H.07, Enhanced Situation Awareness Demonstrations*, is an ATD-class program that will develop and demonstrate hardware and software approaches and techniques that provide aircrews timely threat warning/alert and enhanced situation awareness (SA).
- *H.08, Onboard Electronic Countermeasures Upgrade ATD*, will pursue advanced, integrated monopulse countermeasure techniques as an affordable, robust RFCM capability for use against the difficult coherent, monopulse class of threat radars.
- *H.10, Precision EW Situation Awareness, Targeting, and SEAD Demonstrations*, is a synergistic set of ATD-class efforts that will provide ground, rotary-wing, and tactical aircraft with the capability to precisely locate threat emitters via EW sensors, for SA cueing of onboard weapon indirect fire and SEAD targeting.
- *H.12, Modular Directed Infrared Countermeasures*, will provide advanced laser-based IRCM and missile warning sensors to allow for self-protection of both high-IR-signature (e.g., F–18 E/F, AV–8B) and rotary-wing tactical aircraft against surface-to-air-missiles (SAMs,) air-to-air missiles (AAMs), and antitank guided missiles (ATGMs.)

As emphasized in Section D above, a critical, coordinated tri-service plan to address vulnerability to IR missiles and weapons has been developed under Defense Reliance and is being executed. The program includes near- to mid-term measures to reduce vulnerabilities by using improved missile warning capabilities and advanced flares (DTAP DTOs SE.80 and SE.77, respectively), and by collaborating on how to defeat the emerging class of imaging infrared (IIR) seeker threats (SE.79). Coupled with laser source work under the DTAP (DARPA and WE.43), conventional laser-based IRCM solutions are in progress—notably the work under the recently completed H.02 (for rotary-wing aircraft) and the ongoing H.05 (for large aircraft). DTO H.02, which ended during the winter of FY00, attacked the problems of integrating advanced multi-band laser, fiber optic, and *open-loop* jamming algorithm technologies in order to lay the foundation for planned improvements to the Army's Advanced Threat IRCM (ATIRCM) system (ALQ–211). In fact, H.02 demonstrated the multiline DARPA laser connected to an ATIRCM EMD jam head using a fiber optic cable transmission line, and established preliminary technique requirements to counter the aforementioned IIR threat. H.05 will advance the IRCM state of the art by emphasizing the tough EW issues associated with protecting very large aircraft by implementing laser-based, *closed-loop* techniques. H.05 will proceed with live-fire air-to-air missile tests at the White Sands Missile Range cable car facility in FY00 and follow with a funded captive-carry missile seeker flight test option (a 1997 TARA recommendation). Critical subsystem technology risk reduction efforts are being formulated by the Air Force as a precursor to planned EMD in FY02. DTO H.12 builds upon H.02 and H.05 to apply advanced two-color missile warning and laser-based IRCM to tactical platforms (fighters/helicopters).

Capabilities to attack hostile command and control (C^2) networks will vastly improve with the development of transmitters with more efficient power amplification; modern, digital, EA modulation formats; and greater angular precision. These enhancements will effectively increase jamming power on victim systems and reduce interference with U.S. and allied systems in the vicinity. The three services are working together in developing signal separation, recognition, analysis, and countermeasure techniques against specific waveforms used in C^2 applications. These ES capabilities will be consolidated with the EA jamming improvements to produce an enhanced ability to selectively disrupt hostile communications and weapon control networks. Under an information warfare/information operations (IW/IO) theme, a novel high-power microwave (HPM) concept concluded its ACTD testing in FY99.

Although not of DTO status, efforts continue to develop and integrate critical digital receiver/processor technologies to yield next-generation EW receivers and receiver upgrades. These receivers will be capable of performing warning, signal parameter collection, and situation assessment (SA); and assisting the functions of threat geolocation and combat identification (Combat ID). Associated architectures will integrate the advantages of broadband, channelized monolithic receivers "on a chip" with commercial, real-time, parallel digital signal processors and fast, wideband analog-to-digital converters (ADCs) to yield an affordable, adaptable, software-reconfigurable capability. In conjunction with past DARPA-sponsored work on advanced digital receiver components/interconnects, these capabilities will serve to fill a number of future operational deficiencies that are now represented by more than a dozen individual systems. Meanwhile, in parallel, DTO H.07 is pursuing advanced, defensive threat alert and SA techniques for multiple transitions and insertions to mobility, SOF, and tactical aircraft—plus advanced on-/offboard sensor fusion techniques to aid offensive targeting and mission management functions.

The expanding, major EW push lies in the SEAD area—led by MALD Program ACTD (H.04). A companion DTO from the DTAP is pursuing the adaption of HPM techniques and technologies for the SEAD mission (WE.60). From the ES perspective, H.10 builds on advancements in multispectral threat warning and undertakes advanced technology demonstrations of ES-based targeting for both "low/slow" platforms (rotary-wing aircraft and ground vehicles) and "high/fast" (fighter aircraft) platforms. Thus, the future lethal and nonlethal SEAD solution "set" is fully complemented by decoy, HPM, and ES sensor targeting options that will preemptively defeat integrated air defenses.

To augment the C^2W/EW "triad" of the future (standoff communications jamming, reactive/preemptive SEAD, and support jamming of radars (surveillance, acquisition, tracking)), a joint development effort is being planned to design and demonstrate next-generation support jammer technologies. This effort is proposed to be executed in lock-step with the architecture recommendations of the tri-service, Navy-led Analysis of Alternatives (AOA) that is currently underway. Key to the program is the adoption of a reconfigurable/modular concept that can be adapted to either a podded unmanned aerial vehicle (UAV)/uninhabited combat air vehicle (UCAV) or a potential manned/dedicated airframe configuration—the latter, as is done today in the EA–6B. The foundation for this approach lies in the set of DTAP EW receiver technologies highlighted above and the DTAP DTOs for Coherent RF Countermeasures Technology (SE.78) and Network-Centric Electronic Warfare Technology (SE.81). Subsets of these same technologies will also have joint applications in the form of affordable upgrades to jamming systems of all three services and their respective platforms. H.08 is underway and tackles the tough monopulse threat to tactical aircraft via integration of advanced (classified) techniques and the insertion of modern, affordable technologies.

Figure XI–3 is a roadmap for developing and demonstrating the technologies required to support the operational advances in Electronic Warfare. This roadmap concentrates on the themes of IRCM (air, land, and sea platforms), offensive C^2 warfare/information warfare, precision emitter location and battlespace SA, upgrades to our aging platforms, and the valuable "force multiplier" aspects of SEAD and support jamming.

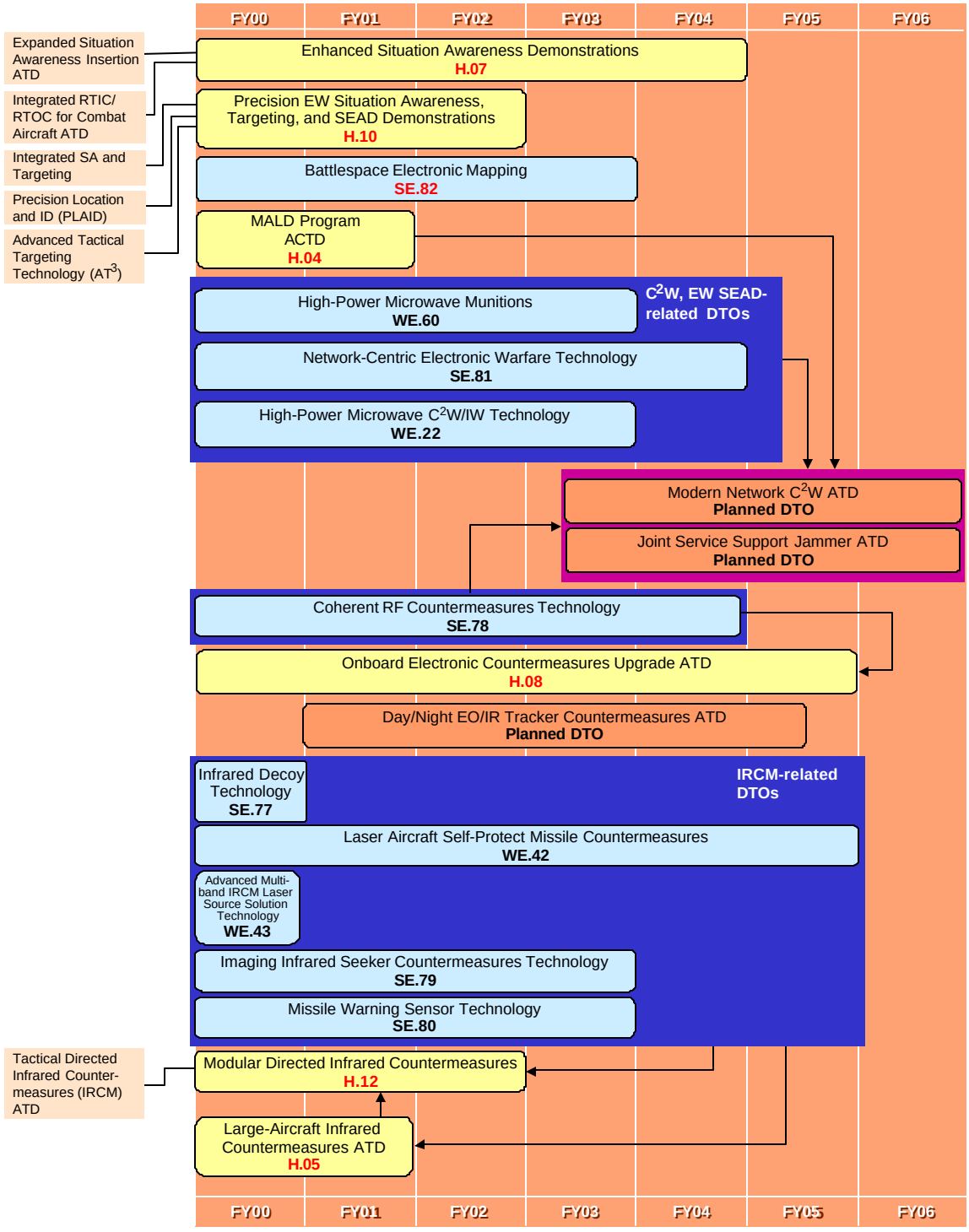


Figure XI–3. Roadmap—Electronic Warfare

F. SUMMARY

Figure XI–4 shows how this investment strategy will provide incremental improvements to Electronic Warfare. This chapter presents a balanced approach to achieve platform protection and electronic support to all joint combatants. This EW plan emphasizes solutions to the formidable, worldwide IR missile threats; multispectral situation awareness; countering the C^2 hierarchies of the hostile force while preserving real-time knowledge of the enemy; and countering the enemy early in the engagement process via the triad of C^2 warfare, SEAD, and RF support jamming.

EW demonstrates vital support to the Chairman of the Joint Chiefs of Staff and his *Joint Vision 2010* concepts of Full-Dimensional Protection, Dominant Maneuver, and Precision Engagement. As an "enabler," EW demonstrates several important synergies with the Information Superiority, Combat Identification, Protection of Space Assets, and Precision Fires JWCOs, *with an overall focus on assuring survivability of the joint warfighters and their platforms.*

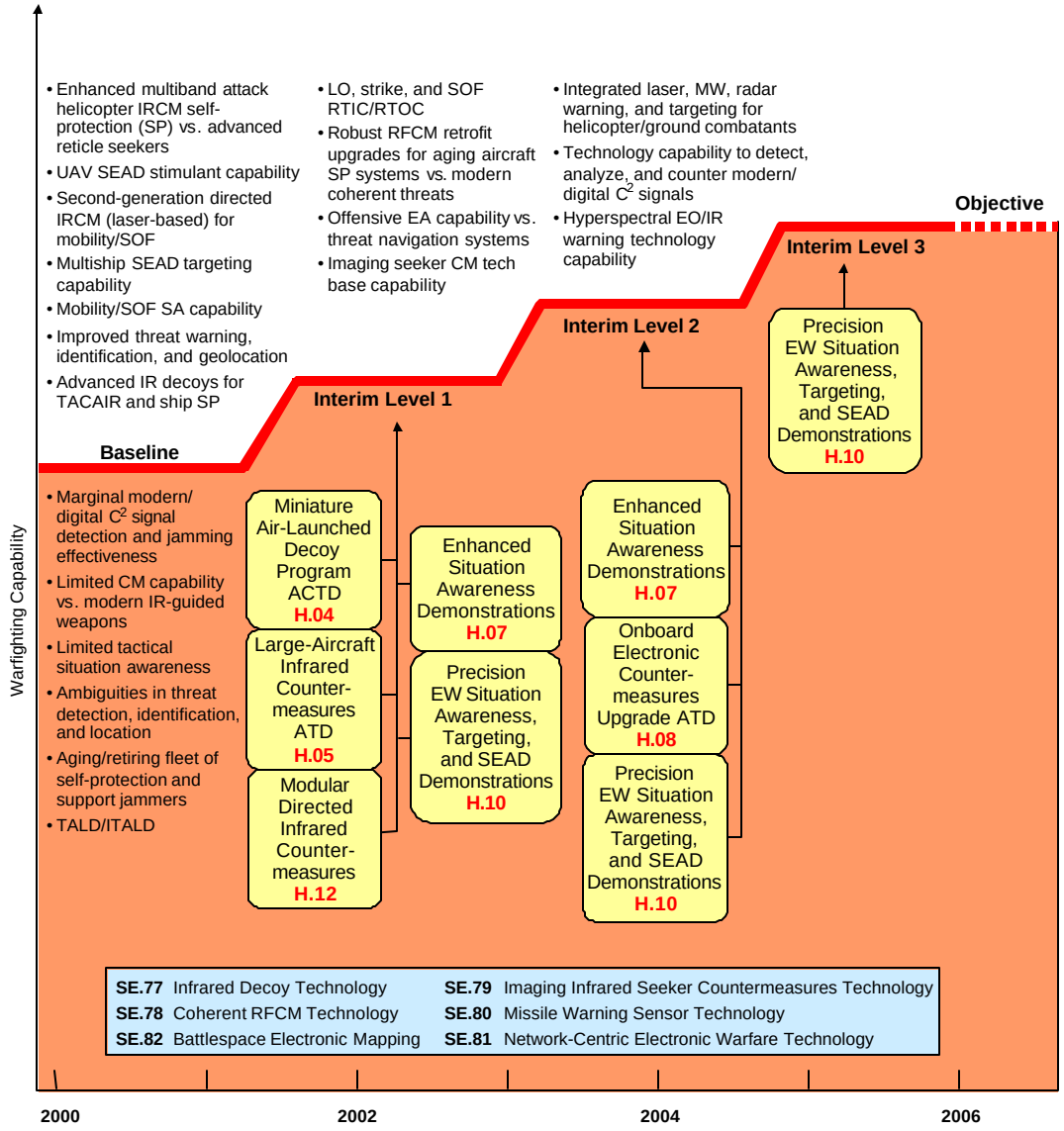


Figure XI–4. Progress—Electronic Warfare