SECTION 9 - INFORMATION WARFARE TECHNOLOGY

SUMMARY

Overview (See Figure 9.0-1) Information warfare (IW) is defined as actions taken to achieve information superiority by affecting adversary information, information based processes, information systems and computer based networks while defending one's own information, information based processes, information systems, and computer based networks. IW is a combination of both old roles and missions, evolving and adapting to a new environment, and new revolutionary capabilities. IW includes both offensive and defensive activities: electronic warfare (EW), physical destruction, deception, information attack, psychological operations, operational security, IW protection and security measures. IW depends upon and embodies related information systems and other supporting technologies as illustrated in Figure 9.0-1. Computer hacking is a form of IW just as is bombing an adversary's C^2 facility since both deny the enemy information. Because of the dependency of military C^4I^2 systems on both civil and military communications, the crossover between civil and military communications is transparent. This section focuses on the technology areas shown in the box above that contain militarily critical technologies. No militarily critical technologies were identified in two other technology areas: Deception and Psychological Operations. For related technologies see subsection 5 - Electronics, 8 - Information Systems, 15 - Sensors and Lasers, 16 - Signature Control and 17 - Space Systems.

Rationale The current concept of IW evolved after Desert Storm, where the use of military and civil resources for communications, sensing and intelligence led to an operational C^4I that was unchallenged. This has now evolved into a paradigm integrating civil and military elements and including command, control

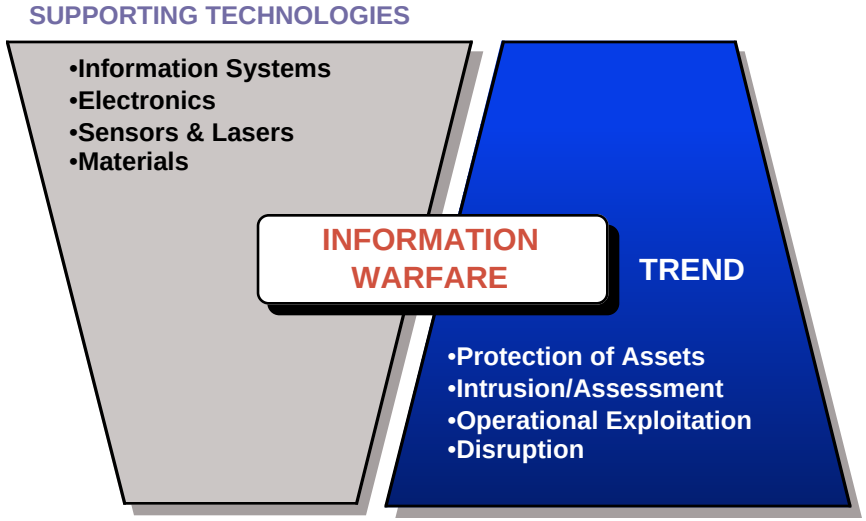

Figure 9.0-1. Information Warfare Overview

1 Also called Electronic Countermeasures (ECM).

2 Also called Electronic Counter-Countermeasures (ECCM).

and communications countermeasures (C^3CM) and electronic warfare command and control warfare (EW/C2W), computer warfare, and national activities. IW enhances the way war is waged. The growing battlefield dependence on information systems presents an inviting target for opposing forces. A computer-savvy force could inject false data into an adversary's battlefield information system, thereby confusing the enemy and/or avoiding battle and resultant friendly losses. Attacking a nation's power grids, telephone systems, radar sites, transportation networks, oil supply lines, and financial networks can severely disrupt military and nonmilitary sectors of a society. The increased dependence on information systems empowers nations that otherwise pose no military threat, terrorist organizations, and even individuals to damage countries electronically.

Foreign Technology Assessment (See Figure 9.0-2) Technologies in electronic combat, which include the four technology areas in Figure 9.0-2, are most advanced in the US. Close behind the US are the UK, France, Germany, Israel, Japan, the Netherlands, and Russia. Most of these nations have developed sophisticated EW suites and maintain high standards for electronic and optical countermeasures.

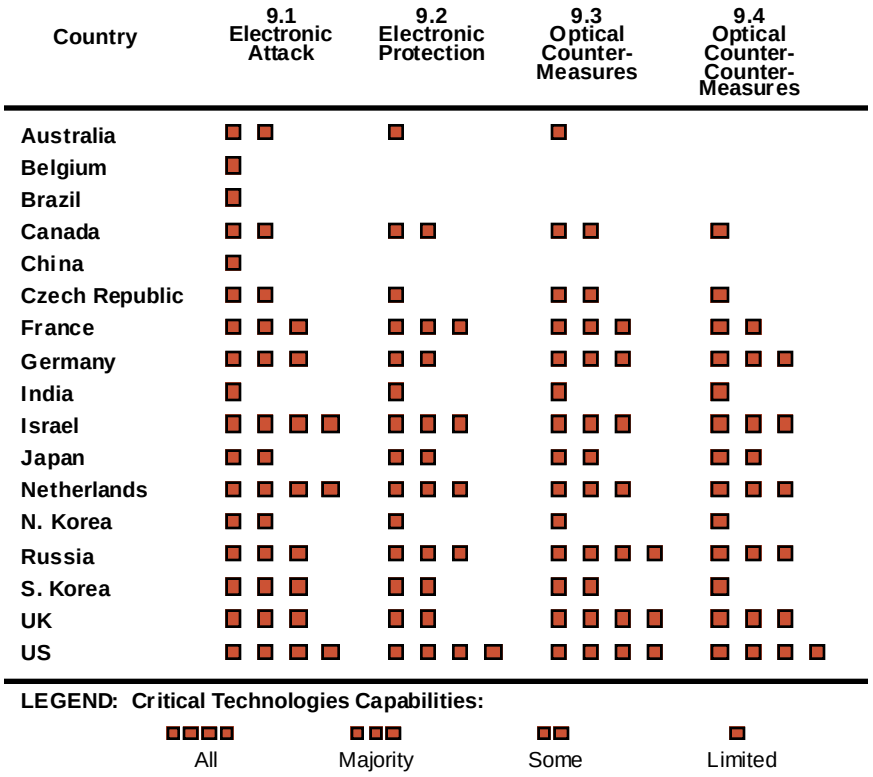

Figure 9.0-2. Information Warfare FTA Summary

SECTION 9.1 ELECTRONIC ATTACK

Overview (See Figure 9.1-1) An early historical example of Electronic Attack (EA)[1] is the Allies' jamming of the giant German Wurzburg radar. The radio frequency (RF) jamming confused the radar's gating mechanism, making few aircraft appear as many. These measures were also used against anti-aircraft radar with considerable success. The increase in the capability of electronic countermeasures grew with the increased use of radio frequency (RF) devices for guidance and control of weapons systems and the concurrent advances in electronics. Add to this capability the sophisticated countering modulations that can be stored as a library of computer algorithms, and the operations of electronic warfare (EW) take on unusual depth. Thus, since the end of World War II, many complex and intricate techniques have been devised to counter the newest weapons systems. Electronic attack is covered by both the DoD S&T Plan and the Joint Staff Electronic Warfare Plan. Each military Service maintains separate Electronic Warfare Plans.

Rationale (See Table 9.1-1) Many of the EW components are part and parcel of electronic systems such as radars, navigation systems, instrument landing system (ILS), identification friend or foe (IFF), and the like. For EA, the difference lies in the sensitivity and capability of the RF devices that must "intercept" the target over a long distance, and if possible, before the target is aware of our existence. EA suites normally contain both receiving and transmitting devices. This combination of intercept and countering makes for a considerable difference in fighting a war. For this reason, several electronic support measures (ESM)[2], in the form of sophisticated receiving equipment, exist to provide radar warning and an intercept capability against these foreign EA suites. Because of the many changes in the sophistication of weapons systems that occur during wartime, EA must employ the leading edge of technology to maintain the advantage in battle. The critical technologies listed in Table 9.1-1 are major contributors to that advantage.

Foreign Technology Assessment (See Figure 9.0-2) Recognition of the need to counter electronic systems such as radar and telecommunications has led to a profusion of EA suites throughout the world, with major emphasis on aircraft and ships. During the Cold War, NATO countries cooperated in developing EA and ES suites and maintained an awesome presence that was sometimes breached by Soviet Bloc countries. The Russians emphasize high power RF jamming devices and the use of noise generation to disorient the "enemy." Today, the profusion of weapons systems is primary, with EA suites running a close second, and virtually every nation with an arsenal of aircraft and ships is deeply involved with EA, either through outright purchase or development. The use of chaff and decoys are common among all countries. Major players are the US, the UK, France, Germany, Netherlands, Sweden, Israel, Russian, and Japan, with some very interesting systems being fielded by China, India, and South Africa.

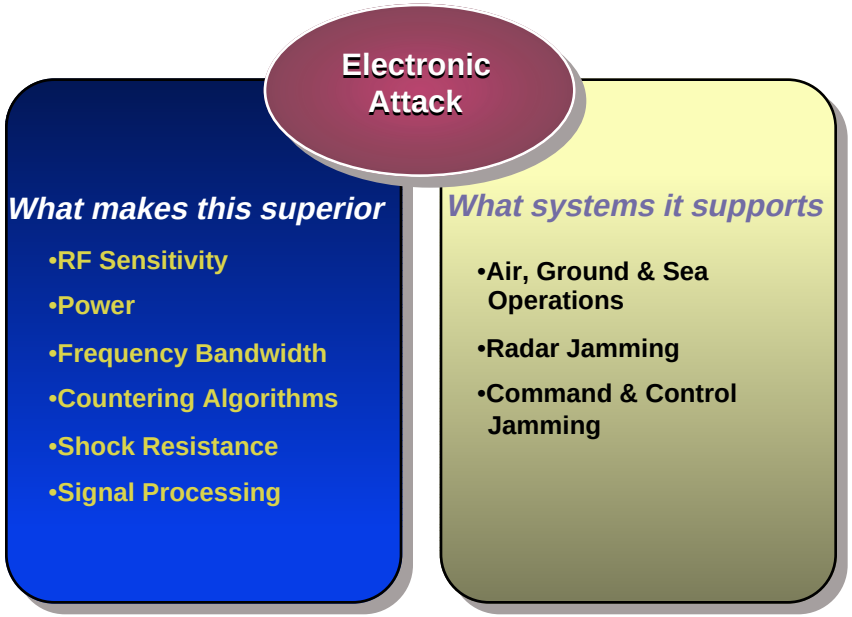

Figure 9.1-1. Electronic Attack Overview

---

1 Also called Electronic Countermeasures (ECM).

2 Also called Electronic Suppression (ES).

Table 9.1-1. Electronic Attack Militarily Critical Technology Parameters

TECHNOLOGY	MILITARILY CRITICAL PARAMETERS MINIMUM LEVEL TO ASSURE US SUPERIORITY	CRITICAL MATERIALS	UNIQUE TEST, PRODUCTION, AND INSPECTION EQUIPMENT	UNIQUE SOFTWARE AND PARAMETERS	CONTROL REGIMES
ECM ANTENNA	< –40 dBm	None identified	Compact range	None identified	WA ML 11
AID & DIA: AUTO RECOGNITION	> 12 bps and 10 GHz	ROM DSP	None identified	None identified	WA ML 11
SYNTHESIZERS	> – 60 dBm, 2–18 GHz	DSP	None identified	None identified	WA ML 11 WA IL Cat 3
RF: WIDEBAND ADAPTIVE POLARIZERS	Null depth > 25 dB Bandwidth > 20%	None identified	None identified	None identified	WA ML 11
DIGITAL RF MEMORIES	Digital memories with clock rate > 200 MHz;	SS power devices	None identified	None identified	WA IL Cat 3
SOLID STATE AMPLIFIERS	2–18 GHz, 10 watt, 40%	None identified	Public domain	None identified	WA IL Cat 4
ECM SIMULATION	Simulations incorporating validated algorithms involving one or more operational or developmental military systems.	None identified	Built-ins	In encryption module	WA ML 11
ESM: RECEIVER DIGITIZATION	10 Gbits samples < 15 W @ 8 bits	None identified	Instrumented antenna range	None identified	WA ML 11
ESM: ANTENNA ARRAYS	< 0.1° DOA accuracy	None identified	Max bandwidth oscilloscope built-in	None identified	WA ML 11
ESM: RF DELAY LINES	> 2 GHz; < 6 dB NF/g > 500 n sec delay	HTS materials	Max bandwidth oscilloscope	None identified	WA ML 11
ESM: SWITCHED DELAY LINES	0.4 dB filter with low sensitivity loss; 20 MHz bandwidth @ 40 dB; 10 µsec switching	HTS materials	Max bandwidth oscilloscope	Steering algorithms	WA ML 11
ESM: LOW RCS ANTENNA	Effective area out of band < effective area in band	HTS materials	Hi tech range (laboratory)	Steering algorithms	WA ML 11
HIGH TEMP SUPERCONDUCTING ANTENNA (ESM)	Size: < 1/4 wavelength	None identified	Hi tech range (laboratory)	Acquisition algorithms	WA ML 11
ESM: MINIATURE MMW INTEGRATED RECEIVER	< 5 dB NF; 75 GHz bandwidth	Detector sensitivity	Isolation, sensitivity and sel test	Ranging formula	WA ML 11
PRECISION PASSIVE RANGING	CEP < 0.1% of range	None identified	None identified	None identified	None

SECTION 9.2 ELECTRONIC PROTECTION

Overview (See Figure 9.2-1) Electronic Protection (EP)[1] are those measures used to defeat electronic attack (EA). The EP device must detect the countermeasure, such as jamming or electronic deception, and use active decoys, RF traps and synchronizers, and devices that read through spectral noise. The vast majority of these "fixes" are derived by the developers and manufacturers of the electronic weapon systems as self protective measures. Major US radar manufacturers, such as Westinghouse, Raytheon, and Hughes, have relied on "in-house" development of EP "fixes."

Rationale (See Table 9.2-1) Throughout the world, a vast difference exists in the quality of EP devices. These differences are largely related to the quality of radars and other RF instrumentation. With greater sophistication in EA devices, more clever and capable EP fixes are needed. The ability to conceive and develop unusual EP devices is critical to the developers of all electronic systems. Intricate circuitry, essential miniaturization, and a fail-safe continuum create a rigid set of requirements resulting in appropriate technologies called "fixes." These "fixes" are the critical technologies of EP.

Foreign Technology Assessment (See Figure 9.0-2) For many years, the "fixes" (EP measures) came from a handful of nations: the US, the UK, France, Sweden, and the Netherlands. These EP measures were nominally built-in to radars, IFF, and navigation systems. In the past few years, some interesting work has been done "ex parte" by Israel and India (the latter working with former Eastern Bloc countries, and the former with France and England). Recently, US engineers visiting Russia were surprised by the sophistication present in Russian "fixes" for a number of radars offered for sale.

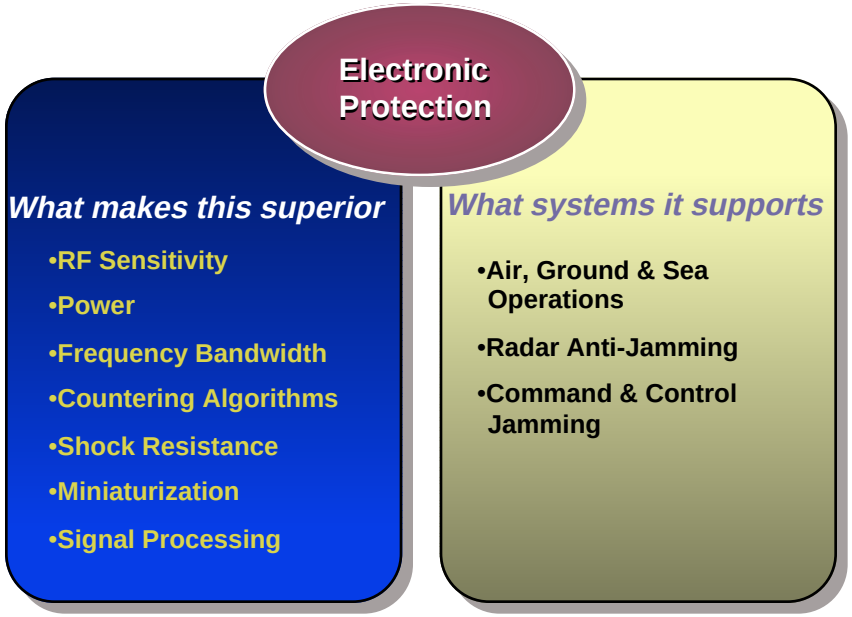

Figure 9.2-1. Electronic Protection Overview

Table 9.2-1. Electronic Protection Militarily Critical Technology Parameters

TECHNOLOGY	MILITARILY CRITICAL PARAMETERS MINIMUM LEVEL TO ASSURE US SUPERIORITY	CRITICAL MATERIALS	UNIQUE TEST, PRODUCTION, AND INSPECTION EQUIPMENT	UNIQUE SOFTWARE AND PARAMETERS	CONTROL REGIMES
DIGITAL RF MEMORIES	Digital memories with clock rate > 200 MHz	None identified	None identified	Compact codes	WA ML Cat 11
SIGNAL SYNTHESIS SOFTWARE	Accuracy > 98%	None identified	None identified	Mimic accuracy	WA ML 11
SEE-THROUGH FILTERING	Comb Filters; Narrow sloped filters < 0.5°	None identified	None identified	Filter codes	WA ML 11

1 Also called Electronic Counter Countermeasures (ECCM).

SECTION 9.3 OPTICAL COUNTERMEASURES

Overview (See Figure 9.3-1) In past MCTL compilations, optical countermeasures were listed under the general field of electronic attack (EA). The increased use of optical devices in many weapon systems necessitated a separate field for this important technology. Optical countermeasures (OCM) include lasers, remote sensing television, the plethora of IR devices, UV sensors, spectrometers, radiometers, and hyperspectral and multispectral devices plus a number of decoys. The OCM field will continue to grow and require more sophisticated answers in the future. The Joint Staff Electronic Warfare Plan and the DoD S&T Plan cover OCM in detail.

Rationale (See Table 9.3-1) The importance of OCM in modern warfare cannot be overestimated. Most important have been the rapid technological changes. The advances in FLIRs and IRSTs and focal plane arrays (FPAs) are covered by MCTL Section 15 (Sensors and Lasers Technology). The critical elements for many optical sensors are inherent in superior lensing and engineering; however, for OCM, the use of microprocessors and digital signal processing equipment is critical. The short time interval between target acquisition to "kill" requires that the processing element must intercept, identify, categorize, and counter the weapon in milliseconds. Technologies that have improved weapon systems include surface acoustic wave (SAW) devices and digital signal processors (DSPs). When combined with readout integrated circuits (ROICs), these devices and processors resolve the measures (EP/OCCM) taken to defeat EA, such as dual band and multispectral operations, by accurate and timely identification of the counterthreats. For OCM, optical hardening is very important because of the extreme operational environments.

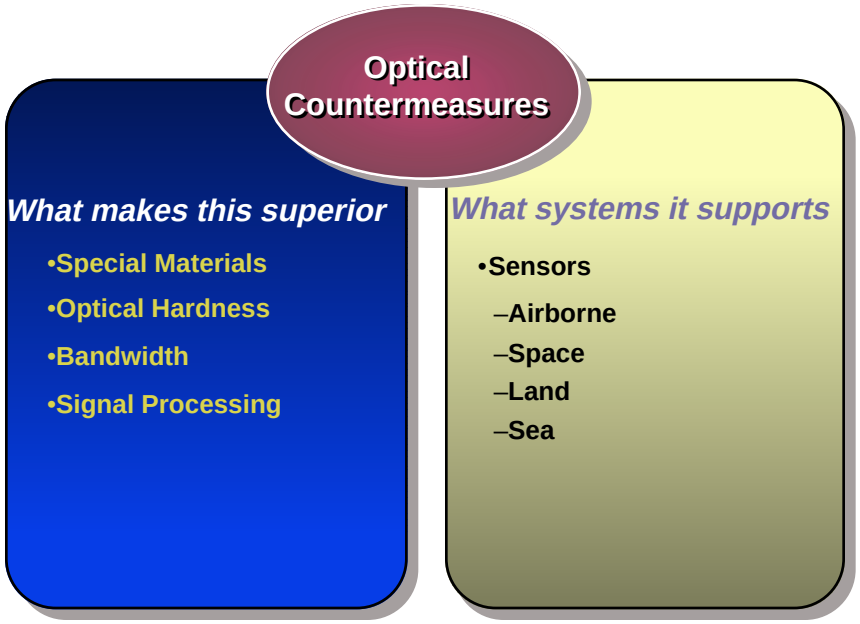

Figure 9.3-1. Optical Countermeasures Overview

Foreign Technology Assessment (See Figure 9.0-2) OCM development closely parallels the capability of a country's optical development posture. Both Germany and Japan have successful optical development companies and advanced OCM equipment. Today's advances in OCM are tied closely to ROICs and DSP in combination with superior optics. NATO countries—France, Germany, the Netherlands, and the UK—share development work on FLIRs and FPAs, and the combination with DSPs has provided a large payoff for these devices in OCM. Russia maintains superior high-power laser devices and some less powerful lasers as well.

Table 9.3-1. Optical Countermeasures Militarily Critical Technology Parameters

TECHNOLOGY	MILITARILY CRITICAL PARAMETERS MINIMUM LEVEL TO ASSURE US SUPERIORITY	CRITICAL MATERIALS	UNIQUE TEST, PRODUCTION, AND INSPECTION EQUIPMENT	UNIQUE SOFTWARE AND PARAMETERS	CONTROL REGIMES
SEMICONDUCTOR LASER: INCL COHERENT AND NON-COHERENT SOURCES	3–12 microns; 200 milliwatts avg power; 1 watt peak power per pulse; 100 µsec pulse width; 75° K operating temperature	None identified	Molecular beam expitaxy production equipment	IR jamming techniques. DIRCM pointing/tracking algorithms	WA IL Cat 6 WA ML 11
SOLD STATE LASERS: INCL COHERENT AND SS SOURCES	3 lines in 1.5–5.0 µ band > 20 kHz PRF	OPOs, CW Pump Diodes > 50 °C, Dichroric coatings	OPO production processes	IR jamming techniques	WA ML 11 WA IL Cat 6
NON-COHERENT ARC LAMPS	Braze temperature > 1400 °C	Proprietary metalizing and brazing materials	High temperature vacuum ovens	IR jamming techniques	WA ML 11
IR DETECTORS AND ARRAYS	EW technical parameters are less stringent than IRST or F4R and imaging missile requirements	InSe, HgCdTe, PtSi, Cryo Coolers	Array production techniques	OCM/OCCM Rx	WA ML 11
UV DETECTOR AND MICROCHANNEL PLATES	Photon thruput efficiency > 50 °C operating temperatures	UV filters	Filter production; microchannel plate production	Critical Element: Temporal; and Spatial	WA ML 11 WA IL Cat 3
CLOSED LOOP IR COUNTERMEASURE	6:1 S/N ratio; > – 105 dBm sensitivity	Detectors, optics, trackers, FFT processors	Algorithms and software test eq.	FFT: analyzers	WA ML 11
VISUALLY COVERT CHEMICAL SOURCES	1200 w/sr, 3–5 µ per condela	Pyrophonic solids spectrally sources	Radiometric squid	None identified	None
SPATIALLY TAILORED EXPENDABLE SOURCES; AIRBORNE	1:3 side to rear 1:5 front to rear	Shielded sources	Radiometric squid	None identified	None
SELF IGNITING PYROTECHNIC SOURCES	Rise time < 0.2 sec to peak	Pyrophonic metal igniters	Radiometric squid	None identified	None
AIR LAUNCH KINETIC DECOYS	Operate up to Mach 1.0 at sea level	Propelled aerodynamic decoys	Radiometric squid	None identified	None

SECTION 9.4 OPTICAL COUNTER-COUNTERMEASURES

Overview (See Figure 9.4-1) Optical Counter-Countermeasures (OCCM) are measures taken to counter optical countermeasures (OCM). As with electronic protection (EP), this means building into optically pointed weapons systems devices that can detect and counter or defeat the OCM. Multispectral, multiband, and adaptive frequency devices are common but can sometimes be defeated by wideband, high-power devices.

Rationale (See Table 9.4-1) Sophisticated combat requires a catalog of "fixes" for a spectrum of scenarios because of the dynamic nature of weapons systems change, which mandates more complicated "fixes" to meet the technological challenges. In this world, the engineer is faced with all types of optical instrumentation from narrow band, high dynamic ranges to broad frequency search in a single instrument. Success in protecting such devices is limited only to the skills of the engineers.

Foreign Technology Assessment (See Figure 9.0-2) OCCM development capabilities vary considerably. Some countries have given little thought to OCCM in FLIRs and the like. Most of the more developed countries have OCCM programs concurrent with sensor and weapon system development. The US, the UK, France, Germany, and the Netherlands have a library of "fixes" to fit most occasions as developed by their major aerospace corporations. The exact position of Russia in the general use of OCCM is not clear, although its laser work is well established.

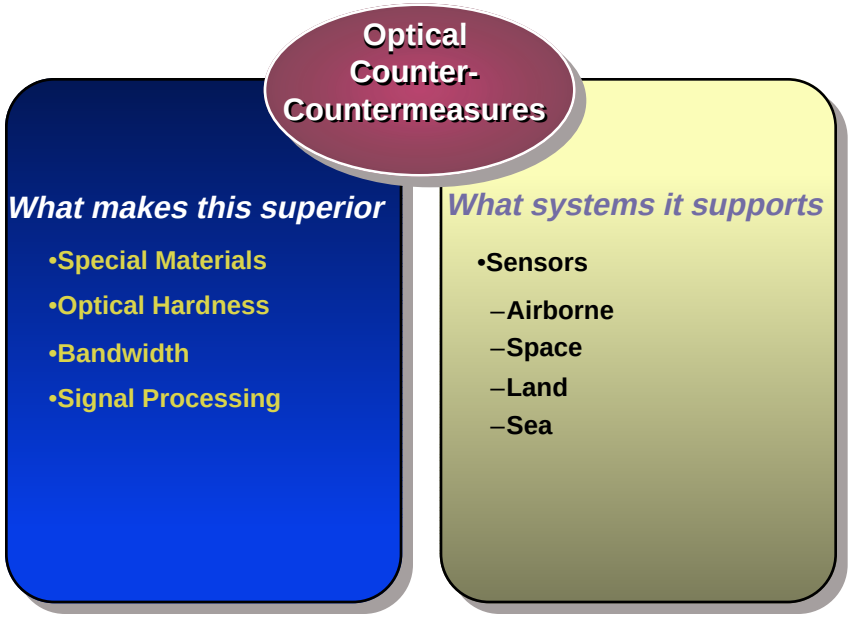

Figure 9.4-1. Optical Counter-Countermeasures Overview

Table 9.4-1. Optical Counter-Countermeasures Militarily Critical Technology Parameters

TECHNOLOGY	MILITARILY CRITICAL PARAMETERS MINIMUM LEVEL TO ASSURE US SUPERIORITY	CRITICAL MATERIALS	UNIQUE TEST, PRODUCTION, AND INSPECTION EQUIPMENT	UNIQUE SOFTWARE AND PARAMETERS	CONTROL REGIMES
SIGNAL SYNTHESIS SOFTWARE	Accuracy > 98%	None identified	None identified	None identified	WA ML 11
SPECTRALLY MOLDED IR SOURCES	Temperature > 1000° C airborne and Temperature > 350 K shipborne when viewed in 2–3 and 3–5 μ bands	Pyroten liquids Pyrophoric solids	None identified	None identified	WA ML 11
SYNTHESIZERS	FOV 0.5 deg Two-color seeker > 1 kHz bandwidth > 270 deg blanking	None identified	None identified	Computer target matching	WA ML 11