ELECTRONIC WARFARE

Electronic warfare (EW) is the systems discipline that exploits an adversary's use of the electromagnetic spectrum to overcome threats that use communications, navigation, and radar systems. It is an important tool in pursuing military objectives and advancing national policy and sovereignty. EW provides the means to counter, in all battle phases, hostile actions that use the electromagnetic spectrum—from the beginning, when enemy forces are mobilized for an attack, through to the final engagement. EW exploits the electromagnetic spectrum through electromagnetic sensing, analysis, and countermeasures to establish operational advantage in a hostile encounter.

The use of electronic warfare accelerated rapidly during World War II, and it has been used in most military conflicts since. The aircraft used by Nazi Germany to bomb the fog-shrouded British Isles were guided by radio beacons from the European mainland. By using false guidance signals, the British were able to redirect the German bombing attacks from densely populated urban areas to less populated rural areas. In this same conflict, US bombers used chaff (packets of tinfoil cut into thin strips) jettisoned from the attacking US aircraft to reflect antiaircraft radar signals, thereby reducing the effectiveness of the German antiaircraft batteries and bomber force attrition. In the Pacific theater of operations during World War II, US Navy submariners detected and determined the bearing and location of Japanese ship radio transmissions for weapons targeting. In the Korean conflict, detection and location of North Korean antiaircraft radar signals provided targeting data for subsequent air strikes. In Vietnam, the exploitation of antiaircraft and missile radars was refined with the use of US Air Force Wild Weasel weapons—suppression aircraft that used sensors to detect and locate the weapons-associated threat signals to provide targeting information for ordnance delivery. Electronic warfare applications are described extensively in military accounts of the past half century.

Military operations use EW as one means to gather tactical intelligence from noncooperative forces and to counter their electromagnetic, radio-, and radar-controlled weapons. Land, sea, and air forces use the electromagnetic spectrum for command and control, weapons targeting, and weapons control. Figure 1 shows multiple land, sea, and air platforms in a typical tactical environment. Also indicated are links for sensing, communications, and navigation in support of the military mission.

Electronic warfare provides use of the electromagnetic (EM) spectrum by the host force and denial or limitation of its use by an adversary. Realization of this goal occurs when host force systems use the EM spectrum while adversary systems are denied its use. Countermeasures (CM) to threat systems that use the EM spectrum can be selectively applied on a time- and/or frequency-multiplexed basis so that host force use of the EM spectrum is uninhibited.

Electronic warfare includes the *operational* functions of electronic support (ES), electronic self protection (EP), and electronic attack (EA). ES provides surveillance and warning information for EW system use. CM to threat systems, including jamming, false target generation, and decoying, are performed for EP (protection of the host platform against an electronically controlled threat). EA performs these same CM functions to protect a battle force composed of several platforms or battle units. The ES, EA, and EP functions are interrelated because EA and EP can be queued using ES informa-

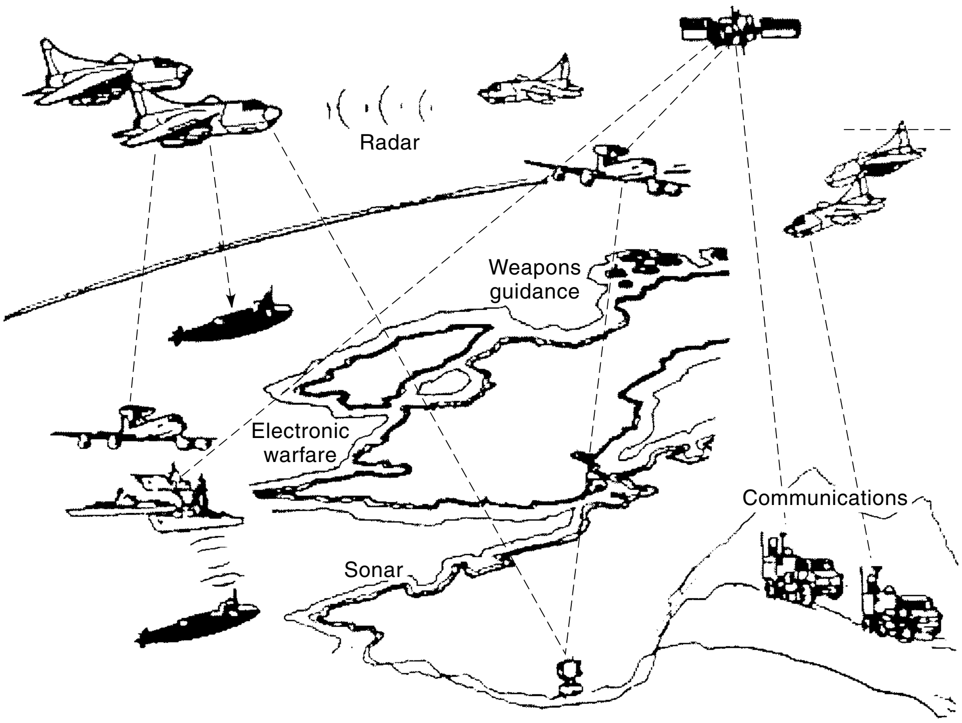

Figure 1. Tactical operational concept indicating systems that use the EM spectrum.

tion, and EA and EP can use some of the same sensing and CM equipment for distinct operational objectives.

This article includes a description of the EW time line and the various phases of conflict. Also provided is a summary description of the signal environment in which EW systems operate. Those interested in more detailed descriptions of the EM communications, radar, and navigation technology against whose signals EW systems operate are referred to the appropriate sections of this encyclopedia. A discussion of EW functional areas ES, EP, and EA provides a functional framework for supporting EW technologies.

ELECTRONIC WARFARE TIME LINE

Electronic warfare is used in a layered operational interaction with electronically controlled threat systems. The electronic warfare system provides its own force with data for self-protection and threat weapons suppression. Figure 2 graphically illustrates the EW functional time line.

Electronic support provides operational intelligence relating to electronically controlled threat systems and communications systems in the battle group or theater environment. Electronic threat-warning information derives from ES surveillance data, recognizing that hostile force deployments or weapons-related transmissions constitute a threat. Air defense combines electronic and radar surveillance with tactics and countermeasures to control the air battle. EA and active EP, using countertargeting (CTAR) jamming, false target generation, and/or decoying, attempt to deny target acquisition by adversary sensors. CTAR endeavors to deny weapon's sensors use of the spectrum, and decoys dispersed into the environment provide preferred target signatures to the threat weapon's sensor.

The EW battle time line provides the general context in which the discipline of EW is used in the tactical environment. The EW time-line stage in a specific engagement depends on the deployment of forces and the perceived imminence of hostile engagement. Note that the technologies used in the various stages of the engagement are dynamic, and EW systems and weapon systems technologies evolve to overcome susceptibilities. The boundaries and definitions of EW time-line stages are redefined with each new advance in weapon and EW technology.

Electronic Support

Electronic support provides operational intelligence that is related to radiated signals in the battle group or theater envi-

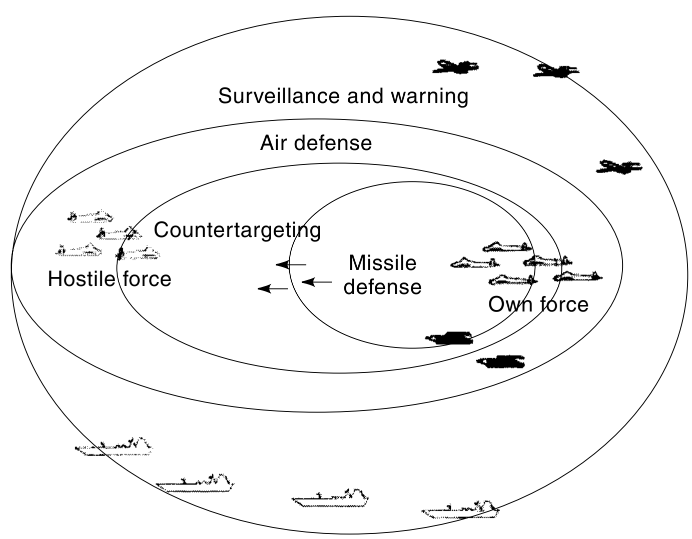

Figure 2. Electronic warfare battle situation showing various phases of the engagement time line.

ronment. Surveillance includes monitoring of both combatants and commercial transports. Control of contraband and critical materials is an EW surveillance mission that provides critical intelligence data to the area commander. Surveillance of noncooperative combatant forces provides deployment intelligence in the area of observation. Early threat-warning information extracted from surveillance data occurs by recognizing hostile force weapons-related transmissions.

Within the lethal range of hostile force weapons, battle space surveillance updates are required rapidly. Deployment and operational modes of hostile forces are monitored closely to determine imminence of hostile activity. In some environments, potentially hostile forces remain within weapons' lethal range and a high level of vigilance is necessary to maintain security.

Air Defense

Air defense is used to maintain control of the battle group airspace and defend against threat aircraft and missiles. Battle group surveillance, implemented by the combination of EW, infrared/electro-optic (IR/EO), and radar sensors, provides environmental data required for air defense. Electronic combat techniques and weapons are used to counter an airborne threat.

Air defense is an extensive, complex, electronic combat interaction between hostile forces. EW assets are a key tool of the battle force commander and of the individual elements within the command. These assets provide information for developing tactical intelligence in all phases of the engagement. The outcome of the air battle is by no means established by the quantity of EW assets possessed by each of the opposing forces, but depends greatly on how the EW assets are used in conjunction with other sensor systems, weapons, and air defense tactics.

Aircraft ships and/or battlefield installations participate in air defense. Own force aircraft operating at altitude can engage a threat force at long line-of-sight ranges. Aircraft, together with ship and battlefield installations, provide coordinated air defense as the hostile force approaches own force locations. The EW objective in the early air defense or outer air battle is to prevent threat force detection and location of own force. Electronic combat actions that prevent or delay own force detection provide a distinct advantage by allowing additional time to develop tactics to counter the threat force. In addition, the threat force battle time line and interplatform coordination are perturbed. Fragmentation or dissolution of the hostile force attack can occur if own force electronic combat is effective in the outer battle.

As the hostile force overcomes the outer battle electronic attack and approaches the own force within weapons range, air defense assumes the role of denying targeting information to the hostile sensors. The EW objective at this stage of the engagement is to prevent hostile force weapons launch by denying targeting data to their sensors. Electronic combat surveillance, warning, and countermeasure assets are used for countertargeting. Surveillance sensors assess hostile force deployment and provide information about the adversarial tactics being used. Warning sensors indicate the status of threat sensors as they attempt to acquire targeting data for weapons systems handoff. Countermeasure assets, including jamming, spoofing, and decoying, continue to provide a virtual environment to threat platform sensors to prevent own force target acquisition by the hostile force.

The terminal phases of an air defense engagement are characterized by heightened activity. The combatants, both hostile and own force, are confined to a smaller portion of the battle space. Weapons and decoys in flight add to the physical and EM signal density. Electronically, both own force and hostile forces struggle to exploit the EM environment to achieve their respective operational objectives. Countermeasures jamming and spoofing are used with full appreciation that coordinated jamming produces degradation of hostile force sensors, but that weapons with home-on-jam (HOJ) capability can exploit this action to the destructive detriment of the radiating platform.

Countertargeting

Countertargeting (CTAR) is a subset of radar electronic countermeasures (ECM) used in electronic attack. CTAR provides specially modulated radio-frequency (RF) signal transmissions to counter hostile force long-range surveillance or targeting radar. The transmission modulation can be amplitude-modulated (AM) or frequency-modulated (FM) noise, or combinations of these, and they can be pulsed or continuous-wave. CTAR transmission is used both to disrupt and interfere with the threat radar operation, thereby preventing it from correctly locating and identifying own force target(s).

Countertargeting success criteria includes mission completion prior to threat force interdiction or weapon launch. Realistically, the results of a CTAR electronic attack against a hostile force are probabilistic, in that some opposing forces at some time during the battle time line succeed in launching missiles. CTAR can delay and reduce the coordination of hostile missile firings and, consequently, reduce the number of missiles fired and the attrition of personnel, ships, and aircraft.

Terminal Defense

Terminal defense against electronically controlled missiles and guns is the final phase of the EW battle time line. Weapons are launched in the terminal phase of hostile force engagement, and EP and EA capability is brought to bear on the weapons and their electromagnetic (EM) guidance and control signals. Onboard jamming and false-target radiation that is effectively used for countertargeting is less effective for terminal defense. Jamming or false-target radiation makes the target platform vulnerable to missiles with home-on-jam capability. Home on jam is an electronic counter countermeasure that exploits the target countermeasure's radiation to steer the missile to the target. Consequently, off board countermeasures, or decoys, are used to lure the missile away from the high-value target.

THE ELECTRONIC WARFARE ENVIRONMENT

Threat Systems

Electronic warfare interacts with an adversary's EM systems for signal exploitation and potentially for electronic attack. Threat systems of EW interest include radar, communications, and weapons control. Some of the threat systems exploited by EW are briefly described in the following.

Radar. Radar uses radio-frequency transmissions ranging from high frequency (HF) to millimeter waves (30 MHz to 40 GHz) in pulsed and continuous-wave (CW) modes to illuminate targets and collect reflected echoes. Radar-transmission-reflected echoes are used to measure target characteristics and determine target location. Military forces use radar for both offensive and defensive weapon systems. Radar functions include target detection and identification, target acquisition, target tracking, and navigation. Weapons systems using radar may be land-based, airborne, shipboard, or in space. A typical radar system contains a transmitter that produces a high-powered RF signal, tunable over a band of frequencies; an antenna system that radiates energy and collects reflected echoes; a receiver that detects signal return; and signal processing electronics that extract target measurements, such as range, bearing, and speed. Target location information is provided to a weapon system to control and direct the weapon onto the target.

Land-based radars function as ground-controlled intercept (GCI) systems, surface-to-air missile (SAM), antiaircraft artillery (AA) batteries, and space tracking systems. GCI is used to direct interceptor aircraft against attacking aircraft and to coordinate the air battle. SAM sites use early warning/surveillance radar, target acquisition radar, target tracking (TT) radar and/or illuminators for missile-guidance, beam-riding systems. AA radars have operating frequencies and data rates similar to SAM tracking radars and usually receive targeting information from SAM surveillance and target acquisition (TA) facilities. Advanced SAM systems handle ballistic missile defense with higher data rates against high-speed targets. Airborne intercept and control (IC) radars provide early warning and information for the command and control of forces operating in the tactical environment. Space surveillance and tracking radars usually use large, fixed, phased arrays operating in the HF (3 MHz to 30 MHz) to 1 GHz frequency range. Table 1 gives parameters of typical radars categorized by radar function. The reader is referred to radar and electromagnetic wave propagation articles within this encyclopedia.

Radar advancements can be expected in the areas of phased-array antennas, complex modulations on the radar pulse, improved signal processing to extract enhanced data from the radar return, and frequency diversity to cover the less used regions of the spectrum. Advanced designs from the US, European, and Russian inventories can be expected because of operational needs for enhanced sensor performance and the availability of affordable technologies to provide additional capability.

Communications. Communications systems provide information exchange for command and control to coordinate between surveillance sites and between combat units. Communications networks range from basic field radio networks to long-distance, wide-area systems and point-to-point, high-data-rate installations. Communications systems cover the spectrum from very low frequency (5 Hz) to the frequencies of visible light, and they can be either free-space transmissions or confined to a transmission line. Free-space transmission links may be line of sight or cover longer distances by reflecting from the ionosphere, atmospheric layers, or troposcatter, or by relaying via satellite.

Command and control communication links, using HF direct microwave and satellite relay, disseminate voice and digital data transmissions to land forces, air forces, and ships. Land combat units use ultrahigh frequency (UHF) (300 MHz to 3 GHz), very high frequency (VHF) (30 MHz to 300 MHz), land lines, and cellular phones over shorter distances mainly for voice transmissions. Surveillance activities and weapons sites may exchange data via voice or digital data link over a transmission path appropriate for the link span. Such links are used to transmit surveillance radar reports to an operations center or directly to a SAM battery. Communication-link data rates depend on link bandwidth, modulation technique, and signal-to-noise ratio. Individual transmission-link throughput rates are in the range of hundreds of megabytes per second. Computer technology has enabled increased communication-link capacity for handling and processing data. The high data rates attainable permit transmission from airborne observers and between precision weapons and launch platforms.

Communications in hostile environments are transmitted via protected cable between fixed sites, thus providing protection from physical damage, security from intercept, and immunity from jamming. Mobile communications require free-space transmissions that are susceptible to intercept and jamming. Communications counter-countermeasures, complex modulation, encryption, and spatial radiation constraints are used to mitigate the effects of EA. The use of modulation techniques increases privacy, reduces interference, improves reception, and reduces the probability of detection. Spread-spectrum communication systems that use four categories of signal modulation (direct sequence-modulated, frequency-hopping, intrapulse FM [chirp], and time-hopping) provide some level of signal protection from detection, demodulation, and interference. However, this is at the expense of increased bandwidth.

Passive Weapons Sensors. Electro-optical and infrared (EO/IR) systems sense spectral energy that is radiated by an object or reflected from an object from a source such as the sun, moon, or stars. The electro-optical spectral regions are categorized according to atmospheric propagative characteristics or

Table 1. Parameter Ranges Associated with Radar Functions

Radar Parameter	Radar Function					
	GCI	IC	Surveillance	TA	TT, AA	Space Surveillance
Frequency Range	30 MHz to 3.0 GHz	3.0 GHz to 10.0 GHz	30 MHz to 3.0 GHz	3.0 GHz to 8.0 GHz	6.0 GHz to 10.0 GHz	30 MHz to 1.0 GHz
PRF Range	100 pps to 500 pps	1000 pps to 3000 pps	100 pps to 500 pps	1000 pps to 2000 pps	2000 pps to 4000 pps	—

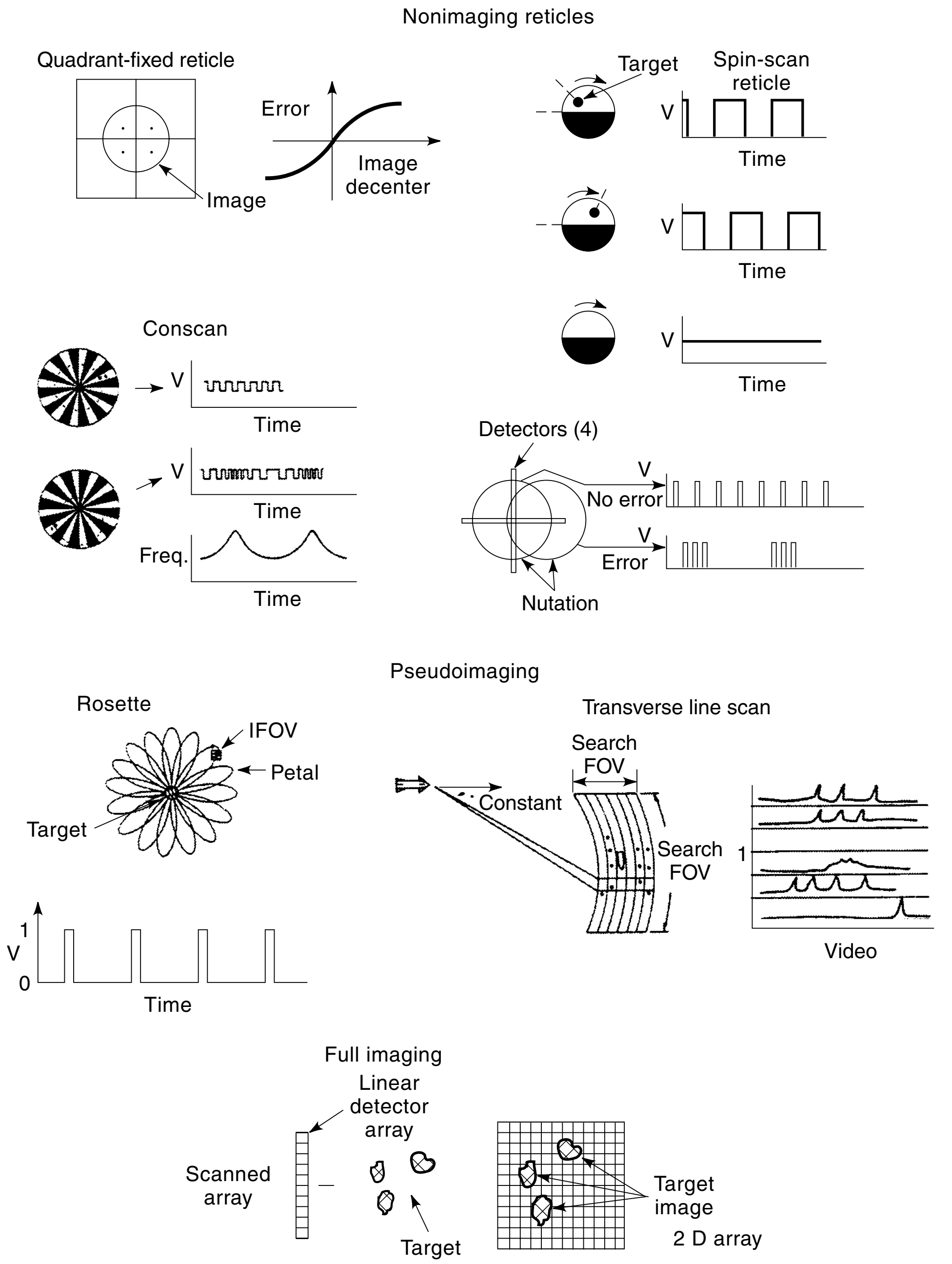

Figure 3. Common IR/EO sensor types including nonimaging reticules, line scanning detectors, and area array imagers.

spectral transmittance. The EO/IR spectrum used for passive weapons sensors spans the 0.2 μm to 15 μm wavelength range.

Electro-optical/infrared guidance provides angle target tracking information only. EO/IR weapons system guidance sensors fall into three classes: nonimaging, pseudoimaging, and imaging. Generally, countermeasure techniques exhibit preferential effectiveness against guidance approach. Some countermeasures techniques may be effective against pseudoimaging sensors and less effective against nonimaging and imaging sensors. Other countermeasures techniques may be preferentially effective against nonimaging and imaging sensors. Figure 3 illustrates the most common seeker-design approaches. These approaches are quadrant, spin scan, conical scan (conscan), transverse-line scan, and rosette scan. In the quadrant approach, an intentionally defocused spot images on a four-element square array. Tracking is achieved by balancing the signal on all four detectors. In spin scan, a spinning reticle provides phase and amplitude information with respect to a fixed reference. With conscan, the target image is nutated by using a scanning mirror or optical wedge imaged onto a fixed reticule or pattern of detectors. The nutated target image generates a modulated frequency proportional to the angular and radial offset from the center. In the transverse-line scan approach, a rotating or reciprocating mirror at a depressed elevation angle generates a scan line transverse to the missile axis, and the forward motion of the missile creates the orthogonal axis of the search pattern. With the rosette scan, a petal pattern is scanned over a small instantaneous field of view (IFOV) by two counterrotating optical elements.

Rosette-scan tracking is accomplished by balancing the signal output from all petals with the target present in the central apex of the rosette. The small IFOV of the transverse-line scan and rosette scan provide high spatial resolution and the ability to resolve multiple sources within the scanned field of view. Focal-plane arrays, scanning-linear arrays, or two-dimensional arrays of detectors in the image plane provide high-resolution "pictures" of the target space. Many image-processing algorithms are available to classify targets and establish track points. Figure 3 illustrates the basic features of common seekers.

Passive electro-optic sensors are desirable targeting and weapons guidance systems because they radiate no energy to warn the target of an impending attack. These sensor systems are vulnerable to decoys, with thermal signatures similar to true targets and to high-intensity sources that can saturate the electro-optic sensor detector or cause physical damage.

ELECTRONIC WARFARE FUNCTIONAL AREAS

Threat systems use the EM spectrum extensively. This section discusses functional aspects of EW. The relationships that govern their systems' application are described in the following section. These functional areas are electronic support (ES), electronic protection (EP), and electronic attack (EA). Electronic attack uses countertargeting (CTAR), jamming, false-target generation, and decoys to defeat the threat sensors. Electronic protection uses electronic support and electronic attack for own-platform self-protection.

Electronic Support

Electronic support provides surveillance and warning information to the EW system. ES is a passive, nonradiating, EW system function that provides a fast accurate assessment of the EM radiating environment. ES is the aspect of EW that involves techniques to search for, intercept, locate, record, and analyze radiated energy for exploitation in support of military operations. Electronic support provides EW information for use in EA and EP and in tactical planning. ES directly provides threat identification/detection and early warning. It also provides data for electronic countermeasures (ECM), electronic counter-countermeasures (ECCM), threat avoidance, target acquisition, and homing.

Electronic support provides timely EM environment information for the EW system. The spatial and spectral environment over which ES operates may span a hemispherical spatial segment and a spectrum of tens of gigahertz. In tactical EW systems, signals in the environment are analyzed and reports of environment activity are provided on the order of a second after threat signal reception.

Electronic Attack

As an EW function, EA provides an overt active response capability against enemy combat systems with the intent of degrading, deceiving, neutralizing, or otherwise rendering them ineffective or inoperative. EA responds to threat systems to protect multiple platform or battle group units. EA includes measures and countermeasures directed against electronic and electro-optical systems by using the electromagnetic spectrum (radio, microwave, infrared, visual, and ultraviolet frequencies). EA technical functions include radio and radar signal jamming, false target generation, and the use of decoys for threat system confusion and distraction.

Electronic attack is reactive to environment threats. To function effectively, therefore, the EA system requires threat information from the environment, including threat classification, bearing and, if possible, range. These functions are performed by the ES system or by other surveillance systems such as radar or infrared search and track (IRST). Effective EA response selection requires knowledge of the threat class and operating mode. Threat signal data are derived from measuring signal parameters (frequency, scan type, scan rates, pulse-repetition frequency, or continuous-wave radiation characteristics). Absence of radiation may indicate that the threat uses a passive RF or an electro-optical sensor. The detected threat electronic parameters are compared to an extensive emitter database. The EW database, derived from intelligence sources, is used to identify the threat and correlate the threat and operating mode with effective EA techniques. Operational threat exploitation is often impeded by intelligence gaps and/or threat use of parameters reserved for wartime.

Nondestructive Electronic Attack. Nondestructive EA produces electromagnetic signals at a predetermined radio, infrared, visual, or ultraviolet frequency with characteristics that temporarily interfere with the threat's receiving system, that is, power level, frequency, and polarization. EA degrades or overcomes threat system operation by overpowering the target signal at the threat sensor. "Dazzling" is laser or high-power lamp EO/IR jamming. Dazzling saturates the detectors or focal-plane arrays of electro-optical (infrared, visual, ultraviolet) guided missiles and target-tracking systems. Deceptive EA presents a confusing signal to the threat sensor that degrades its performance to the point where it is no longer effective. Power levels used for deception are less than those required for jamming because deception does not require threat sensor saturation.

Destructive Electronic Attack. Destructive EA physically damages or destroys the threat electronic system. Specially designed missiles such as the HARM missile, shown being released from an A-6 aircraft in Fig. 4, are equipped with radar-homing seekers that attack the threat radar antenna and nearby electronic equipment within the blast radius of the missile warhead. More recently, similar seekers have been fitted to loitering remotely piloted vehicles for a similar purpose. Advances in high-power microwave and laser technology have made directed energy more practical. At very high power levels, microwave energy destroys the components in a missile seeker or threat radar, rendering them inoperative. High-power lasers also physically damage both RF and electro-optical threat systems.

Electronic Protection

Electronic protection provides EW protection for the host platform. Key environment surveillance and threat-warning information is provided by the ES system function (as it is for EA). EP responds to threats in the environment with information for evasive action and with the countermeasure responses described previously. EP is primarily directed against

Figure 4. HARM missile (shown after separation from an EA-6B aircraft) is an EW weapon for physically destroying the source of hostile radiation.

the terminal threat targeted on the host platform, and preferred EP techniques use decoys that are less susceptible to the home-on-jam weapon mode.

ELECTRONIC WARFARE TECHNICAL AREAS

Technical areas that support the ES, EA, and EP functional EW systems areas are discussed in this section. All aspects of EW are addressed by modeling and simulation because this is the most practical means for functional evaluation. System architectural analyses address the formulation of efficient EW system configurations to provide the operational functions required within the constraints of available equipment, techniques, and technology. Technical areas that address ES primarily are signal detection, measurement, and processing issues that deal with environment surveillance and warning. Technical areas associated with EA and EP include CTAR jamming and false-target generation, EO/IR CM, and decoys. Also included in these technical area discussions are technology challenges to EW technologies for future capability.

Modeling and Simulation for Electronic Warfare

Electronic warfare uses modeling and simulation extensively in three areas of investigation: research into new hardware; threat domination/exploitation; and tactics development. The effectiveness of an EW architecture or equipment suite is assessed by using a computer model and parametric studies run against the model. Estimates of a threat system's capabilities are incorporated into the model as environment sources because acquiring foreign hardware and measuring its performance is difficult. Environment signal models stimulate the EW system model. The EA effectiveness modeled against the threat is measured, and tactics are developed to further reduce threat system efficiency.

Modeling and simulation (M&S) combine detailed antiship missile models with ship models, antiair missile models with aircraft models, electromagnetic propagation models, and chaff RF decoy models. (Chaff RF decoys are described later). Chaff effectiveness evaluation considers the spatial relationship between the missile seeker and the ship while accounting for radar clutter and multipath returns. Signals at the missile are processed through the seeker receiver and missile guidance and tracking logic. A chaff cloud(s) injected into the simulation provides a false radar target signal at the missile seeker. By varying the amount of chaff and/or the chaff round spatial relationship with respect to both the defended ship and the threat missile, chaff effectiveness and tactics can be evaluated. However, the accuracy of the M&S results depends on the accuracy of the models used. An accurate missile sensor and control model is necessary to determine the effects of the complex signal returns from the target ship and the chaff on the missile controls and resultant flight path. In a simulated engagement, detailed missile functions are required to provide an accurate assessment of chaff effectiveness. These functions include monopulse antenna processing, range and angle tracking, missile guidance, and aerodynamics. Multiple threat seeker modes, such as acquisition, reacquisition, track, home-on-jam (HOJ), and simulated coherent combinations of signal segments are also required in the model.

Target ship, aircraft, and chaff radar cross section (RCS) must be accurately modeled. Typically, a multireflector target simulation is used to represent the RCS signature. Ideally, a model of thousands of scatterers would provide greater accuracy. However, careful selection of several hundred scatterers is adequate.

The accuracy of the missile and target interaction depends on the propagative environment model including multipath. Typically, a ray-tracing algorithm models the propagation of RF energy. Useful models rely on a stochastic representation of clutter as a function of wind speed, grazing angle, frequency, polarization, and ducting. Modeling of an ocean environment can be extended to include reflection from wave segments. Models are verified by using measured field test data.

Electronic Warfare System Architectures. The EW system architecture ties system functional elements into an efficient configuration optimized to the operational mission. Figure 5 shows a typical EW system architecture. The system performs signal acquisition and parameter measurement, direction finding, countermeasure generation, and decoy deployment. The system central processing unit (CPU) provides sensor and countermeasure coordination and EW system interface with other onboard systems.

Fusing the measurements of EW sensors and processors is a complex technological challenge. This information includes radar, communications, EO/IR, direction finding, and signal analysis. Data fusion within the EW system requires algorithmic development and significant enhancement in computational throughput. The EW system includes antenna(s), receiver(s), and processor(s) elements that provide data on signals in the environment. System sensors detect and measure threat signal characteristics. Multiple sensor subsystems measure the characteristics of the signal. For example, a signal acquisition detects the presence of a signal and measures the envelope characteristics (frequency, time of arrival, and signal duration). Another sensor that may include multiple antennas and receivers provides signal bearing-angle data. Separate subsystem sensors measure intrapulse signal modulation and/or received polarization.

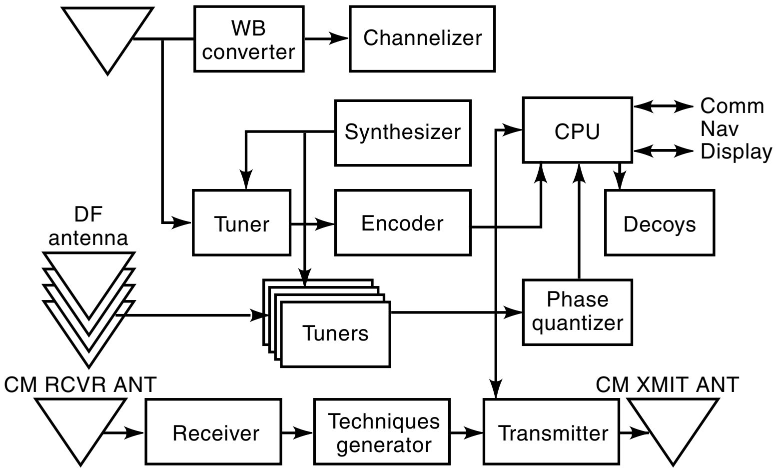

Figure 5. Electronic warfare system architecture indicating system functional elements required to provide ES, EA, and EP functions to the host platform and operational battle group.

A countermeasures receiver may use an independent electromagnetic environment interface. The countermeasures receiver accepts signals from the environment and provides them to the techniques generator. Target signals designated by CPU algorithms are selected for countermeasure generation as are the countermeasure modulation techniques to be applied. The resulting jamming signals are amplified to the desired power levels and radiated into the environment.

Decoys are part of the EW system architecture. This subsystem is controlled by the CPU based on sensor inputs. Decoys provide the important function of separating the countermeasure signal source from the host platform. In this operational mode, decoys provide alternative highly visible targets to divert a weapon from its intended target. Also required are the means, such as the coordination of jamming with the use of decoys, to neutralize the HOJ weapons threat.

Surveillance and Warning

Electronic support surveillance and warning perform the functions of noncooperative intercept and exploitation of radiated energy in the EM environment. Surveillance and warning detection relationships are those associated with communications systems. Additional signal detection constraints result because the signal's spatial location and its characteristics may not be known. Signal unknowns require tradeoffs of detection sensitivity and environment search. Once detected and measured, environment signals require sophisticated signal processing for signal sorting, formation, and characterization before they can be correlated with signal intelligence libraries for classification. Some fundamental tradeoff relationships for detection and warning are discussed below.

Threat Signal Detection. Threat signal detection occurs as the electronic support system is illuminated above the system sensitivity level with signals that satisfy the single-pulse detection criteria. Detection is performed as the ES system scans the environment. Detection metrics include incident radiation sensitivity, detection probability, false detection probability, corruption probability, simultaneous detection, and throughput rate.

Aircraft are often used to carry electronic warfare battlefield surveillance equipment. The operating altitude of surveillance aircraft provides a long line-of-sight range to the horizon. The range to the electromagnetic horizon accounting for nominal atmospheric refractions is given by

$$R = \left[\left(\frac{3}{2}\right)h\right]^{1/2} \tag{1}$$

where h is the aircraft sensor altitude in feet and R is the observer-to-horizon range in statute miles.

The time required to survey the environment depends on the surveillance alert status, system sensitivity, instantaneous observation segment, and rate of environment search. The number of instantaneous environment segments in frequency and bearing establish the number of environment dwell periods required for an environment scan. The larger the environment segments, the more rapidly the system performs the scan. The dwell at a given environment segment is scheduled to span the signal event period. Time to intercept is modeled by

$$T_{\mathrm{I}} = \frac{(T_{\mathrm{D}}NM)}{P_{\mathrm{T}}} \tag{2}$$

where T_{I} is the time required to survey the environment, T_{D} is the EW support system dwell period, N is the number of frequency segments in the environment, M is the number of spatial segments in the environment, and P_{T} is the probability that the signal occurs above the sensitivity level.

In Eq. (2), spatial environment segmentation, spectral environment segmentation, and detection probability combine multiplicatively to define the time required to survey the environment. Wide instantaneous bandwidths and a large instantaneous field of view reduce environment survey time unless equipment choices reduce system sensitivity and the corresponding probability of signal detection. Equations (3) and (4) describe receiver sensitivity and aperture gain functional relationships:

$$S = (\mathrm{NF})(\mathrm{SNR})(kTB) \tag{3}$$

where S is receiver sensitivity, NF is receiver noise factor, SNR is the required sensitivity for detection and false alarm criteria, k is Boltzmann's constant, T is temperature in degrees kelvin, and B is bandwidth in hertz.

$$G = 2K\pi/\theta \tag{4}$$

where G is antenna gain, K is antenna efficiency (less than unity), and θ is antenna beamwidth in steradians.

A tradeoff between sensitivity and time to intercept is implied in Eqs. (3) and (4). By using multichannel processing, the tradeoff can be resolved in either domain. A wideband channelizer provides instantaneous spectral coverage equal to the span of the channelizer frequency coverage, and receiver sensitivity is established by the bandwidth of an individual channel. Multichannel spatial processing provides the instantaneous spatial coverage of the sum of the channels being processed. System antenna gain is based on channel beamwidth.

Detection sensitivity requires consideration of the desired detection range. Equation (5) defines the electronic support detection range in terms of the threat signal parameters and the electronic support antenna, receiver, and processor system parameters:

$$R_{\mathrm{MAX}} = \left[\frac{P_{\mathrm{t}}G_{\mathrm{t}}G_{\mathrm{r}}\lambda^2}{(4\pi)^3\left(\dfrac{S}{N}\right)_{\mathrm{MIN}} kTB_{\mathrm{n}}L}\right]^{1/2} \tag{5}$$

where R_{MAX} is the maximum detection range, P_{t} is the threat signal transmit power, G_{t} is the threat signal antenna gain, G_{r} is the antenna gain of the electronic support subsystem, λ is the wavelength of the threat signal transmission, $(\mathrm{S/N})_{\mathrm{MIN}}$ is the minimum signal-to-noise ratio required by the electronic support subsystem for detection, k is Boltzmann's constant, T is absolute temperature, B_{n} is the effective noise bandwidth of the electronic support receiver, and L represents the combined feed losses of the threat transmitter and the electronic support receiver.

The probabilistic characteristic of signal detection is illustrated by considering the intercept of a threat at a signal level considerably above the receiver threshold level. Detection probability arises primarily from the independent probabilities that the ES system observes the environment in the spatial and spectral location of the threat emitter and that the threat emitter illuminates the receiver with the required power for detection.

Also of importance is the probability of signal detection once the ES system is steered to the signal spatial and spectral location. Then detection probability P_{D} is based on the signal characteristics, that is, the probability that the threat signal illuminates the EW system during the observation period. The time required to perform a detection T_{I} is derived from the scan interval T_{S} and is given by $T_{\mathrm{I}} = T_{\mathrm{S}}/P_{\mathrm{D}}$.

False reports from the electronic support receiver are highly undesirable. Limited computational resources are needed to process each pulse received in an attempt to form an association with other pulse reports. The rate of false reports is established by the proximity of the detector threshold level to the noise level. Figure 6 shows the relationship between the single-event probability of detection, the probability of false signal report generation, and the signal-to-noise ratio. This figure shows that both the probability of detection

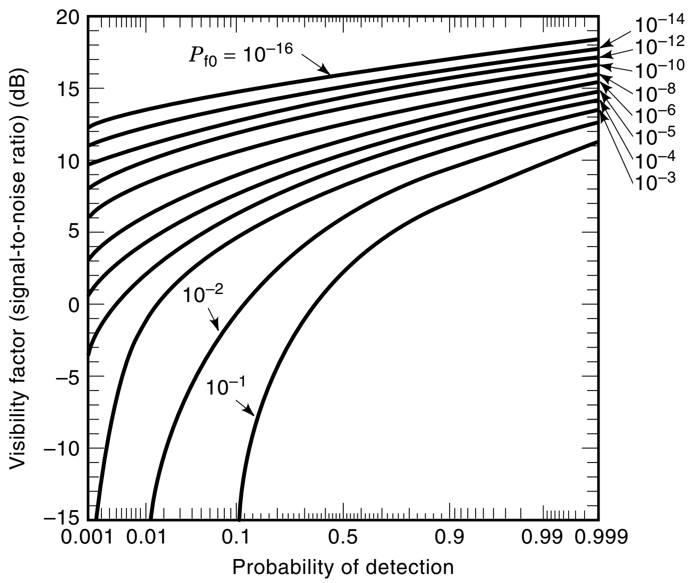

Figure 6. Detection probability and false detection probability for various signal-to-noise ratio conditions.

and the probability of false generation are strong functions of the signal-to-noise ratio.

The probability of pulse interference P_{OL} depends on the duration T_{D} of the signal and the rate R at which signals are expected. A reduction in P_{OL} results from adding parallel measurement channels. The functional relationship approximating P_{OL} is

$$P_{\mathrm{OL}} = \frac{\dfrac{(T_{\mathrm{D}}R)^{\mathrm{N}}}{N!}}{1 + \displaystyle\sum_{\mathrm{N}=1}^{\mathrm{N}} \left(\frac{T_{\mathrm{D}}R}{N}\right)} \tag{6}$$

where T_{D} is the event duration, R is the event repetition rate, N is the number of parallel measurement functions provided, and P_{OL} is less than 0.9.

Electronic Support Signal Processing. The ES signal processor derives signal information from the multitude of environment event measurements. Signal processing is the focal point of the ES subsystem where operationally relevant sense is made of large data inputs. ES processing includes sorting event data and correlating sorted event data with emitter libraries to establish the class or family of signals to which the emitter belongs. Beyond sorting, intensive processing is applied to identify intercepted emitters specifically and to locate them precisely within the battle space.

Sorting, a key electronic support signal processing function, correlates event descriptors from the same emitter. Correlation is performed on the basis of both instantaneous and temporal signal parameters. Instantaneous parameter sorts are less computationally demanding than temporal deinterleaving.

The initial signal sorting is histogramming based on instantaneous signal parameters. The signal parameters used for histogram-based sorting are those available from a single event or pulse measurement. They include external signal parameters, such as signal frequency, start time, duration, power level, and angle of arrival. Other instantaneous parameters used are measurements of signal modulation. Signals measurements with like parameters are binned together, and it is postulated that each bin contains event descriptor data from the same emitter.

After sorting, event descriptors are placed in individual emitter-associated groups. The monopulse and interpulse characteristics of the event group measurements are quantified into a signal descriptor. The signal descriptors are classified into an emitter class by correlation with a library database.

In some instances, high-resolution signal measurements identify specific emitters. As might be expected, identification parameter sets and the processing required to establish them are significantly in excess of that required for classification. Here, as in the case of classification, detailed signal descriptors are correlated with a library to define a specific emitter.

The spatial distribution of threat signals in the environment is operationally important. Determining the threat signal bearing angle with respect to own platform is a key step toward establishing threat signal position information. Conventional techniques used for direction-finding measurements include the use of differential amplitude processing of squinted antennas (antennas aimed in different directions), differential phase measurements from a phased-array antenna, and differential time of arrival measurements from spatially separated receivers.

Both hostile and benign operational scenarios require information about the location of both noncooperative fixed and mobile emitter installations. Electronic warfare target location exploits direction-finding data and navigational data to provide a signal location solution. Single or multiple platforms are used to generate location data.

The accuracy of target location depends on the precision of the direction-finding data and the navigation measurement and on the length of the baseline between measurements and the range to the target. Figure 7 shows target location geometry. The major error location axis A is modeled by

$$A = R\varphi \csc\left(\frac{\psi}{2}\right) \tag{7}$$

where R is the range from observer to the target emitter, φ is the direction-finding measurement error, and ψ is the angle

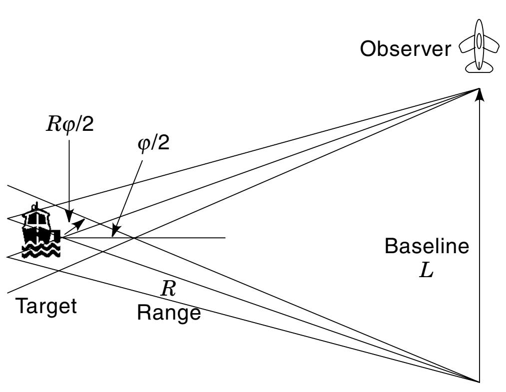

Figure 7. Emitter location geometry supporting Eq. (7), with observer track and signal measurement angles indicated.

subtended by the maximum difference in observation bearings with respect to the target, which provides location measurement error for the condition $\psi < \pi/2$. The range R from the observer to the target is given by

$$R = L\frac{\sin(\pi - \theta - \gamma)}{\sin\theta} \tag{8}$$

where L is the separation between observations, θ is the angle between the baseline and the opposite bearing angle, and γ is the angle between the baseline and the adjacent bearing angle.

Electronic Support Digital Signal Processing Technology. Electronic warfare system processing, both dedicated and programmable, assimilates environment data from the receivers and wideband processors. It uses these data to sort, classify, and identify the sources of emissions to represent the environment relevantly. The digital signal processor provides the means for applying an array of algorithms to both predetection and detection signal data to extract threat information for EW system use. Digital signal processing metrics include high-rate signal throughput processing in a compact module.

Digital signal processing is the heart of the ES function. It provides the flexibility of applying an extensive array of algorithms to system data. Critical digital signal processing technology challenges include processing throughput and developing efficient processing algorithms. Although signal data can be refined by applying sequential algorithms, the ES response is time critical; it must provide the most accurate assessment of available data within the required response time. Great potential exists for advancing digital signal processing technology, but optimum ES performance can be expected from judicious allocation of processing tasks between wideband processors and the digital signal processor.

An example of digital signal processing technology is L-MISPE (little monopulse information signal processing element), a special-purpose signal processor designed to operate with high-quality superheterodyne RF receiver systems. L-MISPE provides extremely accurate pulse analysis and parameter extraction for signal classification and specific emitter identification (SEI). It is contained in a single rack-mounted enclosure.

Surveillance and Warning Technology. Surveillance and warning are the sensor and environment processing functions for the EW system. Speed and accuracy of measurements and processing functions are the primary metrics for ES. Accurate throughput is important in providing sufficient time for effective threat response to the EA or platform commander. In addition, precision threat assessment provided to the EA subsystem facilitates optimum technique selection and conservation of EA power resource for engaging multiple threats. The ES performance challenge is further constrained by space limitations aboard platforms, particularly aircraft. Receiver technology performs environment sensing for the EW application.

Receiver Technology. Electronic support throughput and physical displacement metrics are addressed in developing wideband, small-size monolithic microwave integrated circuit (MMIC) technology. MMIC monolithic integrated analog processing at multigigahertz operating frequencies provides a ca-

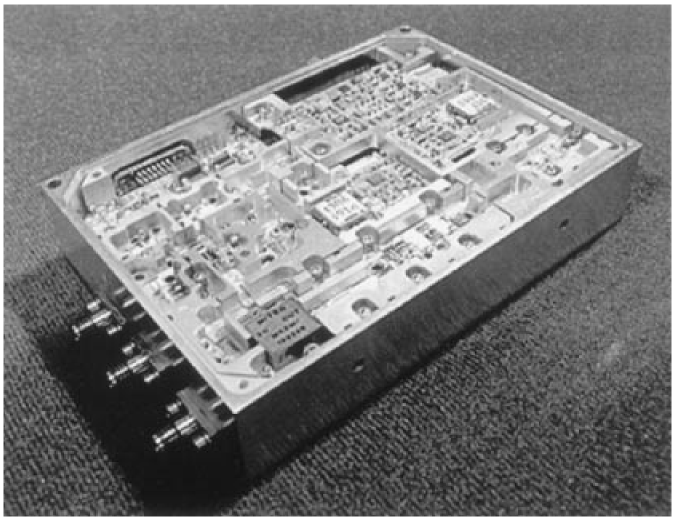

Figure 8. The MMIC receiver, a combination of monolithic microwave, analog, and digital circuits, performs signal selection and conversion to a convenient intermediate frequency.

pability suited to ES receiver applications. Advantages sought in the exploitation of this technology base include economies of size, weight, power, and cost. Increased receiver dynamic range for continuous environment intercept during active countermeasures transmission remains a receiver technology challenge. The MMIC receiver shown in Fig. 8 is an example of this technology.

Wideband Processing. Wideband receivers provide high probability of signal intercept. Wide spectral segment processing is necessary to increase signal detection sensitivity and to provide copulse reception of multiple simultaneous signals and rejection of interference signals. Requirements for wide instantaneous bandwidth, rapid throughput, and small modules are wideband processing metrics.

Acousto-optic channelization technology is being developed for wideband processing as a compact, economical means for performing high-resolution environment segmentation. Wideband-signal frequency demultiplexing is performed using Bragg regime acousto-optic diffraction and electronic signal detection and encoding. Functions performed by these acousto-optic processors include channelized correlation, convolution, and spectral processing.

Acousto-optic channelizers are based on Bragg diffraction of light (Fig. 9). The Bragg cell serves as the optical deflection or optical modulator element within the processor. The Bragg cell is an optically transparent medium, such as a crystal, that is driven at the applied RF frequency by using a piezoelectric RF-to-acoustic transducer. The Bragg cell transduces the RF signal into acoustic waves that are collimated into the Bragg cell crystal. The propagating acoustic wave creates sequential regions of crystal compression and extension that correspond to the period of the acoustic wave. The acoustically induced diffraction grating in the Bragg cell interacts with a coherent optical source to perform RF input frequency demultiplexing. The deflected light beams output from the Bragg cell are focused onto a detector array where light is detected to indicate energy in segments of the applied RF spectrum.

Wideband Interconnections. Electronic warfare sensors require broad access to the electromagnetic environment to provide quick response to hostile electromagnetic activity. For convenience and efficiency, central stowage of signal processing functional elements is important. To assure signal visibility, environment apertures, antennas, and EO/IR sensors must occupy locations on the periphery of the aircraft, ship, or land vehicle. Wideband interconnects transmit electromagnetic environment data from the EW system apertures to processing subsystems.

With the current RF bandwidth of the electronic warfare environment expanding through tens of gigahertz, just finding a medium that supports that level of frequency coverage is a challenge. At light frequencies, however, a 100 GHz spectrum spans less than a third of 1% of light frequency. In addition, low-loss-transmission optical fibers provide a nearly lossless means to transfer wide spectra across a platform. Indeed, wideband interconnect technology is developing the use of fiber optics.

Usable optical fiber bandwidth is limited by dispersion. Conventional fiber exhibits dispersion of 20 ps/km/nm of bandwidth. A typical signal operating within a 10 MHz bandwidth would exhibit dispersion of less than 0.1°. Clearly, bandwidth limitations are elsewhere in the link.

Detectors have also been developed to provide bandwidths on the order of tens of gigahertz. High RF operating frequency detection is performed by using small-geometry detectors that exhibit maximum power limitations. Limitation in maximum power levels applied to the detector restricts the output signal intensity range. Recent developments in distributed detector elements are extending detector power-handling capabilities.

Dynamic range is a significant fiber-optic link metric because the EW sensor system must process low-power signals on the horizon in an environment with high-power local transmissions. Modulator and detector attenuation reductions are technological issues being addressed to enhance the dynamic range performance of fiber-optic links.

Countertargeting

Countertargeting (CTAR) is the technical area that provides the means for protecting the host platform or force from

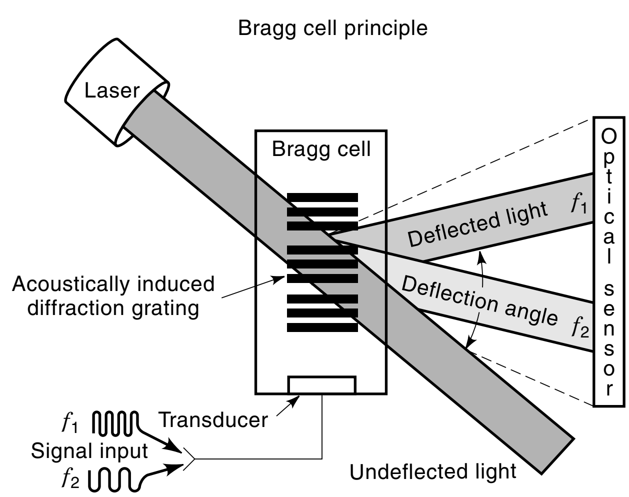

Figure 9. The acousto-optic Bragg regime signal transform processing principle used for signal-frequency analysis, sensitivity enhancement, and direction-finding functions.

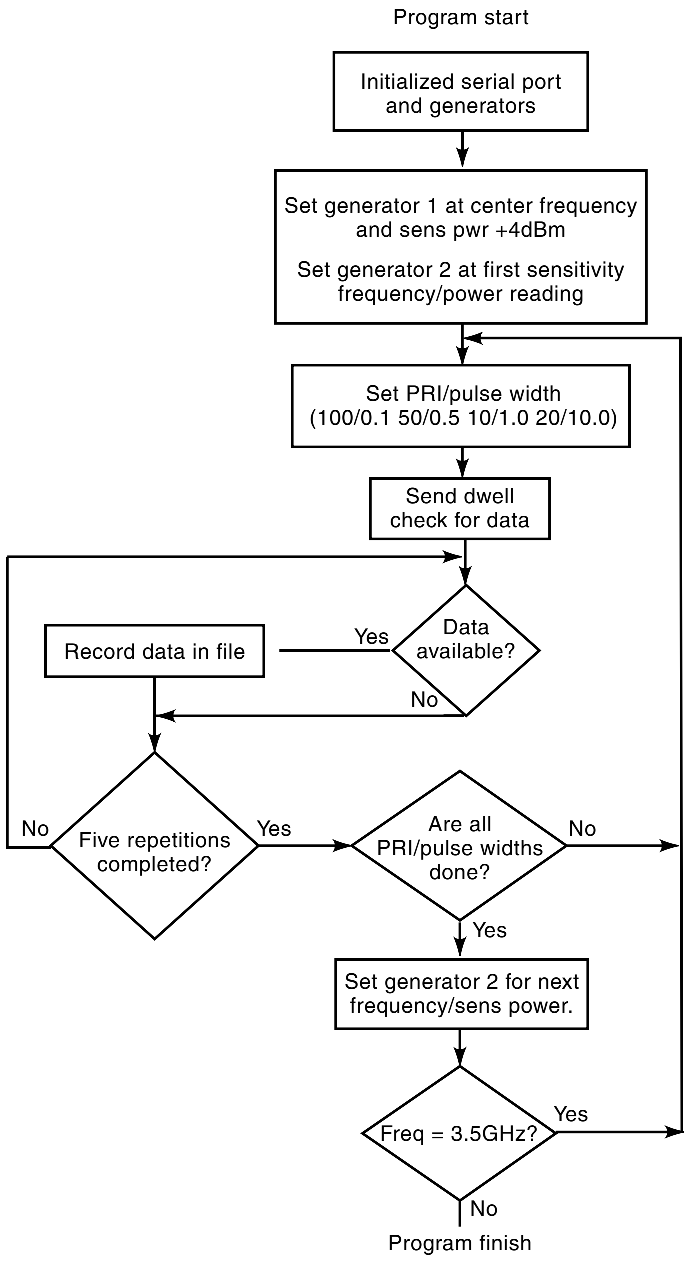

Figure 10. CTAR functional diagram showing sequence used in engaging a surveillance or targeting radar signal.

weapons targeting by a hostile force. CTAR functions include obscuration, false-target generation, and confusion. Associated techniques include jamming and onboard and offboard false-target generation.

Countertargeting operates against radars that feature a target-locating or surveillance mode, as shown in the functional sequence of Fig. 10. Airborne surveillance radar is generally used against ship and ground forces because the aircraft altitude provides extended surface target detection range. Conversely, when defending against aircraft with CTAR, the radar could be ground-based. Some radars are designed with the sole purpose of surveillance, whereas others are multimode and can track targets. By using imaging processing, modern surveillance radars that include synthetic aperture, inverse synthetic aperture, high range-resolution, and moving target indication processing can accurately determine target location and identify the type of target.

Countertargeting Techniques. Figure 10 shows the CTAR functional sequence. CTAR EA techniques are categorized as environment obscuration and jamming and false-target signal generation. CTAR provides either confusing or ambiguous data to adversary surveillance and targeting radar displays to confuse the human operators who interpret these presentations. Radar displays include plan position indicators (PPIs), A- or B-scopes, or combinations of these. Obscuration screens targets over selected portions of the display with a jamming signal power above that of the target signal in environment segments spanning both range and azimuth (see radar articles for descriptions of radar displays). The amplitude of the obscuration CTAR signal exceeds that of any target-reflected signal in the screened sector.

Experienced operators can recognize obscuration and radar jamming and initiate procedures to mitigate its effects. The false-target CTAR technique, however, is a more subtle form of EA that is less apparent to the operator. Here, the CTAR signal creates false indications on the radar display that appear as real targets to the operator. When the display is cluttered with false targets, radar operator time is consumed sorting through them. Selecting a false target for missile engagement dissipates an expensive weapon.

CTAR EA systems can be used to protect an entire military force. CTAR force protection systems are generally large and use human operators for system control. An example is the AN/ALQ-99 system installed on the EA-6B (Fig. 11), and EF-111 EW aircraft. Some EA systems, such as the AN/SLQ-32 installed on surface ships (Fig. 12), are for self-protection and support EA functions.

The EA system selects a specific technique from a large EA technique library. Selection is based on knowledge of the threat location, class, electronic parameters, and operating mode. The EA system, using an embedded receiver subsystem, rapidly adapts to threat signal operating mode changes. The threat changes operating mode as either a counter-countermeasures technique to circumvent EA or as part of the hostile targeting and homing sequence. Adaptive EA provides rapid changes in techniques as the threat sequences through operating modes.

Figure 11. EA-6B aircraft equipped with the AN/ALQ-99 EA system for airborne CTAR.

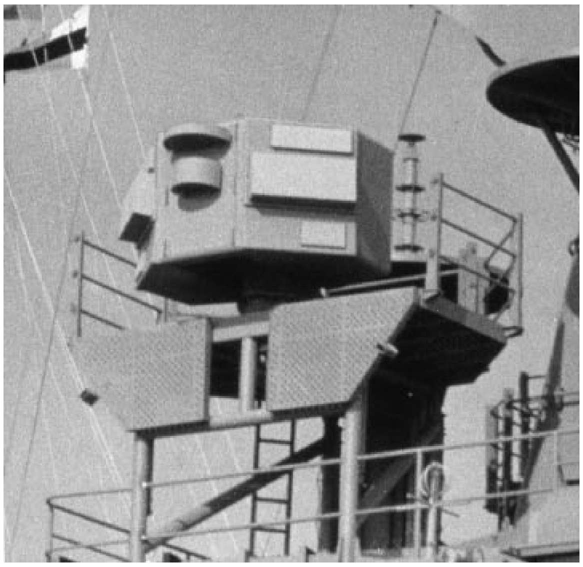

Figure 12. Shipboard installation of the AN/SLQ-32 EW equipment used for CTAR.

Both jamming and deception CTAR techniques may be used. RF jamming techniques are either "barrage" or "spot." Barrage jamming covers a wider frequency band at lower power density levels and is used to jam either several radars at once or spread-spectrum systems where the precise frequency of the threat is uncertain. Spot jamming concentrates the entire jamming power within the bandwidth of a single threat radar receiver with correspondingly better results. In both cases, a radial jamming strobe will appear on the threat radar PPI scope, as shown in Fig. 13. If the ratio of jamming signal power to the reflected radar signal power (J/S) is insufficient, the real target will "burn through" the jamming signal and become visible within the jamming strobe. For greater jamming effectiveness, it is desirable to have sufficiently large J/S to prevent burn through in the main beam and the principal sidelobes (see jam-to-signal calculations later).

Deception techniques are more varied and are generally threat-specific. Many deception techniques are directed against threat-tracking radars or missile-seeker radars. These techniques attack the threat radar target-tracking loops in range, angle, or Doppler. Deception techniques are often used in combinations and can be sequenced as the threat modes vary, or they can sequence according to a programmed pattern. False-target deception techniques are generated to emulate true target returns. The threat-radar operator, in response to deception, may conclude that all detected targets are genuine and simply select false targets for weapons engagement, or, if deception is suspected, time and computational resources must be used to identify the true target prior to engagement. In automated weapons systems, the EA subsystem may create so many false targets that the radar computer becomes overloaded. Because Doppler radar and missile seekers process large numbers of ambiguous radar returns to fix the true target, they are particularly vulnerable to coherent false-target techniques. An effective CTAR approach combines jamming and deception. Jamming creates a radial strobe that obscures the true target, whereas the deceptive CTAR provides false targets that project through the jamming strobe.

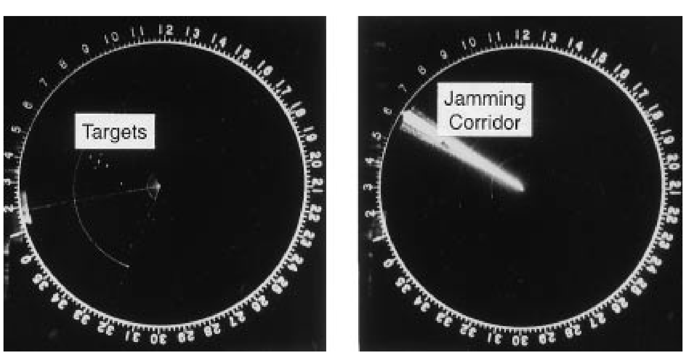

Figure 13. PPI radar scope without and with jamming, showing the effects of CTAR jamming on the threat radar display.

Countertargeting Effectiveness. Countertargeting effectiveness is assessed by comparing threat system performance in benign and CM environments. The ability of the threat system to detect, acquire, and target true targets, including parameters, such as target acquisition time and weapon release range, is assessed by evaluating threat performance against live targets on test ranges. Evaluating missile-seeker countermeasure effectiveness presents a more difficult problem. Computer simulations model the missile fly-out from an actual or surrogate threat system against a live target. A measure of CTAR effectiveness (MOE) is the ratio of the number of missiles that approach their target outside of the missile lethal range to those missiles that approach the target within lethal range. Software simulates multiunit engagements. US Navy ship EA is evaluated by flying test aircraft carrying captive instrumented seekers against the ships and recording the threat system performance.

A statistical technique to assess CTAR effectiveness compares the number of missiles required to defeat an EA-equipped aircraft versus the number required to defeat a non-EA-equipped aircraft. Similar statistics assess the number of antiradiation missiles fired versus the number of radar systems defeated. Additional effectiveness information can also be gleaned from intelligence sources.

Obscuration Burn Through. A measure of CTAR obscuration effectiveness is the range at which the radar displays the target in the presence of jamming. This is called the *burn through* range. At this range, the radar is sufficiently close to the target that the processed target-reflected radar power exceeds the jamming signal display masking. The real target becomes visible superimposed on the jamming signal. Burn through is modeled in Eq. (9) by using the radar range equation and free-space propagation. The radar range equation provides the signal power S that is received at the radar after being transmitted to and reflected from the target. The free-space signal propagation equation models the jammer power J that is received at the radar from the jammer. The quotient of jammer to signal power constitutes a figure of merit known as the jam-to-signal (J/S) ratio. This ratio is unique for each radar and depends on radar processing gain and on the display format and screen phosphor. Operator proficiency also plays a significant role. Rearranging the terms of this equation to solve for range yields the burn through equation:

$$R_\mathrm{b} = \sqrt{\frac{J}{S}\left(\frac{P_\mathrm{R}\sigma B_\mathrm{J}}{P_\mathrm{J}4\pi B_\mathrm{R}}\right)} \tag{9}$$

where R_b is the burn through range, J/S is the ratio of jammer-to-signal power required to jam the victim radar, P_R is the effective radiated power of the radar, P_J is the effective radiated power of the jammer, σ is the radar cross section of the target, B_J is the jamming signal bandwidth, and B_R is the processing bandwidth of the radar receiver. This equation models the case with the jammer located on the radar target platform.

Jammer-to-Signal-Power Relationships. The J/S power ratio at the threat radar is a concept central to predicting EA effectiveness. To degrade the threat radar, an interfering jammer power J of sufficient strength is required to overcome the target-reflected signal at the radar S. For effective EM noise jamming, the J/S required is 0 dB to 6 dB minimum, depending on the noise modulations used and the detailed characteristics of the threat. The minimum J/S ratio required for effective CTAR deception techniques varies from 0 dB for false targets, to 0 dB to 6 dB for range deception, to 10 dB to 25 dB for angle-tracking deception, and to 20 dB to 40 dB for monopulse deception. Equations (10)–(12) are based on two typical EA tactical situations. *Self-protection* CTAR [Eq. (10)] addresses the case with the target in the threat radar main beam. *Support* CTAR [Eq. (11)] addresses the case of the target in the threat main radar beam but with the EA jamming emanating from a separate platform and radiating into an arbitrary bearing of the threat radar antenna pattern. In both cases, the radar is assumed monostatic (i.e., the radar receiver and transmitter are collocated).

J/S for self-protection EP CTAR:

$$J/S = \frac{4\pi P_j G_j B_r R^2}{P_r G_r \sigma g^2 B_j} \tag{10}$$

where P_j is jammer power output; G_j is gain of jammer antenna in direction of radar; B_r is radar receiver noise bandwidth; R is radar-to-jammer range; P_r is radar power output; G_r is gain of radar antenna in target direction; σ is target radar cross section; g^2 is propagation one-way power gain (square of the ratio of field strength to free-space field strength due to direct and reflected ray combination), $0 < g^2 < 4$ (interferometer lobing); and B_j is the jammer noise bandwidth.

J/S for support EA:

$$J/S = \frac{4\pi P_J G_{jr} G_{rj} B_r R_t^4 g_j^2}{P_r G_r^2 \sigma B_j R_j^2 g_t^4} \tag{11}$$

where G_{jr} is the gain of the jammer antenna in the direction of the radar, G_{rj} is the gain of the radar antenna in the direction of the jammer, R_t is the radar-to-target range, g_j is the jammer-to-radar propagation factor, R_j is the radar-to-jammer range, and g_t is the radar-to-target propagation factor. The remaining terms are as defined previously.

Effect of target radar cross-sectional reduction:

$$S = \frac{P_r G_r \sigma \lambda^2 g^4}{(4\pi)^3 R^4} \tag{12}$$

where λ is the wavelength of the radar operating frequency. All of the remaining terms are as defined previously.

Equation (12) defines the signal at the receiver of a monostatic radar. Note that the power received at the radar is directly proportional to the target radar cross section σ and inversely proportional to the fourth power of the range R (R is the separation between the target and radar). Therefore, as the radar cross section is reduced, the signal at the radar is correspondingly reduced. If the cross section is sufficiently reduced, the target becomes indistinguishable from the radar noise and background clutter. Low observable platforms, such as the B-2 and F-117 aircraft, provide sufficiently low radar cross section to make radar detection difficult. The implication of radar cross-sectional reduction technology to CTAR is twofold: first, with sufficiently low radar cross section, EP may not be necessary, and secondly, if the cross section merely lowers the signal power at the radar, then a lower power, low-cost CTAR transmitter becomes sufficient to provide the J/S necessary to achieve the desired level of survivability.

Countermeasure Technology. Countermeasure technology addresses the evolving threat in addition to the need for economic force protection. Significant advances in radar, communications, EO/IR weapons' sensors, and weapons control present heightened challenges to maintaining effective EA capability.

Radar Countermeasures Technology. Countertargeting equipment for use against advanced synthetic aperture radar (SAR) or inverse synthetic aperture (ISAR) surveillance and targeting radar requires wide instantaneous bandwidths and high processing speeds. Furthermore, because these radars use coherent processing, CTAR effectiveness consequently requires coherent radar signal storage and reproduction to enhance effectiveness. Digital RF memory (DRFM) technology is being developed to convert the analog radar RF signals into a digital format for convenient storage. As required, the radar signal is retrieved from storage and converted to RF for use in countermeasure waveform generation. Technology limitations and costs constrain currently available DRFM designs, each optimized for a specific application.

Radio-frequency-tapped delay lines provide precise timing between portions of the CTAR waveform. Analog RF-tapped delay lines use surface acoustic wave (SAW) and acoustic charge-transport technology. Research is underway to create digital tapped-delay lines. Noise modulation is commonly applied to CTAR signals, and high-quality tunable noise sources are required. The output EA stage is the transmitter/antenna combination that generates and radiates the CTAR signal. Antennas for EA applications, once considered a dedicated asset, are currently envisioned as multifunction phased-array antennas with elements fed by solid-state amplifiers.

Radio-frequency isolation between the countermeasures transmitter and the receiver is a common problem of countermeasures-equipped platforms. The countermeasure signal appears at the receiver antenna. When the transmitter and receiver are insufficiently isolated, the countermeasure signal interferes with lower level threat signal reception from the environment. Interference demands careful attention to antenna design, isolation, and platform siting.

Radar Countermeasure Signal Source Technology. Electronic attack transmitters require signal sources that can be rapidly switched in azimuth, elevation, frequency, and polarization to generate multiple high-power beams with low sidelobes over large multioctave bandwidths. CTAR requirements for economical compact transmitters are challenged by the lack of appropriate low-cost EM power sources. Furthermore, few commercial applications exist for wideband EM power-source technology. Research and development in this area is limited primarily to EA applications. Original EW power sources, tunable magnetrons, and cross-field amplifiers provided only narrow operating bandwidths. Traveling wave tubes (TWTs) evolved to fill the need for wide, instantaneous bandwidth. Over time, TWT bandwidths grew from a single-octave 2 GHz to 4 GHz band to multiple octaves at frequencies beyond 40 GHz. However, TWTs are expensive and unreliable. Although new mini-TWTs and microwave power modules have become available, their basic design remains vacuum-envelope-based. MMIC technology is steadily advancing, and it now provides solid-state chips with multioctave signal-generation capability, wide instantaneous bandwidth, and signal power levels approaching 5 W. With MMIC technology, solid-state active aperture arrays become achievable, and such arrays for EA applications are now being developed. Although MMIC active aperture array signal source promises good performance and reliability, the system remains expensive.

Passive Electro-Optic/Infrared Electronic Warfare

Electronic warfare in a passive EO/IR target acquisition and weapons sensors environment applies to a growing threat capability. The open-ocean blue-water scenario requires EO/IR EA and EP ship protection, typically 200 nautical miles or more from shore, against massive and coordinated attack. EO/IR EA applications have recently focused on littoral scenarios involving amphibious operations in support of peacekeeping operations for regional conflicts; providing humanitarian assistance in politically and militarily unstable regions; evacuating civilians from regions of conflict; and ensuring safe passage of commerce through disputed littoral waters and choke points.

The traditional EO/IR threat, the long-range antiship missile, has been intensified in the littoral areas by a large variety of air-to-surface, air-to-air, and surface-to-air EO/IR missile weapons. These missiles can inflict severe damage to the smaller craft used for littoral warfare.

Electro-optic system target detection range depends on detector sensitivity and resolution. A target image is defined by contrast with the background. Sensitivity determines whether the contrast is discernible. Resolution depends on the spatial environment angle illuminating the detector, which is a function of detector surface area and focusing optics. The distance at which target features are resolvable determines the maximum operating range of the system.

The target signature detectability is not determined by the absolute temperature of the object but rather by the contrast between the target and background within a given spectral band. Environment backgrounds range from the cold, uniform background of space to thermally cluttered land areas. Solar interaction with the target and background reflection and heating further degrade the background contrast with the target. Typical target contrasts range from about 1 kW/sr (kilowatt per steradian) in the 2 μm to 3 μm atmospheric window for an aircraft engine to tens of kilowatts per steradian for ships in the 8 μm to 12 μm window. Target aspect, especially the location of hot spots, greatly influences the signature.

Electro-Optic/Infrared Countermeasures. Electro-optic/infrared countermeasures are constrained by specular atmospheric propagative characteristics, as is the threat (Fig. 14). The contrast of the target to the background within the weapon sensor's specular passband, the type of seeker spatial localization processing, and available practical radiation sources are also prime considerations.

The missile fly-out and CM sequence of events occurs in several seconds. As part of an integrated electronic warfare suite, the EO/IR EA system is designed to engage a large number of missiles launched in a coordinated attack. Figure

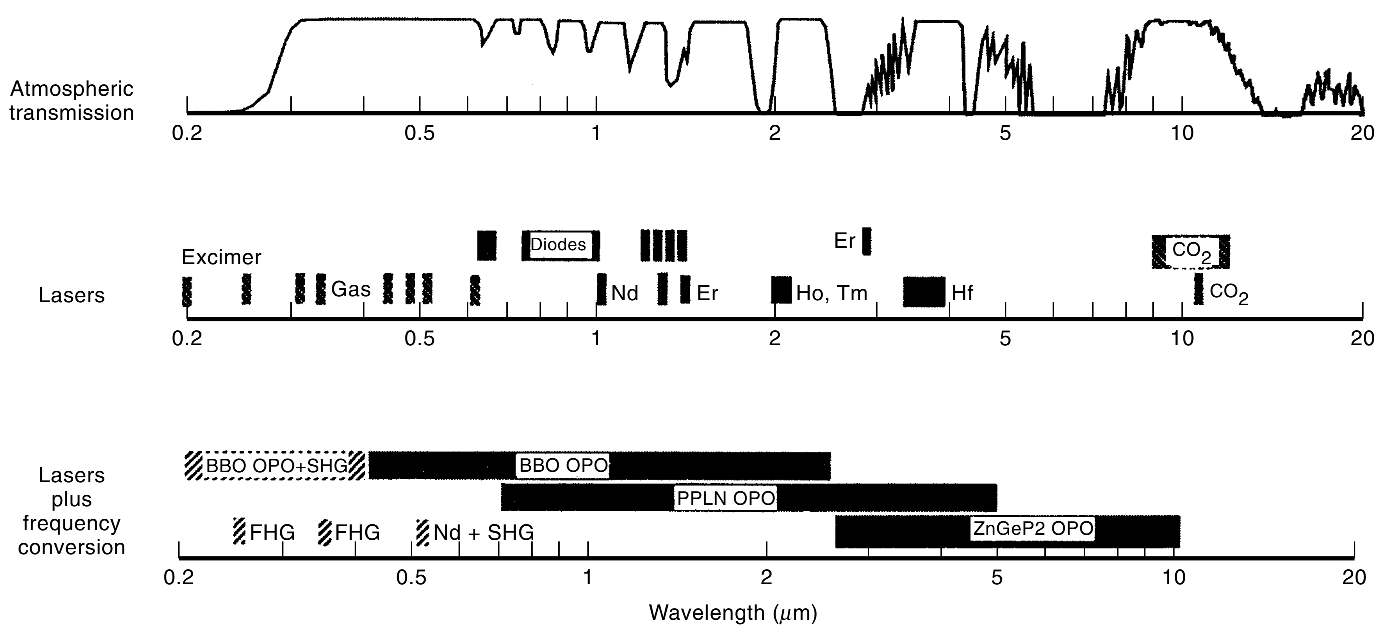

Figure 14. EO/IR atmospheric transmission spectral segments and laser and laser harmonics countermeasures source spectral regions.

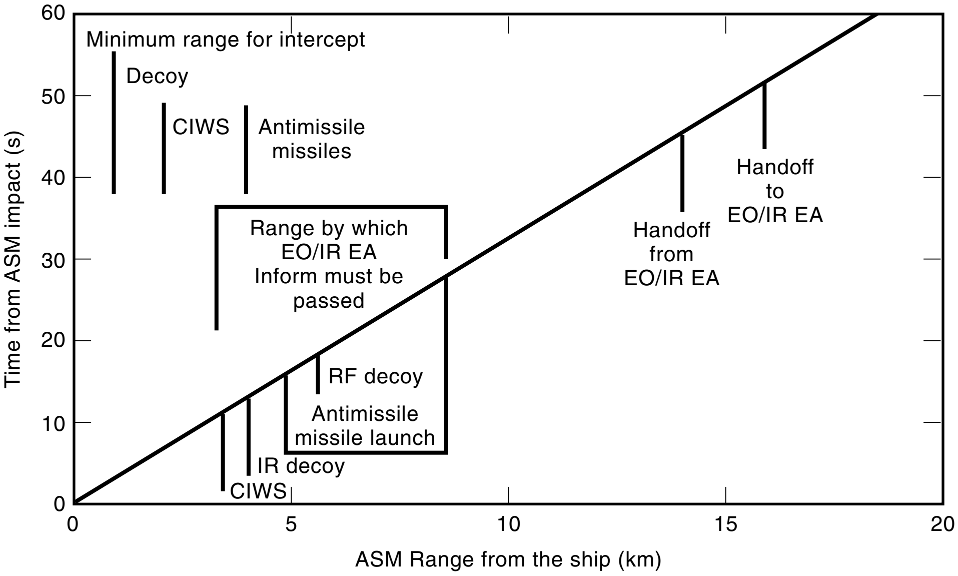

Figure 15. Missile attack time line showing launch, acquisition, and homing phases of the missile as well as the CM attack on missile sensors and control circuits.

15 shows a typical time line of the CM response to an attack by a subsonic antiship missile. The time line indicates the interaction of EO/IR EA with other ship defense systems.

To preclude detection by a threat EO/IR sensor, target signature can be reduced through a combination of convective, conductive, and radiative mechanisms. Exterior surfaces of ship stacks are cooled by convective air flow between the engine exhaust ports and the outer stacks. Engine plume and exhaust gases from all types of engines can be cooled by dilution with air. Radiation from hot spots can be reduced by spectral emissivity modifications or by obscuring the hot areas from view. On new platforms, low-observability design criteria have led to low-signature aircraft and ships.

Onboard aircraft CM sources initially generated false target location and/or guidance degradation through weapon automatic gain control (AGC) manipulation. This technique remains highly effective against many threats. The onboard jammer sources can be chemically fueled IR sources or electrically powered incandescent and metal vapor lamps. As the wavelength passbands of antiair and antiship seekers gradually migrate to longer wavelengths, out to the 8 μm to 14 μm window, noncoherent sources will no longer be practical.

Basic spin scan and conical scan (conscan) "hot spot" seekers are vulnerable to flare decoys. Almost universally, these flares are composed of magnesium and polytetrafluoroethylene and are designed with a radiant intensity several times that of the target. In the distraction mode, the decoy is an excellent target; in the seduction mode, the weapon's seeker control signal is biased by the decoy or transferred to it. Because pseudoimaging seekers exhibit spatial and temporal processing capabilities, simple flares are relatively ineffective, and simple flares perform even more poorly against imaging sensors. Newer decoys overcome advanced seeker-discriminating processing with improved spectral characteristics that more closely match the target platform spectral emissions. Improved decoy spatial distribution in the form of clouds and multiple hot spots, temporal rise times, and persistence match target-signature increase rates and lifetimes, thus preventing time-history discrimination. Kinematics model realistic target movement.

The small beam divergence of lasers can result in high-radiance, low-power sources that provide the J/S power ratios needed for effective EA. Two laser sources, primary lasers and nonlinearly shifted lasers, are available for CM applications. Lasers shifted by nonlinear conversion include harmonic generation and tunable optical parametric oscillators (OPOs). Primary lasers do not produce spectral lines in all of the potential threat passbands of interest and are susceptible to notch-filter counter-countermeasure techniques. Although harmonic generating EA techniques provide additional wavelengths, they are also subject to counter CM. Promising sources for IR/EO CM are tunable OPOs pumped by diode-pumped, solid-state lasers. Two nonlinear materials currently demonstrating the highest potential are periodically poled lithium niobate (PPLN) and zinc germanium phosphide ($ZnGeP_2$). Figure 14 shows the primary lasers of interest and the wavelength coverage possible with PPLN and $ZnGeP_2$ OPOs.

Although noncoherent sources provide wide angular protection, high-resolution detection is necessary to point and track the threat system and effectively use laser power. Timely threat detection and warning ES is essential to the success of all nonpreemptive EA.

Electro-Optic/Infrared Countermeasure Technology. Key EO/IR EA technologies required to counter threat performance improvements include higher throughput data processing using more capable algorithms, laser beam steering, and decoy launcher design. Needed processing improvements include faster signal processing, more efficient image processing, and false alarm reduction. High-performance, high-speed beam steering, preferably nonmechanical, is required to reduce response time in multiple threat environments. Improved decoy launchers to position decoys quickly and accurately within the scenario are also needed.

Low observability technologies are being developed to decrease or mask the IR/EO signatures of targets. Target signature reduction increases the effectiveness of conventional countermeasure responses by reducing the jamming power required to counter the missile system effectively. Low observability enables applying new technologies to IR/EO countermeasures by reducing the size, weight, and power requirements of decoy and laser CM sources. For example, diode laser and diode-pumped nonlinear optical sources can be integrated with unmanned aerial vehicles to produce new classes of CM devices and tactics. Large-area spectrally selective sources and obscurants provide advanced capability against spatially and spectrally discriminating threats. Primary laser and laser-pumped nonlinear sources are important evolving technologies. Launchers and vehicles that provide rapid and precise CM placement with realistic kinematic performance are areas of increasing importance.

Decoy Countermeasures

Decoys are EW devices, usually expendable, deployed from the platforms to be protected. Decoys generate a jamming response to the threat or false targets. In either case, the decoy lures the threat away from the intended target toward the decoy. A jamming decoy generates a cover signal that masks the target signal. Thereby the threat sensor signal fidelity is degraded, making detection and tracking of the intended target more difficult. A jamming signal may also activate the antijam home-on-jam mode of the weapon system. As false targets, the decoys generate credible target signatures to provide weapon system seduction or distraction. Decoys create confusion that causes weapons to attack false targets.

Decoys may be either passive or active. A passive decoy generates a countermeasure response without the direct, active amplification of the threat signal. Principal examples of passive decoys are chaff and corner reflectors in the RF spectrum and flares in the EO/IR spectrum.

Decoy Operational Employment. Decoys provide EA capability across the entire EW battle time line. Decoys are used primarily for EP missile defense and self-protection missile defense but also for countersurveillance and countertargeting applications.

Jamming is used in conjunction with decoys to obscure the target signal at the threat radar during decoy deployment. As decoys are deployed, jamming ceases and the threat radar acquires the decoy as a target or transfers radar tracking from the target to the decoy. Threat radar acquisition of the decoy as a target is probable because decoys present prominent signatures.

Decoys used for missile defense perform either seduction, distraction, or preferential acquisition functions. A single decoy type may perform multiple functions, depending on deployment geometry with respect to the launch aircraft or ship and the stage of electronic combat.

Decoys are used in a seduction role as a terminal defense countermeasure against missile weapons systems. A seduction decoy transfers the lock of the missile guidance radar or EO/IR sensor from the defending platform onto itself. The decoy that generates a false-target signature is initially placed in the same threat tracking gate, missile sensor range, and/or angle segment as the defending target and is subsequently separated from the launching platform. The decoy signature captures the missile guidance sensor, and the target lock is transferred from the ship or aircraft to the decoy. Typically, the decoy is separated in both range and angle from the defending target to assure target-to-missile physical separation greater than the missile warhead's blast range. The seduction decoy missile interaction is typically initiated within 10 s of deployment. Distraction decoys are deployed prior to missile-seeker acquisition and provide multiple false targets from which the seeker may select. Deployed distraction decoys provide a confusing environment to the missile seeker, causing it to attack a decoy rather than the intended target.

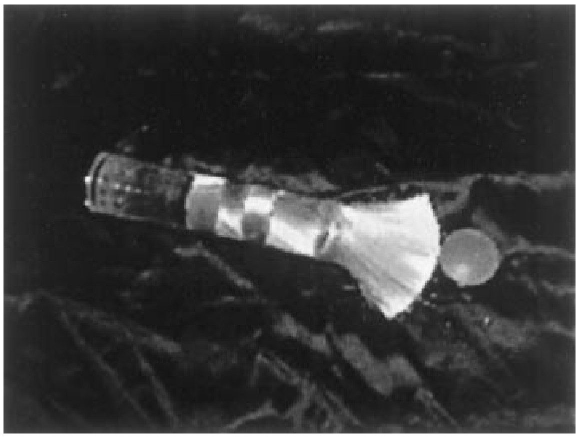

Figure 16. ALE-129 RF chaff round with the bundle of reflector elements partially deployed from the canister.

The ALE-129 chaff decoy (Fig. 16) is representative of RF seduction decoys for aircraft defense. The NATO Sea Gnat MK-214 cartridge shown fired from a shipboard launcher in Fig. 17 provides surface defense against radar-guided weapons. Figure 18 shows a TORCH decoy deployed at sea for IR defense.

Distraction decoys are observed for extended periods in the engagement scenario. Consequently, the distraction decoy must generate a credible signature that is sufficient to preclude short-term and extended missile decoy discrimination.

The AN/SLQ-49 inflatable corner reflector (Fig. 19) and the rocket-launched NATO Sea Gnat MK-216 chaff cartridge (Fig. 20) are representative of distraction decoys for surface ship defense. The TALD decoy (Fig. 21) is an example of a distraction decoy used for aircraft defense.

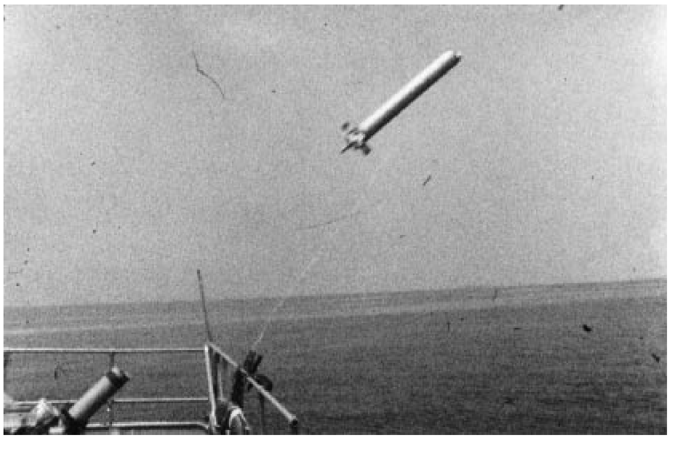

Figure 17. NATO Sea Gnat MK-214 seduction RF decoy deployed from a shipboard rocket launcher.

Figure 18. TORCH EO/IR decoy deployed at sea.

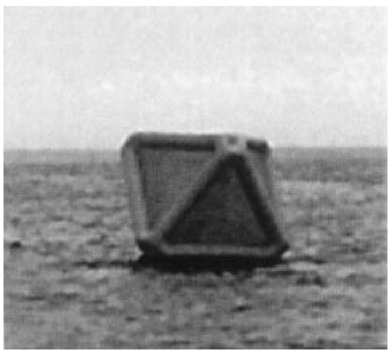

Figure 19. AN/SLQ-49 inflatable corner reflector decoy deployed at sea.

Figure 20. NATO Sea Gnat MK-216 distraction decoy deployed from a rocket launcher.

Figure 21. TALD decoy distraction decoy.

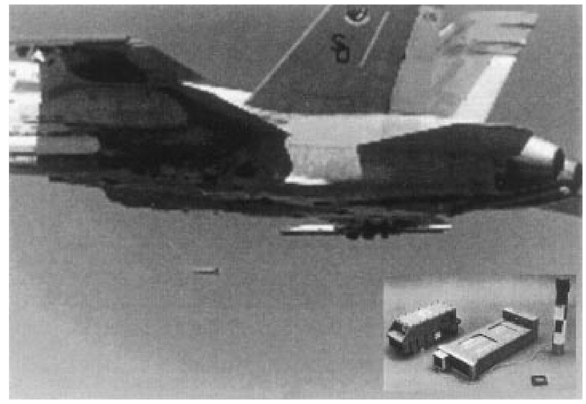

Figure 22. AN/ALE-50 towed decoy deployed from a tactical aircraft in flight.

Frequently, persistent seduction decoys perform a distraction function after separating sufficiently from the defended platform. This "residual distraction" further minimizes the number of distraction decoys required in an engagement.

An EA preferential acquisition decoy provides a signature to the missile seeker such that during acquisition the missile seeker senses the real target only in combination with the decoy signature. In the end game, the decoy signature in the missile field of view biases the aim point of the missile tracker away from the intended target.

The preferential acquisition concept requires decoys positioned close to the defending platform. Decoys can be towed behind the target aircraft or tethered to the defending ship. The AN/ALE-50 (Fig. 22) is a towed decoy used for air defense preferential acquisition, and the EAGER decoy (Fig. 23) is being developed for ship defense preferential acquisition.

Chaff Decoys. A chaff decoy is composed of multiple—tens of thousands to millions—of electrically conductive dipole filament elements deployed in the air to reflect and scatter radar signal radiation and create a false-target radar response. Figure 24 shows a typical deployed chaff decoy. The chaff decoy frequency response is determined by the length of the dipole elements, and the chaff radar cross-sectional (RCS) mag-

Figure 23. EAGER shipboard-tethered decoy in field trials.

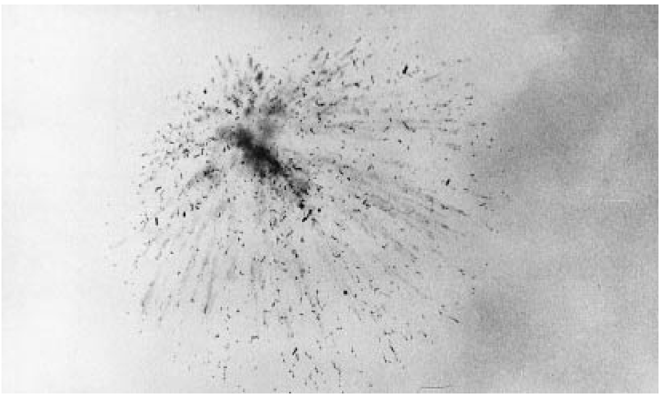

Figure 24. Deployed chaff round shown as a burst of reflector elements against a sky background.

nitude results from the number of dipoles deployed. Figure 25 shows a radar PPI display of an environment containing numerous chaff clouds.

The RCS of a chaff cloud is tuned for a given frequency (with the dipole length one-half the wavelength of the incident radar signal), and its RCS can be approximated by

$$\mathrm{RCS}(\mathrm{m}^2) = \frac{0.018c^2N}{f^2} \tag{13}$$

where c is the speed of light (3×10^8 m/s), f is the frequency in hertz, and N is the number of dipoles in the cloud.

Corner Reflector Decoys. Corner reflectors are conductive geometric structures that are typically shaped in the form of a perpendicular triangular corner. The shape maximizes the reflection of incident radar signals and provides a large ap-

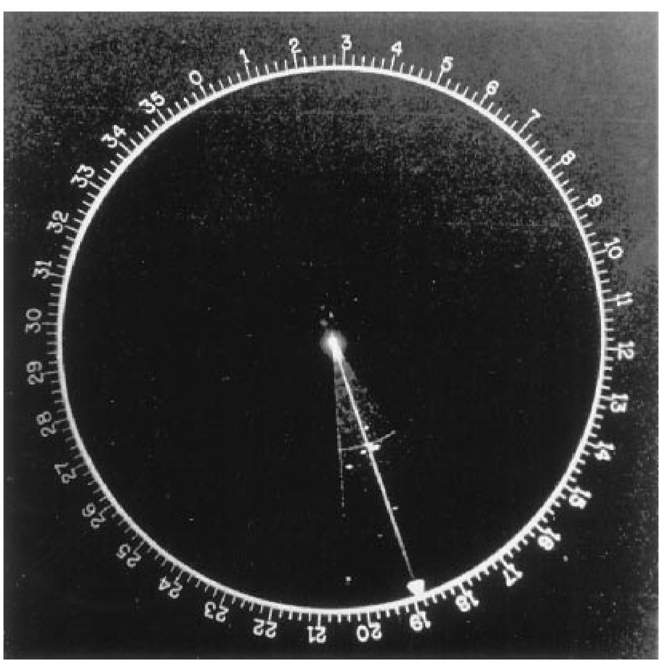

Figure 25. Radar PPI display showing target reflections from multiple chaff decoys.

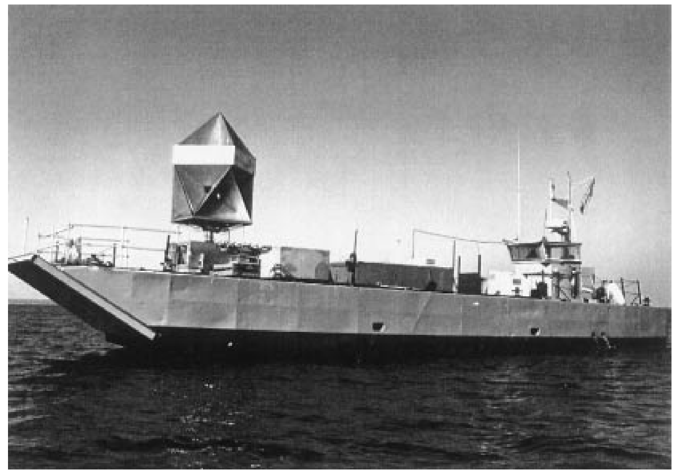

Figure 26. Multifaceted corner reflector deployed on a ship bow to provide a high cross-sectional reflection at several frequencies.

parent target signature. Figure 26 shows a multifaceted triangular corner reflector that provides wide angular coverage.

The apparent RCS normal to a triangular corner reflector is given by

$$\mathrm{RCS}(\mathrm{m}^2) = \frac{4\pi L^4 f^2}{3c^2} \tag{14}$$

where L is the length from the outside corner to the apex of the reflector, f is the frequency in hertz, and c is the speed of light (3×10^8 m/s). The 3 dB beamwidth of this type of corner reflector is 40°.

Flare Decoys. Flares are typically incendiary devices that produce EO/IR radiation to generate a false target. Figure 27 is an IR image of a magnesium-Teflon flare deployed from an aircraft.

Active Decoys. An active decoy uses direct threat signal amplification to generate the countermeasure response. In the case of RF systems, it is generally an RF amplifier (transistor or tube). In the EO/IR spectrum, a laser or flash tube amplifies the threat signal. Jammer and repeater decoys are active decoys.

Repeater decoys receive, amplify, and retransmit the received signal to generate a false target. Multiple signals may be retransmitted to generate multiple target returns. Modulation techniques (amplitude and frequency) may also be ap-

Figure 27. Flare IR decoy deployed from a tactical aircraft in flight.

plied to the signal before retransmission to enhance effectiveness. The apparent radar cross section of an active RF decoy is given by

$$\mathrm{RCS}(\mathrm{m}^2) = \frac{(P_\mathrm{d} G_\mathrm{d} 4\pi R^2)}{P_\mathrm{r} G_\mathrm{r}} \tag{15}$$

where $P_\mathrm{d}G_\mathrm{d}$ is the effective radiated power (ERP) of the decoy, R is the range between the decoy and the radar in meters, and $P_\mathrm{r}G_\mathrm{r}$ is the effective radiated power (ERP) of the radar.

For a decoy operating with linear gain, that is, a decoy whose transmission signal power is directly proportional to the input signal level (up to the signal compression level), the RCS relationship simplifies to the relationship given by

$$\mathrm{RCS}(\mathrm{m}^2) = \frac{(G_\mathrm{t} c^2)}{4\pi f^2} \tag{16}$$

where G_t is the combined electronic and antenna gains (receive and transmit) of the decoy, c is the speed of light (3×10^8 m/s), and f is the frequency in hertz.

Decoy Effectiveness. A distraction decoy is deployed at an extended range from the defending platform and provides an alternate target for seeker lock-on. Distraction decoys require deployment before seeker lock-on to engage the radar in its acquisition process. Usually more than one distraction decoy is used to defend a platform. An estimate of the effectiveness of the distraction decoy is given by

$$P_\mathrm{s} = 1 - \frac{1}{N+1} \tag{17}$$

where P_s is the probability that the missile will be distracted to the decoy and N is the number of distraction decoys deployed.

Equation (17) assumes that all of the distraction decoys exhibit viable target signatures and are equally likely to be acquired by the missile sensor. The number of decoys deployed can be reduced with the same probability of success with knowledge of the seeker acquisition logic, for example, a near-to-far/right-to-left acquisition search.

Seduction decoy effectiveness is primarily determined by the intensity of the decoy signature compared with the target being defended. However, the radar track bias, for example, leading edge tracker and discrimination algorithms, can significantly impact decoy effectiveness. In some cases, the radar track bias can be exploited to increase decoy seduction effectiveness.

Decoy Countermeasure Technology. Diverse technologies are required to support decoy launch and station keeping and countermeasure generation. Because most decoys are single-event, short-term items, cost plays a major role in selecting and developing technology for decoy use. Furthermore, because the defending platform must generally deploy a number of decoys throughout an engagement, decoy size and weight criteria also are critical. Attendant decoy platform technologies include aerodynamics, aircraft/projectile design, propulsion systems, avionics, and mechanical structures. Decoy payload technologies that will have significant importance in future systems include broad bandwidth microwave and millimeter-wave components (e.g., antennas and amplifiers).

Microwave and millimeter-wave output power sources are required with high power, efficiency, and duty cycle to support the projected threat environments. The future RF threat environment is expected to be densely populated with long-pulse radar. Higher decoy radiated power at higher duty cycles will be needed to prevent decoy saturation as the number of simultaneous threat signals in the environment increases.

Ultra high speed countermeasure frequency set on circuitry is necessary to queue jammer frequency rapidly. Signals with rapid frequency hopping and frequency chirping require rapid activation for effective countermeasures. Spatially large and efficient spectrally matched IR materials and radiating structures are needed to counter multispectral, imaging IR seekers. Safe, nontoxic, highly opaque, broad-spectrum IR and electro-optical obscuration materials are required to mask targets and confuse image-processing seekers. Efficient, primary power sources capable of high peak power and dense energy storage are needed to provide the increasing demand for electrical power used in decoy systems.

Reading List

J. S. Accetta and D. L. Shumaker (eds.), *The Infrared and Electro-Optical Systems Handbook;* D. H. Pollock (ed.), Vol. 7, *Countermeasure Systems,* Ann Arbor, MI: Infrared Information Analysis Center, and Washington, D.C.: SPIE Optical Engineering Press, 1993.

B. Blake, *Jane's Radar and Electronic Warfare Systems,* Surrey, U.K.: Jane's Information Group, 1993.

J. A. Boyd et al., *Electronic Countermeasures,* Los Altos, CA: Peninsula Publishing, 1978.

E. J. Chrzanowski, *Active Radar Electronic Countermeasures,* Norwood, MA: Artech House, 1990.

N. C. Currie, *Techniques of Radar Reflectivity Measurement,* Dedham, MA: Artech House, 1984.

R. D. Hudson, Jr., *Infrared Systems Engineering,* New York: Wiley-Interscience, 1969.

W. L. McPherson, *Reference Data for Radio Engineers,* New York: Howard W. Sams, 1977.

R. J. Schlesinger, *Principles of Electronic Warfare,* Los Altos, CA: Peninsula Publishing, 1961.

M. I. Skolnik, *Radar Handbook,* New York: McGraw-Hill, 1970.

L. B. Van Brunt, *Applied ECM,* Vol. 1, Dunn Loring, VA: EW Engineering, 1978.

W. Z. Wolfe and G. J. Zississ (eds.), *The Infrared Handbook,* revised ed., Ann Arbor, MI: Environmental Res. Inst. Michigan, 1985.

ANTHONY E. SPEZIO
ALAN N. DUCKWORTH
FRANCIS J. KLEMM
STANLEY A. MOROZ
JAMES M. TALLEY
Naval Research Laboratory