MIL-HDBK-293 (NAVY)
5 June 1987

MILITARY HANDBOOK

Electronic Counter-countermeasures Considerations in Radar Systems Acquisition

AMSC N/A

EMCS

DEPARTMENT OF DEFENSE
Washington, DC 20363

Electronic Counter-Countermeasures Considerations In Radar Systems Acquisition

1. This standardization handbook was developed by the Department of the Navy with the assistance of industry.

2. This document supplements department manuals, directives, and military standards, etc. It provides basic and fundamental information on electronic counter-counter measures considerations that should be taken into account to ensure the ability of the radar system being acquired to operate within its design specifications when exposed to hostile electronic countermeasures.

3. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: Commander, Space and Naval Warfare Systems Command, Attn: SPAWAR 003-121, Washington, DC 20363, by using the self-addressed Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

FOREWORD

The nature of Naval warfare has undergone an extraordinary transformation since World War II. At the forefront of this change has been the increasing need for reliable radar information in the presence of an expanding electronic warfare (EW) threat technology. The task at hand is to investigate the potential detrimental effects of various hostile EW techniques designed to preclude effective friendly radar operation and to determine the means to eliminate, or at least to minimize, these effects through the use of electronic counter-countermeasures (ECCM).

The technology of ECCM for radar is continually evolving and is often very complex. By its very nature, ECCM must be at the forefront of the ever-advancing state-of-the-art of electronics, and its techniques must always be at least one step ahead of the latest Electronic Countermeasures (ECM) threat. This situation is never stable, and even though a truly effective ECCM-hardened, totally invulnerable system could be developed (an idealistic situation which may never be completely achieved), it would only be a matter of time before the enemy would discover and decode the techniques, or perhaps overpower and evade them. Because of this unstable situation, it is difficult, and sometimes impossible, to properly evaluate the threat and forecast the effectiveness of an ECCM approach in a timely manner, or to establish a reliable long term solution to the problem. Thus, the project director's task is to ferret out enough information, sometimes from highly sensitive and not always complete or readily accessible sources, and evaluate the kinds and extent of required ECCM actions that will provide an acceptable degree of performance for the system's operational mission. Finally, the project director must follow through and ensure that the ECCM design is properly implemented in the radar system.

This handbook provides guidance for establishing an effective ECCM program throughout the life cycle of a U.S. Naval radar system. Presumably, the manager is already completely familiar with the acquisition management process and has a background primarily in management. Following the guidelines presented in the handbook will ensure that the proper emphasis is placed on securing adequate ECCM capability in the operational system.

CONTENTS

CONTENTS - (Continued)

CONTENTS - (Continued)

FIGURES

TABLES

APPENDIX

1. SCOPE

1.1 General. This handbook provides guidelines for incorporating electronic counter-countermeasures (ECCM) into United States Naval radar systems during the system acquisition process. The handbook should be useful to project or acquisition directors and other participants in the acquisition process, particularly cognizant managers in the office of the Chief of Naval Operations (CNO), the Naval Systems Commands (SYSCOM), the Naval Intelligence Center (NIC), the Naval Security Group (NSG), and personnel in the design, development and production agencies. Because of the gravity of the Soviet threat facing the fleet and the Navy's critical need for command and control in performing its various missions, managers must understand the importance of measures necessary to ensure the viability of radar systems. This is the purpose for incorporating ECCM into the design of radar systems. Without ECCM, a radar system will not be capable of fulfilling its military (combat) mission in the presence of a determined threat.

1.1.1 Multidimensional ECCM concerns. Managers need to appreciate the complex nature of the issues involved in developing ECCM-hardened radar systems. ECCM multidimensional concerns involve the issues specified in a through c:

a. Sensitive security issues that relate to potential system weaknesses (susceptibility and vulnerability) to the threat and the means to counter those weaknesses

b. Operational issues in which a variety of Naval missions and platforms must be assured of timely, reliable and adequate radar information to conform to their needs

c. Technical issues, wherein difficult challenges (for example, antijamming (AJ) and anti-electronic warfare support measures (ESM)) must be resolved within the limitations of budget, size, weight, platform, maintenance and environmental constraints.

1.1.2 Electronic Warfare (EW) threat to Naval radar systems. The urgent need for ECCM techniques in Naval radar systems continues to increase with the growing seriousness of the threat and the Navy's vital dependence upon radar information for executing its various missions. A description of the threat is presented in 1.1.2.1 through 1.1.2.6.

1.1.2.1 Threat overview. Since the early 1960s, the Soviet Navy has been transformed from a coastal defensive force to an offensive striking arm with global capabilities. The requirements for U.S. Naval forces, in large measure, have been shaped by this threat, and in particular by the need for command and control in a wartime environment.

1.1.2.2 Hostile Electronic Countermeasures (ECM) operations. The EW capabilities and tactics of the Soviet Union far overshadow the capabilities and tactics of all other Warsaw Pact nations. The EW intercept and jamming capabilities of these European communist countries are comprehensive and continue to grow in sophistication. The advances in Soviet technology from rudimentary, manually operated noise jammers to sophisticated detection and jamming equipment give the U.S. considerable cause for concern about existing U.S. Naval radar systems which need ECCM improvements, and about U.S. Naval radar systems being planned for the future. Soviet jammers are developed to the point where spectrally they are able to cover all of the frequency bands used by the various U.S. Naval radar systems. Soviet jammers are theoretically deployable on virtually every type of operational platform -- surface, subsurface, or aircraft (A/C).

1.1.2.2.1 Passive electronic surveillance systems. In a war involving the Warsaw Pact countries and the North Atlantic Treaty Organization (NATO) alliance, or between the Union of Socialist Soviet Republics (U.S.S.R) and the U.S., the initial battle may be the deciding factor, lasting only hours, with the outcome determined in the first few minutes. Threat indications and warning information are essential to both the NATO and Warsaw Pact forces. National and tactical sensor systems of both sides will be extensively involved. Passive electronic surveillance systems will be keenly attuned to the descriptors and indicators of actions which can tipoff intentions of impending attack.

1.1.2.2.2 Incorporating effective ECCM into radar systems. The Soviet Ocean Surveillance System (SOSS) has capabilities using both sensors and infrared (IR) detectors to locate and track anti-Soviet forces, possibly introducing expendable jammers to suppress radar and communications. This poses a formidable strain on the U.S. Navy to anticipate and defeat the enemy's ESM and ECM systems by incorporating effective ECCM into its radar and communications system. The increased use of powerful jamming methods on U.S. Navy radar frequencies may answer the Warsaw Pact question, Do we jam or do we listen?, and makes more certain the obvious decision to jam our Command, control, and communication (C^3) networks. Following the successful large-scale invasion of Czechoslovakia by the Soviet Union in August 1968, the Warsaw Pact forces have reportedly made considerable investment in EW with particular emphasis upon training. Soviet jamming equipments, techniques and practices are generally less sophisticated than those of the U.S., and the Soviets appear to prefer a brute-force approach like broadband noise jamming. The U.S. must assume that the Soviet Navy knows the technical capabilities, weaknesses and employment tactics of U.S. Naval radar and communications systems and that the Soviets will take full advantage of this knowledge.

1.1.2.2.3 Judicious use of ECCM. Not only is the presence of U.S. Naval radar systems of interest to a potential adversary, but the patterns or combinations of radars associated with the various platforms are also potentially important. The U.S.S.R. has land-based, airborne, satellite and shipborne electronic intercept systems, some of which have active and passive electronic detection systems to locate friendly forces, identify units and the type of operations being conducted. Admiral J.D. Watkins, USN, has written: "In this modern age where electronic deception tecniques and ECM operations have nearly the pronounced effect on Naval maritime operations of hard-kill weapons systems, the at-sea commander places EW high on his list of tactical considerations. Central to these considerations is a full understanding of ECCM and how to use its features judiciously in U.S. equipment and systems."

1.1.2.3 Command, control, communications and intelligence (C^3I). In order to appreciate the seriousness of the threat to U.S. C^3I systems, of which U.S. Naval radar systems constitute a critical part, a basic understanding of the components is required. The basic elements of the C^3I system are specified in a through d:

a. Sensor systems which gather information about an enemy
b. Navigation systems which assist U.S. forces to locate themselves
c. Command and fusion centers which integrate and display information to decision makers
d. Communication links between the elements specified in a through c

The threat to these systems is both passive and active. Soviet military literature and the pattern of Soviet military exercises stress the use of surprise in operational attack situations. Friendly task forces can probably anticipate a massive missile strike executed with a high degree of surprise. The U.S.S.R. must rely on methods to catch U.S. forces off guard and unprepared for counteroffensive opertions or in-depth defense. Consequently, the Soviet use of passive EW collection prior to hostilities and the use of jamming, deception, and so forth after initiation of a conflict is a corner-stone of Soviet warfare doctrine.

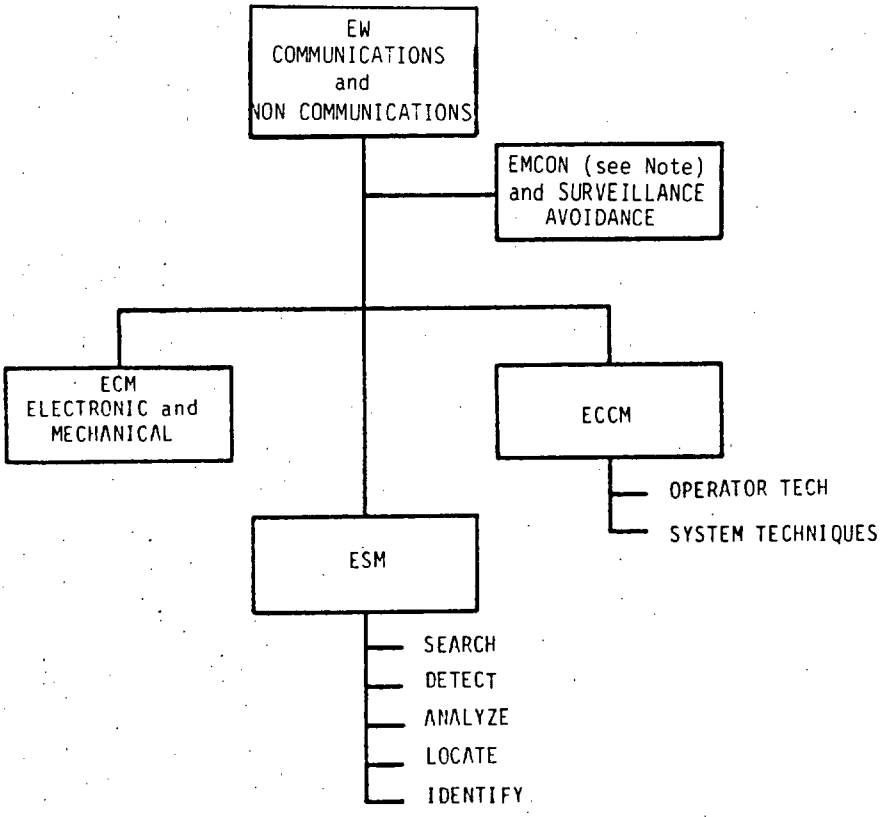
1.1.2.4 The jamming threat to U.S. Naval radars. Soviet efforts to develop a substantial radar jamming system have been well documented. Their use of ECM to inhibit the use of airborne, surface, and land-based radar capability has been demonstrated.

1.1.2.5 Threat growth. The growth of the Soviet armed forces, and in particular their Naval arm, is often expressed in numbers of ships relative to the U.S. During the decade from 1970 to 1980, the Soviet Union increased the ratio of active ships in the fleet from two to four times as many. Soviet Naval EW has also grown faster and increased in sophistication over other fleet warfare technologies. In sheer numbers of warships and the ordnance systems visible upon them, the Soviet Navy far exceeds the U.S. fleet. The numerous EW antennae seen on Soviet units indicate the high priority assigned to this mission area. This potential enemy has capitalized on technological opportunities to amass formidable capabilities in ECM. The U.S.S.R. has launched about twice as many military satellites as the U.S. and has demonstrated effective satellite use in worldwide exercises. These satellites are used for navigation, command and control, and reconnaissance. Although sophistication is lacking in these satellites, they significantly add to an imposing ocean surveillance system and a worldwide C^3 capability. These significant advances have been made partially through technology exchange with the free world and by Soviet research. General B.W. Rogers, USA, provided testimony on Capitol Hill in 1980 that the Soviet Union has the largest research and development (R&D) base in the world. Additionally, Soviet electronic equipment production capability can out-produce NATO countries,

three-to-one. In order to appreciate the overwhelming speed and the complexity of the Soviet Naval buildup, a glimpse of the new Soviet heavy cruiser Kirov may be helpful. First appearing in June 1980, this vessel, approximately the size of a small battleship, was viewed in the Baltic Sea and later in the North Sea. Larger than any American cruiser, and nuclear powered, the Kirov displays the Soviet Navy plan for larger and more versatile vessels with increasing technological sophistication and enhanced survivability. Representing one of the most heavily armed warships in the world, the Kirov exhibits a vast array of sensors and weapons for air, surface, and subsurface encounters. Relative to American ships, the Kirov quantitatively displays many more EW systems, partially because of the Soviet philosophy of using single purpose systems of simple design, and because a wider variety of EW systems have been incorporated.

1.1.2.6 Future weapons. Threats to U.S. command and control systems are not static but constantly evolving. New threats will be uncovered in the coming years. The potential enemy is expected to attempt disruption of C^3I systems by denying the Navy use of its systems, by creating an inability to react to changing situations, and by causing a reduction in U.S. ability to control weapons or other resources through jamming. The enemy's electronic weapons may be used to deceive U.S. forces into taking wrong actions, or the enemy ECM may divert attention so that friendly forces miss acquiring information that may be vital to the conduct of the operation. Today, without question, the Navy that prevents an enemy from using its command and control elements and retains its use of the electromagnetic (EM) spectrum, will win the war at sea.

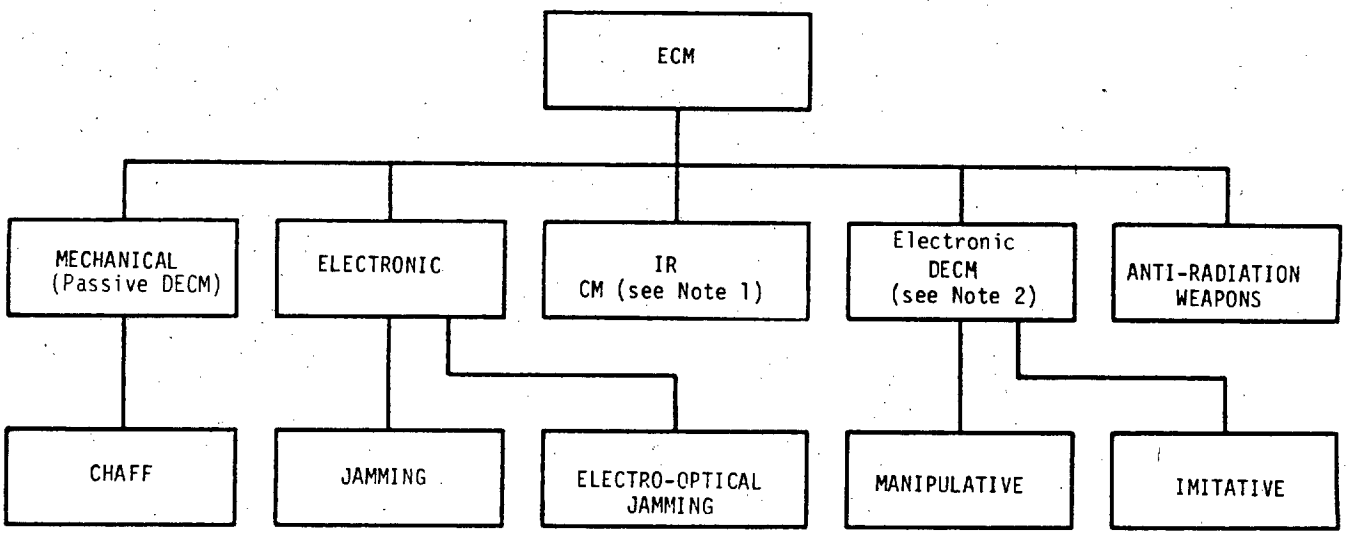
1.2 EW and radar. To fully comprehend the concept of radar ECCM, it is necessary to understand the term EW. EW is a military action involving the use of EM energy to determine, exploit, reduce or prevent hostile use of the EM spectrum, and includes activities designed to preserve advantageous use of the EM spectrum. The three main divisions within EW, as shown in FIGURE 1, are ECM, ESM and ECCM. ECM is further broken down into active and passive components. ESM involves signal intelligence (SIGINT) considerations, and ECCM is divided into system and operator techniques.



NOTE: Emission Control

FIGURE 1. Overview of the functional relationships of EW.

1.2.1 Functional aspects of ECM. ECM is that major subdivision of EW involving actions taken to prevent or reduce the effectiveness of enemy equipment and tactics employing (EM) radiation and to exploit the enemy's use of such radiations across the spectrum. FIGURE 2 represents the functional breakdown of ECM into its major components. While the deception aspects of ECM are not of concern when dealing with the effects on radar operation, these aspects have significant impact on operator interpretation and have been included in FIGURE 2 to provide the reader with a complete ECM picture. The jamming aspects of ECM are concerned with electronic and mechanical jamming or the deliberate radiation, reradiation, or reflection of EM energy to impair the use of electronic devices, equipment, or systems used by an enemy. These include narrowband interference, wideband interference and deception.



NOTES:
1. Countermeasures
2. Deception ECM

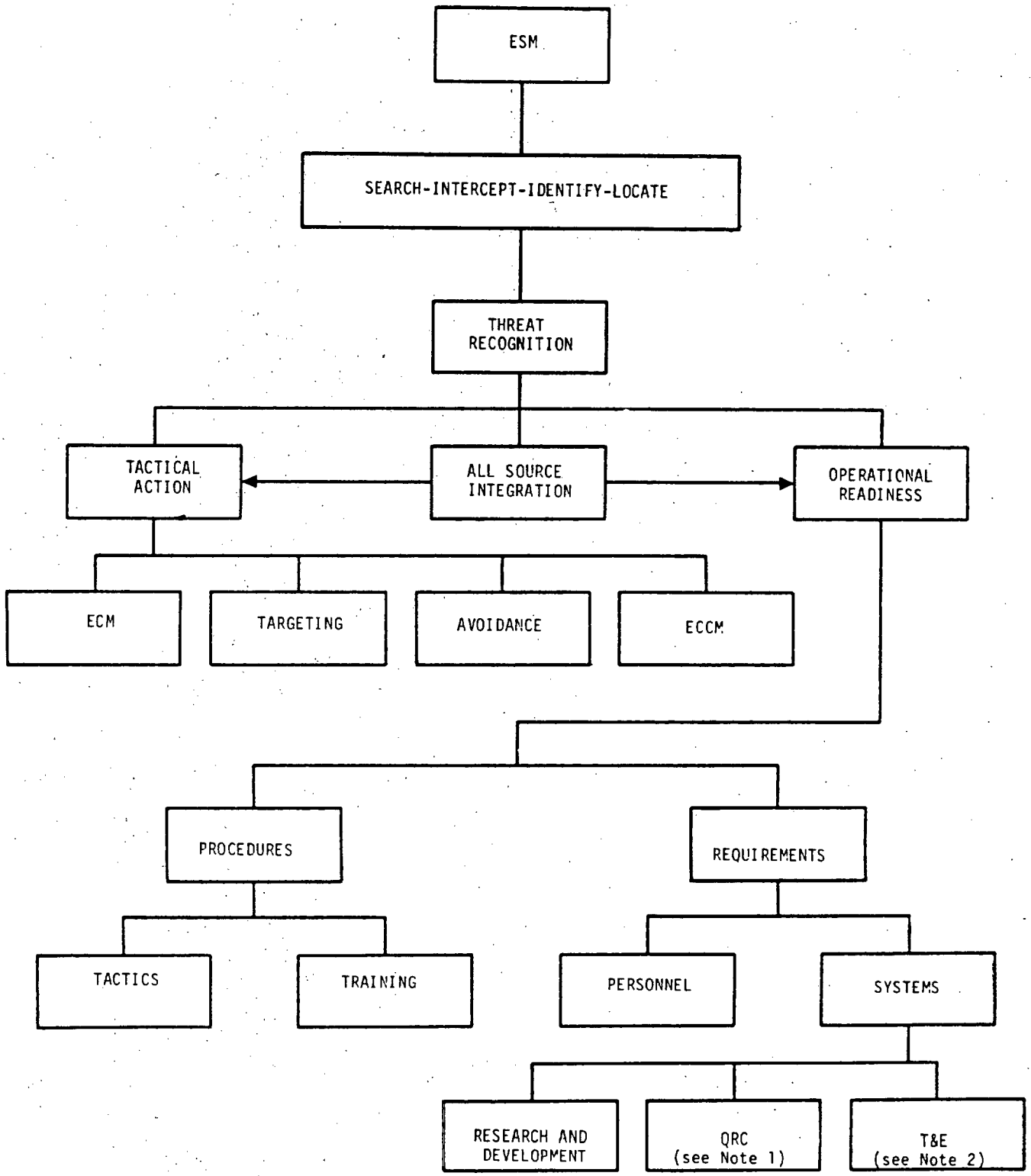
FIGURE 2. Functional aspects of ECM.

1.2.2 Functional aspects of ESM. EW support measures comprise that division of EW involving actions taken to search for, intercept, locate, record, and analyze radiated EM energy for exploiting such radiations in support of Military operations. FIGURE 3 represents the various functional components comprising ESM. ESM is also involved with SIGINT. SIGINT consists of electronic intelligence (ELINT) and communications intelligence (COMINT). Some contributions of ESM include information necessary to conduct ECM, ECCM, threat detection, warning, avoidance, target acquisition and homing.

1.2.3 Functional aspects of ECCM. ECCM is that major subdivision of EW involving actions taken to insure our effective use of EM radiations despite the enemy's use of CM. FIGURE 4 presents the two major divisions of ECCM. This handbook concentrates its efforts on the ECCM arena of EW.

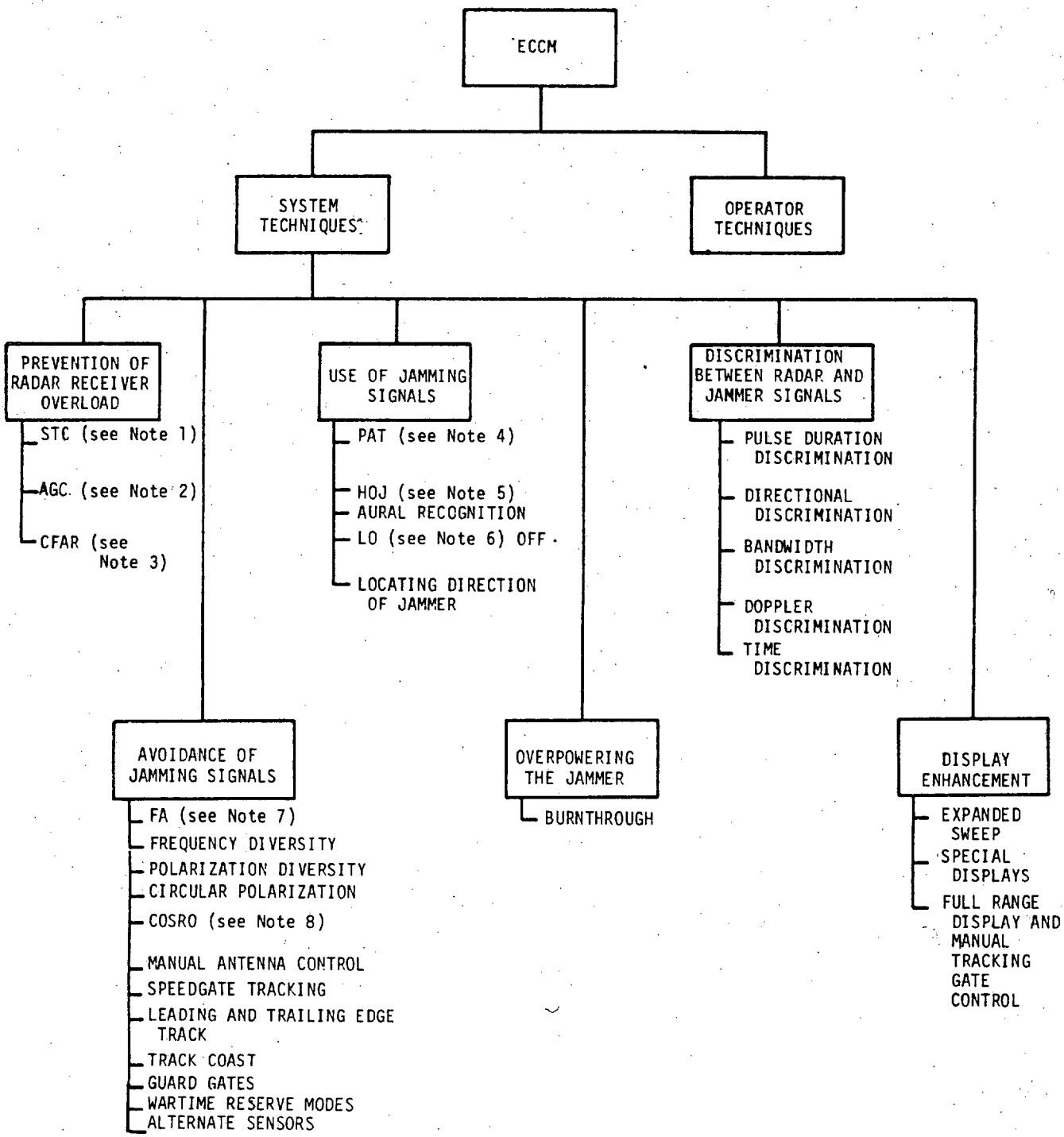
1.3 Applicability. Provisions of this handbook shall be applied by procuring activities and by development and operations activities at appropriate times during the acquisition process. The handbook may also be applied by contractors as a guide for establishing and implementing an ECCM program during the contract phase. Although this handbook is intended for use in the acquisition of U.S. Naval radar systems, it can apply with equal satisfaction in the acquisition of other electronic systems. The handbook should therefore be useful to any other participant in the acquisition process, particularly those in Naval Operations (OPNAV), the Systems Commands (SYSCOM), NIC, and NSG.

1.4 Format. To assure early consideration of ECCM and to provide the continuity for achieving and monitoring the required ECCM, the guide follows the framework of the acquisition process for the system. Section 4 describes the overall acquisition process. Section 5 describes considerations and actions that should be taken by the manager to implement ECCM into radar system design. Together, these actions describe the acquisition process and the responsibilities of the manager for ensuring that his system has a high probability of continued operation in the predicted EW environment.



NOTES:
1. Quick reaction capability
2. Test and evaluation

FIGURE 3. Functional aspects of ESM.



NOTES:
1. Sensitivity time control
2. Automatic gain control
3. Constant false alarm rate
4. Passive angle tracking
5. Home on jamming
6. Local oscillator
7. Frequency agility
8. Control scan on receive only

FIGURE 4. Functional aspects of ECCM.

2. REFERENCED DOCUMENTS

2.1 Government documents.

2.1.1 Government publications. The following Government publications form a part of this handbook to the extent specified herein.

PUBLICATIONS

MILITARY

DEPARTMENT OF DEFENSE (DoD)

DoDDIRC4600.3	Electronic Counter-Countermeasures (ECCM) Policy
DoDINST 5000.2	Major System Acquisition Procedures

JOINT CHIEFS OF STAFF (JCS)

JCS Pub 1	Dictionary Of Military And Associated Terms

SECRETARY OF THE NAVY (SECNAV)

SECNAVINST C3430.2	Department Of The Navy Policy Concerning Electronic Counter-Countermeasures (ECCM) In Electronic Systems

CHIEF OF NAVAL OPERATIONS (OPNAV)

OPNAVINST C3430.4D	Electronic Warfare Policy
OPNAVINST 3811.1A	Threat Support To Weapon Systems Selection And Planning
OPNAVINST 5000.42C	Weapon System Selection And Planning

NAVAL MATERIAL COMMAND (NAVMAT)

NAVMATINST 3882.2A	Threat Support For RDT&E And Weapon System Selection And Planning

(Copies of publications required by contractors in connection with specific acquisition functions should be obtained from the contracting activity or as directed by the contracting officer).

2.2 Other publications. The following documents form a part of this handbook to the extent specified herein. Unless otherwise specified, the issues of the documents which are DoD adopted shall be those listed in the issue of the DoDISS specified in the solicitation. The issues of documents which have not been adopted shall be those in effect on the date of the cited DoDISS.

Radar System Analysis, David K. Barton, Artech House, 1976.
Second International Countermeasures Handbook, S.L. Johnston, EW Communications, Inc., 1976.
Radar Anti-Jamming Techniques, M. V. Maksimov, et al., Artech House, 1979.
Radar Design Principles, Fred E. Nathanson, McGraw Hill, 1969.
Applied ECM Vol. I II, Van Brunt, EW Engineering, Inc., 1978, 1982.

3. DEFINITIONS

3.1 Definitions of electronic terms by complete word. The frequently used EW terms specified in 3.1.1 through 3.1.362 are, in the main, extracted from the Second International Countermeasures Handbook, June 1976.

3.1.1 Accidental jamming. Accidental jamming is interference due to transmission by friendly equipment.

3.1.2 Automatic cancellation of extended targets (ACET).

3.1.3 Acoustic jamming. The deliberate radiation or reradiation of mechanical or electro-acoustic signals with the objectives of obliterating or obscuring signals which the enemy is attempting to receive and of deterring enemy weapons systems.

3.1.4 Acquisition. A mode of operation in which a fire control radar detects a target in a designated volume of space and defines target range and angle data prior to lock-on and coordinates tracking of the target.

3.1.5 Active ECM. The impairment of enemy electronic detection, control or communications devices and systems through deliberate jamming or deception.

3.1.6 Active jamming. Intentional radiation or reradiation of EM waves with the object of impairing the use of a specific portion of the EM wave spectrum.

3.1.7 Aided tracking. A system of tracking a signal in azimuth, elevation, or range, in which a constant rate of motion of the tracking mechanism is maintained by mechanical means so that an equivalent constant rate of motion of the target can be followed.

3.1.8 Amplitude modulation-carrier wave (AM-CW) jamming. Jamming in which a carrier wave is amplitude modulated at a recurring rate. The recurrence rate of amplitude modulation (AM) is variable and causes a noticeable change in the radar scope. Because of the spiraling or chaining effect produced, AM-CW jamming is easily identified.

3.1.9 Angel.

a. Radar returns which are not desired in a particular situation and which are caused by atmospheric inhomogeneities, refractive index discontinuities, insects, birds, or unknown phenomena. Originally when some physical target could not be identified through direct visual observation, all echoes from such unknown causes were designated as angels.

b. A type of confusion reflector often having the reflecting material suspended from parachutes or balloons to give delayed descent.

3.1.10 Angle jamming. ECM technique, when azimuth and elevation information from a scanning fire control radar is jammed by transmitting a jamming pulse similar to the radar pulse but with modulation information out of phase with the returning target angle modulation information. See inverse gain.

3.1.11 Angle noise (in radar). The noise-like variation in the apparent angle of arrival of a signal received from a target, caused by changes in phase and amplitude of target scattering sources and including angular components of both glint and scintillation error.

3.1.12 Antenna crosstalk. A measure of undesired power transfer through space from one antenna to another. Ratio of power received by one antenna to power transmitted by the other, usually expressed in decibels (dB).

3.1.13 Anti-clutter circuits (in radar). Circuits which attenuate undesired reflections to permit detection of targets otherwise obscured by such reflections.

3.1.14 Anti-jam (AJ). The technique of minimizing the effect of enemy electronic jamming to permit echoes from targets detected by radar to be visible on the indicator.

3.1.15 Anti-radiation missile (ARM). A missile that homes passively on a radiation source.

3.1.16 Artificial echo.

a. Received reflections of a transmitted pulse from an artificial target, such as an echo box, corner reflector, other metallic reflecting surface.

b. Delayed signal from a radio pulsed frequency signal generator.

3.1.17 A-scope. A radar display in which a constant intensity electron beam is swept from left to right across the display to produce a range scale. Received echoes cause a vertical deflection of this beam. The horizontal distance between the start of the sweep and the target echo represents the target range.

3.1.18 Asynchronous pulsed jamming. This is the most effective form of pulsed jamming. The jammer nearly matches the pulse repetition frequency (PRF) of the radar; then it transmits multiples of the PRF. It is more effective if the jammer pulsewidth (PW) is greater than that of the radar. Asynchronous pulsed jamming is similar to synchronous jamming except that the target lines tend to curve inward or outward slightly and appear fuzzy in the jammed sector.

3.1.19 Automatic back bias. A technique which consists of one or more automatic gain control (AGC) loops to prevent overloading of a receiver by large signals, whether jamming or actual radar echoes.

3.1.20 Automatic gain control (AGC).

a. A feature involving special circuitry designed to maintain the output of a radio, radar, or television receiver essentially constant, or to prevent its exceeding certain limits, regardless of variations in the strength of the incoming signal. In a radio receiver, in particular, though something of a misnomer, sometimes also known as automatic volume control.

b. A self-acting compensating device which maintains the output of a transmission system constant with narrow limits, even in the face of wide variations in the attenuation of the system.

c. A radar circuit which prevents saturation of the radar receiver by long blocks of received signals, or by a carrier modulated at low frequency.

3.1.21 Automatic noise leveling (ANL). When heavy jamming is present, the ANL control sets the receiver gain (noise level) to a lower level. It will usually cause targets in the jammed sector to fade as the jammer closes in range. This control should be used only in the jammed sector or with a jamming strobe.

3.1.22 Automatic scanning receivers. Receivers which can automatically and continuously sweep across a preselected frequency either to stop when a signal is found or to plot signal occupancy within the frequency spectrum being swept.

3.1.23 Automatic search jamming. An intercept receiver and jamming transmitting system that automatically searches for and jams enemy signals of specific radiation characteristics.

3.1.24 Automatic threshold variation. This constant false alarm rate (CFAR) technique is an open loop-type AGC in which the decision threshold is varied continuously in proportion to the incoming intermediate frequency (IF) and video noise level. When properly instrumented, this technique is reasonably successful in removing effects of antenna scanning modulation.

3.1.25 Automatic tracking. Tracking in which a system employs some mechanism, for example, servo, or computer to automatically follow some characteristic of the signal.

3.1.26 Automatic video noise leveling (AVNL). In this CFAR technique, the video noise level at the receiver output is sampled at the end of each range sweep and the receiver gain is readjusted to maintain a constant video noise level at the output. Under some jamming conditions, a fixed video noise can be maintained at the display.

3.1.27 Azimuth blanking. Blanking of the radar receiver as the scan traverses a selected azimuth region.

3.1.28 Azimuth gain reduction. A technique which allows control of the radar receiver system throughout any two azimuth sectors.

3.1.29 Azimuth versus amplitude. ECCM receiver with plan position indicator (PPI) type display attached to the main antenna used to display strobes due to jamming A/C. Azimuth versus amplitude is useful in making passive fixes when two or more radar sites can operate together.

3.1.30 Babble signal. A type of electronic deception signal used to confuse enemy receivers. Generally, it has characteristics of enemy transmission signals. Babble signal can be composed by super imposing incoming signals on previously recorded intercepted signals. This composite signal can then be radiated as a jamming signal.

3.1.31 Back bias.

a. A degenerative or regenerative voltage which is fed back to circuits before its originating point. Back bias is usually applied to a control anode of a tube.
b. A voltage applied to a grid of a tube (or to the grids of tubes) to restore a condition which has been upset by some external cause.
c. See Instantaneous Automatic Gain Control (IAGC).

3.1.32 Balloon reflector. In EW, a balloon-supported confusion reflector used to produce fraudulent echoes.

3.1.33 Barrage jamming. Simultaneous electronic jamming over a broad range of frequencies. See Jamming.

3.1.34 Baseline break. A technique in radar which uses the characteristic break in the baseline on an A-scope display due to a pulse signal of significant strength in noise jamming.

3.1.35 Beacon stealing. A loss of beacon tracking by one radar due to interfering interrogation signals from another radar.

3.1.36 Beam-to-beam correlation (BBC). BBC is used by frequency scan radars to reject pulse jamming and jamming at a swept frequency. Correlation is made from two adjacent beams. The receiver rejects targets (signals) that do not occur at the same place in two adjacent beams.

3.1.37 Big photo. An unclassified general call sign for A/C engaged in active ECM.

3.1.38 Bird nesting. Clumping together of chaff dipoles after they have been dispensed from an A/C.

3.1.39 Bistatic operation. The use of radar equipment having antennas at different locations for transmission and receiving to detect the same target. Bistatic operation provides the capability of discriminating against decoys and repeater jammers.

3.1.40 Bistatic radar. A radar using antennas at different locations for transmission and reception.

3.1.41 Black chaff. Chaff that absorbs the radar energy incident on it, thereby masking targets behind the chaff.

3.1.42 Blanketing. Action of a powerful radio signal or interference rendering a receiving set unable to receive desired signals.

3.1.43 Blind speed. Those relative target velocities which result in zero moving target indicator (MTI) response. They are present in pulse radar, but not continuous wave (CW) radar because Doppler is measured by discrete samples at the PRF rather than continuously.

3.1.44 Blinking. ECM technique employed by two A/C separated by a short distance and within the same azimuth resolution so as to appear as one target to a tracking radar. The two A/C alternately spot jam, causing the radar system to oscillate from one plane to another, making an accurate solution of fire control problem impossible. A method of providing information by modifying the signal at its source so that the signal presentation on the display at the receiver alternately appears and disappears; for example, in loran, blinking is used to indicate that a station is malfunctioning.

3.1.45 Blocking. The process of obscuring guidance signals by active jamming.

3.1.46 Break lock. The moment at which an automatic tracking system has lost contact with the target or the process of causing loss of tracking.

3.1.47 Broad pulse jamming. Transmission of broad pulses for control system jamming when little is known about the command pulse group. For example, a broad pulse might cover a whole group of command pulses, thus jamming that command.

3.1.48 Burnthrough range. The maximum distance at which a specific radar can discern targets through the external interference being received. (The interference is normally associated with jamming.)

3.1.49 Buzzer. An unclassified brevity code word signifying a type of jamming.

3.1.50 Camouflage factor. The ratio of the root-mean-square (rms) noise power to the peak signal power required to provide effective jamming. The ratio of rms noise power to peak signal power where the rms noise power is determined on the basis of the bandwidth of the receiver up to the second detector.

3.1.51 Capture. Where the jammer takes control over the guidance signal by active jamming.

3.1.52 Capture of AGC. Domination of the radar receiver AGC level by strong transmitted jamming or deception signals. This tends to remove weak targets from the radar display and tracking channels.

3.1.53 Capture effect. The tendency of a receiver to suppress the weaker of two signals within its band pass.

3.1.54 Chaff. An ECM consisting of many reflective dipoles which reflect radar energy back to the radar.

3.1.55 Chaff bursts. A series of short chaff corridors or individual chaff presentations with clear areas between them. The primary purpose is to dilute or confuse targeting.

3.1.56 Chaff corridors. Long, continuous cloud of chaff formed by dispensing chaff so that the returns overlap on the radar display.

3.1.57 Chirp. A pulse compression technique characterized by linear frequency modulation on pulse (LFMOP).

3.1.58 Chirp mode. The chirp mode enables the operator to transmit the outgoing pulse in steps of increasing or decreasing frequency. This feature is similar to frequency agility (FA) except that each pulse is broken into smaller sections which are transmitted at separate frequencies. The radar system compiles these smaller sections back into the original pulse before being sent to the receiver, thus providing a coding that is difficult for the jammer to match.

3.1.59 Chirp radar. Radar in which a swept-frequency signal is transmitted, received from a target, and then compressed in time to give a final narrow pulse called the chirp signal. It has high immunity to jamming and an inherent rejection of random noise signals.

3.1.60 Circularly polarized jamming. The techniques of radiating jamming energy in both planes of polarization simultaneously. With this method there is a loss of 3 dB of effective power in either plane, but the enemy using linearly polarized antennas cannot cross-polarize his antenna to escape jamming. More complex analysis will be required if circularly polarized antennas are used.

3.1.61 Clipped noise modulation. A clipping action is performed to increase the bandwidth of the jamming signal. This results in more energy in the sidebands, correspondingly less energy in the carrier, and an increase in the ratio of average power to peak power.

3.1.62 Clutter elimination. The clutter eliminator circuit discriminates against any target echo that exceeds three times the transmitted PW and will not display them on the indicator. It is normally employed on the lower beams of a high frequency radar. This will allow targets above a preset signal strength to be presented, while the clutter (land) will be eliminated.

3.1.63 Clutter gating. This technique provides switching between MTI and normal videos. This technique results in the normal video being displayed in regions with no clutter and the MTI video being switched in only for the clutter areas. Clutter gating is achieved automatically by the PW discrimination or the use of storage tubes. Clutter also can be achieved by a manually operated range azimuth gate. The clutter gate vastly increases the effectiveness of noncoherent MTI against chaff.

3.1.64 Coast. A radar memory feature that causes the range or angle systems to continue to move in the same direction and at the same speed that an original target was moving; used to prevent lock-on to a stronger target near the target being tracked.

3.1.65 Coded pulse anti-clutter (CPAC). A form of pulse expansion - compression in which a long transmitted pulse is made up of phase-coded segments and the received echo is compressed into a short signal by decoding and summing the segments.

3.1.66 Coherent MTI (in radar MTI). A system in which the target echo is selected on the basis of its Doppler frequency when compared to a local reference frequency maintained by a coherent oscillator.

3.1.67 Coherent repeater jammer. A jammer that uses the phase information of the received radar signal in creating false targets.

3.1.68 Coherent sidelobe cancellation (CSLC). An ECCM technique to use the jamming signal from an auxillary antenna or array of auxiliary antennas to cancel the jamming signal received by the main radar antenna.

3.1.69 Coherent video. Bipolar video obtained from a synchronous (coherent) detector. See Coherent MTI.

3.1.70 Coherent video mode. In the coincidental video (CV) mode, the radar transmits and receives twice. The receiver samples the returning echoes and only those that coincide in time will be presented to the indicator.

3.1.71 Communications CM. ECM used specifically against communications.

3.1.72 Communications deception. Use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system.

3.1.73 Communications jamming. The part of electronic jamming used against a medium that employs EM radiation to convey information from one person or headquarters to another.

3.1.74 Communications security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. COMSEC includes:

a. Cryptosecurity. The component of COMSEC which results from the provision of technically sound crytosystems and their proper use.
b. Transmission security. The component of COMSEC which results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis.
c. Emission security. The component of COMSEC which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems.
d. Physical security. The component of COMSEC which results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof.

3.1.75 Confusion reflector. Reflector of EM radiation used to create echoes for confusion against radar, guided missiles, and proximity fuses. See Chaff.

3.1.76 Conical scanning. A technique to derive target angular information, using a narrow beam antenna feed that is rotated to describe a cone in space. When the received target echo signal is constant (that is, no amplitude modulation at the scan frequency), during the scan period, the target is along the cone centerline and the target angle error is zero.

3.1.77 Conical scan on receive only (COSRO). A radar feature which, instead of physically scanning the antenna beam of the transmitter to derive target angle information, processes (or scans) the received signal to derive angle data. This technique has the advantage of not revealing to an enemy the antenna scan frequency which would be useful for angle deception.

3.1.78 Conopulse. This radar angle-tracking technique uses dual antenna beams, two receiver channels, and combination monopulse - conical-scan tracking intervals. This technique's main advantage is its independence from target cross-section fluctuations and from target self-screening jamming amplitude variations.

3.1.79 Constant false alarm rate (CFAR). A radar receiver with automatic detection circuits designed to produce a constant number of erroneous target detections independent of noise level at the receiver input. CFAR techniques are intended primarily to prevent receiver saturation and overload, and to present clean video information to the display and a constant noise level to an automatic detector. A device that accomplishes these objectives may respond to the signal-to-noise ratio (S/N) rather than the absolute signal level above a fixed threshold. CFAR does not usually permit the detection of a target if the target is weaker than the jamming, but it attempts to remove the confusing effects of the jamming.

3.1.80 Continuous wave (CW) jamming. The transmission of constant-amplitude, constant-frequency, unmodulated jamming signals to change the S/N of a radar receiver.

3.1.81 Correlation detection (modulation system). Detection based on the averaged product of the received signal and a locally generated function possessing some known characteristics of the transmitted wave. The averaged product can be formed, for example, by multiplying and integrating or by the use of a matched filter whose impulse response, when reversed in time, is the locally generated function. Strictly, this definition applies to detection based on cross correlation. The term correlation detection may also apply to detection involving autocorrelation, in which case the locally generated function is merely a delayed form of the received signal.

3.1.82 Correlation direction finder. A satellite station separated from a radar to receive jamming signals. By correlating the signals received from several such stations, range and azimuth of many jammers may be obtained.

3.1.83 Configuration management (CM). That form of military science which by the employment of devices or techniques, or both, has as its objective the impairment of the operational effectiveness of enemy activity. See also ECM.

3.1.84 Criss-cross. The name given to that pattern produced on an A-scope by CW modulated with a medium frequency signal. Criss-cross appears as diagonal lines in two directions above the baseline.

3.1.85 Cross-eye jamming. A jamming technique, used against monopulse systems, that distorts the phase front of echo signal as seen by the tracking radar.

3.1.86 Cross-gated CFAR. This CFAR technique is employed to achieve the fast switching required for an optimum combination of normal and MTI modes. In this case, the MTI video signals are used to gate on the normal video when the MTI indicates a target in clutter. CFAR action is achieved by the wideband as in the zero-crossing and DICKE FIX CFARs.

3.1.87 Cross modulation. A type of intermodulation due to modulation of the carrier of the desired signal by an undesired signal wave.

3.1.88 Crossover range. The range at which the received target echo signal power equals the received jamming power on a single received pulse.

3.1.89 Crystal-video receiver. A broadband receiver consisting of a crystal detector, followed by a high gain video amplifier. Selectivity is determined only by the antenna as there are no tuned circuits.

3.1.90 Dead time. An interval following response to one signal or event during which a system is unable to respond to another.

3.1.91 Deceiver. An ECM equipment which attempts to deceive or mislead a radar by emitting a pulse-like signal similar to the radar signal.

3.1.92 Deception. Measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests (see Electronic deception, Imitative deception, or Manipulative deception).

3.1.93 Deception controlled devices. The technique of deliberately radiating or reradiating EM transmissions to generate false control data within an enemy-controlled device.

3.1.94 Deception device. A device that works to deceive an enemy by transmitting signals with false or erroneous information components.

3.1.95 Decoy. A device or devices used to divert or mislead enemy systems.

3.1.96 Delayed opening chaff. Chaff which blooms at a specific elapsed time after it is dispensed.

3.1.97 Detector back bias (DBB). This technique performs much the same function as IAGC, except that it operates at the diode detector instead of the IF amplifier.

3.1.98 Detector balanced bias. Controlling circuit used in radar systems for anti-clutter purposes.

3.1.99 DICKE FIX. The DICKE FIX is a technique that is specifically designed to protect the receiver from fast sweep jamming of the carcinotron type. The basic configuration consists of a broadband limiting IF amplifier, followed by an IF amplifier of optimum bandwidth. The limit level is preset at approximately the peak amplitude of receiver noise, the bandwidth may vary from 10 megahertz (MHz) to 20 MHz, depending on the jamming environment. This device provides excellent discrimination against fast sweep jamming (10 MHz to 500 MHz), usually something on the order of 20 dB to 40 dB, without appreciable loss in sensitivity. However, strong CW jamming will seriously degrade the performance of the DICKE FIX because the CW signal captures the radar signal in the limiter. This is also known as a Lamb suppressor.

3.1.100 DICKE FIX CFAR. DICKE FIX with CFAR.

3.1.101 DICKE FIX moving target indicator (MTI) CFAR. This is an MTI CFAR technique, similar to DICKE FIX CFAR. Limiting and narrowbanding follow wideband amplification, phase detection, and cancellation, so as not to impair the MTI performance.

3.1.102 Diplex. Two transmitters operating alternately on approximately the same radio frequency (RF) and using a common antenna. The normal procedure is to pulse each transmitter at one-half of the desired PRF, 180 degrees out-of-phase. The advantage is that higher peak power per transmitter is possible because each transmitter is operating at one-half the normal duty cycle.

3.1.103 Diplex operation. Simultaneous transmission or reception of two signals using a specified common feature, such as a single antenna or a single carrier.

3.1.104 Direct noise amplification (DINA). DINA, without a carrier frequency, is used to increase (saturate) the radar receiver's noise level. The biggest danger from this type of jamming is that the radar operator may not realize he is being jammed when the AGC or the ANL are employed. This is a barrage type of jamming with a bandwidth normally in excess of 50 MHz. DINA appears as a black wedge when the radar is operated with AGC or ANL. DINA appears as bright, high intensity wedges when the manual gain is employed.

3.1.105 Down-link jamming (DLJ). Some command guidance missiles carry a beacon (down-link) which is used by the parent radar to track the missile. If this beacon reply can be hidden from the parent tracking radar, the missile guidance solution can be defeated. Hence, down-link (beacon) jamming is intended to screen the missile beacon signal from the parent radar's view.

3.1.106 Dummy load. A dissipative, but essentially nonradiating, substitute device having impedance characteristics simulating those of the substituted device.

3.1.107 Duplex. In radar, a condition of operation when two identical and interchangeable equipments are provided: One in an active state and the other immediately available for operation.

3.1.108 Duplication jamming. See Imitative jamming.

3.1.109 Dynamic range.

a. The difference, in dB, between the overload level and the minimum acceptable signal level in a system or transducer. The minimum acceptable signal level of a system or transducer is ordinarily fixed by one or more of the following: noise level, low-level distortion, interference, or resolution level.

b. Ratio of the specified maximum signal level capability of a system or component to its noise or resolution level, usually expressed in dB.

c. Figure of merit in ECCM receiver system.

3.1.110 Echo intensifier. A device, located at the target, that is used to abnormally increase the amplitude of the reflected energy.

3.1.111 Effective confusion area. The amount of chaff whose radar cross section (RCS) area equals the RCS area of the protected target at a particular frequency.

3.1.112 Electromagnetic compatibility (EMC). The capability of electronic equipment and systems to operate in the intended environment at designated levels of efficiency without degradation due to unintentional interference, usually caused by other emitters.

3.1.113 Electromagnetic (EM) cover and deception. The suppression, control, alteration, or simulation of EM radiations associated with friendly systems, equipment, devices or weapons components to deny any enemy a source of knowledge of the location of combat elements or mislead him as to their location, capabilities and intentions. EM cover and deception tactics include deceptive emission control (EMCON) signal suppression, profile alteration, and electronic deception.

3.1.114 Electromagnetic interference (EMI). Impairment of the reception of a wanted EM signal caused by an EM disturbance.

3.1.115 Electromagnetic (EM) intrusion. The intentional insertion of EM energy into transmission paths in any manner with the objective of deceiving operators or of causing confusion.

3.1.116 Electromagnetic (EM) reconnaissance. See Electronic reconnaissance.

3.1.117 Electromagnetic (EM) test environment. A range complex of radars such as that at Eglin Air Force base, Florida, operating in different frequency bands and modes to provide a very flexible facility for evaluating A/C antenna patterns, reflectivity measurements, IR reconnaissance, airborne interceptors, and EM warfare devices and techniques.

3.1.118 Electronic confusion area. Amount of space that a target appears to occupy in a radar resolution cell, as it appears to that radar beam.

3.1.119 Electronic counter-countermeasures (ECCM). That division of EW involving actions taken to ensure friendly effective use of the EM spectrum despite the enemy's use of EW.

3.1.120 Electronic counter-countermeasures (ECCM) improvement factor. The power ratio of the ECM signal level required to jam a radar with ECCM techniques in use to the power required to jam the same radar without the ECCM techniques.

3.1.121 Electronic countermeasures (ECM). That division of EW involving actions taken to prevent or reduce an enemy's effective use of the EM spectrum.

3.1.122 Electronic deception. The deliberate radiation, reradiation, alteration, absorption, or reflection of EM radiations in a manner intended to mislead an enemy in the interpretation of or use of, information received by his electronic systems. There are two categories of electronic deception:

a. Manipulative deception. The alteration or simulation of friendly EM radiations to accomplish deception.

b. Imitative deception. The introduction of radiations into enemy channels which imitate his own emissions.

3.1.123 Electronic defense evaluation. A mutal evaluation of radar(s) and A/C with the A/C trying to penetrate the radar's area of coverage in an ECM environment.

3.1.124 Electronic intelligence (ELINT). The intelligence information product of activities engaged in the collection and processing, for subsequent intelligence purposes, of foreign, noncommunications, and EM radiations emanating from other than nuclear detonations or radioactive sources.

3.1.125 Electronic intelligence (ELINT) parameter limits list (EPL). A compilation of identified signals which have been assigned ELINT notations.

3.1.126 Electronic interference. Any electrical or EM disturbance that causes undesirable response in electronic equipment. Electrical interferences refer specifically to interference caused by the operation of electrical apparatus that is not designed to radiate EM energy.

3.1.127 Electronic jammers.

a. Expendable jammer - A transmitter designed for special use jamming which can be expended from ships or A/C.

b. Repeater jammer - A receiver-transmitter device which, when triggered by enemy radar impulses, returns synchronized false signals to the enemy equipment.

c. Independent jammer - A transmitting device designed for jamming independent of the EM environment.

3.1.128 Electronic jamming. The deliberate radiation, reradiation, or reflection of EM energy with the object of impairing the use of electronic devices, equipment, or systems being used by the enemy.

3.1.129 Electronic order of battle (EOB). A listing of all the electronic radiating equipment of a military force giving location, type, function, types of units to which assigned, and so forth.

3.1.130 Electronic reconnaissance (EL Recon). The detection, identification, evaluation, and location of foreign EM radiations emanating from other than nuclear detonations or radioactive sources.

3.1.131 Electronic security (ELSEC). The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from their interception and study of friendly noncommunications EM radiations: for example, radar. A component signal security (SIGSEC).

3.1.132 Electronic tuning.

a. Altering the frequency of a reflex klystron oscillator by changing the repeller voltage.

b. Frequency changing in a transmitter or receiver by changing a control voltage, rather than circuit components.

3.1.133 Electronic warfare (EW). Military action involving the use of EM energy to determine, exploit, reduce, or prevent hostile use of the spectrum, and action which retains friendly use of the EM spectrum. There are three divisions within EW: ESM, ECM and ECCM.

3.1.134 Electronic warfare (EW) intelligence. EW intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information concerning foreign nations or areas of operation which are significant to EW.

3.1.135 Electronic warfare support measures (ESM). That division of EW involving actions taken to search for, intercept, locate, and identify radiated EM energy for immediate threat recognition. Thus, EW support measures provide a source of information required for immediate action involving ECM, ECCM, avoidance, targeting, and other tactical employment of forces.

3.1.136 Electro-optic counter-countermeasures (EOCCM). Actions taken to ensure the effective friendly use of the electro-optic spectrum despite the enemy's use of CM in that spectrum.

3.1.137 Elevation versus integrated log (EVIL). This technique provides a capability for obtaining an elevation angle report on target A/C that are jamming with sufficient intensity to deny range or height information to the active radar. With the addition of EVIL, a total passive-only air defense capability is available if the amount of jamming still exceeds that required to effectively deny active data to the air defense system.

3.1.138 Emission control (EMCON).

a. The management of EM radiations to counter an enemy's capability to detect, identify, or locate friendly emitters for exploitation by hostile action.

b. Controlling the radiation of an active system, such as a radar, so that it emits RF energy only when absolutely necessary to perform its mission.

3.1.139 Emission control (EMCON) orders. Orders used to authorize, control, or prohibit the use of electronic emissions.

3.1.140 Emission security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from other than cryptographic equipment and telecommunications systems.

3.1.141 Essential elements of information (EEI). The critical items of information regarding the enemy and his environment needed by the commander by a particular time to relate with other available information and intelligence to assist him in reaching a logical decision.

3.1.142 Extraneous emission. Any undesired emission of a transmitter or transponder, other than the output fundamental, plus only those sidebands intentionally employed for the transmission of intelligence.

3.1.143 Extraneous response. Any undesired response of a receiver, recorder, or other susceptible device, due to the desired signals, undesired signals, or any combination or interaction among them.

3.1.144 False alarm. An erroneous radar target detection decision caused by noise or other interfering signals exceeding the detection threshold.

3.1.145 False-alarm number. The average number of possible detection decisions during the false alarm time.

3.1.146 False-alarm probability. The probability that noise or other interfering signals will erroneously cause a target detection decision.

3.1.147 False-alarm time. The average time between false alarms, that is, the average time between crossings of the target decision threshold by signals not representing targets. In the early work of Marcum, it is the time in which the probability of one or more false alarms is one-half, but the usage is deprecated.

3.1.148 False echo device. A device that produces an echo different in character or time from that normally observed.

3.1.149 False target generator (FTG). A DECM device that presents false targets to a radar.

3.1.150 Fast automatic gain control (FAGC). This is an AGC scheme characterized by a response time that is long with respect to a pulsewidth and short with respect to the target. An ultrafast FAGC will reduce the CW capture effect on the DICKE FIX.

3.1.151 Fast-time constant (FTC) (in radar).

a. A circuit with short time-constant used to emphasize signals of short duration to produce discrimination against extended clutter, long-pulse jamming, or noise.

b. A resistance-capacitance differentiating network with a time constant about equal to the transmitted PW and employed in the video portion of the receiver to provide discrimination against jamming with low modulating frequencies. FTC is effective against CW, long jamming pulses, swept jamming, and clutter. It is also fairly effective against chaff corridors. Based on time, the radar receiver will allow only pulses equal to its own PW to pass and be presented on the indicators as targets. Because of this, only the leading edges of long pulses will be displayed.

3.1.152 Fence.

a. Line or network of early warning radars.

b. Concentric steel fence erected around a ground radar transmitting antenna to serve as an artificial horizon and to suppress ground clutter that would otherwise drown out weak signals returning at a low angle from the target.

3.1.153 Ferret. An A/C, ship or vehicle especially equipped for the detection, location, recording, and analyzing of EM radiations.

3.1.154 Frequency agility (FA). This term refers to a radar's ability to change frequency within its operating band. Pulse-to-pulse frequency shift, or changing the transmitter frequency radically during every interpulse, is the ultimate in FA.

3.1.155 Frequency azimuth intensity. Type of radar display in which frequency, azimuth, and strobe intensity are correlated.

3.1.156 Frequency diversity. Method of transmission or reception, or both, using a number of frequencies simultaneously to minimize the effects of selective fading, deliberate jamming, or interference.

3.1.157 Frequency modulation (FM)-by-noise modulation. A method of FM with the use of random noise. Considered a highly effective jamming method against AM and fixed-tuned FM receivers. Not very effective against continuously tunable FM receivers; careful tuning can defeat a great portion of the jamming signal. For this reason, FM-by-noise is not considered optimum as a type of modulation for the jamming of FM receivers.

3.1.158 Frequency modulation (FM)-CW jamming. This is a highly efficient jammer that utilizes two variants in producing a jamming signal. First, the FM rate is variable; and second, the jamming signal is swept in frequency through, and usually beyond, the radar's bandpass (also variable). FM-CW jamming appears on a radar screen as shifting noise spokes.

3.1.159 Frequency modulation (FM) jamming. Technique consisting of a constant amplitude RF signal that is varied in frequency about a center frequency to produce a signal over a band of frequencies.

3.1.160 Frequency time intensity. Type of radar display in which frequency, time, and strobe intensity are correlated.

3.1.161 Fruit. In a radar beacon system, there is a type of interference called fruit caused by beacon replies to interrogations asynchronous with the observer's interrogator. The largest amount of this interference is received through the sidelobes of the interrogating antenna, but it can become dense enough to cause false target indications.

3.1.162 Gain (antenna). The increase in signal power in one direction by a directional antenna, relative to theoretical isotropic radiator.

3.1.163 Gain (transmission gain). The increase in signal power in transmission from one point to another under stated conditions. Power gain is usually expressed in dB.

3.1.164 Gain (manual). The receiver gain control allows the operator to vary the receiver sensitivity. It is not designed as an AJ feature; however, when properly employed it may greatly reduce the effects of jamming. The radar detection capability is also reduced by an equal amount.

3.1.165 Gain control. A device for adjusting the gain of a system or transducer. The gain control is designed to prevent the gain from reaching a value that will cause saturation or instability of the system. See Gain margin.

3.1.166 Gain margin (control system, feedback) (loop transfer function for a stable feedback system). The reciprocal of the gain at the frequency at which the phase angle reaches -180 degrees. Gain margin, sometimes expressed in dB, is a convenient way to estimate relative stability by Nyquist, Bode, or Nichols diagrams. For systems with similar gain and phase characteristics in a conditionally stable feedback system, gain margin is understood to refer to the highest frequency at which the phase angle is -180 degrees.

3.1.167 George box. An amplitude sensitive device employed in an IF amplifier. This unit rejects small jamming signals not of sufficient amplitude to operate its circuits. However, jamming signals of sufficient amplitude are not affected.

3.1.168 Ghosts.

a. In passive detection, the intersection points of lines of position that do not represent actual targets but are only crossover points of multiple plotted lines of position from two or more detection stations.

b. Unwanted signal appearing on the screen of a radar indicator, caused by echoes which experience multiple reflections before reaching the receiver.

3.1.169 Glint (in radar).

a. The random component of target location error caused by variations in phase front of the target signal (as contrasted with scintillation error). Glint may affect angle, range of Doppler measurements, and may have peak values corresponding to locations beyond the true target extent in the measured coordinate.

b. ECM that use the scintillating, or flashing, effect of shuttered or rotating reflectors to degrade tracking or seeking functions of an enemy weapons system.

3.1.170 Ground photo. An unclassified general call sign for ground radar stations engaged in active ECM.

3.1.171 Gull. A floating radar reflector used to simulate surface targets for deceptive purposes.

3.1.172 High pass filter. A filter having a transmission band of all frequencies above some cutoff frequency, not zero.

3.1.173 High video pass (HVP). HVP is an improved or super FTC, and is effective against CW, swept, pulse jamming and clutter or chaff, or both. Based on time, the radar receiver will pass much shorter pulses than FTC, and will then present these on the indicator. HVP is good for distinguishing between targets that are too close together to be resolved as individual targets.

3.1.174 Home on jam (HOJ). A method of passive guidance designed to use the jamming signal emitted by the target to track the target in angle.

3.1.175 Identification friend or foe (IFF). An electronic beacon system for identifying friendly and enemy A/C on radar displays. This is generally accomplished by an airborne transponder on friendly A/C that replies to a radar interrogation with a coded signal.

3.1.176 Interference rejection unit (IFRU). A tunable filter or wave-trap which can be adjusted to reject any frequency within the IF bandpass and allow the remainder of the bandpass curve to remain intact. The filter is adjusted to reject an interference signal and as such is a form of AJ.

3.1.177 Imitative deception. The introduction of radiations into enemy channels which imitates his own emissions.

3.1.178 Imitative jamming. The jamming technique of transmitting a signal identical to the original guidance signal.

3.1.179 Infrared counter-countermeasures (IRCCM). Actions taken to effectively employ our own IR radiation equipments and systems despite the enemy's actions to counter their use.

3.1.180 Infrared countermeasures (IRCM).

a. CM used specifically against enemy threats operating in the IR spectrum.
b. Actions taken to prevent or reduce the effectiveness of enemy equipment and tactics employing IR radiation are termed IRCM.

3.1.181 Instantaneous automatic gain control (IAGC).

a. That portion of a system that automatically adjusts the gain of an amplifier for each pulse to obtain a substantially constant output pulse peak amplitudes; the adjustment being sufficiently fast to operate during the time a pulse is passing through the amplifier.
b. (Radar). A quick-acting AGC that responds to variations of mean clutter level or jamming over different range or angular regions, avoiding receiver saturation (also known as back-bias). IAGC automatically adjusts the gain of the radar receiver so that strong signals do not block adjoining weak signals. IAGC is not quick enough to block short pulse jamming, but is capable of reducing the effects of long pulse jamming or extended clutter.

3.1.182 Instantaneous frequency.

a. The time rate of change of the angle of a sinusoidal wave. If the angle is measured in radians, the frequency in hertz (Hz) is the time rate of change of the angle divided by 2π.
b. Zero-crossing CFAR device takes the form of the IF DICKE FIX. CFAR, except the phase detector, is replaced with a frequency discriminator.

3.1.183 Instantaneous frequency CFAR (IFCFAR). This CFAR technique is similar to the IF DICKE FIX CFAR, except for having a phase detector instead of a frequency discriminator. The primary use of this technique, in conjunction with rapid random frequency changes, is to make chaff signals appear noise-like so they can be handled in a conventional manner.

3.1.184 Instantaneous frequency measuring receiver (IFM). A type of wide band receiver that can measure the frequency of an incoming signal. Modern IFMs approach 100 percent signal reception probabilities.

3.1.185 Intercept receiver. A special calibrated receiver which can be tuned over a wide-frequency range to detect and measure radio signals transmitted by the enemy. Also called search receiver.

3.1.186 Interference (electronic). An electrical or EM disturbance that causes undesirable responses on electronic equipment. Electrical interference refers specifically to interference caused by the operation of electrical apparatus that is not designed to radiate EM energy.

3.1.187 Interference spectrum. The frequency distribution of the jamming interference in the propagation medium external to the receiver.

3.1.188 Intermediate frequency (IF) DICKE FIX CFAR. This CFAR technique uses a broadband limiting IF amplifier that precedes a coherent detection and narrowband video filter. The limit level is present well below the receiver noise level. Consequently any increase in noise power at the input will not affect the output noise level. A usable S/N is established by the ratio of the filter bandwidths, usually on the order of 10 to 1.

3.1.189 Intermediate frequency (IF) jamming. A form of jamming that is accomplished by transmitting two signals separated by a frequency equal to the center frequency of the radar receiver IF amplifier or by a single jamming signal at the IF.

3.1.190 Intrusion. The intentional insertion of EM energy into transmission paths in any manner with the objective of deceiving operations or of causing confusion.

3.1.191 Inverse-gain (IG) repeater jammer. A deception jamming technique which amplitude modulates a jamming signal at the same frequency, but 180 degrees out of phase from the detected modulation of a conical scan tracking radar.

3.1.192 Jaff. Expression for the combination of electronic and chaff jamming.

3.1.193 Jam attenuator control. The jam attenuator control is used to prevent receiver saturation from any strong signals, including electronic jamming, chaff, or clutter; it also permits the determination of the bearing and elevation of jammers that would cause wide sectors of the scope to be obscured. The jam attenuator control reduces all signals equally, jamming as well as targets. This control should be used in the jammed sector only and not for an entire antenna revolution. Targets in the jammed sector would only be seen if they were stronger than the jamming. However, the jammed sector may be reduced enough in size to allow the operator to determine either bearing or elevation.

3.1.194 Jammer. A transmitter used to jam radio or radar transmission.

3.1.195 Jammer finder. Radar which attempts to obtain the range of the target by training a highly directional pencil beam on a jamming source.

3.1.196 Jammers tracked by azimuth crossing. A semiautomatic strobe processing and tracking device which permits automatic detection and tracking on azimuth only data gathered from the jamming signals emanating from an airborne vehicle.

3.1.197 Jamming. See Acoustic jamming, Barrage jamming, Electronic jamming, or Spot jamming.

3.1.198 Jamming (in radar).

a. A form of ECM in which noise or noise-like signals are transmitted at frequencies in the receiver bandwidths of a radar to obscure the radar signal.

b. The deliberate radiation, reradiation, or reflection of EM energy with the object of impairing the use of electronic devices, equipment, or systems by an enemy.

3.1.199 Jamming to signal ratio (J/S). The inverse of the signal-to-jamming ratio.

3.1.200 Jamming strobe indicator. An ECCM technique for use on search radars under the influence of noise jamming, wherein the radar received jamming signal direction and strength are indicated on the PPI as a function of bearing.

3.1.201 Jam resistant data link. An electronic data transmission system which uses various techniques to reduce the effect of enemy ECM (jamming) on its operational use by friendly elements.

3.1.202 Jam strobe. Jam strobe is also called JAVA (jamming amplitude versus azimuth). This circuit generates a marker on the PPI to indicate signal strength as a function of bearing by sampling the jamming intensity once each repetition period. In addition to showing the direction of the jammer, the jam strobe also indicates the severity of main and sidelobe jamming.

3.1.203 Jittered PRF. A term used to describe the random variation of the pulse repetition period. Jittered PRF provides a discrimination capability against repeater type jammers.

3.1.204 Large scale ECM mission. The conduct of active airborne ECM by six or more A/C working as a unit.

3.1.205 Limiter. A device which prevents its output signal from exceeding a predetermined value.

3.1.206 Linearly frequency modulated pulse (LFMOP). See Chirp and Pulse compression.

3.1.207 Lin-log amplifier. An AGC amplifier that operates in a linear manner for low amplitude input signals, but responds in a logarithmic manner to high amplitude input signals.

3.1.208 Lobe-on-receive-only (LORO). A passive scanning technique in which a nonscanning beam is used to illuminate the target and a nonradiating, receiving antenna is scanned. Normally used with conical, lobe-switching or unidirectional sector scans.

3.1.209 Local oscillator (LO) OFF. This is a simple expedient of shutting off the LO during barrage jamming. The barrage jammer will not be seen unless there is a beating signal such as a target; therefore, targets will appear. Since targets will not appear in directions where no jamming arises, either an automatic azimuth switch or an additional receiver-display is required.

3.1.210 Lock-on. The condition when a radar is switched so that it automatically tracks a target electronically.

3.1.211 Logarithmic fast time constant (LOG-FTC). This device consists of a logarithmic IF amplifier followed by an FTC circuit. The LOG-FTC combination is very effective in removing variations (in the video output noise level) caused by spot noise, wideband noise, and slow sweep noise modulated AM jamming.

3.1.212 Logarithmic receiver (LOG). A receiver whose response approximates the logarithm of the strength of the incoming signal. A special type of receiver having a large dynamic range of AGC which gives considerable protection against receiver saturation by strong jamming on interference signals. Useful against weather, clutter, chaff, and spot jamming.

3.1.213 Logarithmic video (LOG-Video). Log-video reduces strong signals to prevent display saturation at a logarithmic or varying rate.

3.1.214 Look-through.

a. When jamming, a technique whereby the jamming emission is interrupted irregularly for extremely short periods to allow monitoring of the victim signal during jamming operations.

b. When being jammed, the technique of observing or monitoring a desired signal during interruptions in the jamming signals.

c. A visual display which continuously monitors the target signal in time and frequency. Look-through derives its primary importance from the desirability for rapid acquisition, setting, and jamming of a signal while jamming other signals.

3.1.215 Masking. In EW the use of additional transmitters to hide a particular EM radiation as to location of source or purpose of the radiation, or both.

3.1.216 Manipulative communications deception (MCD). The use of friendly communications to falsify information which a foreign nation can obtain from communications analysis.

3.1.217 Manipulative deception. The alteration or simulation of friendly EM radiations to accomplish deception.

3.1.218 Manipulative radar deception. Accomplished by deliberately radiating or reradiating EM radar like signals to mislead the enemy.

3.1.219 Manual rate-aided tracking. Radar circuit which tracks individual targets by computing the velocity from position fixes inserted manually into the circuitry.

3.1.220 Matched-filter receiver. A radar receiver whose signal processing circuits are designed to discriminate against signals with characteristics different from those of the transmitted RF pulse.

3.1.221 Meaconing. A system of transmitting actual or simulated radio navigational signals for confusing navigation.

3.1.222 Modulated CW jamming. A CW carrier waveform that has been modulated with some other signal such as noise, low, medium or high frequencies, and is transmitted for deception. This may be AM, FM, pulse modulation (PM), pulse, and so forth.

3.1.223 Modulated PRF (MPRF). The deliberate modulation of the interpulse spacing in a pulse train. This includes pulse frequency modulation (PFM) in which the modulation wave is used to frequency modulate a series of pulses. See PRF jitter and PRF stagger.

3.1.224 Modulation on pulse (MOP). The modulation, in frequency or phase, of an RF carrier wave during the pulse, either in a discrete or continuous pattern. This is normally employed for pulse compression.

3.1.225 Monopinch. AJ appliction of the monopulse technique where the error signal is used to provide discrimination against jamming signals.

3.1.226 Monopulse. A radar technique in which information concerning the angular location of a target or source is derivable from each return pulse by a comparison of signals received simultaneously in two or more antenna beams, as distinguished from techniques such as lobe switching or conical scanning which requires multiple pulses.

3.1.227 Moving target indicator (MTI). A radar receiver circuit for separating moving targets from stationary clutter, or clutter moving at a different rate, by recognizing the Doppler frequency or phase shifts of the receiver echo signals.

3.1.228 Moving target indicator (MTI) CFAR. This technique provides a CFAR capability in an MTI receiver. The cancellation of ground clutter is not impaired during ECM action.

3.1.229 Multiband radar. This type of radar uses simultaneous operation on more than one frequency band through a common antenna. This technique allows for many sophisticated forms of video processing and requires that the jammer jam all channels at the same time.

3.1.230 Multiple frequencies. Simultaneous transmission on more than one frequency.

3.1.231 Multitarget generator jamming. This generator takes the radar's PRF, scan rate, and antenna lobe pattern, and computes when to transmit false targets at the radar's frequency. The targets appear as true targets, but normally only about 20 percent of the targets are programmed to give a logical course and speed. The numerous targets saturate the tracking operator's capability. Multitarget generation jamming is identified by the sudden appearance of multiple targets or many targets either stationary or on illogical courses and speeds or maneuvers such as 90 degree turns at high speeds but with no displacement. Also, targets may appear in back and sidelobe positions.

3.1.232 Music. In air intercept, a term meaning electronic jamming.

3.1.233 Narrowband linear (NBL). NBL is not really an AJ feature except that it connects the manual gain control into the system. It is used to vary the receiver gain level at a linear rate.

3.1.234 Narrowband (NB-1). NB-1 narrows the receiver frequency, making it more selective. It limits the target signals and the jamming signal to a set level of amplitude and reduces the level of a jamming signal if the jammer is not tuned to the radar's exact frequency.

3.1.235 Narrowband (NB-2). NB-2 is the same as NB-1 except that the receiver sensitivity is set 20 dB higher, which increases the resolution of the radar. NB-2 will not exclude all of the jamming signals from display because of the higher sensitivity of the radar.

3.1.236 Navigation CM. The detection and evaluation of enemy electronic aids to navigation, and the use of jamming and deception to interfere with enemy use of such aids.

3.1.237 Noise. Any unwanted disturbance within a dynamic electrical or mechanical system, such as undesired EM radiation in any transmission channel or device.

3.1.238 Noise jamming. Noise jamming is direct (straight), AM, or FM noise on a carrier frequency that has a highly variable bandwidth for increasing the radar receiver's noise level. Noise jamming may be swept through a frequency spectrum at various rates or spot speeds. Noise jamming is identified by video saturation at all ranges in one or more sectors of the scope; the size of the sector is dependent upon the power and range of the jammer and the sidelobe levels of the radar. Noise jamming may be amplified and radiated directly, or a carrier may be modulated with the noise.

3.1.239 Noise modulated jamming. A jamming signal modulated, either AM or FM, or both, by a noise or noise like source.

3.1.240 Noise source. A device employed for the generation of noise. Tubes used for this purpose include photomultiplier and gaseous discharge types.

3.1.241 Noncommunications jamming. Electronic jamming used against electronic devices other than those that are used as a means of communications. Examples are: navigational aids, radar, guided missiles, guidance and control signals, proximity fuses, and similar devices.

3.1.242 Off-board jamming. Jamming from a source not on the target platform.

3.1.243 Off-line jamming (off-target). Jamming from a station away from the vicinity of the target which necessarily must be active jamming.

3.1.244 On-line jamming. The use of the jamming device in line with the target and the radar set. This may be either active or passive jamming.

3.1.245 Out-phasing antenna system. A second antenna or group of antennae used with the basic antenna system in such a manner as to pick up jamming signals; then, with certain phasing adjustments, the jamming signal is essentially cancelled as far as the receiver is concerned.

3.1.246 Optical CM. Applications of ECM in the visible light portion of the EM spectrum. Actions taken to prevent or reduce an enemy's effective use of the visible spectrum. Also called visual CM.

3.1.247 Passive angle tracking (PAT). A target may be tracked passively if that target emits an EM radiation; for example, a jamming, radio, or radar signal of sufficient duration that direction finding (DF) bearing may be obtained. The emission from the target is DFd in azimuth or elevation, or both. No range information will be available unless cross DF techniques are used by two or more passively tracking sites.

3.1.248 Passive detection and tracking. By combining azimuth data on jamming strobes from several stations, intersections are obtained which indicate the position of the jammers. The number of ghosts can be reduced by increasing the number of friendly station intersections and obtaining elevation angles of strobes when available.

3.1.249 Passive electronic CM. Electronic CM based on the reflection, absorption, or modification of the enemy's EM energy. This distinction between active and passive CM is not currently used, but it is based on the presence or absence of an electronic transmitter.

3.1.250 Passive jamming. The techniques of deception by employing confusion reflectors to return spurious and confusing signals to the transmitting radar set.

3.1.251 Penetration aids. Techniques or devices employed by aerospace systems to increase the probability of weapon system penetration of an enemy defense. Examples are: low altitude profiles, trajectory adjustments, reduced radar cross sections of attack vehicles, improved vehicle hardness to effects of defense engagements, terrain avoidance radar, bomber defense missiles, decoys, chaff, ECM, and so forth. Penetration aids are used by an offensive system to penetrate enemy defenses more effectively. Also called PENAIDS.

3.1.252 Phantom signals. Signals appearing on the screen of a cathode ray tube (CRT) indicator, the cause of which cannot readily be determined and which may be caused by circuit fault, interference, propagation anomalies, jamming, and so forth.

3.1.253 Phantom target.

a. An echo box, or other reflection device, that produces a particular blip on the radar indicator.

b. A condition, maladjustment, or phenomenon (such as a temperature inversion) that produces a blip on the radar indicator resembling blips of targets for which the system is being operated.

3.1.254 Polarization diversity. This technique involves the variation of polarization (such as horizontal, vertical, circular, or elliptical for radar use) either simultaneously or singly.

3.1.255 Power out control. With power out control the transmitter peak power is variable to give higher average power, longer detection ranges, and increased burnthrough range.

3.1.256 Pulse compression. The coding and processing of a signal pulse of long time duration, down to one of short time duration and high range resolution, while maintaining the benefits of high pulse energy. This technique uses matched filter techniques for discriminating against signals that do not correspond to the transmitted code. The technique's implementation involves stretching the transmitted pulse and compressing the received pulse. It permits an increase in average transmitted power (without increase in peak power) with no loss in range resolution.

3.1.257 Pulse repetion frequency (PRF). The rate at which radar transmitter pulses are generated.

3.1.258 Pulse repetition interval (PRI). Time between successive pulses. The reciprocal of the PRF.

3.1.259 Pulse repetition frequency (PRF) change (jittered PRF). The PRF is rapidly varied at a random rate so that false targets appear to jitter or appear fuzzy on the scope. An alternative to jittered PRF is to change the PRF momentarily. This causes the false targets to change their position on the scope.

3.1.260 Pulse repetition frequency (PRF) stagger. The technique of switching PRF or pulse repetition interval (PRI) to different values on a pulse-to-pulse basis such that the various intervals follow a regular pattern. This is useful in compensating for blind speeds in pulsed MTI radars. Interpulse intervals differ but follow a regular pattern.

3.1.261 Pseudonoise. A modulation technique resulting in low signal selectibility and low vulnerability to ECM.

3.1.262 Pulse discriminator (PD). Device which responds only to a pulse having a particular characteristic, such as duration, period, or phase relationship.

3.1.263 Pulse interference eliminator. A device which removes pulsed signals which are not precisely on the radar operating frequency.

3.1.264 Pulse interference suppression and blanking (PISAB). This PRF device is an automatic interference blanker. PISAB will blank all video signals that are not synchronous with the radar PRF. PISAB does not require any trigger and operates on both normal and MTI modes. PISAB is effective against random pulse signals.

3.1.265 Pulse jitter. Random variation of interpulse interval.

3.1.266 Pulse modulated jamming. Use of jamming pulses of various widths and repetition rates.

3.1.267 Pulsewidth discriminator (PWD). This device measures the pulse length of video signals and passes only those whose time duration falls into some predetermined design tolerances. PWD offers good discrimination against long pulse jamming and ECM with low frequency noise modulation. PWD affords little or no discrimination against short pulses and HF noise modulations. PWD will give a small gain against barrage jamming, similar to that of a matched filter in the video.

3.1.268 Quick reaction capability (QRC). QRC is designed to conform to urgent operational requirements in support of the service mission. This applies only to designated EW reconnaissance, and intelligence programs for which special management procedures are used.

3.1.269 Rabbits. Interference from another radar on or near the frequency of the receiving radar. Rabbits show on the indicators as interference at the rate of the relative PRF of the interfering radar.

3.1.270 Radar absorbent material (RAM). RAM is used as a radar camouflage device to reduce the echo area of an object.

3.1.271 Radar CM. See ECM.

3.1.272 Radar deception. See Electronic deception.

3.1.273 Radar decoy. A reflecting object used in radar deception, having the same or similar reflective characteristics as a target, or appear to be a valid target to a specific type of radar.

3.1.274 Radar homing and warning (RHAW). Typically, a radar homing and warning system consists of an airborne, wideband crystal video receiver designed to intercept, identify, and display the direction to pulse-type emitters. See Radar warning receiver.

3.1.275 Radar intelligence.

a. Intelligence concerning radar or intelligence derived from the use of radar equipment. In this sense, the term has been used with several specific meanings. These are:

1. That aspect of electronic intelligence that deals with radar.
2. Intelligence concerning the radar aspects of a radar mission, especially a radar-bombing mission.
3. Radar target intelligence derived from information procured by radar, particularly with regard to bomb damage assessment and bomb scoring.

b. An organization or activity that deals with such intelligence.

3.1.276 Radar reconnaissance. Reconnaissance by radar to obtain information on enemy activity and to determine the nature of terrain.

3.1.277 Radar silence. An imposed discipline prohibiting the transmission by radar of EM signals on some or all frequencies. A form of EMCON.

3.1.278 Radar warning receiver (RWR). A wideband crystal video receiver (usually airborne) designed to intercept, identify, and display the type of, and sometimes the direction to, radar emitters, not a homing system. See also Radar homing and warning.

3.1.279 Radiation intelligence (RINT). Intelligence derived from a collection and analysis of noninformation bearing elements extracted from the EM energy unintentionally emanated by foreign devices, equipments, and systems, excluding those generated by the detonation of atomic or nuclear weapons.

3.1.280 Radio CM. See ECM.

3.1.281 Radio deception. The employment of radio to deceive the enemy. Radio deception includes sending false dispatches, using deceptive headings, employing enemy call signs, and so forth. See also electronic deception.

3.1.282 Radio frequency interference (RFI). Unintentional interfering signals present in electronic equipment. Although these signals are designated as RF, there is no implication that they are transmitted by EM radiation through space and enter the equipment through an antenna. RFI may enter the equipment through the case or may be conducted along power lines or other wires that enter the equiment.

3.1.283 Radio recognition. The determination by radio means of the classification, or the individuality, of another.

3.1.284 Radio silence. A period during which all or certain radio equipment capable of radiation is kept inoperative. (In combined or United States joint or intraservice communications, the frequency bands or types of equipment affected, or both, will be specified.)

3.1.285 Railing.

a. Pertains to radar pulse jamming at high recurrence rates 50 kilohertz (kHz) to 150 kHz. Railing results in an image on a radar indicator resembling fence railing.

b. The name given to that pattern produced on an A-scope by CW modulated with a high frequency signal. Railings appear as a series of vertical lines resembling target echoes along the baseline.

3.1.286 Rainbow. A technique which applies pulse-to-pulse frequency changing to identify and discriminate against decoys and chaff.

3.1.287 Random modulated CW jamming. A CW carrier modulated by a random signal. This nonperiodic function can be used to AM, FM or, AM and FM the carrier. Noise modulation of a CW Carrier will produce effects on the radar similar to those produced by a direct noise source. Random pulse-modulated CW produces pulses with a random PRF.

3.1.288 Random noise. EM energy with no particular modulation or pattern. Random noise may be generated by either natural atmospheric phenomena or by EM radiating devices.

3.1.289 Random noise (fluctuation noise). Noise that comprises transient disturbances occurring at random, the part of the noise that is unpredictable except in a statistical sense. The term is most frequently applied to the limiting case where the number of transient disturbances per unit time is large, so that the spectral characteristics are the same as those of thermal noise. Thermal noise and shot noise are special cases of random noise.

3.1.290 Random pulse jamming. The technique whereby a pulse transmission system is pulsed irregularly by random noise signals.

3.1.291 Range gate capture. ECM technique used to capture the range gate of the tracking radar for range gate walk off or pulloff purposes.

3.1.292 Range gate pulloff (RGPO). ECM technique to cause the range gate of a tracking radar to lose track on the target. An amplified pulse is successively delayed a greater and greater time (range) and then the ECM is turned off thus dropping the target to the victim radar.

3.1.293 Range gate push-off (RGPsHO). Opposite of RGPO.

3.1.294 Range gate walk off (RGWO). Generic term covering RGPO and RGPsHO.

3.1.295 Range height indicator (RHI). A display used with three-dimension (3-D) search radars showing range along the horizontal scale and height along the vertical scale. Elevation angle may also be indicated.

3.1.296 Reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.

3.1.297 Recovery time. The time for a part of a receiver to recover to a zero-signal condition after receiving a jamming pulse of saturation intensity. If recovery is accomplished before the next controlling pulse arrives, the jamming is ineffective.

3.1.298 Repeater jammer. Equipment to confuse or deceive the enemy by causing his equipment to present false information. This is done by a system that intercepts and reradiates a signal on the frequency of the enemy equipment, the reradiated signal being modified to present erroneous data on azimuth, range, number of targets, and so forth. See FTG.

3.1.299 Responsive noise jammer. A noise repeater jammer that transmits spot noise at the frequency of the received radar signal. If the radar changes operating frequency, it automatically changes its jamming frequency to cover it.

3.1.300 R-scope. Similar to A-scope, except that the left to right sweep is delayed in time and does not start at the instant a pulse of energy is radiated by the transmitter. Usually, it expands a portion of the radar's range presentation, thus providing a more detailed display.

3.1.301 Rope. An element of chaff consisting of a long roll of metallic foil or wire which is designed for broad, low-frequency response. See Chaff.

3.1.302 Rope-chaff. Chaff which contains one or more rope elements. See Chaff.

3.1.303 Rotating polarization. The result of a rotating feed. This should not be confused with circular polarization where the electric field rotates about the axis of propagation at the radar frequency.

3.1.304 Saturating signal. In radar, a signal of an amplitude greater than the dynamic range of the receiving system.

3.1.305 Sawtooth modulated jamming. An ECM technique where the carrier is modulated, either in amplitude or frequency, by a sawtooth waveform. There may also be a noise component added.

3.1.306 Scan on Receive Only (SORO). See Lobe on receive only.

3.1.307 Self-screening jammer (SSJ). A target that transmits jamming signals to prevent search or tracking radars from accurately determining its coordinates in space, or to cause a tracing radar to break lock.

3.1.308 Self-screening range. The minimum range at which a jamming platform will not be detected by a radar.

3.1.309 Sensitivity time control (STC). Programmed variation of the gain (sensitivity) of a radar receiver as a function of time within each PRI or observation time in order to prevent overloading of the receiver by strong echoes from targets or clutter at close ranges. STC reduces the gain of the radar receiver for detection of close-in targets. STC is particularly effective in removing close-in clutter and strong nearby signals. When adjusting STC, particular attention must be paid to close-in ranges so that small reflecting surfaces are not eliminated.

3.1.310 Sidelobe blanking (SLB). A device which employs an auxiliary wide-angle antenna and receiver to sense whether a received pulse originates in the sidelobe region of the main antenna and to gate it from the output signal if it originates in that sidelobe region. This technique uses an omnidirectional antenna and compares relative signal strength between the omni and the radar antenna. The omnichannel (plus receiver) has slightly more gain than the sidelobes of the normal channel, but less gain than the main beam. Therefore, any signal that is greater in the omnichannel must have been received from a sidelobe, and is blanked. This technique is effective in removing spoofer signals with a duty cycle up to approximately 50 percent.

3.1.311 Sidelobe canceller (SLC). A device which employs one or more auxiliary antennas and receivers to allow linear subtraction of interfering signals from the desired output, if they are sensed to originate in the sidelobe of the main antenna. This technique employs the same antenna and receiver configuration as the SLB, except that a gain matching and cancelling process takes place. Extraneous signals entering the sidelobe of the main antenna are cancelled while the targets remain. This type of system exhibits cancellation on the order of 20 dB against a single noise jammer. With multiple jammers at various azimuths, the performance of this device rapidly deteriorates. For relatively narrow-band systems with relatively small antennas, this requires one canceller loop for each jammer and azimuth anticipated. Wider band systems with larger antennas may require additional canceller loops.

3.1.312 Sidelobe jamming. Jamming through a sidelobe of the receiving antenna in an attempt to mask the target reflection received through the mainlobe of the receiving antenna.

3.1.313 Sidelobe-reduction. Reducing the sidelobe level of main antenna.

3.1.314 Sidelobe suppression. The suppression of that portion of the beam from a radar antenna other than the mainlobe.

3.1.315 Signal intelligence (SIGINT). A category of intelligence information comprising all communications, electronic and telemetry intelligence.

3.1.316 Signal security (SIGSEC). A generic term which includes both COMSEC and ELSEC.

3.1.317 Signal-to-jammer power ratio (S/J). The ratio of the signal power to the jamming power (S/J). This ratio is often expressed in dB.

3.1.318 Sinewave modulated jamming. Jamming signal produced by modulating a CW signal with one or more sinewaves.

3.1.319 Single beam blanking (SBB). The SBB feature is used by phased array radars as an alternative method of BBC. SBB is effective to some degree against many multiple target generators and swept frequency jammers. Because of overlapping beamwidths, a target signal will appear in more than one beam as the beams are scanned past a true target. When jamming signals are transmitted along one beam, that beam is blanked by the radar receiver.

3.1.320 Small scale ECM mission. Conduct of active airborne ECM by a single A/C or by two to five A/Cs working as a unit.

3.1.321 Speed gate. A circuit used to track the Doppler shift of a target.

3.1.322 Spoking (RADAR). Periodic flashes of the rotating time base on a radial display, sometimes caused by mutual interference.

3.1.323 Spoof. EW tactic that causes an enemy to be misled and commit errors in tactics.

3.1.324 Spoofer. In air intercept, a contact employing electronic or tactical deception measures.

3.1.325 Spoofing. A type of deception using an electronic device to transmit a target echo. The spoofing transmitter must operate at the same frequency and PRF as the radar to be deceived. The radar main pulse triggers the spoofing transmitter which, after a delay, transmits a false echo.

3.1.326 Spot jamming. The jamming of a specific radar bandwidth or frequency.

3.1.327 Standoff jamming (SOJ). An ECM support A/C tactic that orbits in the vicinity of the intended target. As the fighter-bomber pilot starts his strike penetration, the ECM A/C directs jamming against all significant radars in the area. This technique provides broad frequency band ECM without affecting performance of the strike A/C.

3.1.328 Staggered PRF. Staggered PRF allows an increase in MTI blind speeds such that no zeros exist in the velocity response at lower velocities. In a two period mode, the usual blind speed or occurrence of a zero in the velocity response is multiplied by a factor which is a function of the ratio of the two repetition periods.

3.1.329 Stream.

a. Dispensing of chaff (corridor or random, interval or bursts).
b. An unclassified brevity code word signifying chaff dispensing type of active ECM.

3.1.330 Subclutter visibility. The degree to which a radar can detect targets in clutter.

3.1.331 Subjamming visibility. Relates to how well a particular radar AJ technique can see through jamming signals.

3.1.332 Susceptibility.

a. Capability of or capacity to be acted upon. A device is susceptible to any force to which it responds. A system is susceptible to noise jamming if it is of such a nature to admit noise jamming.

b. The degree to which a device, equipment, or weapons system is open to effective attack due to one or more inherent weaknesses.

3.1.333 Sweep jammer. Electronic jammer which sweeps a narrow band of electronic energy over a broad bandwidth.

3.1.334 Sweep-lock-on-jammer. A transmitter in which a narrow band jamming signal can be tuned over a broad frequency band and the signal locked on a particular frequency.

3.1.335 Sweepthrough. Jamming transmitter that sweeps through a RF band and jams each frequency briefly producing a sound like that of an A/C engine.

3.1.336 Swept audio. A deceptive ECM technique that is produced by AM of the transmitted signal at a frequency that is varied through the anticipated scanning ratio of a SORO tracking radar.

3.1.337 Swept local oscillator receiver (SLOR). SLOR provides a capability for receiving and processing jamming energy, differentiating mainlobe antenna response from sidelobe responses and for determining and transmitting an accurate estimate of the jammer's azimuth.

3.1.338 Synchronized pulse jamming. The technique of attempting to insert jamming pulses into a receiver each time the receiver gate opens.

3.1.339 Synchronous pulsed jamming. This jammer matches exactly the PRF of the victim radar, then transmits multiples of the PRF, and is most effective if the jammer also matches the PW of the radar. Synchronous pulsed jamming is easily recognized since the spacing between successive target lines is equal, and each target line is the same in depth from the center outward. The width of the jammed sector is dependent upon the range of the jammer from the radar.

3.1.340 Tactical EW. That application of EW to tactical air operations. Tactical EW encompasses the three major subdivisions of EW: ESM, ECM and ECCM.

3.1.341 Tangential sensitivity. The strength of the target signal, measured at the receiver terminals, which would give a signal pulse twice the apparent height of the noise.

3.1.342 Target susceptibility. The degree to which a target is capable of being affected by outside forces. A missile is susceptible to energy transmissions to which it reacts.

3.1.343 Target vulnerability. The susceptibility to specific measures, or CM, actually employed against a system.

3.1.344 Time discrimination circuits. Employed in video amplifiers for AJ. Pulses may be discriminated according to their widths, their location with respect to the expected repetition rate, the rate of change in this position, and the coincidence of one or more pulses.

3.1.345 Track on jam. A method of passive target tracking using the jamming signal emitted by the target.

3.1.346 Tramlines. The name given to that pattern produced on an A-scope by CW modulated with a low frequency signal. Tramlines appear as a number of horizontal lines above the baseline.

3.1.347 Two signal jamming (also called straddle jamming). A method of jamming whereby two signals are transmitted on two RF frequencies only slightly separated. Effective against certain types of radar where receiver bandwidth is narrow enough to defeat noise jamming.

3.1.348 Unintentional radiation exploitation (URE). Exploitation for operational purposes of noninformation bearing elements of EM energy unintentionally emitted by targets of interest.

3.1.349 Unipolar video CFAR. This CFAR technique takes advantage of the baseline-break phenomenon in a slightly different form. The device consists of a wideband IF amplifier, followed by an envelope detector and a video limiter. The proper detection bandwidth is established by a low-pass video filter. This technique generally is not as acceptable as the DICKE FIX CFAR.

3.1.350 Unmodulated CW jamming. Unmodulated CW jamming is the transmission of a high-power carrier frequency that causes an overload effect to occur in the radar receiver. CW jamming is used against radars that have a limited tuning capability. Unmodulated CW jamming can be identified by a blackening of the scope background (no video present) in a wedge-shaped sector, or by a solid brightening of a wedge or sector, normally exceeding one bandwidth.

3.1.351 Velocity gate deception. A self-screening ECM technique for use against a velocity tracking radar system, wherein the velocity-gate is first walked off the true skin return, and then angle deception is applied. Also velocity gate walk off (VGWO).

3.1.352 Video correlator. ECCM device that accepts only targets which correlate with previously received pulses.

3.1.353 Video DICKE FIX CFAR. This CFAR technique also provides for a linear mixer to precede a video limiter. The technique is used in conjunction with MTI receivers, and its operation is essentially the same as the unipolar video CFAR.

3.1.354 Video discrimination. Radar circuit used to reduce the frequency band of the video amplifier stage in which it is used.

3.1.355 Video integrator.

a. An ECCM device used to reduce the response to nonsynchronous signals such as noise and useful against random pulse signals and noise.

b. A device which uses the redundancy of repetitive signals to improve the output SNR by summing the successive video signals.

3.1.356 Vulnerability.

a. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designed mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. EW vulnerability is the measure of the systems inability to perform in the face of hostile ECM. EW vulnerability can only be measured in its intended operational environment (actual or simulated) and must take into account such factors as: susceptibility of the system to intercept by hostile ESM activities, and the nature and extent of the hostile EW threat.

b. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.

3.1.357 Warning receiver (EW). A receiver with the primary function of warning the user that his unit is being illuminated by an EM signal of interest.

3.1.358 Wideband CFAR receiver (WB-1). WB-1 is used against individual or combinations of rapidly swept EM-CW, noise, or CW. This mode has nonlinear limiting and gives poor resolution of overlapping targets.

3.1.359 Wideband limit (WB-2). WB-2 is used against narrow pulse (spike) or swept type jamming. This mode uses wideband limiters preceding narrowband filters to prevent filter ringing. WB-2 gives better resolution of overlapping targets.

3.1.360 Wide pulse blanking (WPB). The WPB circuit eliminates clutter and noise pulses from the video display in much the same manner as the clutter eliminator circuit.

3.1.361 Window. British World War II code name for chaff.

3.1.362 Zero-crossing counting. This CFAR technique uses a wideband limiting IF amplifier followed by a zero-crossing counter that indicates the target when the rate of crossings falls below a predetermined value. The limiting action of the wideband amplifier and the random nature of the noise permit the use of a fixed threshold detection level that is independent of the jamming signal amplitude.

3.2 Acronyms and abbreviations.

A/C	Aircraft
ACAT	Acquisition category
ACET	Automatic cancellation of extended targets
ADM	Advanced development model
ADP	Automatic data processing
AGC	Automatic gain control
AM	Amplitude modulation
AM-CW	Amplitude modulation-carrier wave
AJ	Anti-jam
ANL	Automatic noise leveling
ARM	Anti-radiation missile
ASU	Approval for service use
AVNL	Automatic video noise limiting
BBC	Beam to beam correlation
BITE	Built-in-test equipment
CDR	Critical design review
CEP	Circular error probable
CFAR	Constant false alarm rate
CG	Coast Guard
CM	Configuration management

CMC	Commandant of the Marine Corps
COMINT	Communications intelligence
COMM	Communication(s)
COMOPTEVFOR	Commander, Operational Test and Evaluation Forces
COMSEC	Communications security
COSRO	Conical scan on receive only
CPAC	Coded pulse anti-clutter
CRT	Cathode ray tube
CSLC	Coherent sidelobe cancellation
CV	Coincident video
CW	Continuous wave
C^3	Command, control, and communications
C^3I	Command, control, communications, and intelligence
dB	Decibel
DBB	Detector back bias, detector balanced bias
dBm	Decibels, referred to one milliwatt
dBW	Decibels, referred to one watt
DCP	Decision coordinating paper
DECM	Deception ECM (also Defensive ECM in common military usage)
DF	Direction finding
DINA	Direct noise amplification
DLJ	Down link jamming
DNI	Director of Naval intelligence
DoD	Department of Defense
DON	Department of the Navy
DP	Development proposal
DSARC	Defense Systems Acquisition Review Council
DVAL	Datalink Vulnerability Analysis
ECCM	Electronic counter-countermeasures
ECM	Electronic countermeasures
ECP	Engineering change proposal
EDM	Engineering development model
EEI	Essential elements of information
ELINT	Electronic intelligence
EL RECON	Electronic Reconnaissance
ELSEC	Electronic security
EM	Electromagnetic
EMC	Electromagnetic compatibility
EMCON	Emission control
EMI	Electromagnetic interference
EMP	Electromagnetic pulse
EOB	Electronic order of battle
EOCCM	Electro-optic counter-countermeasures
EPL	ELINT parameter listing
ERP	Effective radiated power
ESM	Electronic warfare support measures
EVIL	Elevation versus integrated log
EW	Electronic warfare
E^3	Electro magnetic environmental effects
FA	Frequency agility
FAGC	Fast automatic gain control
FEWSG	Fleet electronic warfare support group
FM	Frequency modulation
FM-CW	Frequency modulation continuous wave
FTC	Fast time constant
FTG	False target generator
HOJ	Home on jam
HVP	High video pass
Hz	Hertz
IAGC	Instantaneous automatic gain control
IEEE	Institute of Electrical and Electronic Engineers
IF	Intermediate frequency
IFCFAR	Instantaneous frequency CFAR
IFF	Identification friend or foe
IFM	Instantaneous frequency measuring (receiver)

IFRU	Interference rejection unit
IG	Inverse gain
ILS	Integrated logistics support
ILSP	Integrated logistic support plan
IPS	Integrated program summary
IR	Infrared
IRCCM	Infrared counter-countermeasures
IRCM	Infrared countermeasures
JAVA	Jamming amplitude versus azimuth
JCS	Joint Chiefs of Staff
J/S	Ratio of jammer signal level to radar signal level
kHz	kilohertz (Hz x 10^3)
kV/m	kilovolts per meter
LFMOP	Linear frequency modulation on pulse
LO	Local oscillator
LOG	Logarithmic receiver
LOG-FTC	Logarithmic fast time constant
LOG-VIDEO	Logarithmic video
LORO	Lobe on receive only
LPI	Low probability of intercept
MCD	Manipulative communications deception
m^2	Square meter
MENS	Mission element need statement
MHz	Megahertz
MIJI	Meaconing, Intrusion, Jamming and Interference
MOP	Modulation on pulse
MPRF	Modulated pulse repetition frequency
MRF	Milestone reference file
MTI	Moving target indicator
NATO	North Atlantic Treaty Organization
NAVMAT	Naval Material Command
NB	Narrowband
NBL	Narrowband limiting
NDCP	Navy decision coordinating paper
NFOIO	Navy field operational intelligence office
NIC	Naval intelligence center
NISC	Naval intelligence support center
nmi	Nautical miles
NONCOMM	Noncommunication
NSA	National Security Agency
NSG	Naval Security Group
OPEVAL	Operational evaluation
OPNAV	Naval Operations
OPTEVFOR	Operational test and evaluation force
OR	Operational requirement
P-P	Peak-to-peak
PAT	Passive angle tracking
PFM	Pulse frequency modulation
PD	Pulse discriminator
PDR	Preliminary design review
PENAIDS	Penetration aids
PISAB	Pulse interference suppression and blanking
PM	Pulse modulation
PPI	Plan position indicator
PRF	Pulse repetition frequency
PRI	Pulse repetition interval
PW	Pulsewidth
PWD	Pulsewidth discriminator
QRC	Quick reaction capability
RAM	Radar absorbent material
RCS	Radar cross section
R D	Research and development
RF	Radio frequency

RFI	Radio frequency interference
RFQ	Request for quote
RGPO	Range gate pull-off
RGPsHo	Range gate push-off
RGWO	Range gate walk-off
RHAW	Radar homing and warning
RHI	Range height indicator
RINT	Radiation intelligence
rms	Root-mean-square
RWR	Radar warning receiver
SBB	Signal beam blanking
SECDEF	Secretary of Defense
SIGINT	Signal intelligence
SIGSEC	Signal security
SLB	Sidelobe blanking
SLC	Sidelobe cancellation
S/J	Signal-to-jammer power ratio
SLOR	Swept local oscillator receiver
S/N	Signal to noise ratio
SOJ	Stand-off jamming
SORO	Scan on receive only
SOSS	Soviet ocean surveillance system
SOW	Statement of work
SPAWAR	Space and Naval Warfare Systems Command
SSJ	Self-screening jammer
STC	Sensitivity time control
STILO	Scientific and technical intelligence liaison officer
SYSCOM	Systems command
TACEW	Tactical electronic warfare
T and E	Test and evaluation
TDOA	Time difference of arrival
TECHEVAL	Technical evaluation
TEMP	Test and evaluation master plan
TW	Threat warning
URE	Unintentional radiation
U.S.	United States
U.S.S.R.	Union of Soviet Socialist Republics
VGWO	Velocity gate walkoff
WB	Wideband
WPB	Widepulse blanking
2-D	Two dimension
3-D	Three dimension

4. GENERAL REQUIREMENTS

4.1 General. Management, engineering, and technical personnel must establish and implement a procedure for integrating ECCM into the various phases of the life cycle of the system. This approach is required to ensure early consideration of ECCM and to provide the continuity for achieving and maintaining the required ECCM capability. The approach should include modeling, analyzing, simulating, and testing to determine the susceptibility characteristics and operational constraints. Final requirements are postulated by tailoring the peculiar characteristics and operational requirements of the system in the individual specification.

4.2 Life cycle flow. The principal phases in the life cycle of a major radar system are as specified in a through f:

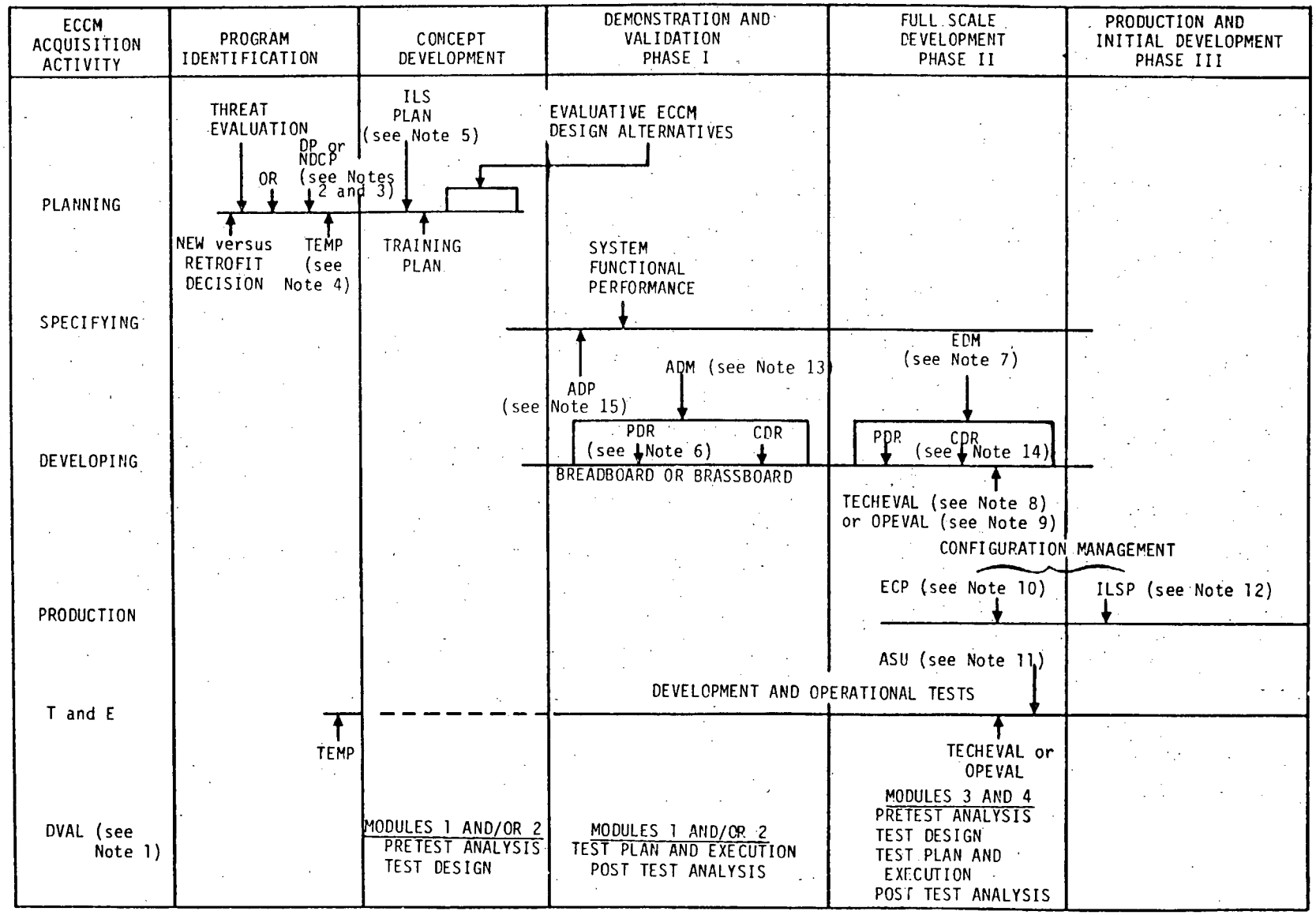
a. Program identification
b. Concept development
c. Concept validation
d. Full scale development
e. Production
f. Deployment

Numerous departmental and agency directives contain the policies that specify the activities and decisions made during each phase. A flow diagram which specifies an approach designed to integrate an ECCM program into the overall acquisition process is shown in FIGURE 5. The relationship between these activities and specific actions required by the manager is presented in other sections of this handbook.

4.2.1 Program identification. The acquisition cycle begins with the identification of a specific deficiency within a given mission area. A position paper is produced identifying the threat, the deficiency, an estimate of the impact if the deficiency is not corrected and the necessary corrective action. From these inputs a mission element need statement (MENS) is produced that initiates the decision process. The incorporation of planning for ECCM in the early position papers and the MENS is essential. The threat environment and the necessary ECCM to permit satisfactory operation of the radar system in that environment can substantially affect the thresholds for cost, scheduling, performance, supportability, and ultimately, the affordability of the system. Approval of the MENS is followed by a Secretary of Defense Decision Memorandum that justifies the start of the acquisition program.

4.2.2 Concept development. During this phase, technical and financial baselines for a development and acquisition program are established. Included are definitions of required operational capability, doctrines, and specific material requirements. Critical technical and operational issues are identified for study and resolution in subsequent phases whereas performance characteristics are established only in general terms. A statement of work (SOW) and a request for quote (RFQ) will be prepared where required. Outputs of this phase are alternate concepts, estimated operational schedules, and estimated procurement costs. Proper consideration of ECCM during this phase will have significant impact throughout the life cycle. An assessment of the ability of the system to perform its function during the system life cycle must include a threat analysis using both the friendly and hostile EM environment that may be encountered. These factors must be addressed not only in performing tradeoff studies and risk assessments, but also in estimating program costs. The culmination of these activities will be the first major design review by the Defense Systems Acquisition Review Council (DSARC I), the program initiation decision.

4.2.3 Concept validation. The primary objective of this phase is the selection of the single concept that will be carried out through full scale development. To accomplish this, the estimates made in the concept development phase must be refined. Areas of risk must be reassessed to ensure that they have been adequately defined and can be resolved or minimized. Frequently, this phase includes the construction of prototypes to evaluate operational, technical, and environmental factors and to refine costs. An SOW and RFQ for R and D contract support will be prepared, when required. The studies, analyses, and testing are culminated in the second design review, DSARC II, where a decision is made whether to proceed to full scale development.



Notes:

1. Data link vulnerability analyzer
2. Development proposal
3. Navy decision coordinating paper
4. Test and evaluation master plan
5. Integrated logistic support
6. Preliminary design review
7. Engineering development model
8. Technical evaluation
9. Operational evaluation
10. Engineering change proposals
11. Approval for service use
12. Integrated logistics support plan
13. Advanced development model
14. Critical design review
15. Automatic data processing

FIGURE 5. Major ECCM acquisition activities.

4.2.4 Full scale development. During this phase, the objective is the design and fabrication of an EDM in accordance with requirements tailored to the specific procurement, mission, environmental factors, and so forth. The system must be fully tested and evaluated to verify that the design not only conforms to its specifications, but that the system performs its assigned missions in the operating environment. This phase must also provide the documentation, including testing and analysis reports, to enable a decision to proceed to production. An ASU must be obtained prior to proceeding to production. An SOW and specification will be prepared and used for the development contract.

4.2.5 Production. The period following approval for production through the delivery and acceptance of the last item being procured is the production phase. Acceptance tests will be performed to demonstrate conformance to the requirements in the production specification and to ensure satisfactory performance when the item is in operational use. Strict quality control methods are required to ensure that proposed changes to the configuration do not degrade the performance of this or other systems. When acquisition is complete, responsibility to support the system is assigned to the logistics manager.

4.2.6 Deployment. This phase begins with the acceptance of the first operational system and continues until all are phased out of the inventory. There is usually an overlap with the production phase. In-service performance must be monitored by a reliable, established feedback system to detect, report, and correct operational problems. Modifications, ECPs and overhaul plans must be reviewed in accordance with the program configuration control system.

4.2.7 DVAL methodology. The DVAL T and E methodology incorporates the component parts of vulnerability into a four-module approach for the T and E of AJ features of C^3 reconnaissance and intelligence; and weapons RF data links. The methodology facilitates the determination and quantification of the four components so that a vulnerability assessment, based on fact and data instead of assumption and theory, can be accomplished. The four components represented by a corresponding DVAL module are: susceptibility module, interceptability module, accessibility module, and feasibility module. The relationship of the DVAL methodology is shown in FIGURE 5.

4.3 Procedural method for addressing ECCM. FIGURE 5 summarizes the procedures specified in 4.2 and provides the program manager with an orderly and coherent approach for addressing ECCM involving systems. When the contractor does the detailed design and production, the project director's major responsibilities in ECCM are to define the applicable requirements and monitor the contractor's efforts to comply with the requirements. When the procuring activity does the detailed design, and a contractor is responsible for production in accordance with Government-furnished information, the program director must conduct all aspects of the ECCM effort, including establishing installation criteria, performing analyses, and so forth. In any case, the program director may delegate those responsibilities to the ECCM authority in his activity.

4.4 Operational requirement (OR). The OR is the basic requirement for all Navy acquisition programs. Each OR is limited to three pages and includes a description of the operational need of the threat, the operational concept, performance goals, desired fleet introduction date, and related efforts. The OR should contain sufficient details of required ECCM capabilities, in a realistic operational scenario, to allow preliminary consideration of requirements for susceptibility and vulnerability assessments, design tradeoffs and future T and E plans. The scenario should relate system usage to specific mission requirements. The threat portion of the OR, provided by NIC and NSG, should ensure that ECCM capabilities in the electronic system make hostile exploitation as difficult, time consuming, and costly as possible. All categories of threat capability specified in a through g should be included:

a. Signal detection and interception
b. Emitter geoposition DF and locating
c. Analysis of external signal parameters
d. Enemy use of deception
e. Jamming
f. Exploitation of unintentional radiations and modulations
g. ARM

ORs, which clearly lead to a major weapon system acquisition or require costly R and D programs, must be submitted to the CNO Executive Board, the Acquisition Review Committee or the Ship Acquisition and Improvement Panel for approval before promulgation. The basic instructions for preparation of an OR are taken from OPNAVINST 5000.42C.

4.5 Development proposal (DP). The DP is provided in response to an OR. The DP is not limited to a preferred solution; rather the DP describes various technical approaches to satisfy the OR. The DP identifies key issues, compares effectiveness and estimated costs, highlights technical risks, proposes T and E and indicates possible milestones. The threat evaluation, provided by the NIC, is based on the OR and the operational scenario, and is used to guide the preparation of inputs included in the DP. The results of this evaluation are in the form of a current and predicted baseline EW threat for the expected lifetime of the electronic system being developed. The threat description is basically a restatement or expansion of that contained in the OR. All DPs for electronic systems are supported by a plan for conducting an analysis of the various alternatives which impact system ECCM. The analysis should include the level of ECCM protection afforded by each alternative. These levels should be commensurate with the baseline threat and the total environment in which the system will operationally exist. Alternative concepts, methods, and associated costs of providing levels of protection at each decision point in the development cycle will be evaluated. The minimum goal for ECCM protection is to provide capabilities comparable to the protection afforded the complete radar system. ECCM attributes, such as operating frequencies, modes of operations, and pulse coding, used only in time of war, should be identified as well as the use of simple ECCM tactics such as deployment techniques and procedural measures.

4.6 Navy decision coordinating paper (NDCP). The NDCP supports, authorizes and promulgates the SECNAV and CNO decision to initiate programs and establish advanced or engineering development line items. The NDCP is prepared by the CNO program sponsor. For programs requiring higher level approval, the NDCP authorizes planning and conceptual effort within already established Navy funding authority and provides the basis for preparation of a decision coordinating paper (DCP). The NDCP is updated for major reviews and designated milestones, and when actual or threatened problems occur. The NDCP presents program issues, considerations supporting the operational need, program objectives, program plans, performance parameters, areas of risk, and development alternatives. Every NDCP requires a statement of the current and projected threat to a level of detail appropriate to the radar system being developed. The NDCP must be updated annually to ensure that it reflects the actual status of the program and the latest analysis of the current and projected threat.

4.7 Test and evaluation master plan (TEMP). During the development of a new radar system a series of T and Es from early development to final production is required. These T and Es are conducted in accordance with a TEMP, a concise planning document describing the T and E for a particular acquisition category (ACAT) I, ACAT II, or ACAT III program. The TEMP is prepared by the project director and the staff of the Operational Test and Evaluation Force (OPTEVFOR). The TEMP must be approved by the CNO prior to the start of the conceptual phase of the program.

4.8 Decision Coordination Paper (DCP). The DCP is the basic document for use by the DSARC members to arrive at the recommendation for the Secretary of Defense (SECDEF) milestone decision. The DCP includes: a program description; revalidation of the mission need, goals, and thresholds; a summary of the DoD component acquisition strategy; system and program alternatives; and issues affecting the decision. The DCP shall be limited to 10 pages, including annexes. The DSARC advises the SECDEF on milestone decisions for major systems. Formal DSARC reviews are normally held at Milestone I, Milestone II, and Milestone III to see if the system design seems adequate to conform to the threat and if approval should be given for continuation of the program. It is therefore vital that ECCM be adequately addressed and documented in each phase, and reviewed at every milestone, since the DSARC process could deny system approval if this area is weak.

4.9 Integrated program summary (IPS) and the milestone reference file (MRF). The IPS summarizes the implementation plan for the life cycle of the system. The IPS provides information for a management review of the entire program. The format and directions for the IPS are contained in DoDINST 5000.2. The MRF is established at each milestone to provide a central location for existing program documentation referenced in the DCP and IPS. The MRF will be used by DoD personnel who need more detailed information. Both documents are needed for Milestone I, Milestone II, and Milestone III.

4.10 Policies for ECCM. Policies for ECCM shall be as specified in 4.10.1 through 4.10.6.

4.10.1 DoD ECCM Policy. An important aspect of maintaining national security and a direct concern of the SECDEF is an effective ECCM capability in the development of electronic systems. The importance of ECCM and specific guidance for ECCM incorporation into electronic systems is emphasized in DoDDIR C4600.3. The objectives of DoDDIR C4600.3 are to ensure:

a. That the necessary decisions relative to ECCM capability be made early in the system development cycle.

b. That proper consideration be given to the expected threat environment encompassing both the development cycle and the operational life of the system, the related operational need for protection and the associated increases in program cost.

c. That a conscious decision be made on the level of protection desired. In essence, this instruction provides the foundation for incorporating ECCM into radar systems.

4.10.2 SECNAV. SECNAVINST C3430.2 defines the Department of the Navy (DON) policy concerning ECCM in electronic systems. SECNAVINST C3430.2, which implements DoDDIR C4600.3, provides specific guidance for incorporating ECCM capabilities into electronic systems being developed for DON use. SECNAVINST C3430.2 stresses the need for effective ECCM hardened systems, specifies requirements to be included in acquisition program documentation, lists the responsibilities of pertinent Naval commands to ensure the incorporation of ECCM-related capabilities into new electronic systems and assess those capabilities throughout the system acquisition process.

4.10.3 CNO. The CNO prescribes and supports the incorporation of ECCM policy as a division of EW. OPNAVINST C3430.4D provides the basic guidance for the conduct of EW throughout the Navy. The importance of EW cannot be over-emphasized. As specified in OPNAVINST C3430.4D, almost every weapon system in modern warfare utilizes the EM spectrum for successful operations. Effective employment of electronic systems and subsystems determines the success of military operations. Therefore, EW must be considered a prime factor in the planning and execution of all operations involving Naval forces. The CNO is required to budget for, organize, train, and maintain EW forces and systems which will ensure the attainment of U.S. military objectives.

4.10.4 Director of Naval Intelligence (DNI). The DNI is responsible to the CNO for managing and implementing the procedures for all aspects of intelligence throughout the DON. The NIC was created to basically manage the production of Naval intelligence and the requirements for intelligence collection. The provision of threat support, a requirement for any new acquisition system, is a function of the NIC. Within NIC, the Naval intelligence Support Center (NISC) coordinates all responses to requests for threat support concerning technical matters. NISC produces a series of Soviet threat and capabilities publications which are intended to serve as the basic threat data base. NISC provides these materials directly to the requestor throughout the life cycle of a program.

4.10.4.1 Navy Field Operational Intelligence Office (NFOIO). NFOIO produces a series of Naval Warfare Publications. NFOIO has the responsibility for exploiting and evaluating special intelligence information against the existing Naval intelligence data base to provide timely operational intelligence to the Navy, the Defense Intelligence Agency and other designated recipients. Where NISC generated data will tend to describe the threat by its technical parameters, NFOIO's aim will be to describe the threat from more of an operational point of view. NFOIO assistance is probably best obtained for any of the SYSCOMS through direct liaison of the Command's Scientific and Technical Intelligence Liaison Officer (STILO) with NFOIO. NFOIO is organized into support and liaison, intelligence analysis, and ocean surveillance information divisions.

4.10.4.2 NIC. NIC and its field components are responsible for identifying and providing threat criteria, which are items for inclusion in the validation and selection process for weapon systems selection and planning. Further information on threat support criteria is specified in OPNAVINST 3811.1A. The format for requesting threat data is specified in NAVMATINST 3882.2A. Requests to the intelligence community originate within one of the SYSCOMS and are usually coordinated by the command's STILO. The STILO aids in relating information between the SYSCOMS and the intelligence community. Specific types of threat requirements and categories which must be considered for any acquisition system concerning ECCM in electronic systems are documented in DoDDIR C4600.3 and SECNAVINST C3430.2. Areas addressed include the categories of threat to be considered, development of realistic operational scenarios, resources of signals vulnerability assessment, and levels of protection commensurate with the baseline threat and the total environment in which the system will operationally exist.

4.10.5 NSG. The NSG was activated in 1968 and reports directly to the CNO. NSG is assigned overall DON responsibilities for cryptology. Besides providing support, technical guidance and supervision to the operating forces of the Navy on cryptologic matters, NSG supports and provides technical guidance for EW programs and operations. The Commander, NSG command, under the command of the CNO, will:

a. Assist program sponsors in the preparation of the OR, NDCP, and DCP to ensure that ECCM capabilities in electronics systems make hostile exploitation as difficult, time-consuming, and costly as possible.

b. As specified in the TEMP, test and evaluate the susceptibility and assess the vulnerability of EM systems to the ECM or ESM threat and recommend, as appropriate, to the Commandant of the Marine Corps (CMC) or Commander, Operational Test and Evaluation Forces (COMOPTEVFOR).

4.10.6 SYSCOMS. The systems commands, laboratories, and centers provide centralized coordination, monitoring and integration control over development, procurement and support of EW systems. As participants in the supportability review at each major decision point in the acquisition process, the SYSCOMS coordinate with NIC and NSG on the threat data; develop and specify the technical requirements on all electronic systems, including ECCM details; recommend alternatives and associated costs for the levels of ECCM protection; and coordinate T and E and manpower and training requirements of EW programs. The CNM will initiate appropriate action to identify ECCM test assets for the electronics system developed in accordance with procedures specified in SECNAVINST C3430.2. Fleet Electronic Warfare Support Group (FEWSG) and NSG services will be used to the maximum extent possible to test and evaluate the ECCM capabilities incorporated into electronics systems. T and E will occur as early as possible in the development cycle to ensure that adequate threat signal simulation and signals exploitation equipment are available to support T and E. Funds shall be provided by each project for ECCM test support to FEWSG, NSG, or other designated ECM test sites.

5. DETAILED REQUIREMENTS

5.1 Introduction to ECCM for radar systems. In order to address EW in its relationships to other systems, the terms susceptibility and vulnerability require some explanation. Susceptibility is a system characteristic which describes the degree to which a device, equipment, or weapons system will respond to an undesired source. Vulnerability is the measure of its inability to perform as a result of having been subjected to a hostile environment. Susceptibility is a system characteristic which can be exploited to the enemy's advantage or to the detriment of the system or macro-system (for example, the platform on which the system is installed), without regard to any capability to do so. Vulnerability, on the other hand, requires susceptibility, but susceptibility does not necessarily imply vulnerability. These are important distinctions. This terminology will be followed throughout this text.

5.2 ESM functions. There are many types of ESM systems, generally differentiated by function. Types are summarized in TABLE I. The classical performance functions of ESM are detection, classification, identification, location, and exploitation. Depending on the specific tactical purpose of the specific ESM system, some of these functions may be emphasized to the de-emphasis or exclusion of others. Detection (as used herein) is the receipt of a signal of sufficient amplitude to create a recognition that a signal exists. Classification is the measurement of signal characteristics and comparison with previously stored characteristics. Identification is the correlation of the measured characteristics to a specific type of emitter, platform class, specific platform, or nationality. Location is the determination of the direction of arrival of a signal (for one ESM system) or the triangulation or other means of determining geographic location (for two or more ESM systems). Exploitation is the action taken to take advantage of the information gained from the ESM. This can range from location for future use, to avoidance, jamming, deception, attack, or all possible combinations thereof. The several uses of ESM range from the strategic to the tactical; from intelligence collection to missile homing. Some of these are briefly described in 5.2.1 through 5.2.1.3 with typical receiver types for each function.

5.2.1 ELINT collection. Electronic intelligence is defined by JCS Publication 1 as technical and intelligence information derived from foreign, noncommunications, electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT. The purpose of ELINT collection is the acquisition of information on enemy or potential enemy radars and other emitters (excepting communications) for later use in recognition and location of these emitters. These are the parameters later used for the classification and identification functions specified in 5.2. ELINT receivers are generally very sensitive and can measure parameters of interest very precisely. These measurements, coupled with other intelligence sources, can provide estimates on the radar characteristics which can lead to the development of CM against that specific type of radar. ELINT can be collected by all types of platforms suitably equipped, ranging from land sites, surface ships, and submarines, to specially configured A/C and space satellites.

5.2.1.1 EL RECON. EL RECON is defined by JCP Publication 1 as the detection, identification, evaluation, and location of foreign electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. There is some amount of overlap with ELINT. EL RECON is more concerned with detecting, identifying, and locating known types of emitters for the operational commander than with detection and measurement of new signals. Thus, measurement accuracy, while important, need only be sufficient to identify already known signals. Types of platforms can be the same as ELINT platforms, but for wide area coverage, rapid or real time information gathering, and reconnaissance platform protection, high performance A/C and satellites are most appropriate.

5.2.1.2 Tactical ESM. This category covers all remaining ESM functions, including real time emitter location for immediate action; jammer set-on, ARM attack, and threat warning (TW).

5.2.2 TW receivers. TW receivers (also called RWRs and radar homing and warning (RHAWs) are carried on board tactical A/C (and possibly on small combat craft and in submarine periscopes) to provide warning of illumination by a threat radar. These receivers are generally of low sensitivity (-25 decibels referred to one milliwatt (dBm) is typical) to prevent false alarms caused by sidelobe radiation. The complexity can range from very simple visual or audio warning with quadrant DF indication, to fairly sophisticated receivers with signal processing to include signal strength, type of radar, and radar mode with priority sorting and DF.

5.2.3 IFM receivers. IFM receivers are specialized versions of crystal video receivers with, in many cases, RF preamplification to increase sensitivity. The receivers can provide a detection on a single pulse and provide an indication of RF by a cursor on a CRT (or digitally). One advantage of the IFM is the ability to detect FA radars, which are difficult to detect for narrowband superheterodyne receivers. Both crystal video and IFM receivers require special circuits to detect CW signals. IFMs are most appropriate as TW receivers.

TABLE I. ESM Types.

	ESM TYPES				
	CRYSTAL VIDEO	IFM	CHANNELIZED	SUPERHETERODYNE	COMPRESSIVE
FUNCTION:	TW (see Note)	TW LOCATION, ACQUISITION AND JAMMER SET-ON	LOCATION, ACQUISITION, AND JAMMER SET-ON ELINT AND SURVEILLANCE	LOCATION, ACQUISITION, AND JAMMER SET-ON ELINT AND SURVEILLANCE	ELINT AND SURVEILLANCE
SENSITIVITIES:	-25 dBm TO -45 dBm	-55 dBm TO -70 dBm	TYPICALLY -80 dBm	-75 dBm TO -90 dBm	
PROBABILITY OF DETECTION: (OR INTERCEPT)	HIGH THRESHOLD	MODERATE	HIGH	LOW	HIGH
COST:	LOW	MODERATE	HIGH	LOW TO MODERATE	VERY HIGH
SORTING PARAMETERS:	RF, PRF, PW, SCAN TYPE AND RATE, PRF MODULATION, SIGNAL STRENGTH, DIRECTION OF ARRIVAL				
NOTE: Threat warning					

5.2.4 Channelized receivers. Channelized receivers are essentially ganged narrowband fixed-tuned receivers providing a high probability of intercept over a frequency band. Cost is high, and accuracy of RF measurement is limited to the bandwidth of the individual receivers. These receivers are most appropriate for an ELINT system or for set-on of a superheterodyne receiver.

5.2.5 Superheterodyne receiver. The sweeping superheterodyne receiver is probably the oldest type of ESM receiver. The earliest of these were manually tuned. Later versions provided mechanical scan tuning across the limited bandwidths. Modern superheterodyne receivers are voltage tuned, which can provide for simultaneous scanning of multiple bands (each band typically being one octave in width). Advantages of the superheterodyne receivers are good RF resolution, rejection of unwanted signals, high dynamic range, and high sensitivity. Disadvantages are low probability of intercept for short duration signals and single signal processing. Superheterodyne receivers are useful for ELINT and long range intercept or area surveillance.

5.2.6 Compressive receivers. The compressive receiver provides a method to combine the high sensitivity of a superheterodyne receiver with a high probability of intercept. This is done by very rapid scanning of the frequency band(s) so that the entire band is scanned in the time of one pulse (on the order of 1 microsecond).

5.2.7 ESM parameter measurement. ESM sorting parameters will depend on the type of ESM being employed. For ELINT and signal identification purposes, the parameters and variations must be measured as precisely as possible for later analysis. For other purposes, some parameters may be used while others are either ignored or de-emphasized (for example, crystal video receivers can determine only the frequency band). Parameters of interest are specified in a through g:

a. RF and any pattern associated with change
b. PRF and any pattern
c. PWs
d. Scan type(s) and rate(s)
e. Signal strength and correlation with other parameters
f. Associated platforms
g. Direction of arrival

A special type of ESM (although not normally included in this category) is the sensor for ARMs. This weapon, designed for defense suppression, was used with success during the Vietnam War. Examples include the Shrike, the standard ARM (derived from the standard missile), and the high speed anti-radiation missile. These weapons have some peculiar characteristics which can include such factors as angle gating and PRF gating. Some of these may be used to advantage for ECCM.

5.3 ECM. ECM is defined in Section 3. ECM can be subdivided either by technique or intent. ECM will be subdivided by intent; namely, jamming and deception.

5.3.1 Electronic jamming. Electronic jamming is the primary means of disrupting force command and control systems. As such, it is both the primary focus of defensive (ECCM) effort and a primary weapon in defensive operations for self-protection and defense suppression.

5.3.2 Active jamming. Active jamming covers those portions of the JCS Publication 1 definition of electronic jamming which refers to deliberate radiation or reradiation of EM energy. This can take many forms, depending on the type of jamming transmitter and modulation involved.

5.3.3 Radar fundamentals. Before addressing the applied aspects of ECM, the radar fundamentals that have most bearing on the ECM and ECCM problem must be addressed. There are several parameters of interest, many or most of which are a result of engineering compromises. In general, these parameters are chosen to achieve the operational requirements that have been established for the particular radar. The parameters are specified in 5.3.3.1 through 5.3.3.9.

5.3.3.1 RF. The RF of a radar transmission is selected on the basis of the radar application. For a long range search radar, the RF will generally be at the low end of the allowable spectrum (100 MHz to 3000 MHz) because of the increased attenuation in weather at the higher frequencies. This has implications on antenna beamwidths and gain, since the gain is proportional to the antenna area and the square of the frequency.

5.3.3.2 Transmitted power. The transmitted power of the radar will determine the detection range of a target. Because the energy is reflected, the detection range will be a function of the inverse fourth power of the transmitted power. That is, to double the detection range by power alone, the power must be increased by a factor of 16. Effective radiated power (ERP) is the transmitted power times antenna gain.

5.3.3.3 Antenna gain and beamwidths. Antenna gain is the increase in power radiated in one direction over that of an isotropic radiator; that is, a theoretical radiator that radiates in all directions. Gain is usually expressed in dB, where dB is 10 times the logarithm of ratio of the power radiated in the direction of maximum gain to that of the theoretical isotropic radiator (gain of 1, or 0 dB). The gain is proportional to the area of the antenna reflector (in many radar applications) and the square of the RF (as addressed herein). The gain is inversely proportional to the horizontal and vertical beamwidths of the antenna, where the beamwidths are the angular widths of the radiated energy of a directional antenna. The beamwidths will define the angular resolution obtainable both horizontally and vertically. These factors will, in turn, impact on the scan rate, or the rate at which the antenna beam is shifted in direction. For long range search radars, for example, a rather narrow azimuth beamwidth is desirable for good resolution in bearing, while generally a broad vertical beamwidth is desirable. For shipboard radars, this can mitigate the effects of ship motion, and still permit scanning of a large volume of space in a comparatively short time. One special antenna vertical beamshape is the cosecant squared antenna, which is designed to return a constant level of return signal from a target to high elevation angles regardless of range. The other aspects of antenna gain versus RF tradeoff is the amount of real estate available for the antenna. Since the gain is proportional to antenna size, there is some lower limit to the RF for a given angular resolution and gain. With the exception of some types of radars (for example, CW radars) the same antenna is usually used for transmission and reception.

5.3.3.4 Antenna sidelobes. Sidelobe is the term for the angular areas of increased gain in an antenna other than that of the direction of maximum radiation (termed the mainlobe). FIGURE 6, for a representative radar antenna, illustrates the main beam and the sidelobe radiation. Sidelobes are an important factor in consideration of ECCM, since effective jamming can be done through the radar sidelobes.

5.3.3.5 Target RCS. Target RCS is a factor which provides a number corresponding to the degree to which a particular target reflects radar energy. Typical values range from one tenth of a square meter (m^2) to 100 m^2 for A/C, and up to 1 million m^2 or more, for a large ship. RCS is generally used to specify the detection range goals of any specific radar.

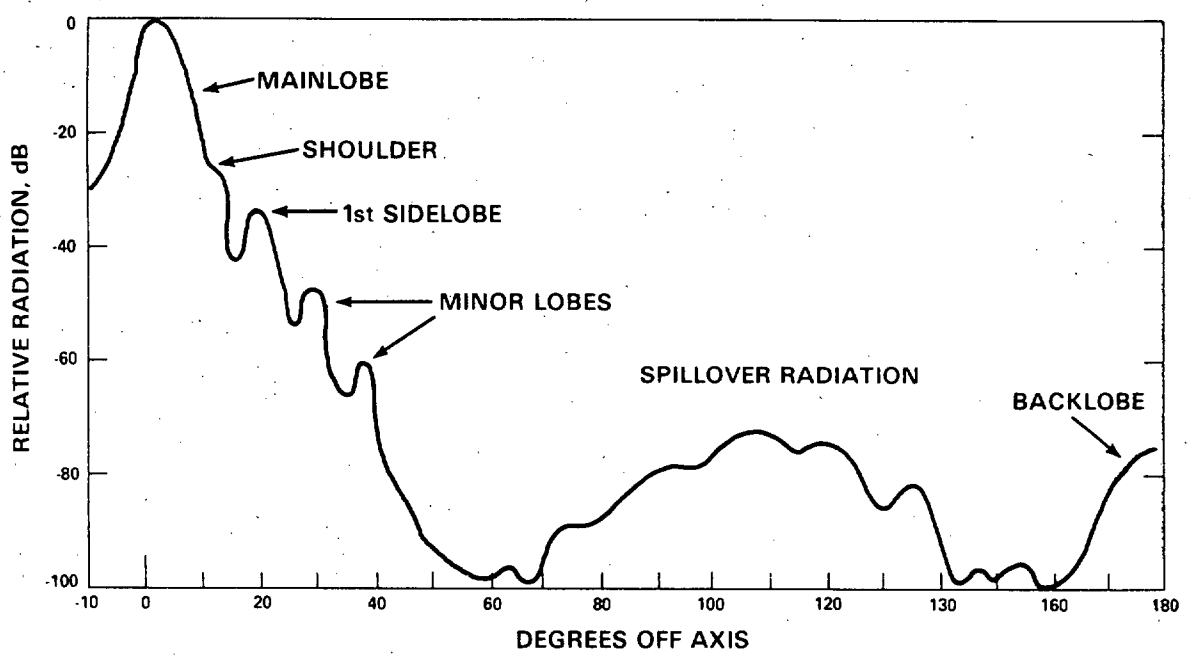


FIGURE 6. Radiation pattern for a parabolic reflector antenna illustrating the main beam and the sidelobe radiation.

5.3.3.6 Receiver noise threshold or sensitivity. The threshold of a receiver can be defined in many ways. The noise threshold is that level of unavoidable noise generated by the thermal motion of the conduction electrons in the receiver input stages. It is given by the equation:

Available thermal-noise power = kTBn

where: K = Boltzman's constant
T = Temperature, in degrees Kelvin (Standard room temperature is taken to be 290°K)
Bm = Receiver noise bandwidth (approximately equal to the 3 dB bandwidth for superheterodyne receivers)

5.3.3.7 Signal-to-noise (S/N) required. S/N required is a measure of the signal level required to give a particular probability of detection at a particular false alarm rate. S/N required is generally given in dB. For example, the single pulse (S/N) required for a 50 percent probability of detection with a 10^{-6} probability of false alarm against a typical A/C target is on the order of 13 dB.

5.3.3.8 Radar system losses. Radar system losses are all factors that result from physics and engineering compromises. As specified in Radar Systems Analysis, for a well designed radar, the losses may be 11 dB to 13 dB.

5.3.3.9 Integration improvement factor. For most radars, several pulses are received and processed for any target. This is referred to as integration improvement, and, depending on type of target and number of pulses, can result in an improvement of several dB over the S/N required for a single pulse.

5.4 Jammer characteristics. The primary characteristics of a jammer system are output power, antenna gain, bandwidth, modulation type, and scan type and rate.

5.4.1 Output power. Because of the requirement to operate over a broad band of frequencies, the output power at any specific frequency will, in general, be less than that of a radar at that frequency. The power will also relate to the instantaneous bandwidth and the type(s) of modulation employed. Because it is one way rather than reflected, the power received is proportional to the inverse square of the distance rather than the inverse fourth power as for radar.

5.4.2 Antenna gain. Since a jammer antenna is generally directed in a specific direction, antenna pointing problems will generally mandate a wider beamwidth than that of a radar, thus resulting in lower gain.

5.4.3 Jammer bandwidth. Jammer bandwidth will depend on the type of jammer and the operational use. In general, the bandwidth will be greater than that of the radar. The jamming effect is thus proportional to the ratio of the radar bandwidth to that of the jammer.

5.4.4 Jamming tactics. For noise jamming, there are three tactics of interest:

a. standoff jamming
b. escort jamming
c. self-screening jamming

5.4.4.1 Standoff jamming. Standoff jamming is a situation where typically a special purpose jamming A/C stays beyond weapons' range and provides jamming support for attacking tactical A/C. In general, the jamming will be directed against the search and acquisition radars of the target air defense system. Both mainlobe and sidelobe jamming would consequently occur. A typical geometry might be that shown in FIGURE 7. The jamming effect is proportional to the gain of the mainlobe for the mainlobe jamming or the ratio of sidelobe to mainlobe levels for sidelobe jamming, as well as the ratio of the square of the jammer range to the fourth power of the target range. A special case of standoff jamming using the same equation is stand forward jamming, which occurs when the jammer is between the radar and the target. One example of this case is the expendable jammer. This is generally battery powered and designed to operate for a limited period of time. One application is for break lock of a missile or gun fire control radar. If, for example, the missile has a HOJ mode, the expendable jammer will cause the missile to home on the jammer. Another form of expendable jammer is contained in a packet and is fired forward from ingressing A/C. The jammer is deployed in the vicinity of the victim radar and radiates for a given period of time. The lower power of an expendable jammer is acceptable in this case because of the range advantage, as may be seen in the standoff jamming equation. In this case, the jammer would be a stand forward jammer.

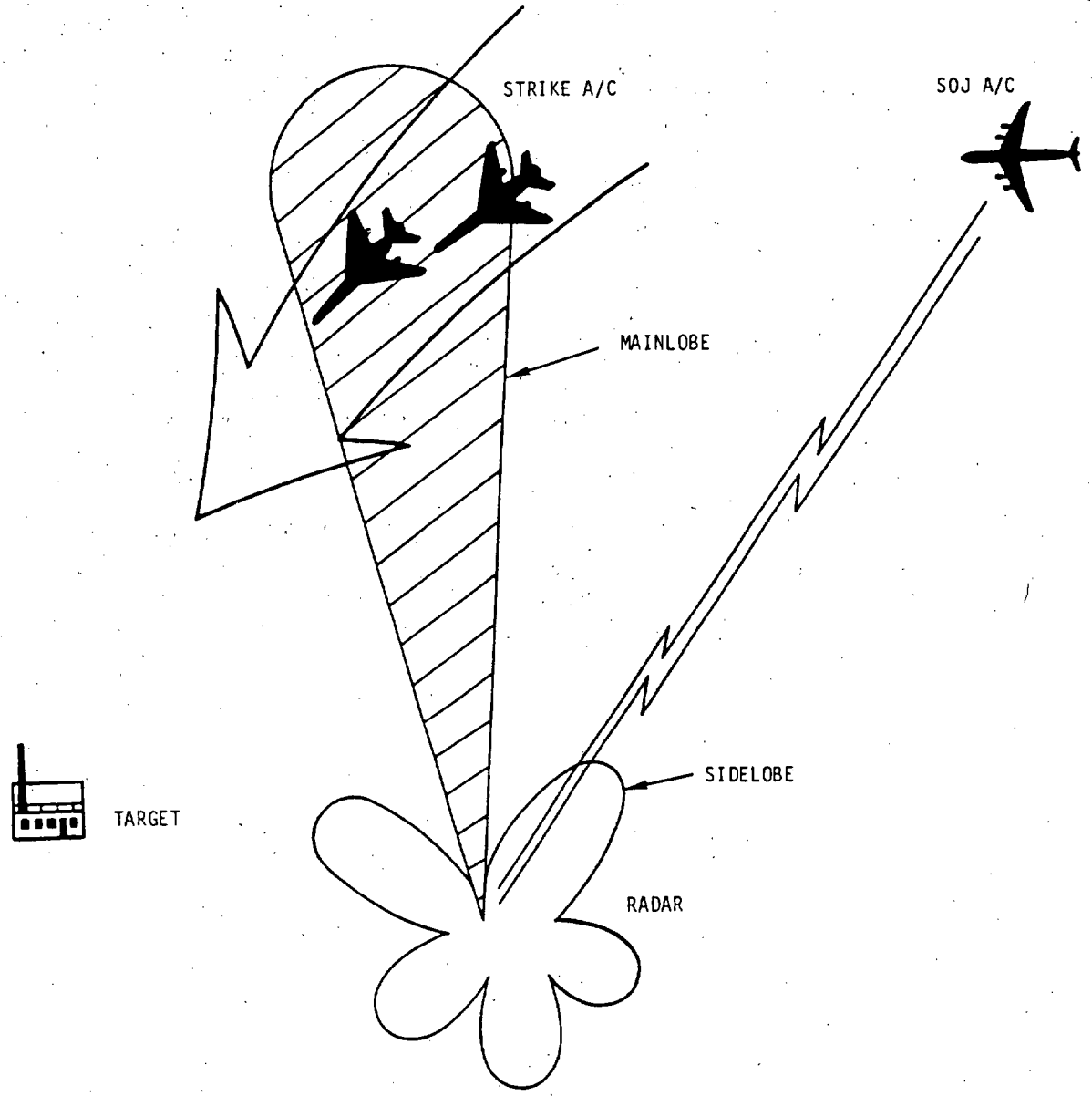


FIGURE 7. Representation of standoff jamming.

5.4.4.2 Escort jamming. Escort jamming is conducted when the attack element is accompanied by the jamming A/C. Search and acquisition radars and weapons direction radars will be jammed. The jamming is generally into the mainlobe only. Possibly both mainlobes and sidelobes will be jammed, but the main purpose of escort jamming is mainlobe jamming.

5.4.4.3 Self-screening jamming. Self-screening jamming is performed by the attack A/C. The primary targets of self-screening jamming are the weapons direction and fire control radars. Mainlobe jamming is the primary concern of self-screening jammers.

5.4.5 Jamming techniques. The three main active jamming techniques are spot, swept, and barrage jamming. Each has its advantages and limitations and will fulfill specific tactical requirements.

5.4.5.1 Barrage jamming. Barrage jamming is the generic term given to a variety of techniques for the simultaneous or near simultaneous jamming of a broad band of frequencies. This frequency band can range from 100 MHz to an octave bandwidth. The objective of barrage jamming is to jam most or all of the radars in a particular band. The advantage is that all of the target radars will be jammed. The disadvantage is that the jammer power is spread over a wide frequency range so that no single radar is jammed with high power.

5.4.5.1.1 Barrage noise techniques. As specified in Applied ECM, several techniques are classified as barrage jamming. These are briefly specified in a through g:

a. Class I - Low power source. This technique includes DINA and provides for the purest noise available. However, since noise spikes can be 10 dB, or more, above the average noise level, amplifying all noise equally would require operating at a low efficiency; thus, the noise spikes are frequently clipped which suppresses lower level noise and reduces the noise quality.

b. Class II - High power noise source. In this technique, a high power noise source is modulated in frequency by a sinewave plus noise and amplitude modulated by noise. Van Brunt states that a very effective jamming spectrum can be produced this way. However, since at least half the jammer power is carrier, the noise quality coefficient will be 0.5 or less.

c. Class III - Swept jamming. This technique uses a high power voltage controlled oscillator such as a carcinotron, frequency modulated by a fast sawtooth voltage. The frequency is caused to sweep across the entire barrage bandwidth. Further, spectral lines will appear in the receiver bandwidth at the intervals of the sweep speed. This is also called comb jamming.

d. Class IV - Swept modified. The modified swept technique uses a sawtooth frequency plus additional noise frequency and AM. This jamming signal has good noiselike characteristics.

e. Class V - Pseudo-random. For this class, a regenerative shift register is used to generate a pseudo-random sequence across the barrage bandwidth. Another term for this is digital noise. Variants of this can include sequencing at the victim radar PRF which will generate multiple false targets on the radar PPI.

f. Class VI - Pulse. This technique, also called noise cover pulse, covers the entire barrage band, but is not on all the time. The purpose is to cover the skin return of the radar target with a noise pulse, primarily to preclude range tracking.

g. Class VII - Impulse. This technique uses the high frequency content of very short pulses to cover the barrage bandwidth. Because of the short PW, amplitude must be very high to develop sufficient energy for effective jamming.

5.4.5.1.2 Barrage jammer installation. There are basically two means of combining barrage jammers for coverage of a band in practical installations. These are stacking and staggering which are shown in FIGURE 8. There are advantages and disadvantages to each as specified in a through g:

a. Assuming that the same number of jammers is available and that the same amount of jamming power would be available across the band, stacking is more reliable should one jammer go down, since the remainder can still operate although the system will be degraded by the amount of jamming power lost.

b. For stacking, there must be as many antennas in the band as there are jammers. This requires care in design and installation.

c. For stacking, each jammer has a wide bandwidth so that out-of-band power fall-off occurs only at the low and high ends of the complete jamming band.

d. Staggering permits the ECM operator greater control and interaction (if such is desired) by permitting jamming power to be directed in areas of the spectrum where radar activity is detected.

e. Staggering is more dynamic in that large transient effects can be caused in the victim radar, while stacking is of a steadier state which can possibly be more easily countered.

f. For stacking, each additional jammer contributes an additional power in the ratio (N/N-1), where N is the number of jammers after the addition. In logarithms, the total power available is:

$$P_t = \overline{P_{ji}} \cdot \frac{N!}{(N-1)!}, \text{ or, in dB,}$$

$$P_t = P_{ji} \text{ (in dBW or dBm)} + 10 \log \frac{N!}{(N-1)!}$$

where $\overline{P_{ji}}$ = mean power of individual jammer

dBW = decibels, referred to one watt

After the first two or three jammers, additional ones do not gain that much even though the space, weight, and power required for each one is a linear function of the number of jammers. In other words, to halve the burnthrough range one must quadruple the power each time (6 dB increase).

g. Noise jammer antenna patterns tend to vary with frequency as does the noise spectrum of any single jammer. Stacking thus helps fill the holes.

Probably the primary factor in the choice between staggering and stacking is the degree to which operator interaction is a feature of the jamming system. For countering threat radars for which good intelligence is available, operator interaction and control is probably more desirable. In general, barrage jamming is more likely to be used by large, standoff jamming A/C in support of bombing or missile raids by attack or bomber A/C. At sufficient altitude the radar density is likely to be such that broadband stacked jammers will be used, and the primary standoff jammer targets will be early warning two dimension (2D) and acquisition 3D radars.

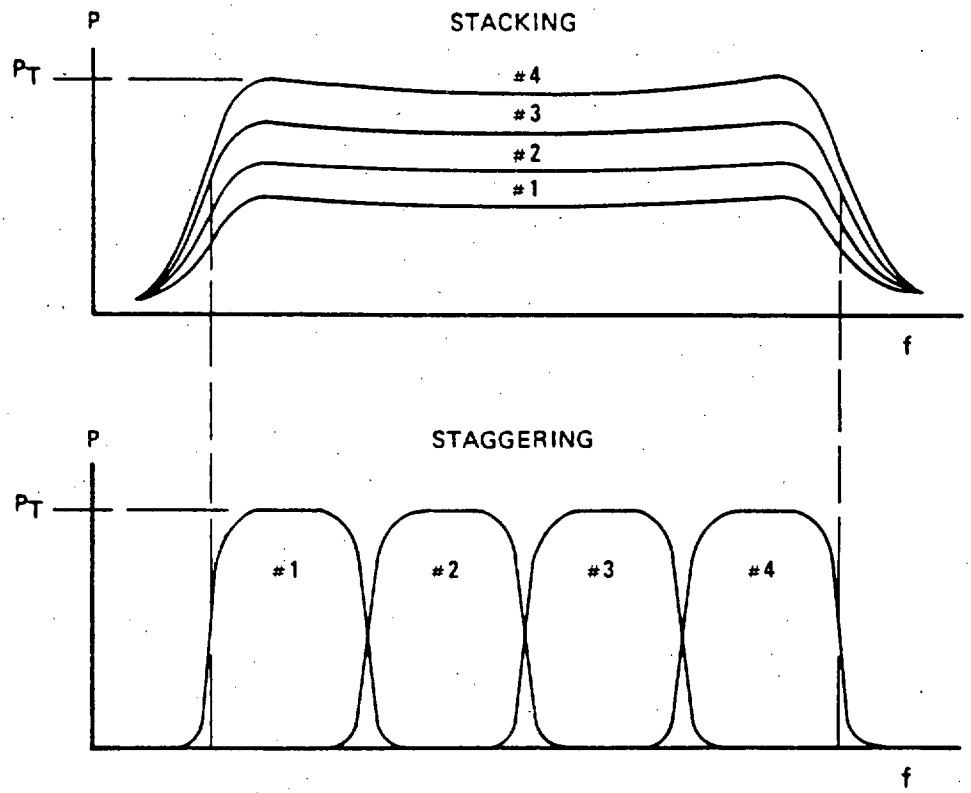


FIGURE 8. Stacking versus staggering for jamming systems.

5.4.5.2 Spot jamming. Spot jamming is a self-screening or escort jamming technique wherein the entire (or almost the entire) power of the jammer is directed within a single radar bandwidth. The advantage is that all the jammer power is concentrated into the victim radar (and alternatively, less jammer power is required). The disadvantage is that only one radar can be jammed at a time (although reradiated jamming could be considered one form of spot jamming). Spot noise jamming uses many of the same techniques specified in 5.4.5.1.1; namely, Class I, Class II, Class IV, Class V, and Class VI. Ideally, a jammer would be capable of either barrage or spot jamming as needed by bandwidth widening or narrowing. If the jammer uses a traveling wave tube amplifier, various modulation types may be used, including but not limited to noise. If good intelligence information is available on a given radar system, optimum jamming modulations and techniques can be used against that specific radar type. For this to be most effective, operator interaction or computer control, or ideally both, are required.

5.4.5.2.1 PM jamming. This technique is included under jamming although, depending on pulse rate and modulation methods, it can be considered a deception technique. PM jamming can cause many false targets to be presented to the radar operator or, if the pulse rate is high enough and no ECCM features are in use, can cause ringing in the receiver and effectively blank the PPI scope.

5.4.5.2.2 Active jamming reradiation. For this class of jamming, the signal is detected, amplified, modulation imposed (in most cases), and retransmitted in the direction from which the signal was received. In some cases (and from some modulations), this would be considered a deception jamming technique. If only a single pulse is returned for each pulse received, the jammer is called a repeater (or, for the nonECM type system, a beacon). Modulation for the returned signal can include noise or other types of modulation. As described in Applied ECM, one use of this type of jamming is where the radar has a sophisticated ECCM technique called ECM prelook FA. For this ECCM technique, the radar will have an associated receiver which can scan the frequency range of the radar tuning capability after each pulse to determine the frequency with the least jamming. The next pulse would then be transmitted on that frequency. The jamming counter is called barrage/spot noise sequence jamming. The ECM equipment would barrage jam a band with the exception of one frequency slot. When the radar, settled in that slot, the radar would be spot jammed for the duration of its dwell time.

5.4.6 Passive jamming ECM. The term passive jamming refers to those techniques which do not actively generate energy for radiation, but either reflect or absorb energy for confusing or denying information.

5.4.6.1 Reflective passive jamming. By far the most common reflective CM is chaff, which is the name given to reflective elements cut specifically to counter particular radar wave lengths. The material can be made of aluminum foil or other reflective materials, but the most common is aluminum coated fiberglass. The chaff is normally cut to about one-half wavelength of the radar frequency to be countered.

5.4.6.2 Radar cross section (RCS). RCS is normally designated by the symbol σ. For a dipole, the maximum RCS is given by:

$$\sigma m = 0.86\lambda^2; \text{ where } \lambda = \text{wavelength}$$

For randomly oriented dipoles, total available cross section is

$$\sigma = 0.17\lambda^2 N, \text{ where } N = \text{number of dipoles}$$

For a given cross sectional area, the total RCS is given by:

$$\sigma = A\,(1-e^{-Na\bar{\sigma}}),$$

where: A = the cross sectional area of the cloud
Na = number of dipoles per unit area (Na = N/A where N is the total number dipoles in the cloud)

$\bar{\sigma}$ = cross section per dipole

For the higher frequency radars, a large number of aluminum coated fiberglass dipoles can be packed in a very small space. For example, the U.S. Navy RR-129 chaff cartridge contains over one half million dipoles in a cylinder. As estimated in Radar Design Principles: at S-Band, a single pound of chaff could provide an RCS of one thousand m^2.

5.4.7 Other reflective CM. While in most cases other reflectors are used for deception or false targets, it is conceivable that other reflectors could be used for confusion masking. The most prominent reflectors are corner reflectors and lens reflectors as specified in 5.4.7.1 and 5.4.7.2.

5.4.7.1 Corner reflectors. Corner reflectors provide a means of reradiating an incident signal in the direction of arrival. The amount of reradiated energy is proportional to the angle of incidence relative to the corner reflector axis of symmetry and the area presented by the corner. Two types of corner reflectors are shown in FIGURE 9. In each of the corner reflectors shown, the 3 dB lobe width of the reflection is ±22 degrees either side of the symmetrical axis.

FIGURE 9. Types of corner reflectors.

5.4.7.2 Lens reflectors. Lens reflectors are less likely to be used than corner reflectors because they are larger, heavier, and more expensive. For the lens, the EM energy is bent by changing the dielectric constant in the lens to cause the energy to be reflected in the direction of arrival.

5.4.8 Absorptive passive ECM. The most familiar application of absorptive ECM is the well-publicized Stealth A/C. A combination of shaping and RAM is used to reduce RCS and thus reduce detection range. Another absorptive ECM would be absorptive chaff, which absorbs rather than reflects EM energy. This could be deployed ahead of the protected radar target, or could be used to break track of a tracking radar.

5.5 DECM. Electronic deception is defined in JCS Publication 1 as the deliberate radiation, reradiation, alteration, absorption, or reflection of electromagnetic radiations in a manner intended to mislead an enemy in the interpretation of data received by his electronic equipment, or to present false indications to electronic systems. The definition is sufficiently broad to incorporate a wide variety of tactics and techniques of which radar DECM is a subset. Radar DECM includes generation of false targets and decoys to a search radar as well as specific modulation techniques against generic or particular radar tracking systems.

5.5.1 Active DECM. Active DECM can range from a simple radar repeater to very complex and intelligence sensitive techniques against specific systems. As radar systems get more complex and designers and project directors are more aware of ECCM requirements, the task of the ECM designer grows more demanding; and of course, the converse is also true.

5.5.2 Active false target techniques. Many techniques exist for generating false targets. These include such techniques as pulsed spot jamming, swept barrage jamming (see 5.4.5.1.1), repeater systems with variable delays, and systems designed against sophisticated radars, including FA, chirp, and phase coded pulse types. Some of these are briefly described in 5.5.2.1 through 5.5.2.3.

5.5.2.1 FTG against chirp radars. A chirp radar provides some clutter rejection and high average power by stretching the pulse on transmit and varying the frequency of the pulse. When the pulse is received, it is again compressed to provide required resolution. The false targets generated must replicate the chirp with possibly some Doppler added. If the radar has jittered or staggered PRF, false targets generated after the time of the maximum range of the radar, but prior to arrival of the next pulse, will be decorrelated; that is, they will not occur at the same time for each succeeding pulse unless the jitter or stagger rate can be predicted. Thus, the false targets would normally occur only farther in range than the jamming platform range.

5.5.2.2 FTG versus FA radars. In general, an FA radar is one which changes the RF of transmission with each pulse. This technique can be performed either in a semirandom manner (for example, using a spin-tuned magnetron) or by a preprogrammed pattern. If the hopping is preprogrammed, a jamming system could detect the hopping pattern and follow it, generating false targets at all ranges. If randomly hopped, the false targets could only be generated farther in range than the jamming platform. This technique would only work against one radar at a time.

5.5.2.3 FTG versus phase coded pulse radars. To generate false targets against a radar using phase coded pulses, either the phase code would have to be known and generated from memory, or the phase coding would have to be detected and replicated. A currently manufactured device that could perform this is the digital RF memory, manufactured by Raytheon. The ability to duplicate the phase coding would depend on the phase code rate of the pulse and the sampling rate of the detection device.

5.5.3 Active break lock techniques. Break lock deception is primarily used against automatic tracking circuits of a missile or gun fire control radar. These techniques generate deception signals against the methods used by the radars for tracking the target.

5.5.3.1 Angle deception techniques. Angle deception techniques are used to break or prevent angle tracking by a tracking radar. Some examples of these are given in 5.5.3.1.1 through 5.5.3.1.3.

5.5.3.1.1 IG. IG is used against conical scan tracking, wherein the modulation of the conical scan is detected, reversed in phase, amplified and retransmitted to the radar, causing the antenna to slew off target.

5.5.3.1.2 Swept audio. Swept audio is used against tracking radars that use SORO techniques, wherein the modulation cannot be detected by the target ESM or repeater detector. An audio modulation swept in frequency is imposed on the detected and amplified pulses which are then retransmitted to the tracking radar. A more sophisticated version of this technique would use a jog detector to detect perturbations in the signal received from the radar antenna as the audio is swept, thus determining the most effective audio modulation frequency.

5.5.3.1.3 Crosseye. The crosseye technique uses two antennas spaced apart to return out of phase signals to the radar. A receive antenna and receiver would receive the radar signal, preserving phase. One of the transmit antennas would retransmit an in-phase signal, while the other would transmit an out-of-phase signal, thereby distorting the phase front as seen by the tracking radar antenna and receiver(s). This technique can be effective against monopulse tracking radars, which is not true of the two techniques specified in 5.5.3 and 5.5.3.1.

5.5.3.1.4 Terrain bounce. A self-screening or support technique that consists of aiming the ECM antenna in a direction other than the victim radar's direction in order to jam the victim radar. Special antennas are used that have a null in the victim radar's direction and whose main beam points at the surface between the jammer vehicle and the radar.

5.5.4 Range deception techniques. In addition to tracking in angle, tracking radars generally track in range. This prevents other targets or clutter from breaking track on the desired target. Range tracking is accomplished by gating on the radar receiver(s) at a time determined by the previous target location. In general, split gates are used, wherein an equal energy is maintained in each portion of the gate. RGWO or RGPO technique receives the radar signal, amplifies it, and retransmits to the radar slightly delayed in range. Each successive pulse is retransmitted with a greater range delay until the tracker is pulled off the target platform, whence the DECM is shut off. This can be an effective technique, especially when used in combination with other CM.

5.5.5 Velocity deception techniques. CW, pulse-Doppler, and MTI trackers can track the Doppler shift generated by a moving target. VGWO techniques generate an increasing or decreasing Doppler signal from that received by the platform. After the change in frequency, the DECM is shut off, leaving the Doppler tracker (or velocity gate) at some different frequency. This technique can be effective against missile systems which use CW illumination for missile guidance.

5.5.6 Passive DECM. Passive DECM uses chaff and other reflective techniques for deception. These techniques have both false target and break lock effects, depending on the type and usage.

5.5.6.1 Passive false target techniques. These techniques use chaff or other reflectors to create multiple false targets to saturate or confuse the radar operator or cause automatic systems to lock up on false targets. While the chaff target's Doppler spectra will approach zero after dispensing, for some applications (for example, ship protection) this is not the significant factor. For protection of A/C, a decoy with a corner or lens reflector could be launched from ingressing A/C to cause air defense resources to be expended on the decoy as well as to reveal their locations.

5.5.6.2 Passive break lock techniques. Reflectors, such as chaff, can be launched from targets being tracked to cause the tracking radar to transfer track from the target to the reflector(s). The main criteria for effectiveness are that the reflector(s) should equal or exceed the RCS of the target, and that the time response must be sufficiently rapid so the radar tracking cell contains the reflector(s) at the same time as the target. Passive break lock can be used with other techniques.

5.6 Destructive CM. Destructive CM, while not strictly included as such in JCS Publication 1, is a useful concept in highlighting the threat. As used herein, destructive CM are measures used to destroy or neutralize an EM system, for example, in defense suppression. Two means of accomplishing this are identified in 5.6.1 and 5.6.2.

5.6.1 Electromagnetic pulse (EMP). An EMP can be created by both nuclear and nonnuclear means. EMP consists of a short very high intensity voltage pulse (field strength on the order of 50 kilovolts per meter (kV/m) to 100 kV/m which can have destructive effects on electronic circuits. The frequency content is generally below E/F Band (Institute of Electrical and Electronic Engineers (IEEE) S-Band). If generated within the atmosphere by either nuclear or nonnuclear means, the range of effectiveness is fairly short. Exo-atmospheric nuclear bursts, however, can generate the field intensity everywhere within line of sight.

5.6.2 ARM. ARMs are used by attack and bomber A/C to suppress antiaircraft defenses (although one version was modified for shipboard use). Because of cost and complexity, ARMs will generally be designed to have the maximum effect by being targeted against search and acquisition radars rather than fire control radars, although it is conceivable that cheap, short range ARMs could be developed for encountering tracking radars. ARMs are, in general, targeted against specific radars by use of a narrowband receiver, gating the receiver on during the expected arrival time of the radar pulse, and limiting inputs to certain angles of arrival. Homing elevation angle is generally quite steep (40 degrees to 90 degrees) and final homing is performed by tracking on radar sidelobe energy.

5.7 ECCM. As the third subcategory of EW, ECCM is assuming increasing importance. JCS Publication 1 defines ECCM as that division of EW involving actions taken to retain effective friendly use of the EM spectrum. In modern or future systems, ECCM considerations must be also given to the susceptibility of embedded digital computers and their associated networks. Areas of concern include: the enemy may concentrate an attack on the radar system detection, acquisition, track, control, and logic algorithms and programs/software; the enemy will attempt to load up track files and memory with false targets; the digital target sorter and target identification sections may be attacked. Therefore, digital signal and data processing ECCM must be carefully considered.

5.8 ECCM and Counter-EW. Philosophically, although not included in the JCS Publication 1 definition, ECCM is related to those policies, procedures, tactics, and techniques which encompass the definition of EW as specified in 5.2. This includes ELSEC and EMCON.

ELSEC: The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from their interception and study of non-communications EM radiations, for example, radar.
EMCON: The selective control of emitted EM or acoustic energy to minimize its detection by enemy sensors or to improve the performance of installed friendly sensors.

Thus ECCM and the related categories of ELSEC and EMCON could be termed counter EW. The radar project director must address this overall need. The two categories of EMCON and ELSEC are not, however, synonymous. For example, spatially selective EMCON could be implemented (and has been in at least one system) within a selected sector (or sectors) of the radar search area. Thus, the radar could be blanked so that mainlobe detection could not occur in that sector. Alternatively, ELSEC of a radar signal could be enhanced or accomplished by designing the system so that the parameters can be varied and appear similar or identical to other types of radars. This can afford a degree of security through electronic anonymity, while not unduly restricting the surveillance capability of the host platform. While some of the ELSEC and EMCON (or ANTI-ESM) requirements are procedural and tactical rather than technical, provision must be made in radar systems for these procedures and tactics. This provision can take a number of forms; for example, the ability to start or stop radiation quickly or to sector blank would be methods of conforming to ELSEC and EMCON objectives.

5.8.1 ECCM dimensions. The other dimensions to ECCM specified in a through e relate to the method of accomplishing ECCM. A general explanation and examples of the dimensions are contained in 5.8.2 through 5.8.4.6.2.

a. Time: One example of ECCM in time is the video integrator, where received signals are inputted to a delay line, the delay time of which is equal to the PRI of the radar. If there is coincidence between a signal on two (or more in some cases) successive pulses, a detection is declared and appears on the display. This technique is useful against random pulses or noise, but can be defeated by pulse, repeater, or swept noise jamming correlated to the radar PRF.

b. Space: Probably the best examples of ECCM in space are those that relate to the radar antenna sidelobes such as sidelobe reduction, cancellation, and blanking. Sidelobe reduction also has counter-ESM benefits since sidelobes are reduced for both transmission and reception.

c. Frequency: Three examples of ECCM in frequency are FA, frequency diversity, and MTI. FA is the ability to change frequency rapidly (as rapidly as each pulse). This can limit jamming capability and discriminate against clutter (including chaff). Frequency diversity is the use of two or more different radars for the same purpose (that is, air search) to cause the jammer to spread its power to cover widely spaced frequencies, thereby reducing the power into any single radar frequency bandwidth. MTI discriminates against stationary or slow moving targets by cancelling these targets and providing detection of only targets with sufficient Doppler frequency shift to avoid cancellation.

d. Amplitude: Examples of ECCM in amplitude are limiting and log amplifiers. Limiting prevents receiver saturation by limiting the amplitude of strong input signals. Log amplifiers amplify as a function of the logarithm of the input signal so that weak signals are greatly amplified and stronger signals amplified less.

e. Structure: The structure referred to here relates to the structure of the transmitted signal, which can include pulse compression techniques (FM and pulse coding), approximations of a noise-like signal, polarization switching or circular polarization, and so forth.

5.8.2 Physical and fiscal considerations. In addition to the fixed dimensions of ECCM specified in 5.8.1, physical and fiscal considerations are important. These relate to where (within the radar) the particular ECCM techniques are used as well as the relative costs of various techniques. Physical implementation is based on the location of the principal portion of the ECCM. These can be broken down into transmitter, antenna system, receiver processor system, and operational. Additionally, the ECCM techniques must be consistent with the type and mission of the radar system. For example, radars which frequency scan in elevation are constrained to certain frequencies; therefore, FA to avoid jamming may not be consistent with this type of radar. As another example, burnthrough is a technique where a specific azimuth sector is illuminated for a comparatively long period so that many pulses will be integrated and jamming effectiveness will be reduced. However, this can also reduce the data rate from other sectors which may be undesirable.

5.8.3 Counter ESM. Counter ESM can be related to the five ECCM dimensions specified in a through e which are interrelated to some extent:

a. Time: The ESM equipment must be on and tuned to the correct frequency at the time of arrival of the emitter signal.

b. Space: The ESM equipment must be close enough to the emitter to detect the mainlobe or transmission of the emitter.

c. Frequency: The ESM equipment must cover the frequency of the emitter and have sufficient bandwidth to cover any signal excursions.

d. Amplitude: The ESM equipment must have sufficient sensitivity to detect the mainlobe or transmission of the emitter at sufficient range to perform the desired tactical task.

e. Structure: The ESM equipment must be capable of detecting the type of signal of interest. ECCM (or ELSEC) against these ESM requirements can be related to the five dimensions as well as to the tactical utilization of ESM and the specific functions that ESM must perform. TABLE I and TABLE II address specific ECCM techniques. TABLE II addresses ECCM to counter the operational functions of ESM in the five dimensions, while TABLE III specified ECCM techniques to render the ESM process less effective, and indicates the point of ECCM application to accomplish the primary objectives.

TABLE II. ECCM versus ESM tactical objectives and dimensions.

	ELINT	EL RECON	TACEW[1]			
			LOCATION	JAMMER	ARM	TW
TIME	FA PRF jitter. Variation PRF Random scan Blinking Imitation	FA Changed Pattern PRF Jitter and war reserve. Random scan, reduced radiation, imitation time blinking	FA Random scan Blinking	FA	Frequency diversity PRF jitter	Change mode PRF change agility Random scan
SPACE	Low side-lobes, Sector blanking	Low side-lobes, Sector blanking	Low side-lobes	Low side-lobes	Low side-lobes Blinking Blanking	
FREQUENCY	FA Frequency diversity (war reserve) Imitation	FA War reserve	FA Blinking	FA Frequency diversity Rapid tuning	FA EMCON	
AMPLITUDE	Low side-lobes,	Low side-lobes, LPI[2] mode sector blanking	Low side-lobes	Low side-lobes	Low side-lobes	
STRUCTURE	Use of LPI signal format. Imitation	Use of LPI signal format. Imitation	Use of LPI signal format	Noise like signal	Noise like signal	CW or noise like signal

1/ Tactical electronics warfare
2/ Low probability of intercept

TABLE III. ESM functions and primary point of ECCM implementation.

	Detect	Classify	Identify	Locate	Exploit
Transmitter	FA CHIRP CW LPI mode Noise like blinking signal	FA Variable PRF Blinking Imitation	FA War reserve modes Imitation	Blinking Frequency diversity	FA War reserve modes PRF agility Signal Format Exchange Blinking
Antenna	Low sidelobes Random scan Sector blanking	Variable scan Random scan	Variable scan Imitation	Random scan Low sidelobes	Low sidelobes Sector blanking
Operational	EMCON	Vary parameters	Vary parameters		EMCON

The main lesson to be understood from TABLE II and TABLE III is that there are several ways of limiting or denying information collectible by ESM. Each has advantages and disadvantages as it relates to operational, technical, and financial considerations. A summary is provided in TABLE IV.

TABLE IV. Generic counter ESM technique summary.

Technique	Examples	Effects	Advantages	Disadvantages
Denial	EMCON, Sector blanking, Dummy load	No ESM targets No mainlobe detection within sector. Permits testing of radar without radiation.	Denial of information may force active search. Radar data available from unblanked sector.	No radar information No radar data from sector. Added radar complexity.
Broaden parameter limits	Increase Randomness of signals.	Uncertainty as to all ESM parameters.	Increase emitter platform anonymity DF difficult, Force use of different ESM equipment.	Increase radar complexity, cost Operates in less than optimum mode(s).
Imitate other radars	War reserve modes.	Render ELINT data base unusable.	Render ELINT data base unusable	
	Imitate threat or commercial radars.	Difficulty in sorting parameters.	Easy to implement for certain radars.	Applicable only to certain mode or types, must operate in nonoptimum mode. Own forces must be informed.
Generate difficult to detect signal	Noise like signal	Appears as noise to ESM.	Nondetection	Increased complexity in transmitter signal processing.

5.8.4 ECCM versus ECM. ECCM to counter the ECM techniques of 5.4 are specified in 5.8.4.1 through 5.8.4.5.2. In addition to transmitter, antenna, and operational techniques, techniques in the receiver and signal processor are important.

5.8.4.1 ECCM against active jamming. Technical and operational techniques used to counter active jamming have the objectives specified in a through c:

a. Minimize, as far as practicable, the radar susceptibility to known, specific jamming types which can be employed against that particular radar type or class.
b. Force the enemy to expend much greater resources to counter the radar systems and to force the use of generic technique.
c. Cause the enemy to dilute efforts he employs to counter the radars.

To accomplish these goals requires not only specific ECCM techniques, but good radar design, including wide dynamic range for the receivers, larger power than the minimum required, and possibly larger antenna apertures than required as a minimum for the radar functions only. The radar must not be considered in isolation from the totality of the system of which it is a part. While a determined enemy can expend enough resources and effort to counter a single radar, the weapons or air defense system of which the radar is a component is the purpose of the radar's existence. If all components of the macrosystem are designed conservatively with attention to ECCM features, the enemy's capability and mission effectiveness are correspondingly downgraded, and the probability of mission success decreases. Many techniques which enhance ECCM effectiveness can have other beneficial effects. For example, FA not only can force the enemy to spread jamming power, but also can decorrelate sea (and possible chaff) clutter and fill in elevation nulls caused by multipath and phase cancellation. These techniques, by no means all-inclusive, are specified in terms of the dimensions and of the effects desired. The techniques specified herein are against ECM techniques specified in 5.4.4 and 5.4.5. TABLE V provides examples of ECCM techniques sorted according to the dimension of primary effect. This list is neither exhaustive nor definitive, but merely serves to highlight techniques that can perform certain ECCM functions.

TABLE V. Examples of ECCM techniques to counter active radiation jamming.

Dimension	Type of radar	ECCM technique	Jamming type countered	ECCM effect	Other effect of ECCM
Time	Search	Pulse integration	Random pulses, noise, barrage	Cancels random pulses and noise	Repeater FTG jamming not affected
	Search, track	PRF variation (includes jitter, stagger, coding)	False target jamming	False targets appear only when farther in range than jammer	Must be modified for MTI systems
	Search, track	Integration	Noise, random pulses	Only shows targets for pulses integrated over dwell time	False target jamming not affected
	Search	Random pulse blanker	Nonsynchronous pulses	Requires two synchronous pulses for detection	Requires stable PRF
	Track	Range gate	Random pulse jamming	Excludes pulse not within gate	Simple types can be countered by deception
Space	Search, track	Sidelobe reduction	Standoff or other jamming in the sidelobes	Reduces effects of sidelobes jamming	Requires unobstructed field of view in vicinity of antenna
	Search, track	Sidelobe cancellation	Sidelobe jamming, noise, pulse, and so forth	Subtracts energy received by auxiliary antenna from that of main antenna	Mainlobe still jammed; requires one loop for each jammer
	Search	Sidelobe blanking.	Pulsed jamming in sidelobes	Blanks video when sidelobe pulse received	Mainlobe still jammed; can blank target returns
	Search	DF strobe	Various	Provides line of Bearing toward jammer	Obtain direction but not range
Frequency	Search or track	FA	Spot jamming, swept jamming, narrowband jamming	Forces jammer to spread power or react on a pulse-by-pulse basis	Must modify for MTI; decorrelates clutter; fills in nulls in pattern

TABLE V. Examples of ECCM techniques to counter active radiation jamming. (Continued)

Dimension	Type of radar	ECCM technique	Jamming type countered	ECCM effect	Other effect of ECCM
	Search, track	Frequency diversity	Spot jamming, swept jamming	Jamming of one frequency ineffective	Increasd complexity
	Search, track	Prelook receiver	Spot jamming, Narrow multiband jamming; slow swept jamming	Look at Band for area of least interference for next FA pulse	More costly
	Search, track	Balanced mixer	Various	Cancels jamming signal	
Amplitude	Search, track	Increased power	Various	Increases detection range	Not most effective method
	Search, track	Power management or burnthrough	Various	Concentrates power in one sector to increase average power	Reduces data rate in other directions
	Search, track	Compressive IF amplifier	Various	Increases dynamic range to prevent receiver saturation	
	Search or track	DICKE FIX techniques	Pulse, fast sweep jamming	Limits received saturation and ringing	Susceptible to CW jamming
	Search, track	Gain control techniques	Various, depending on technique	Prevent receiver saturation	
	All	Log receive techniques.	Pulse, slow swept, CW jamming	Increase dynamic range	
	Search	CFAR techniques	Wide swept frequency jamming	Prevents receive display saturation	Weak targets not displayed
	Search	Jammer strobe	Various active ECM	Direction to jammer	

TABLE V. Examples of ECCM techniques to counter active radiation jamming. (Continued)

Dimension	Type of radar	ECCM technique	Jamming type countered	ECCM effect	Other effect of ECCM
Structure	Search, track	Pulse compression -chirp	Barrage noise, short pulse, fast sweep, random pulse	Frequency shifts during pulse; increases average power while retaining range resolution	Repeater jamming difficult; ESM requires special techniques
	Search, track	Pulse compression -phase coding	Barrage noise, short pulse, fast sweep random pulse	Phase is changed during pulse in a pattern; noncoded returns are rejected	Increases land, sea clutter, and chaff rejection; Reduces EMI between similar radars
	Search, track	Polarization techniques	Fixed polarization jammers	Can cancel or reduce effectiveness of jamming	Select most appropriate polarization
	Search, track, radar altimeter	Pseudo-noise signal	CW jamming, noise jamming	Only detects signals with same pseudo-random coding as transmitted	Difficult to detect with ESM, difficult to implement

5.8.4.2 ECCM against active jamming-reradiation. The techniques against reradiation are used to minimize the effects of the ECM reradiation techniques of 5.4.5.2.2. These ECM techniques include repeater jamming and other techniques which require the reception of the radar signal. There is a great overlap between reradiation techniques for jamming and for deception. Consequently, the deception ECCM techniques are covered in 5.8.4.1.

5.8.4.3 ECCM against passive jamming. The term passive jamming as used herein refers to techniques used to confuse, mask, or obscure the radar targets as opposed to deception techniques. There is a considerable gray area between deception and jamming for confusion, since passive techniques originally used for deception (or break lock) can serve as jamming elements after dispersal.

5.8.4.3.1 ECCM against passive jamming - chaff. In the use of ECCM against chaff jamming, the chaff may be dispensed by rockets. The chaff covers a large area, generally in corridors, and can last for several minutes to hours, depending on weather conditions. The following bomber or missile A/C fly down the previously laid corridor, trusting in the high radar reflectivity of the chaff to prevent or render difficult radar detection and tracking. ECCM techniques to discriminate against chaff primarily rely on differences between the chaff and the target. These can be differences of target type (point target versus distributed), target fluctuation (decorrelation of chaff and other echoes), and rejection of echoes with zero or small Doppler components. As with all ECCM, however, good radar design practice is mandatory, including wide receiver dynamic range to prevent saturation. TABLE VI provides examples of ECCM techniques to counter jamming that may be incorporated into the radar design.

TABLE VI. Examples of ECCM techniques to counter chaff jamming.

Dimension	Type of radar	ECCM technique	ECCM effect	Other effect of ECCM
Time	Track	Short pulse	Improves resolution. Permits discrimination of targets from chaff	Increased bandwidth required
	Track, search	Staggered PRF	Not officially ECCM but permits use of MTI while increasing minimum blind speed	May be affected by second time around clutter
	Track	Automatic range track or leading edge track	Permits track of chaff laying A/C	Requires large SNR
Space	Search	Monopinch	Provides beam sharpening effect to track point targets and eliminate distributed targets	
	Track, search	High angular resolution (narrow beamwidth)	Resolves targets from chaff, clutter	Requires larger antenna, reduced data rate
	Track	Coast	Causes range or angle tracker to continue to move in the same direction and rate	Cannot prevent break-lock if target changes course or speed
Frequency	Search, track	Multi-frequency	Combined target returns can differentiate against chaff	Also useful against active jamming of many types. May be incompatible with certain MTI
	Search, track	MTI	Discriminates against targets with no or low radial velocity. Can achieve 40 dB improvement	Incompatible with pulse-to-pulse FA
Amplitude	Search, track Search, track	CFAR techniques FA FAGC techniques	Can make chaff appear noiselike Reduces saturation	Requires FA
	All Search, track	Log techniques FTC techniques	Large dynamic range, reduces saturation Reduces saturation; discriminate targets at leading edge	 Useful only in clutter; reduces detectability otherwise

TABLE VI. Examples of ECCM techniques to counter chaff jamming. (Continued)

Dimension	Type of radar	ECCM technique	ECCM effect	Other effect of ECCM
Structure	Search, track	Pulse compression phase coded pulse	Rejects clutter by nearly the compression ratio	Requires duplication of pulse code for false jamming; reduces interference with some types of radar
	Search, track	Pulse compression -chirp	Provides gage resolution; high average power	Difficult to detect by same ECM; difficult to jam with active means
	Search, track	Circular polarization	Rejects rain, corner reflectors, some chaff	Can be jammed by any polarization jammer

5.8.4.4 ECCM against deceptive ECM. The most common DECM techniques are specified in 5.6 through 5.6.6.1. With the exception of false target deception jamming, most deception jamming is designed against tracking radars and automatic tracking circuits. The various ECCM techniques are addressed in TABLE VII and compared to the DECM type, which these techniques most likely will be targeted against.

TABLE VII. Examples of ECCM techniques to counter DECM.

Dimension	Radar type(s)	ECCM technique	DECM types countered	ECCM effect	Other effects
Time	Search, track	PRF variation	FTGs, RGPO	Only correlated false targets appear beyond jammer in range	If prestaggered, blind speed for MTI radars increases
	Search, track	Short pulse radar	Chaff breaklock and decoys, repeater or false target jammers	Improves resolution; short pulse may not trigger repeater	Requires increased bandwidth
	Track	Automatic range tracker	False targets, decoys	Tracks target in range automatically; rejects targets not within range gate	May require acceleration limiting, leading edge tracking, and so forth
	Track	Leading edge track	RGWO break lock chaff	Radar tracks leading edge of target with very narrow split gate. Jamming must respond within gate width; chaff blooms beyond gate	Requires high SNR

TABLE VII. Examples of ECCM techniques to counter DECM. (Continued)

Dimension	Radar type(s)	ECCM techniques	DECM types countered	ECCM effect	Other effects
	Track	Coast	Chaff false targets	Tracking circuits continue to track at same angle and range rate	Could cause break lock if target jinks
	Track	Acceleration limiting	RGWO (some), VGWO	Limits rate at which track gate can accelerate	
Space	Track	Monopulse	Angle deception	Tracks target on pulse by pulse basis	Simple types have high sidelobes, more complex types expensive
	Track	Conopulse (scan with compensation)	Inverse gain, swept audio	Tracks on target regardless of modulation	Complex
	Track	SORO LORO	Inverse gain	Does not present obvious modulation to generate IG signal	Can be disrupted by swept audio if approximate scan rate is known
	Search	Sidelobe blanking	False targets in sidelobes	Blanks signals greater than or equal to those in mainlobe	May blank valid targets
	Search, track	Sidelobe reduction	False targets in sidelobes	Reduces detection range of sidelobes and requires much greater ECM ERP	Requires unobstructed area around antenna
	Search, track	Sidelobe cancellation	False target in sidelobes	Cancels jamming energy from auxiliary antenna(s)	Requires one canceller or loop for each jammer Also works against noise jammers
	Track	Manually aided track	Angle deception, range deception	Operator can adjust to continue track despite DECM	

TABLE VII. Examples of ECCM techniques to counter DECM. (Continued)

Dimension	Radar type(s)	ECCM techniques	DECM types countered	ECCM effect	Other effects
	Track	Optical track capability	IG, swept audio	Tracks in angle optically	Requires clear weather or daylight; range limited
Frequency	Search, track	FA	False targets, RGPO	DECM can respond only after receipt of each pulse at a different frequency	Effective against most jammer types, clutter
	Search, track	MTI techniques	Chaff-false targets and break lock; FTG	Need Doppler for detection	Incompatible with FA peak-to-peak (p-p)
Structure	Search, track	Pulse compression by chirp or phase coding	False targets	False target must duplicate modulation of radar signal	
	Search, track	Noiselike signal	Repeater jammers	Jammer must replicate signal if detectable	

5.8.4.5 ECCM against destructive CM techniques. The two techniques of particular interest in destructive CM are EMP and ARMs.

5.8.4.5.1 ECCM against EMP. The primary ECCM against EMP is careful design and installation of the radar system. If the system operates within the frequency generation capability anticipated for EMP, there should be receiver protection by installation of a limiter before the receiver. Careful bonding and shielding is required, and, if possible, data transfer should be via fiber optic cables or well shielded and bonded cables.

5.8.4.5.2 ECCM against ARMs. A number of techniques can reduce the ARM threat against radars. In general, the project director should ensure that all detectable and analyzable parameters of the radar should be as random as possible, consistent with other requirements. These parameters can include FA, variable PRF, variable or random scan rate, sector blanking, and others. Radar parameter war reserve modes for frequency, PRF, PW, and so forth, would be extremely useful. Another useful CM would be actively radiating decoys in the vicinity of the anticipated ARM target. However, the radar must provide a means of forcing the ARM to start tracking the decoy, which implies a rapid on-off (or blinking) capability. This can be eased somewhat (as can the decoy ERP requirements) if the radar antenna has very low sidelobes, since the ARM must track on sidelobe energy during its terminal phase. Another very effective ARM CM is the ability to rapidly establish an EMCON silence condition, which refers to counter ESM and ELSEC.

6. NOTES

6.1 Subject term (keyword) listing.

Acquisition life cycle
Anti-jamming
Electromagnetic compatibility
Electronic counter-countermeasures
Electronic counter measures
Electronic intelligence
Electronic reconnaissance
Electronic warfare
Electronic warfare support measures
Jamming
Radar systems (Naval)

PLANNING AND SPECIFICATION OUTLINE

10. SCOPE

10.1 Scope. This APPENDIX provides an outline for use to incorporate ECCM into radar systems during systems acquisition.

20. APPLICABLE DOCUMENTS

This section is not applicable to this APPENDIX.

30. REQUIREMENTS

30.1 Outline application. This APPENDIX is intended to be a guide which stimulates managers' thinking about ECCM aspects and features of radar systems during ECCM planning and specification preparation.

Planning and Specification Outline

A. What type of radar system is involved?

1. Air search (2D) _____
   a. Airborne _____
   b. Surface _____
   c. Land based _____
2. Acquisition (3D) _____
3. Surface search or navigation _____
4. Gun fire or missile control _____
5. Target illumination _____

B. Do the following exist? (Yes or No)

1. The OR _____
2. The DP _____
3. The NDCP _____
4. The Type A system specification _____
5. The TEMP _____

C. Has assistance been requested or obtained from the following? (Yes or No)

1. STILO sources _____
2. NISC, NFOIO or National Security Agency (NSA) sources _____
3. NSG sources _____
4. Experts in: _____
   a. SYSCOMS _____
   b. Navy laboratories _____
   c. Industry _____

D. Questions relating to the threat
(Threat parameters or capabilities)

1. What are the jamming ECM characteristics?

a. Estimated power out effective isotropic radiated power.

(1) Peak _____ dBW

(2) Average _____ dBW

(3) Duty cycle _____ percentage

b. Anticipated ECM signal type

Modulation type(s), rates

c. Probable operating frequencies Low _____ MHz High _____ MHz

Stationary _____ MHz

Swept (limits) _____ upper _____ lower _____ MHz

d. Anticipated radiation modes (Yes or No)

Continuous _____

Burst _____

Intermittent _____

e. Estimated antenna characteristics

Gain _____ dB

3 dB beamwidths:

Vertical _____ degree

Horizontal _____ degree

Polarization _____ degree

Asst. type _____ degree

Asst. orientation _____ _____ degree

f. Platform(s) on which ECM threat is likely to be mounted _____.

g. What are threat ECM tactics or operations?

(Anticipated operational setting for ECM threat systems or platforms)

Describe anticipated threat versus radar system geometrics _____

Estimated ranges at which ECM threat will be employed

(maximum and minimum) _____ nautical miles (nmi) (for each threat)

Probable threat densities _____ (how many)

RCS of jamming platform at frequency _____.

RCS of support platform at frequency _____.

h. Expected jamming tactics (Yes or No)

Standoff _____

Escort _____

Self screening _____

Chaff corridor _____

Chaff burst _____

Decoys _____

2. What are the DECM characteristics?

a. Chaff characteristics - (frequency coverage, rope, burst, corridor)

b. DECM equipment

c. Gulls

d. Kites

Active DECM characteristics?

RGWO

RGPO

IG

VGWO

CROSSEYE

3. What are threat ESM characteristics?

a. Probable types of detection systems

Superheterodynes _____

IFMs _____

Tuned radio frequencies _____

Crystal video _____

Spectrum analyzers _____

Radiometers _____

Altitude _____

Other _____

b. Estimated system operating sensitivities of detection systems (including antenna gains and installation losses)

_____ dBm

_____ dBm

_____ dBm

_____ dBm

c. Estimated DF accuracies (at operating sensitivity listed in b).

From ships ± _____ degrees.

From A/C ± _____ degrees.

From shore site ± _____ degrees

From satellites sites ± _____ degrees.

d. Estimated location capabilities of threat (triangulation, time difference of arrival (TDOA), and so forth,) against U.S. Naval radar sources.

From multiple ships, circular error probable (CEP) _____ nmi radius σ _____ range.

From multiple A/C, CEP _____ nmi radius σ _____ range.

From multiple shore sites, CEP _____ nmi radius σ _____ range.

From multiple satellites, CEP _____ nmi radius (a function of distance off satellite track).

e. What are threat ESM tactics or operations? (Anticipated operational settings for threat ESM systems or platforms).

Describe anticipated threat versus radar system geometries and tactics _____
_____

Estimated ranges at which threat will be employed

(maximum and minimum) _____ nmi.

Platform(s) on which ESM threat is likely to be mounted _____.

E. What are the radar system parameters?

1. Operating frequencies

a. Operating frequency bands _____

b. Frequency limits _____ MHz lower _____ MHz upper, change rate

2. Signal (modulation type(s))

a. PRF(s) (limits) _____

b. PW(s) (limits) _____

c. Stagger, jitter rates _____

d. Any modulation _____

3. Scan type _____, rates _____.

4. Antenna

a. Scan rate _____

b. Scan type _____

c. Polarization _____

d. Mainlobe gain _____ dBi

e. Mainlobe beamwidth _____ degrees

f. Sidelobe _____ gain, dB.

g. Pattern type _____.

5. Peak power

a. Controllable? _____

b. Output _____ watts.

c. Power use elevation for 3D.

6. Automatic search functions?

_____

_____

7. Transmitter characteristics?

a. Pulse compression, MTI, type; coherent, number of cancellers.

b. FA limits

c. Pulse stagger

8. IFF, (Yes or No)

a. MK XII. _____

b. Secure. _____

F. What are the operational requirements and features of system?

1. Maximum operating range _____ nmi (no jamming)

2. Minimum operating range _____ nmi (maximum jamming)

3. System acquisition time _____ seconds

4. Performance in clutter _____

5. Target type and size (from specification)

a.

b.

6. Operational environment.

a. Propagation expected?

b. High density or low?

c. Training concerns?

7. Describe special operating modes, features and characteristics of system.

a. Will propagation prediction methods be used? _____

b. EMCON control features? _____

c. Are there any special receiver requirements? _____

Such as: STC, AGC, FTC, CFAR, DICKE FIX, _____

Other? _____

d. Antenna null-generation and control features? _____

Sidelobe reduction, blanking, cancellation

e. Other? _____

8. Describe interoperability concerns.

a. On radar system platform _____

(What platform(s) will system be mounted on?)

Ships _____ type _____?

A/C _____ type _____?

Shore _____

b. In task force and area-wide operations _____

c. In interservice operations

(Which radar system(s) must it be compatible with?)

Marine _____ type(s) _____ module, type(s) _____

AF _____ type(s) _____ module, type(s) _____

Coast Guard (CG) _____ type(s) _____ module, type(s) _____

Army _____ type(s) _____ module, type(s) _____

NATO _____ type(s) _____ module, type(s) _____

G. Define E^3 issues

1. EMC _____

2. EMI _____

3. EM vulnerability _____

4. EMP _____

H. Will there be special test requirements?

1. Automatic built-in test equipment (BITE) routines for an on-line check of ECCM effectiveness? _____

2. Other? _____

I. Are there special security requirements?

1. For testing the system and its ECCM features?

2. Related to the security of associated IFF?

J. Have all areas of the specification been examined to try to apprehend unrealistic or over-specified portions that may greatly increase program costs?

1. In testing prescribed for the earlier (pre-TECHEVAL or OPEVAL) stages of the development? _____

2. In making use of as much of the less-expensive ways to achieve ECCM as possible (for example, tactical procedures, propagation, and certain antenna techniques) rather than relying solely on high power methods.

3. Other? _____

K. Has a requirement to identify and request frequency allocations/assignments supporting experimentation, demonstration, development and procurement phases been specified?

Preparing Activity:
NAVY - EC

(Project EMCS-N108)

User activities:

Navy - AS, OS

U.S. GOVERNMENT PRINTING OFFICE: 1987 - 704-036/74504

(TO DETACH THIS FORM, CUT ALONG THIS LINE.)

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

(See Instructions – Reverse Side)

1. DOCUMENT NUMBER	2. DOCUMENT TITLE

3a. NAME OF SUBMITTING ORGANIZATION	4. TYPE OF ORGANIZATION *(Mark one)*
	☐ VENDOR ☐ USER ☐ MANUFACTURER ☐ OTHER *(Specify)*: _____
b. ADDRESS *(Street, City, State, ZIP Code)*	

5. PROBLEM AREAS

a. Paragraph Number and Wording:

b. Recommended Wording:

c. Reason/Rationale for Recommendation:

6. REMARKS

7a. NAME OF SUBMITTER *(Last, First, MI)* – Optional	b. WORK TELEPHONE NUMBER *(Include Area Code)* – Optional
c. MAILING ADDRESS *(Street, City, State, ZIP Code)* – Optional	8. DATE OF SUBMISSION *(YYMMDD)*

DD FORM 82 MAR 1426

PREVIOUS EDITION IS OBSOLETE.