DEPARTMENT OF THE NAVY
Office of the Chief of Naval Operations
Washington DC 20350-2000

OPNAVINST 3430.26
N6
18 January 1995

OPNAV INSTRUCTION 3430.26

From: Chief of Naval Operations
To: All Ships and Stations (less Marine Corps field addressees not having Navy personnel attached)

Subj: IMPLEMENTING INSTRUCTION FOR INFORMATION WARFARE/COMMAND AND CONTROL WARFARE (IW/C2W)

Ref: (a) DODINST TS 3600.1 of 21 Dec 92 (NOTAL)
(b) CJCS MOP 30 of 8 Mar 93 (Rev 1) (NOTAL)
(c) OPNAVINST 3430.25 of 1 Apr 94 (NOTAL)

Encl: (1) Information Warfare/Command and Control Warfare (IW/C2W) Responsibilities
(2) IW/C2W Terminology

1. Purpose. To issue implementation guidance and organizational relationships for IW/C2W.

2. Background. Reference (a) issues new Department of Defense policy on Information Warfare (IW) and directs each Service to implement IW. Reference (b) issues Joint policy and acknowledges the importance of IW/C2W. It changes "Command, Control, and Communications Countermeasures" (C3CM) to "Command and Control Warfare" (C2W), and replaces "counter-C3" and "C3-protection" with "counter-C2" and "C2-protection," respectively. It focuses C2W on warfighting and clarifies responsibilities for C2W. Chief among these are responsibilities for: Joint coordination of C2W evaluation and support; integration of C2W into exercise and operation(s) plans and orders; and ensuring C2W portions of plans are comprehensive. Reference (c) issues overall Navy policy concerning IW/C2W, assigns responsibilities within Navy, and directs implementation within its forces.

3. Discussion

a. Information Warfare is the action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems. C2W is the action taken by the military commander to realize the practical effects of IW on the battlefield. It involves both offensive and defensive aspects: It encompasses actions that deny adversary Command and Control (counter-C2), while protecting friendly Command and Control (C2-protection). As defined, C2W integrates physical destruction of enemy C2 targets, Electronic Warfare (EW), military deception, Psychological Operations (PSYOP), and Operations Security (OPSEC). Navy C2W encompasses these disciplines and uses surveillance, intelligence, communications, computers, and database management to ensure effective C2W execution. The underlying rationale for C2W evolves from the following:

(1) Military forces are highly dependent on C2 for effective application of combat power.

(2) This dependence on C2 creates an opportunity for offensive actions.

(3) Thus, relative combat power can be significantly enhanced by effective offensive C2W.

(4) Conversely, our own C2 systems can be vulnerable to like enemy actions and must be protected from such actions.

b. Effective IW/C2W can be attained through various forms of attack. The fundamental approaches to countering adversary C2 are destruction, disruption, deception, and the denial of information. Each approach or function is valid in its own right for countering adversary C2, i.e., denying information to, influencing, degrading or destroying the adversary C2 system. Maximum effectiveness of IW/C2W strategies is usually attained from the integrated employment of these methods or functions.

c. The effectiveness of counter-C2 to seize and maintain command and control dominance is highly dependent on the ability to protect the C2 of our own forces. Effective C2-protection, like counter-C2, is achieved by the integrated employment of the five C2W actions and their support elements.

d. Theater and Unified Commanders in Chief are responsible for coordination of IW/C2W at the joint force level. Combatant commanders will expect Naval forces to be manned, equipped, and trained to accomplish joint IW/C2W, as well as Naval IW/C2W.

4. Implementation. This instruction implements policy for employment of Navy resources in support of IW/C2W. It supports the development of doctrine, equipment procurement, and training of Naval forces to develop a force that can effectively conduct IW/C2W as assigned.

5. Action and Responsibilities. See enclosure (1).

6. Reserve Applicability. This instruction is applicable to the Naval Reserve.

S. R. ARTHUR
Vice Chief of Naval Operations

Distribution:
SNDL Parts 1 and 2

Chief of Naval Operations
(Code N09B34)
2000 Navy Pentagon
Washington DC 20350–2000 (287 copies)

SECNAV/OPNAV Directives Control Office
Washington Navy Yard Building 200
901 M Street SE
Washington DC 20374–5074 (60 copies)

Stocked:
Naval Aviation Supply Office
ASO Code 103
5801 Tabor Avenue
Philadelphia PA 19120–5099 (500 copies)

INFORMATION WARFARE/COMMAND AND CONTROL WARFARE (IW/C2W) RESPONSIBILITIES

1. Chief of Naval Operations

a. The Deputy Chief of Naval Operations (DCNO) (Plans, Policy and Operations) (N3/N5) will:

(1) Develop Service IW/C2W Policy, Strategy, and Operational Concepts and coordinate with the Joint Staff.

(2) Act as Navy's representative to the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS)/Joint Staff, the other Services, and other agencies regarding IW/C2W policy matters.

(3) Act as the primary point of contact for external policy boards and committees which interface with the Secretary of Defense, the Office of the Joint Chiefs of Staff, and other military Services to ensure Navy IW/C2W matters are considered in joint and combined actions.

(4) Establish and chair a Strategic Planning Cell for development and coordination of overall OPNAV IW/C2W strategy and policy.

b. The Director of Space and Electronic Warfare (N6) will:

(1) Provide overall IW/C2W development and implementation guidance.

(2) Serve as the cross platform resource sponsor for Navy IW/C2W.

(3) Establish Navy IW/C2W objectives and procedures consistent with DoD Directives, Chairman, Joint Chiefs of Staff Memorandum of Policy (CJCS MOP) 30, Joint Publications, and Navy Policy.

(4) Exercise principal staff cognizance over matters relating to Navy IW/C2W. Monitor and review Navy IW/C2W programs, doctrine, missions, and concepts of employment.

(5) Evaluate Navy's IW/C2W posture and the effectiveness of Navy IW/C2W programs and provide implementation guidance as required.

(6) In conjunction with CNO (N3/N5) keep the Joint Staff, Navy Commanders in Chief (CINCs), and other Service components informed of actions taken to correct identified IW/C2W deficiencies.

(7) Function as the point of contact on the CNO staff for assistance regarding research, development, acquisition, and emergent requirements for current and future Navy IW/C2W systems. Ensure standardization, interoperability, and compatibility with other Service's/nation's IW/C2W systems.

(8) Ensure C2 capabilities are adequate to support Unified Command requirements for the planning and conduct of IW/C2W.

(9) Serve as Navy's advocate for IW/C2W programs under development in support of planning, programming, and budgeting system (PPBS) requirements. Review applicable PPBS documentation on IW/C2W systems and provide comments/recommendations to the appropriate agency on the adequacy of those programs with respect to approved Navy IW/C2W requirements/capabilities. Coordinate PPBS documentation review with Deputy Chief of Naval Operations (N8) concerning IW/C2W systems under development.

(10) Coordinate with Navy programming activities within the framework of the PPBS to ensure Navy IW/C2W requirements are accurately reflected in the Program Objectives Memorandum (POM) submitted to the Secretary of Defense by the Secretary of the Navy.

(11) Identify to other appropriate Navy staff agencies, Commander, Naval Doctrine Command (COMNAVDOCCOM), Naval Systems Commands (NAVSYSCOMs), and Commander, Naval Security Group Command (COMNAVSECGRU) any existing or potential adverse impacts on any IW/C2W system(s) currently fielded or under development.

(12) Monitor and participate in liaison between the Services and private industry involving the exchange of information pursuant to improving Navy IW/C2W capabilities.

(13) Retain administrative control (ADCON) of the Fleet Information Warfare Center (FIWC).

(14) Serve as the advocate for Fleet CINC requirements for an IW/C2W specific opposition force.

(15) Execute presently assigned responsibilities and roles in the area of information systems security (INFOSEC).

(16) In conjunction with N3/5, review and align current OPNAV instructions to reflect approved Navy IW/C2W policy.

c. The Deputy Chief of Naval Operations (Resources, Warfare Requirements and Assessments) (N8) will:

(1) Serve as the resource and warfare requirements sponsor for Navy single platform (platform unique) IW/C2W systems.

(2) Coordinate with CNO (N6) and COMNAVDOCCOM for the initiation of long term studies concerning Navy IW/C2W capabilities, requirements, and systems.

(3) In conjunction with CNO (N6), review operational requirements and required operational capabilities dealing with Navy IW/C2W systems.

(4) Review applicable PPBS documentation of IW/C2W programs and provide comments/recommendations to CNO (N6) on the adequacy of those programs with respect to approved Navy IW/C2W requirements.

(5) Review, in coordination with CNO (N6), COMNAVSECGRU, NAVSYSCOMs, and other agencies, documents dealing with requirements for development, procurement, training, deployment, and life cycle support of applicable Navy IW/C2W systems.

(6) Review, monitor, and validate Navy IW/C2W requirements, acquisition, and programming documents to ensure alignment with the following:

(a) Appraisal results.

(b) Budget, programming, and resource realities.

(c) Defense Planning Guidance.

(d) Unified Commanders' Integrated Priorities Lists.

(e) Naval/other Services/Joint/OSD program capabilities, and issues.

(7) Act as the single resource sponsor for EW opposition force services.

d. Director of Naval Intelligence (N2) will:

(1) Act as the focal point for intelligence and threat support, including foreign material acquisition, to Navy-related IW/C2W programs/efforts and Navy's advocate for IW/C2W within the National Intelligence Community. Coordinate with National Intelligence Organizations for the satisfaction of Navy IW/C2W intelligence requirements that are beyond the purview of N2.

(2) In coordination with CNO (N6) and COMNAVSECGRU, prepare programs and training related to intelligence support of IW/C2W.

(3) Provide threat evaluation of foreign intelligence and adversary IW/C2W organizations.

(4) Plan, program, and budget adequate resources to ensure Navy intelligence and cryptologic systems implement joint and Navy C4I data standards. Coordinate the acquisition, integration, maintenance, and dissemination of intelligence and maritime databases for Navy IW/C2W systems.

(5) Develop all source intelligence indicators that will contribute to establishing Measures of Effectiveness (MOEs) for Navy IW/C2W tactics and weapons. Identify criteria, potential observables, and collection actions to measure effectiveness.

(6) Ensure all appropriate intelligence supporting IW/C2W is available to operational commanders and planners as quickly as possible in usable formats.

(7) Ensure all relevant intelligence, including data from national sources, is fully integrated into threat assessments.

(8) Coordinate with appropriate Service entities and national agencies for review of sensitive or compartmented data to ensure a coherent releasability policy to support IW/C2W operations.

(9) Review applicable National Foreign Intelligence Program (NFIP) documentation of IW/C2W programs. Provide comments/recommendations to CNO (N6) and COMNAVSECGRU, as appropriate, on how well those programs meet approved Navy IW/C2W requirements.

related matters dependents education system related to the above enume

e. The Deputy Chief of Naval Operations (Manpower and Personnel) (N1) will:

(1) Perform actions as necessary for matters under his functional responsibility to support Navy IW/C2W forces and missions.

(2) Liaise with COMNAVSECGRU as the executive agent on matters relating to IW/C2W manning.

(3) Ensure IW/C2W personnel have the proper background, expertise, and training to fulfill key IW/C2W billets.

f. The Director of Naval Training (N7) will:

(1) Provide overall policy and guidance for IW/C2W training through the Total Force Training Strategy (OPNAVINST 1500.51B) (NOTAL).

(2) Establish, issue, and update IW/C2W training and education which cross multiple resource sponsors or claimants.

(3) Coordinate the actions of OPNAV offices, Systems Commanders, and Fleet CINCs to identify and satisfy Naval and Joint schoolhouse training and education requirements.

g. The Deputy Chief of Naval Operations (Logistics) (N4) will:

(1) Coordinate with NAVSYSCOMs and COMNAVSECGRU for the life cycle support of IW/C2W systems being developed for Navy.

(2) Provide personnel to serve as members or observers of commissions, boards, advisory groups, or committees external to Navy which require representation from the DCNO (N4) for IW/C2W logistic matters.

h. Special Assistant for Naval Investigative Matters and Security (N09N) will:

(1) Assess the vulnerabilities of Navy IW/C2W facilities to sabotage and other forms of attack.

(2) Assist in preparing physical security requirements for IW/C2W facilities.

i. Director of Test and Evaluation and Technology Requirements (N091) will:

(1) Conduct research, development, and evaluation of applicable IW/C2W systems.

(2) Identify and evaluate new technologies, and advise CNO (N6/N8) and NAVSYSCOMs of capabilities which may be achievable through the application of these technologies.

j. Director of Naval Reserve (N095)/Commander, Naval Reserve Force will:

(1) Ensure the concepts of IW/C2W are fully integrated into the Naval Reserve Force.

(2) Modify those inactive duty training programs to incorporate the elements of IW/C2W.

(3) Include proficiency in IW/C2W as a measure of individual and unit readiness, where appropriate.

2. The Chief of Naval Education and Training (CNET) will:

a. Develop Naval and Joint schoolhouse IW/C2W training and education in support of existing and newly developed Naval, Joint, and combined IW/C2W doctrine.

b. Ensure IW/C2W training is incorporated into all pertinent Navy training and appropriate formal schools (e.g., Navy Service schools, Amphibious Warfare School, Naval War College, Naval Postgraduate School, etc). This training will be coordinated with COMNAVSECGRU, the Fleet Information Warfare Center (FIWC), NAVSYSCOMs, and COMNAVDOCCOM. At a minimum this training will include:

(1) Basic IW/C2W terminology/concepts/theories/doctrine.

(2) Examples of topical/potential IW/C2W threats.

(3) Navy IW/C2W capabilities.

(4) Joint Force IW/C2W capabilities.

(5) Employment of IW/C2W and IW/C2W techniques.

c. Ensure the appropriate level of pipeline training is provided to personnel enroute to IW/C2W billets.

3. The Naval Systems Command(s) (NAVSYSCOMs) will:

a. In coordination with the Director of Test and Evaluation and Technology Requirements (N091) and the Chief of Naval Research (CNR), identify and evaluate new technologies, and advise CNO (N6/N8) of IW/C2W combat capabilities which may be achievable through the application of these technologies.

b. Develop and procure applicable IW/C2W systems.

c. Ensure Navy IW/C2W systems meet approved operational requirements and capabilities, and are interoperable with other Service's/nation's IW/C2W systems.

d. Ensure inclusion of training aids, devices, and simulators in the basic development plan for Navy IW/C2W systems.

e. Ensure Naval Warfare Tactical Data Base (NWTDB) standards and component data elements are implemented in IW/C2W systems. Submit requirements to CNO (N6/N2) for changes or additions/ deletions to those standards.

f. Ensure provisions for adequate IW/C2W protect features are incorporated into Navy electronic systems under development.

g. Provide technical support and other data, as necessary, for requirements documents.

4. Commander, Naval Doctrine Command (COMNAVDOCCOM)will:

a. Serve as the primary authority for the development of Naval IW/C2W concepts and integrated Naval IW/C2W doctrine.

b. Serve as the coordinating authority for the development and evaluation of Navy Service unique IW/C2W doctrine.

c. Provide a coordinated USN/USMC naval voice in joint and combined IW/C2W doctrine development.

d. Ensure naval and joint IW/C2W doctrine are addressed in training and education curricula and in operations, exercises, and wargames.

5. Commander, Naval Security Group Command (COMNAVSECGRU) will:

a. Serve as CNO's (N6) Executive Agent (EA) for Navy IW/C2W manpower, training, and equipment requirements.

b. Review, in coordination with CNO (N6/N8), NAVSYSCOMs, and other agencies, documents dealing with the requirement for development, procurement, training, deployment, and life cycle support of Navy IW/C2W systems. Provide recommendations and inputs to CNO (N6/N8).

c. Coordinate with appropriate CNO staff to ensure operational suitability of current and future IW/C2W systems.

d. Coordinate with CNET, COMNAVDOCCOM, and FIWC to ensure IW/C2W doctrine and concepts are included in appropriate Navy training programs, and continuous and progressive IW/C2W training is provided to Navy personnel throughout their careers.

e. Review Navy training requirements for IW/C2W equipment, and coordinate with NAVSYSCOM program managers for inclusion of training aids, devices, and simulators in the basic development plan.

f. Ensure necessary training and qualifications requirements are identified and met for IW/C2W personnel in non-systems related areas (i.e., deception, PSYOPS, operations security, and EW).

g. Manage Navy IW technical analysis, vulnerability assessment, and coordinate modeling and simulation activities supporting IW applications.

h. Provide oversight/advocacy of IW/C2W officer career development.

6. The Fleet Information Warfare Center (FIWC) will:

a. Be Navy's IW Center of Excellence and will be located in the Norfolk area. The FIWC will be established by merging the present Command and Control Warfare Groups Atlantic/Pacific and the Electronic Warfare Operational Programming Facility.

b. Act as the Fleet CINC's principal agent for development of IW/C2W tactics, procedures, and training, under the operational control of Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), additional duty to Commander in Chief, U.S. Pacific Fleet (CINCPACFLT), Commander in Chief, U.S. Naval Forces Europe (CINCUSNAVEUR), and Commander, U.S. Naval Forces Central Command (COMUSNAVCENT). Deploy personnel trained in the IW/C2W disciplines of exploit, protect, and attack with appropriate

counter-C2/C-2 protect hardware and software systems to support battle group and joint task force operations.

c. Augment Commanders (including Carrier Groups, Cruiser Destroyer Groups, Amphibious Squadrons, and Amphibious Groups) as required with highly trained officer/enlisted IW/C2W staff personnel.

d. Provide deploying commanders with tailored IW/C2W training, advice, and assistance throughout all phases of predeployment.

e. Provide tailored IW/C2W training, advice, and assistance to shore support establishments as required, to include regularly scheduled assist visits.

f. Provide tailored IW/C2W training, advice, and assistance to USMC units as required, to include regularly scheduled assist visits.

g. Provide advanced IW/C2W training to seniors enroute C2WC staff billets.

h. Coordinate with CNET, COMNAVSECGRU, and the Fleet Training Groups to ensure standardization and completeness in naval IW/C2W training curricula.

i. In coordination with the Fleet CINC's, Numbered Fleet Commanders, and COMNAVDOCCOM, develop and disseminate integrated naval IW/C2W tactics, techniques, and procedures to Fleet units and shore support establishments worldwide.

j. Coordinate naval IW/C2W tactics, procedures and training with the joint centers and the other Services' IW/C2W related centers.

k. Assist commanders in exercise and operational planning, to include specialized technical IW exploit/attack/protect equipment support.

l. Maintain liaison with national agencies, other Service centers, and the Naval Information Warfare Activity (NAVINFOWARACT) to facilitate satisfaction of IW/C2W related requirements submitted by the Fleet.

m. Provide responsive operational IW/C2W information support to deploying/deployed groups and shore support establishments worldwide, as required.

n. In conjunction with CNO (N2) and appropriate intelligence centers, commands, and agencies, develop and maintain appropriate IW/C2W target set (red/gray/white) databases. In conjunction with CNO (N6), coordinate the acquisition and integration of U.S. operational (blue) C2W information into the NWTDB.

o. Provide to the CNO, Fleet CINCs, COMNAVSECGRU, and NAVSYSCOMs advice, assistance and recommendations on requirements and priorities for research and development, procurement, and training which support IW/C2W applications.

p. Validate and host the IW/C2W lessons learned data base.

q. Provide IW/C2W protect teams to support operational and shore establishments.

r. Develop and coordinate strategic planning concepts and their application to operational plans. Augment Naval Component Commanders with dedicated strategic planner support, as required.

s. When requested by CINCLANTFLT, CINCPACFLT, CINCUSNAVEUR, COMUSNAVCENT, provide qualified, trained, and properly equipped IW/C2W personnel to the Joint Commander's Staff. These personnel should be prepared to assist in the planning and execution of joint IW/C2W.

7. The Naval Information Warfare Activity (NAVINFOWARACT) will:

a. Act as CNO's principal technical agent and interface to Service and national level agencies engaged in the pursuit of information warfare technologies.

b. Conduct technical liaison with appropriate national agencies and provide resulting information warfare data/data bases to CNO (N6), COMNAVSECGRU, and the FIWC, et al.

c. Conduct and/or manage all technical partnership activities with national level agencies for technology development and IW applications and provide relevant IW data to CNO (N6), COMNAVSECGRU, FIWC, to support IW/C2W operations planning.

d. Act as the principal technical interface with FIWC for transition of IW special technical capabilities for naval and Navy-supported joint operations.

e. In accordance with current tasking, and subject to coordination responsibilities to be made explicit in a forthcoming SECNAV Instruction, act as technical agent for development and acquisition of Navy special technical capabilities supporting IW systems.

f. Conduct technical threat analysis and vulnerabilities assessment studies, develop technical requirements for, and evaluate/assess new information technologies, competitive architectures, and advanced concepts for offensive and defensive IW systems.

g. Coordinate with other Services and agencies to plan special technical operations, to include operating selected cells and detachments for Navy within other Service organizations and agencies to implement selected special technical capabilities.

h. Maintain principal on-line access and technical authority over appropriate compartmented IW related data in support of mission planning and C2 systems.

i. Provide IW technical/special technical operations support to designated naval elements.

j. Act as Navy's technical agent for appropriate simulation and modeling activities supporting IW.

k. Act as Navy's technical agent for exploitation of selected foreign material, acquired primarily in response to specific IW requirements. Provide the CNO (N2) with IW related requirements for the acquisition of foreign material.

8. The Naval Criminal Investigative Service will:

a. Assist the CNO (N2) in providing threat evaluation of foreign intelligence organization and in identifying counterintelligence requirements in support of IW/C2W.

b. Investigate incidents of computer crime in support of C2-protect.

c. Collect and disseminate threat information and conduct other counterintelligence activities in support of IW/C2W.

9. Fleet CINCs will:

a. Identify Fleet IW/C2W requirements.

b. Assess Fleet IW/C2W readiness.

c. Ensure deploying commanders are manned, trained, and equipped to conduct IW/C2W.

d. Provide FIWC with manning and training requirements for battle group IW/C2W staff augmentations.

e. Exercise operational control (OPCON) of FIWC.

f. When required, provide qualified, trained, and properly equipped IW/C2W personnel to the Joint Commander's Staff.

g. Initiate and execute a dynamic IW/C2W program.

h. Plan for and employ IW/C2W to support operations, exercises, tests, and evaluation in accordance with Navy and Joint directives.

i. Exercise and evaluate IW/C2W system performance and operational employment tactics, techniques, and procedures in Joint and Navy combat operations, operational tests, and training exercises.

j. Conduct training and operations to ensure IW/C2W tactical and procedural expertise. Identify and report training deficiencies beyond the capabilities of their command to the chain of command.

IW/C2W TERMINOLOGY

1. Information Warfare (IW). Information Warfare is the use of information in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems. Information Warfare is implemented in national military strategy by C2W.

2. Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (Joint Pub 1-02)

3. Command and Control Dominance. That degree of superiority in all aspects of command and control that permits effective friendly command and control at any given time and place while denying the same to the opposing force. (draft NWP 1-02)

4. Command and Control Warfare (C2W). The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities and to protect friendly command and control against such actions. There are two divisions within C2W:

a. Counter-C2. That division of C2W comprising measures taken to deny adversary commanders and other decisionmakers the ability to command and control their forces effectively.

b. C2-Protection. That division of C2W comprising measures taken to maintain the effectiveness of friendly C2 despite both adversary and friendly counter-C2 actions. (CJCS MOP 30; proposed for inclusion in Joint Pub 1-02)

5. Cryptology. Action taken to exploit and attack foreign communications and other electromagnetic signals, while protecting our own, for the purposes of command and control warfare, electronic warfare, signals intelligence and signals security. (Proposed NWP 1-02)

6. Electronic Warfare (EW). Military action involving: (1) The use of electromagnetic or directed energy to attack an enemy's combat capability, (2) protection of friendly combat capabilities against undesirable effects of friendly or enemy use of the electromagnetic spectrum warfare, or (3) surveillance of the electromagnetic spectrum for immediate threat recognition in support of electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. There are three divisions within electronic warfare: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES).

a. Electronic Attack (EA). That division of electronic warfare involving the use of electromagnetic or directed energy to attack personnel, facilities, and/or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. EA includes: (1) Actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and (2) employment of weapons that either use electromagnetic or directed energy as their primary destructive mechanism (lasers, particle beams) or use an enemy source of electromagnetic energy as their primary means of terminal guidance, for the purpose of damaging or destroying personnel, facilities, or equipment.

(1) Electromagnetic Jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. As used in this order, jamming includes the use of flares, chaff, and corner reflectors, since these devices radiate or reflect electromagnetic energy.

(2) Electromagnetic Deception. The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are:

(a) Manipulative Electromagnetic Deception. Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces.

(b) Simulative Electromagnetic Deception. Actions to represent friendly notional or actual capabilities to mislead hostile forces.

(c) Imitative Electromagnetic Deception. The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.

b. Electronic Protection (EP). That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability.

c. Electronic Warfare Support (ES). That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. Electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT) and electronics intelligence (ELINT). (CJCS MOP 6; proposed for inclusion in Joint Pub 1-02)

7. Emission Control (EMCON). The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security (OPSEC), detection by enemy sensors; to minimize mutual interference among friendly systems; and/or to execute a military deception plan. (Joint Pub 1-02)

8. Frequency Deconfliction. A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. (Approved for inclusion in Joint Pub 1-02)

9. Information Systems Security (INFOSEC). The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. A shorthand term recognized and widely used to denote the blending of telecommunications and automated information systems security or COMSEC and COMPUSEC.

a. Communications Security (COMSEC). Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC materials. Synonymous with telecommunications security.

b. Computer Security (COMPUSEC). Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer. Synonymous with automated information systems security.

c. Cryptosecurity. Component of communications security that results from the provision of technically sound cryptosystems and their proper use.

d. Transmission Security (TRANSEC). Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

e. Emission Security (EMSEC). Protection resulting 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 and automated information systems.

f. Compromising Emanations. Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled or otherwise processed by telecommunications or automated information system equipment. NOTE: TEMPEST is the short name referring to investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

g. Information System. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of voice and/or data, and includes software, firmware, and hardware.

10. Military Deception. Military deception is defined in CJCSI 3211.01A as being those "military actions executed to deliberately mislead foreign adversary decisionmakers causing them to take (or refrain from taking) specific actions that will benefit the originator's military objectives." There are five categories of military deception:

a. Strategic Military Deception. Military deception planned and executed by senior military commanders that are designed to influence a foreign adversary's national security policies, military strategies, and military actions in a manner that will benefit the originator's military strategies, operations, and objectives.

b. Operational Military Deception. Military deception planned and directed by operational-level commanders that are designed to influence a foreign adversary's operational-level intentions, preparations, and military actions in a manner that will benefit the originator's military operations and objectives. Operational military deceptions are planned and conducted to support campaigns and major operations.

c. Tactical Military Deception. Military deception planned and directed by tactical commanders that are designed to influence a foreign adversary's tactical intentions, preparations, and military actions in a manner that will benefit the originator's military operations and objectives. Tactical military deceptions are planned and conducted to support battles and engagements.

d. Service Military Deception. Military deception planned and executed by the Services pertaining to Service responsibilities (weapon systems, doctrine, tactics, techniques, personnel, or operations). Service military deceptions are designed to influence a foreign adversary's military capabilities in a manner that will preserve or enhance the originator's military capabilities.

e. Military Deception in support of Operations Security. Military deception planned and directed at all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away form, or provide cover for, sensitive military operations and activities conducted by the originator.

f. Counterdeception. Effort to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. (Joint Pub 1-02)

11. Nondestructive Electronic Warfare. Those EW actions, not including employment of Wartime Reserve Modes (WARM), that deny, disrupt, or deceive rather than damage or destroy. (CJCS MOP 6; proposed for inclusion in Joint Pub 1-02)

12. Operations Security. A process of analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

13. Signals Intelligence (SIGINT). A category of intelligence information comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. (Joint Pub 1-02)

a. Communications Intelligence (COMINT). Technical and intelligence information derived from foreign communications by other than the intended recipients. (Joint Pub 1-02)

b. Electronics Intelligence (ELINT). Technical and intelligence information derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (Joint Pub 1-02)

c. Foreign Instrumentation Signals Intelligence (FISINT). Technical information and intelligence information derived from the intercept of foreign instrumentation signals by other than the intended recipients. Note: Foreign instrumentation signals include, but are not limited to signals from telemetry, beaconry, electronic interrogators, tracking/fusing/arming/firing command systems, and video data links. (Approved for inclusion in Joint Pub 1-02)

14. Spectrum Management. Planning, coordinating, and managing joint use of the electromagnetic spectrum through operational, engineering, and administrative procedures, with the objective of enabling electronic systems to perform their functions in the intended environment without causing or suffering unacceptable interference. (CJCS MOP 64; proposed for inclusion in Joint Pub 1-02)