COMSCINST **3430.1**	**COG CODE** **N3/5**	DATE **8 FEB 99**

DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
WASHINGTON NAVY YARD BLDG 210
914 CHARLES MORRIS CT SE
WASHINGTON DC 20398-5540

COMSCINST 3430.1
N3/5
8 February 1999

COMSC INSTRUCTION 3430.1

Subj: IMPLEMENTING INSTRUCTION FOR INFORMATION OPERATIONS (IO)

Ref: (a) DODINST TS 3600.1 dated Dec 1992
(b) CJCS MOP 30 of 08 Mar 1993 (Rev 1)
(c) OPNAVINST 3430.25 dated 01 April 1994
(d) USTC IO Master Plan

Encl: (1) IO Terminology

1. Purpose. To issue implementation guidance and organizational relationships for Information Operations (IO).

2. Background. Reference (a) issues new Department of Defense (DOD) policy on Information Warfare (IW) and directs each service to implement IW. Reference (b) issues Joint policy and acknowledges the importance of IO. It clarifies responsibilities for IO, chief among these are responsibilities for: joint coordination of IO evaluation and support; integration of IO into exercise and operation plans and orders; ensuring IO portions of plans are comprehensive. Reference (c) promulgates overall Navy policy concerning IO, assigns responsibilities within the Navy and directs implementation within its forces. Reference (d) establishes and promulgates the U. S. Transportation Command (USTRANSCOM) vision, strategies and objectives concerning IO.

3. Discussion

a. IO involve actions taken to affect adversary information and information systems while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations and at every level of war. The goal of IO is to secure peacetime national security objectives, deter conflict, protect DOD information and information systems and to shape the future information environment.

b. Military Sealift Command (MSC) IO are conducted through information assurance (IA), computer network defense (CND), physical security, operations security (OPSEC) and communications security (COMSEC). Additionally, synchronization between offensive and defensive IO plans of supported CINCs in their areas of responsibility is essential for MSC to conduct its peacetime and wartime mission.

4. Implementation. This instruction implements policy for employment of MSC resources in support of IO.

5. Action and Responsibilities

a. The Director, Operations and Plans (N3/5) will:

(1) Develop MSC IO policy, strategy and operational concepts and coordinate with USTRANSCOM.

(2) Act as the MSC representative to USTRANSCOM, the Chief of Naval Operations (CNO), the other Services and other agencies regarding IO policy matters.

(3) Act as the primary point of contact for external policy boards and committees which interface with military services to ensure MSC IO matters are considered in joint and combined actions.

(4) Establish and chair an IO Planning Cell for development and coordination of the overall MSC IO strategy and policy.

(5) Designate an IO Officer to supervise the IO cell to ensure capabilities and activities are planned, coordinated and integrated within MSC directorates and with higher echelon, adjacent and subordinate staffs.

(6) Ensure all appropriate intelligence supporting IO 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) Ensure the incorporation of IO objectives in training exercises, emphasizing protection and defense of information and information systems. Defensive capabilities normally available should be exercised.

b. The Information Operations Officer will:

(1) Supervise the IO Planning Cell to ensure capabilities and activities are planned, coordinated and integrated within the joint force staff and with higher echelon, adjacent, subordinate and multinational staffs.

(2) Represent IO concerns at critical planning meetings, lead the IO Planning Cell and/or directly facilitate coordination between the components or staff organizations responsible for planning and execution of IO.

(3) Serve as the central point of contact for IO and coordinate all IO functional areas.

(4) Ensure deconfliction and unity of effort for information activities within MSC.

(5) The IO officer normally ensures the following functions are performed:

(a) Establishing IO priorities to accomplish planned objectives.

(b) Determining the availability of IO resources to carry out IO plans.

(c) Consolidated tasking ensures efficiency of effort in planning and executing integrated IO.

(d) Coordinating the N3/5 planning and execution of IO within MSC staff elements (including Area Commands) responsible for each element of IO.

c. The IO Planning Cell

(1) The IO Planning Cell is formed from select representatives from each staff element, component and supporting agencies responsible for integrating capabilities and related activities. This cell merges capabilities and related activities into a synergistic plan. Representation in the IO Planning Cell will consist of, but is not limited to, members from the following directorates: Operations and Plans (N3/5), C4S (N6) and Public Affairs (N00P) as follows:

(a) The IO Officer will chair the IO Planning Cell and will coordinate integration of IO with Command Center operations, serve as primary integrator of IO into exercises, ensure resulting lessons learned are incorporated into the Joint Universal Lessons Learned System, coordinate collection requirements and analytical support for compartmented and non-compartmented IO, integrate IO into the deliberate planning process, coordinate OPSEC activities and military deception planning and provide policy advice as appropriate.

(b) N6 representatives facilitate IA coordination between information system planners and managers and members of the IO cells, serve as the principal liaison with USTRANSCOM Defensive Information Operations Center (DIOC) and Navy IO technical managers and coordinate information system support to the IO cell.

(c) N00P Representative coordinates and deconflicts PA activities with planned IO.

(2) The Information Operations Planning Cell will:

(a) Develop and promulgate IO guidance.

(b) Serve as the focal point for IO planning, to include coordination, integration and deconfliction.

(c) Exchange information with cell members about plans in development, focusing on integration and deconfliction of capabilities to accomplish mission objectives.

(d) Provide a forum to coordinate, integrate and deconflict IO within MSC.

(e) Provide the overall integration strategy for IO and ensure capabilities are integrated.

1. The IO cell normally has the assigned personnel, communications linkages, and connectivity with N6 and defensive IO providers to effectively integrate defensive IO planning.

2. The IO cell also maintains connectivity with other government organizations and activities such as USTRANSCOM, CNO, NSA, DIA and DISA, who have a distinct role in defensive IO.

d. The C4S Director (N6) will:

(1) Provide overall technical and systems-oriented IO implementation and guidance.

(2) Establish MSC IO technical objectives and procedures consistent with DOD directives, USTRANSCOM objectives, Navy policy and the MSC common operating environment.

(3) Exercise principal staff technical cognizance over matters relating to MSC IO. Monitor and review MSC IO programs, doctrine, missions and concepts of employment.

(4) Evaluate MSC's IO technical and C4S posture and the effectiveness of Navy and USTRANSCOM IO programs and provide guidance as required.

(5) In conjunction with N3/5, keep USTRANSCOM, CNO, CINCs and other Service components informed of actions taken to correct identified MSC IO technical deficiencies.

(6) Function as the point of contact for assistance regarding research, development, acquisition and emergent requirements for current and future MSC IO systems. Ensure standardization, interoperability and compatibility with USTRANSCOM, Navy and other services' IO systems.

(7) Ensure C2 defensive capabilities are adequate to support unified command requirements for the planning and conduct of IO.

(8) Serve as the MSC technical advocate for IO programs under development in support of planning, programming and budgeting system (PPBS) requirements. Review applicable PPBS documentation on IO systems and provide comments/recommendations to the appropriate agency on the adequacy of those programs with respect to approved Navy and USTRANSCOM IO requirements/capabilities. Coordinate PPBS documentation review with Deputy Chief of Naval Operations (N6) and USTRANSCOM (TCJ6) concerning IO systems under development.

(9) Coordinate with Navy and USTRANSCOM programming activities within the framework of the PPBS to ensure MSC IO requirements are accurately reflected in the Program Objectives Memorandum (POM) submitted to the Secretary of Defense by the Secretary of the Navy and USTRANSCOM.

(10) Identify to other appropriate USTRANSCOM and Navy staff agencies, NAVDOCCOM, NAVSYSCOMs and NAVSECGRU any existing or potential adverse impacts on any IO system(s) currently fielded or under development.

(11) Monitor and participate in liaison between USTRANSCOM, Navy and private industry involving the exchange of information pursuant to improving MSC IO capabilities.

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

(13) Provide a representative to serve on the IO Planning Cell.

e. The Public Affairs Officer (N00P) will:

(1) Ensure compliance of the MSC public web site with applicable USTRANSCOM and Navy display and presentation guidelines and regulations.

(2) Expedite the flow of accurate and timely information to internal and external audiences.

(3) Create an awareness of the MSC military goals during a campaign or operation.

(4) Satisfy the desires of the internal and external audiences to be kept informed about the MSC involvement in the campaign or operation.

(5) Inform internal and external audiences of significant developments affecting them.

(6) Provide a representative to serve on the IO Planning Cell.

f. Area Commanders will establish appropriate IO Planning Cells to respond to taskings as required from the COMSC IO Planning Cell.

g. Program Managers will coordinate shipboard related actions as required by taskings initiated by the COMSC IO Planning Cell.

6. IO Terminology. See enclosure (1).

JOHN J. BEPKO, III
Deputy Commander

Distribution:
COMSCINST 5000.19
List I (Case A, B, C)
SNDL 41B (MSC Area Commanders)

IO TERMINOLOGY

1. Information Warfare (IW). Information Warfare is the use of information in support of national security strategy to rapidly 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. (Proposed 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 decision makers 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 purpose 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 disclosed 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 decision makers causing then 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)