



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, DC 20350-2000

OPNAVINST 3430.26A  
N2/N6  
30 Aug 2013

OPNAV INSTRUCTION 3430.26A

From: Chief of Naval Operations

Subj: NAVY INFORMATION OPERATIONS

Ref: (a) Joint Publication 3-13, Information Operations, November 2012  
(b) Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, March 2012  
(c) OPNAVINST C3501.2K (NOTAL)  
(d) SecDef Memo 12401-10, Strategic Communication and Information Operations in the DoD of 25 Jan 2011  
(e) DoD Directive 3600.01 of 2 May 2013  
(f) DHE-M 3301.001, Jan 2009 (SECRET/NOFORN) (NOTAL)

1. Purpose. To update the guidance and organizational relationships for Navy information operations (IO) (formerly information warfare command and control warfare).
2. Cancellation. OPNAVINST 3430.26 and OPNAVINST 3430.25.
3. Background. This revision provides updated terminology, concepts, and guidance for IO due, in part, to the removal of information warfare as a mission area from references (a) and (b), and command and control warfare as a mission area from reference (c). Per reference (d), IO is defined as the integrated employment, during military operations, of information-related capabilities (IRC) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting the nation's own. Per reference (e), these IRCs include a variety of technical and non-technical activities that intersect the traditional areas of computer network operations, electronic warfare (EW), military deception (MILDEC), military information support operations (MISO) and operations security (OPSEC).

4. Responsibilities

a. The Chief of Naval Operations shall advise the Chairman of the Joint Chiefs of Staff concerning U.S. Navy support to joint IO matters.

b. The Deputy Chief of Naval Operations for Information Dominance (CNO (N2/N6)) shall:

(1) Develop Navy IO policy and strategy and coordinate with the Joint Staff (JS).

(2) Act as the Navy representative to the Office of the Secretary of Defense (OSD), the JS, other Services, policy boards and committees, and other military and civilian agencies regarding IO, and ensure Navy IO matters are considered in joint and combined actions.

(3) Monitor and review Navy IO-related activities and programs, doctrine, missions, and concepts of employment for their consistency with Department of Defense (DoD) directives, JS publications, and Navy policy.

(4) Ensure Navy IRCs are adequate to support unified command IO requirements.

(5) In conjunction with Deputy Chief of Naval Operations for Operations, Plans, and Strategy (CNO (N3/N5)), keep the JS, combatant commanders (CCDR), fleet commanders, and other Service components informed of Navy actions to develop IRCs and systems.

(6) Function as the Office of the Chief of Naval Operations (OPNAV) point of contact regarding research, development, acquisition, and emergent requirements for current and future Navy IO systems. Ensure standardization, interoperability, and compatibility with other Service and national IO systems.

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

(8) Serve as the resource sponsor for all Navy IO programs.

(9) Direct Fleet Cyber Command/Commander 10th Fleet (FLTCYBERCOM/COMTENTHFLT) to transition and integrate select IO developmental efforts into Navy programs of record (POR) in close coordination with Navy systems commands (SYSCOM).

(10) Ensure Navy IO requirements are accurately reflected in the program objectives memorandum submitted to the OSD by the Secretary of the Navy (SECNAV).

(11) Liaise with other Services, unified commands, JS Global Operations (J39), private industry, and other appropriate organizations regarding Navy-related IO staffing, training, education, and processes to improve Navy IRCs.

(12) Act as the focal point for intelligence and threat support, including foreign material acquisition, to Navy-related IO programs and efforts.

(13) Coordinate with FLTCYBERCOM/COMTENTHFLT, Navy IO executive agent, on all IO related matters.

(14) Ensure Navy IO personnel are trained and educated to support standards established in joint IO policy and DoD IO workforce requirements.

(15) Provide overall policy and guidance for IO manpower and training which crosses multiple resource sponsors or claimants.

(16) Coordinate with OPNAV, SYSCOMs, and fleet commanders to identify and satisfy Navy and joint schoolhouse IO training and education requirements.

c. The Deputy Chief of Naval Operations for Warfare Systems (CNO (N9)) shall support CNO (N2/N6) to:

(1) Review IO-related operational requirements and required operational capabilities.

(2) Ensure appropriate capabilities are developed and integrated into Navy systems to meet Navy IO-related operational requirements.

(3) Review applicable IO programs to provide comments and recommendations to CNO (N2/N6) on the adequacy of those programs with respect to approved Navy IO requirements.

d. Fleet commanders shall:

(1) Identify and submit fleet IO requirements to meet CCDR objectives.

(2) Prepare for and employ IO to support exercises, tests, evaluations, and operations per Navy and joint directives.

e. FLTCYBERCOM/COMTENTHFLT shall:

(1) Serve as CNO (N2/N6) executive agent for Navy IO.

(2) Evaluate Navy's ability to integrate IO capabilities into plans at the joint force commander and joint force maritime CCDR staff-level and submit recommendations for program improvement to Naval Warfare Development Command (NAVWARDEVCOM) and U.S. Fleet Forces Command.

(3) In coordination with CNO (N2/N6), SYSCOMs, and other agencies, review documents dealing with the requirement for development, procurement, training, and life cycle support of Navy equipment that supports IO. Provide recommendations and inputs to CNO (N2/N6).

(4) Coordinate with CNO (N2/N6) to ensure operational suitability of current and future equipment that supports IO.

(5) Coordinate with NAVWARDEVCOM to ensure IO doctrine and concepts are included in appropriate Navy training programs, and that continuous and progressive IO training is provided to Navy personnel throughout their careers.

(6) Review Navy training requirements for equipment that supports IO. Coordinate with SYSCOM program managers for inclusion of training aids, devices, and simulators in the basic development plan.

(7) Ensure necessary training and qualification requirements are identified and met in conjunction with CNO (N2/N6) at subordinate commands for IO personnel in computer network operations, EW, MILDEC, MISO, and OPSEC.

(8) Manage Navy IO technical analysis and vulnerability assessment. Coordinate modeling and simulation activities supporting IO applications, such as use of the IO and information assurance ranges.

f. Consistent with SECNAV direction, SYSCOMs will:

(1) Identify and evaluate new technologies, and advise CNO (N2/N6) of IO combat capabilities which may be achievable through the application of these technologies.

(2) Ensure Navy IRCs and related systems meet approved operational requirements and capabilities and are interoperable with other Service and Navy IRCs, and related systems.

(3) Ensure inclusion of training aids, devices, and simulators in the basic development plan for Navy IRCs and related systems.

(4) Provide IO technical support and other data, as necessary, for requirements documents.

(5) Support transition and integration of select IO developmental efforts into Navy PORs.

g. Navy Cyber Forces (NAVCYBERFOR) will:

(1) In coordination with OPNAV and fleet commanders, ensure Navy IO training, manpower, and equipment supports fleet requirements.

(2) Track and report individual training readiness in support of fleet commanders and FLTCYBERCOM/COMTENTHFLT.

h. NAVWARDEVCOM shall:

(1) Serve as primary Navy IO concept and doctrine development authority.

(2) Provide authoritative Navy position during joint and combined IO doctrine development.

i. Navy Information Operations Command (NAVIOCOM) Norfolk shall:

(1) Serve as Navy's primary IO-related doctrine review authority.

(2) Act as the fleet commander's principal agent for development of Navy IO tactics, techniques, and procedures (TTP) and concept of operations.

(3) Coordinate Navy IO TTPs with joint IO organizations and other Service IO elements.

(4) Augment operational staffs with trained IO personnel and specialized IO equipment as required for specific missions.

(5) Provide tailored IO training, advice, and assistance to fleet commanders who are planning, executing, or supporting joint IO.

(6) Assist commanders in IO exercise and operational planning.

(7) Provide IO training to officers en route to staff IO billets.

(8) Provide their chain of command with advice, assistance, and recommendations on requirements and priorities for research and development, procurement, and training that supports IO applications.

(9) Develop and coordinate operational plans and applications from strategic IO planning concepts.

j. Navy Cyber Warfare Development Group shall:

(1) Develop and acquire Navy special technical capabilities for IO missions.

(2) Conduct and manage all technical partnership activities with national-level agencies for technology development and applications to support Navy IO capabilities.

(3) Act as principal technical interface with NAVIOPCOM Norfolk for the fleet's transition to Navy IO special technical capabilities and Navy-sponsored IO systems.

(4) Coordinate with Naval Criminal Investigation Service (NCIS) and the Office of Naval Intelligence (ONI) to conduct technical threat analysis and vulnerabilities assessment studies; develop technical requirements; and evaluate and assess new IO technologies, competitive architectures, and advanced concepts for offensive and defensive IO systems.

(5) Maintain principal on-line access and technical authority over appropriate compartmented IO related data in support of mission planning and C2 systems.

(6) Provide IO technical and special technical operations support to designated Navy elements.

(7) Act as Navy's technical experts for operational simulation and modeling activities supporting IO.

(8) Act as Navy's technical experts, in coordination with ONI, for exploitation of selected foreign material acquired primarily in response to specific IO requirements.

k. Naval Education and Training Command shall:

(1) Develop and deliver IO training and education solutions for naval and joint schoolhouses to meet validated and resourced requirements, as determined by CNO (N2/N6).

(2) Support FLTCYBERCOM/COMTENTHFLT, NAVCYBERFOR, SYSCOMs, NAVWARDEVCOM, and NAVIOPCOM Norfolk to ensure that validated and resourced training requirements are incorporated into pertinent Navy training courses and appropriate formal schools.

(3) Coordinate and facilitate human performance requirements reviews to revalidate IO training course requirements as required.

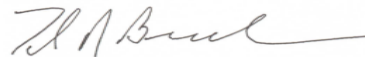
1. Consistent with SECNAV direction, NCIS will:

(1) Prepare finished intelligence that characterizes threats posed to Navy IO programs and capabilities per the Naval Intelligence Program of Analysis and in coordination with ONI.

(2) Investigate incidents of computer and cyberspace intrusion in support of IO operations and conduct other counterintelligence activities in support of IO.

(3) In coordination with ONI, collect and disseminate intelligence affecting Navy IO capabilities and programs per reference (f).

5. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 January 2012.



TED N. BRANCH  
Deputy Chief of Naval Operations  
(Information Dominance)

Distribution:

Electronic only, via Department of the Navy Issuances Web site  
<http://doni.documentservices.dla.mil/>