REVISION ONE

Department of Defense
DIRECTIVE

October #, 2001
Number 3600.1

ASD(C3I)

SUBJECT: Information Operations (IO)

References: (a). DoD Directive S-3600.1, "Information Operations (U)," December 9, 1996 (hereby canceled)
(b). DoD Instruction S-3600.2, "Information Operations Security Classification Guidance (U)," August 6, 1998

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update Information Operations policy, definition, and responsibilities within the Department of Defense (DoD).

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the DoD, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as “the DoD Components”).

C. DEFINITIONS

1. Information Operations (IO). Actions taken to affect adversary information, information systems and decision making, while defending one's own information, information systems and decision making.

2. All other terms used in this Directive are defined in the enclosure.

D. POLICY

1. The DoD supports the national security strategy and national objectives through the accomplishment of a variety of missions that range the spectrum of military operations, from peace to war. In peacetime the DoD conducts activities to accomplish these missions and shape the international environment. In conflict, as in peacetime, information superiority enables the DoD to direct the full power of Information Age concepts and technologies; transforming capabilities for maneuver, strike, logistics, protection and situation awareness into full spectrum dominance.

a. A primary focus of IO (defensively and offensively) is ultimately on decision-makers; the information they acquire and use to make decisions, the information they generate in making decisions and the full range of systems and organizations involved in handling, processing and implementing this information. IO may also be used to effect the automated component of a weapon system.

b. IO, conducted as an integral element of land, sea, air, space, special and joint operations, contributes to information superiority by protecting military decision-making from adversary attacks and as necessary degrades an adversary's decision-making, thereby producing a relative information advantage.

(1) One set of IO activities employed by the DoD Components focuses on the perceptions and attitudes of decision-makers or groups.

(2) A second set of IO activities also employed by the DoD Components focuses on attacking or defending the electromagnetic spectrum, information systems, and information which supports decision makers, command and control and automated responses.

c. The DoD's activities to conduct IO include psychological operations (PSYOP), electronic warfare (EW) (including directed energy), computer network operations (CNO), information assurance (IA), military deception, security, and counterintelligence.

2. IO exploits the opportunities and vulnerabilities inherent in dependence on information supporting military activities. Therefore, IO will be considered by DoD components when developing policy, doctrine, and capabilities (to include the full range of responsibilities to train and equip forces from acquisition through maintenance and sustainment) as well as the planning and execution of operations.

3. Public affairs (PA) and civil affairs (CA) represent related activities which, like IO, can contribute to achieving a commander's overall objectives in shaping the information environment.

a. The intent of PA is to truthfully inform the public and thus shall not focus on directing or manipulating public actions or opinion. As such, PA can be useful as a counter to adversary propaganda and disinformation. DoD components must ensure PA offices are aware of the military objective and ensure mutually supporting efforts.

b. CA activities support DoD informational objectives by influencing, developing, or controlling indigenous infrastructures in foreign operational areas, and can be an alternate means to communicate with the host nation and foreign public.

4. DoD shall integrate IO into theater engagement strategies and campaign plans to support national policy and strategy**.**

5. DoD shall coordinate with other USG agencies, as appropriate, DoD engagement strategies and the employment of IO.

6. DoD shall ensure intelligence supports an array of DoD IO requirements, to include indications and warning, research, development and acquisition and operational support. Detailed intelligence on the information systems, decision-making processes, and human factors is required.

7. To facilitate efficient development of IO capabilities, the DoD Components shall share tactics, techniques, procedures and technologies to the maximum extent practicable.

8. DoD shall develop and conduct education, training and exercise programs to ensure the successful planning and execution of IO.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) shall:

a. Serve as the principal staff assistant to the Secretary of Defense for IO.

b. Provide overarching strategy, policy and guidance for the development and integration of capabilities to conduct IO.

c. Conduct oversight of the DoD Component’s efforts to plan, program, and develop capabilities in support of validated IO capability requirements.

d. Serve as the DoD proponent for the Information Operations Technology Center.

e. In coordination with Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), support and guide science and technology efforts to develop IO capabilities.

f. Lead interagency coordination and allied cooperation concerning intelligence support, information assurance, counterintelligence, security and the development of IO related capabilities.

g. Support Under Secretary of Defense for Policy (USD(P)), in reviewing IO aspects of CINC OPLANS and Theater Engagement Plans.

h. Coordinate with USD(P) on IO matters that pertain to PSYOP, military deception or International Public Information.

i. Coordinate with USD(AT&L) when IO matters pertain to acquisition issues, EW or special programs.

j. Require the Director, Defense Security Information Agency to:

(1) Serve as the DoD focal point to oversee the application of information assurance (IA) for the Global Information Grid.

(2) Plan, develop, coordinate, and support IA activity to protect and maintain automated information systems (including the command, control, communications, and computer systems) which serve the needs of the National Command Authority.

k. Require the Director, Defense Intelligence Agency to:

(1) Manage DoD intelligence community’s all-source production to support the full range of DoD IO intelligence requirements.

(2) Oversee IO intelligence requirements, and serve as the DoD intelligence community focal point, for development, management, and maintenance of information systems and databases which facilitate timely collection, processing, and dissemination of all-source, finished intelligence for DoD IO.

(3) Coordinate with the DoD Components to support the development of IO capabilities.

(4) Provide political-military assessments to support the full range of IO, including the validation of IO threats.

(5) Provide human factors intelligence support, and integrate human factors analysis with U.S. Special Operations Command (USSOCOM) to support and leverage the capabilities of the PSYOP components.

2. The USD(AT&L) shall:

a. Coordinate with ASD(C3I) when developing policy and conducting oversight that pertains to EW or other IO related activities.

b. Consider IO threats in the review and approval of acquisition programs.

c. Ensure that adequate science and technology programs exist to support the development of IO capabilities.

d. As the proponent for EW, develop and maintain a technology investment strategy to support the development and integration of EW capabilities.

3. The USD(P) shall:

a. As the principal staff assistant to the Secretary of Defense for policy, strategy and review of operational plans, provide policy guidance and oversight of the DoD Component’s employment of offensive IO capabilities, PSYOP and International Public Information.

b. Lead interagency discussions and coordination as well as international cooperation and dialog concerning the employment of IO.

4. The DoD General Counsel shall provide legal advice and assistance to the Secretary of Defense and other DoD officials on IO plans and capabilities employed.

5. The Secretaries of the Military Departments and the Commander in Chief, USSOCOM (within their respective U.S. Title X and Major Force Program 11 responsibilities respectively) shall develop IO doctrine and tactics; and organize, train and equip to ensure that IO become effective elements of, and integral to, U.S. military capabilities.

6. The Chairman of the Joint Chiefs of Staff shall:

a. Serve as the principal military advisor to the Secretary of Defense on IO.

b. Validate IO requirements through the Joint Requirements Oversight Council.

c. Establish doctrine to facilitate the integration of IO concepts into joint operations. Ensure all U.S. military plans and operations include and are consistent with IO policy, strategy, and doctrine.

7. Commander in Chief, U.S. Joint Forces Command shall ensure that joint concept development, experimentation, and exercises routinely test and refine IO capabilities, including the application of realistic wartime stress to information systems.

8. Commander in Chief, U.S. Space Command shall:

a. Coordinate and conduct DoD CND to protect the Defense Information Infrastructure from adversary CNO.

b. Provide planning and coordination support to the CNA missions of supported combatant commands.

c. On behalf of other CINCs and in coordination with the Joint Staff, USCINCSPACE will advocate CNA requirements and assist in Joint Requirements Oversight Council (JROC) validation as appropriate.

9. The Director, National Security Agency (NSA), shall:

a. Provide a conduit for deconfliction of DoD CNO activities with the intelligence community (IC) and IC intelligence gain/loss assessments and targeting strategies to support proposed IO courses of actions.

b. Assess and provide information systems security threat and vulnerability information, in conjunction with appropriate agencies, to support IO requirements.

c. Coordinate IO support activities with Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, and the heads of the DoD Components.

10. The Heads of the DoD Components shall assign responsibilities and establish procedures within their organizations to implement the policies in section D., above. The Component heads shall apprise the ASD(C3I), of developmental efforts consistent with subsection E.1., above.

F. <u>EFFECTIVE DATE</u>

This Directive is effective immediately.

\\SIGNED\\
Paul Wolfowitz
Deputy Secretary of Defense

Enclosure
Definitions

DEFINITIONS

1. Computer network attack (CNA). Operations to [manipulate] disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

-OR-

1. Computer network attack (CNA): Operations using computer hardware or software, or conducted through computers or computer networks, with the intended objective or likely effect of disrupting, denying, degrading, or destroying information resident in computers and computer networks, or the computers and networks themselves.

2. Computer network defense (CND). Efforts to defend against the CNO of others, especially that directed against U.S. and allied computer networks.

-OR-

2. Computer network defense (CND): Those measures, internal to the protected entity, taken to protect and defend information, computers, and networks from intrusion, exploitation, disruption, denial, degradation, or destruction.

3. Computer network exploitation (CNE). Intelligence collection and enabling operations to gather data from target adversary automated information systems (AIS) or networks.

-OR-

3. Computer network exploitation (CNE): Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. CNE is composed of two types of activities: (1) enabling activities designed to obtain or facilitate access to the target computer system where the purpose includes foreign intelligence collection; and, (2) collection activities designed to acquire foreign intelligence information from the target computer system.

4. Computer network operations (CNO) Comprises CNA, CND and CNE collectively.

5. Computer network response (CNR) ["Active Computer Network Defense"]: Those measures, that do not constitute CNA, taken to protect and defend information, computers, and networks from disruption, denial, degradation, destruction, or exploitation that involve activity external to the protected entity. Computer Network Response, when authorized, may include measures to determine the source of hostile CNA or CNE.

6. Deception. Those measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

7. Electronic warfare. Electromagnetic and directed energy used to control the electromagnetic spectrum or to attack an adversary.

8. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing and storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all [USG] owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority.

9. Human Factors. The psychological, cultural, behavioral, and other human attributes that influence decision making, the flow of information, and the interpretation of information by individuals or groups at any level in a state or organization.

10. Information. Facts, data, or instruction in any medium or form.

11. Information assurance (IA). IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

12. Information superiority. The capabilities to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

13. Information system. The entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate, and act on information.

14. Operations security (OPSEC). A process of identifying critical information and subsequently 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.

15. Psychological operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of Psychological Operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives.