DEPARTMENT OF DEFENSE
OFFICE OF FREEDOM OF INFORMATION
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

09 MAY 2008

Ref: 06-F-2688

Mr. Steven Aftergood
Senior Research Analyst
Federation of American Scientists
1725 DeSales Street, NW, 6th Floor
Washington, DC 20036

Dear Mr. Aftergood:

This is in response to your August 29, 2006, Freedom of Information Act (FOIA) request for "DOD Directive O-3600.1, 'Information Operations,' 8/14/2006." We received your request on September 12, 2006. I apologize for the inadvertent delay in completing this action on your request.

Enclosed is a copy of the responsive document described above, totaling 11 pages. There are no assessable fees associated with this response. With this action, we are closing your request in this Office.

Sincerely,

Suzanne Council
for Will Kammer
Chief

Enclosure:
As stated

Department of Defense
DIRECTIVE

NUMBER O-3600.01
August 14, 2006

USD(I)

SUBJECT: Information Operations (IO)

References: (a) DoD Directive S-3600.1, "Information Operations (U)," December 9, 1996 (hereby canceled)
(b) Section 165 of title 10, United States Code

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues Reference (a) to update IO policy, definitions, and responsibilities in the Department of Defense (DoD) to support the objective of making IO a core military competency.

1.2. Provides authority to develop separate instructions for implementation of the guidance contained in this Directive.

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS

3.1. Information Operations (IO). The integrated employment of the core capabilities of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

3.2. Other terms used in this Directive are defined in Enclosure 1.

4. POLICY

It is DoD policy that:

4.1. IO shall be employed to support full spectrum dominance by taking advantage of information technology, maintaining U.S. strategic dominance in network technologies, and capitalizing upon near real-time global dissemination of information, to affect adversary decision cycles with the goal of achieving information superiority for the United States.

4.1.1. In peacetime, IO supports national objectives primarily by influencing adversary perceptions and decision-making. In crises short of hostilities, IO can be used as a flexible deterrent option to demonstrate resolve and communicate national interest to affect adversary decision-making. In conflict, IO may be applied to achieve physical and psychological results in support of military objectives. During post conflict or stability operations, IO continues to support national objectives and influence foreign perceptions.

4.1.2. IO contributes to information superiority by both defending military decision-making from adversary attacks and by influencing and degrading an adversary's decision-making capability, thereby producing an information advantage. IO contributes directly to the national security strategy, which uses all elements of national power in a synchronized and coordinated manner to influence adversary perceptions and behavior.

4.2. IO capabilities shall be developed that can be employed in concert with various core, supporting, related, and intelligence capabilities to provide a fully integrated warfighting capability.

4.2.1. Core IO Capabilities. IO employs five core capabilities to achieve desired Combatant Commander effects or prevent the enemy from achieving his desired effects: EW, CNO, PSYOP, MILDEC, and OPSEC. They are operational in a direct and immediate sense; they either achieve critical operational effects or prevent the adversary from doing so. They are interdependent and increasingly need to be integrated to achieve desired effects.

4.2.2. Supporting Capabilities

4.2.2.1. Counterintelligence (CI) investigations, operations, collection, analysis, production, and dynamic functional services shall be employed in support of appropriate IO activities to detect and mitigate foreign intelligence, hacker, and insider threats to DoD information and information systems.

4.2.2.2. Physical (kinetic) attack may be employed alone or integrated with non-kinetic attack options to influence or disrupt adversary decision-makers or groups and provide support for full spectrum dominance.

4.2.2.3. Physical Security shall support IO by preventing unauthorized physical access to personnel, equipment, installations, material, and documents, and by safeguarding information and information systems against espionage, sabotage, damage, and theft.

4.2.2.4. Information Assurance (IA) shall provide capabilities to protect and defend information and information systems. IA activities shall be conducted independently to achieve these objectives or combined with specific CNO activities.

4.2.2.5. Combat Camera shall provide clear, timely, unaltered documentation of military operations to the Combatant Commander. This documentation provides a source of video and still images that can be used to counter disinformation, misinformation, and propaganda.

4.2.3. Related Capabilities

4.2.3.1. Public Affairs (PA), as a function of command, shall support the continuing public information and communication requirements of the Department. PA activities contribute to the broader U.S. Government (USG) communications effort by providing truthful, accurate and timely information to the public, the domestic and international media, military members, and their families. PA shall provide operational capabilities to communicate military objectives, counter misinformation and disinformation, deter adversary actions, and maintain the trust and confidence of the U.S. population, as well as our friends and allies. Effective military operations shall be based on credibility and shall not focus on directing or manipulating U.S. public actions or opinion.

4.2.3.2. Civil-Military Operations (CMO) activities shall 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. CMO shall be performed by designated civil affairs personnel, other military forces, or a combination of both.

4.2.3.3. Defense Support to Public Diplomacy (DSPD) ensures the Department sends a coherent and compelling message in concert with other USG agencies. The prevalence of access to global communications requires a comprehensive and proactive USG communication strategy. The Department of State maintains the lead for public diplomacy with the Department of Defense in a supporting role. Through DSPD, the Department collaborates with other USG agencies for public diplomacy programs that directly support the DoD mission. It is critical that all DoD information activities be conducted in concert with the broader USG communications strategy and support the National Security Strategy.

4.2.4. Intelligence Support. Intelligence shall be developed, consistent with the National Intelligence Priorities Framework, to provide data about adversary information systems or networks; produce political-military assessments; conduct human factors analysis; and provide indications and warning of adversary IO, including threat assessments.

4.3. To achieve the objective of establishing IO as a core military competency, a cadre of IO Capability Specialists and IO Planners shall be developed.

4.4. IO shall be integrated into Security Cooperation Guidance for theater planning, as well as deliberate and contingency planning, to support national policy and strategy.

4.5. IO activities shall be coordinated and appropriately synchronized during peacetime and crisis actions and will include interagency coordination to ensure deconfliction with other agency programs, operations, and activities.

4.6. Tactics, techniques, procedures, and technologies shall be shared among the DoD Components to fully facilitate synchronization and integration of IO.

4.7. IO capabilities shall be integrated into joint exercises and joint training regimes to the maximum extent possible.

4.8. The DoD Information Operations and Space Executive Committee shall serve as the senior corporate body advising the Secretary of Defense on issues relating to IO.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall:

5.1.1. Serve as the Principal Staff Assistant to the Secretary of Defense for IO.

5.1.2. Develop and oversee DoD IO policy and integration activities.

5.1.3. Assess the performance of Defense and Military Intelligence and the responsiveness of intelligence activities to support DoD IO.

5.1.4. Serve as the DoD lead within the Intelligence Community (IC) regarding IO issues.

5.1.5. Coordinate, oversee, and assess the efforts of the DoD Components to plan, program, develop, and execute capabilities in support of IO requirements.

5.1.6. Establish specific policies for the development and integration of CNO, MILDEC, and OPSEC as core IO capabilities.

5.1.7. Ensure the Director, National Security Agency, will:

5.1.7.1. Support IO planning and operations with Signals Intelligence, technology, and access.

5.1.7.2. Support proposed IO courses of action with the intelligence gain/loss assessments and potential targeting strategies.

5.1.7.3. Host and serve as Executive Secretary for the process to deconflict Department CNO activities with the IC.

5.1.7.4. Assess the overall security posture of national security systems and conduct CND activities as directed.

5.1.7.5. Provide OPSEC assistance, products, and services.

5.1.8. Ensure the Director, Defense Intelligence Agency, will manage DoD all-source intelligence collection, analysis, and dissemination in support of DoD IO intelligence requirements.

5.2. The Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) shall:

5.2.1. Establish specific policies for the development and integration of EW as a core IO capability.

5.2.2. Develop and maintain a technology investment strategy to support the development, acquisition, and integration of EW capabilities.

5.2.3. Incorporate IO threat countermeasures in acquisition programs.

5.2.4. Invest in and develop the science and technologies needed to support IO capabilities.

5.3. The Under Secretary of Defense for Policy (USD(P)) shall:

5.3.1. Provide DoD oversight of IO planning, execution, and related policy guidance including the establishment of an OSD review process to assess IO plans and programs submitted by Combatant Commanders to verify that proposed employment of IO capabilities are appropriately coordinated and consistent with DoD policy and the National Military Strategy.

5.3.2. Lead interagency coordination, exclusive of the IC, and international cooperation involving the planning and employment of IO capabilities.

5.3.3. Establish specific policy and oversight for the development and integration of PSYOP as a core IO capability.

5.3.4. In coordination with USD(I) and ASD(PA), establish specific policy and oversight for the development and integration of DSPD as a related IO capability.

5.4. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall:

5.4.1. Develop policy and procedures on matters pertaining to the establishment and management of an IO career force in coordination with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the USD(P), the USD(I), and others, as appropriate.

5.4.2. Provide training policy and oversight as it pertains to the integration of all IO capabilities into joint exercises and joint training regimes.

5.5. The Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer shall:

5.5.1. Establish specific policy for the development and integration of IA and Computer Network Defense (CND) as related to CNO as a core IO capability.

5.5.2. Oversee and assess the efforts of the Heads of the DoD Components to plan, program, develop, and field IA and CND capabilities in support of CNO.

5.6. The Assistant Secretary of Defense for Public Affairs shall:

5.6.1. Establish specific policy for the relationship of PA to IO.

5.6.2. Oversee PA planning and coordination efforts as related to IO within the Department of Defense.

5.6.3. Oversee the development and conduct of appropriate training and education that defines PA's relationship to IO for PA and visual information personnel at the Defense Information School.

5.6.4. In coordination with USD(I) and USD(P), oversee and develop DoD policy that addresses DoD efforts to communicate information to the public and the media.

5.7. The Heads of the DoD Components shall:

5.7.1. Assign responsibilities and establish procedures within their organizations to implement the policies in Section 4 of this Directive.

5.7.2. Inform PA officials of military plans and operations and establish synchronized IO and PA efforts.

5.7.3. Develop policy, doctrine, and the capabilities to execute IO across the range of military operations.

5.7.4. Develop and conduct education, training, and exercise programs to provide for the successful planning, integration, and execution of IO.

5.8. The General Counsel of the Department of Defense shall provide legal advice and assistance to the Secretary of Defense and other DoD officials on DoD IO, including the IO planning process and execution.

5.9. The Secretaries of the Military Departments and Commander, U.S. Special Operations Command, shall develop IO doctrine and tactics, and organize, train, and equip for IO within their respective responsibilities pursuant to Section 165 of title 10, U.S. Code (Reference (b)), and Major Force Program 11 responsibilities, respectively.

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

5.10.1. Serve as the principal military advisor to the President of the United States, the National Security Council, and the Secretary of Defense on IO.

5.10.2. Validate capability-based IO requirements through the Joint Requirements Oversight Council.

5.10.3. Develop and maintain joint doctrine for core, supporting, and related IO capabilities in joint operations.

5.10.4. Ensure all joint education, training, plans, and operations include, and are consistent with, IO policy, strategy, and doctrine.

5.11. The Commanders of the Combatant Commands shall integrate, plan, and execute IO when conducting campaigns across the range of military operations and shall identify and prioritize IO requirements. IO shall be integrated into appropriate Security Cooperation plans and activities. The following Combatant Commanders have these specific responsibilities:

5.11.1. The Commander, U.S. Strategic Command (USSTRATCOM), shall integrate and coordinate DoD IO core capabilities of EW, CNO, PSYOP, MILDEC, and OPSEC that cross geographic areas of responsibility or across the core IO areas, in addition to the responsibilities in paragraph 5.11.

5.11.2. The Commander, U.S. Special Operations Command (USSOCOM), shall, in addition to the responsibilities in paragraph 5.9 and 5.11.:

5.11.2.1. Integrate and coordinate DoD PSYOP capabilities to enhance interoperability and support USSTRATCOM's information operations responsibilities and other combatant commanders' PSYOP planning and execution.

5.11.2.2. Employ other special operations force IO capabilities as directed.

6. EFFECTIVE DATE

This Directive is effective immediately.

Gordon England 8/14/06

Enclosure - 1
E1. Definitions

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

E1.1.2. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. CND employs IA capabilities to respond to unauthorized activity within DoD information systems and computer networks in response to a CND alert or threat information. Note: CND also employs intelligence, counterintelligence, law enforcement, and other military capabilities to defend DoD information and computer networks.

E1.1.3. Computer Network Exploitation (CNE). Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

E1.1.4. Computer Network Operations (CNO). Comprise CNA, CND, and related CNE enabling operations.

E1.1.5. Defense Support to Public Diplomacy (DSPD). Those activities and measures taken by the DoD Components to support and facilitate the overt public diplomacy efforts of USG Departments and Agencies designed to promote U.S. foreign policy objectives.

E1.1.6. Electronic Warfare (EW). Any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy.

E1.1.7. 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.

E1.1.8. Information. Facts, data, or instruction in any medium or form with context comprehensible to the user.

E1.1.9. Information Assurance (IA). Measures 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. Note: CND provides operational direction and guidance through global network operations and defense for employment of IA in response to a CND alert or specific threats.

E1.1.10. Information Operations Specialists and Planners. Functional experts in one or more of the highly specialized core capabilities of CNO, EW, or PSYOP, who plan and execute the full spectrum of IO. IO planners shall understand basic principles associated with EW, CNO, and PSYOP, as well as understand an adversary's cultural and political context, in order to be capable of integrating IO effects into Combatant Commanders' plans and orders. Both IO Capability Specialists and IO Planners should be fully educated and trained to understand the planning principles associated with OPSEC and MILDEC.

E1.1.11. Information superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

E1.1.12. Information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, and disseminate information.

E1.1.13. Military Deception (MILDEC). Those measures designed to mislead an adversary by manipulation, distortion, or falsification to induce him to react in a manner prejudicial to his interests.

E1.1.14. Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

E1.1.14.1. Identify those actions that can be observed by adversary intelligence systems.

E1.1.14.2. Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

E1.1.14.3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

E1.1.15. 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 government, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

E1.1.16. Public Affairs (PA). Those public information, command information, and community relations activities directed toward both the external and internal audiences with interest in the Department of Defense. Effective PA is based on credibility and shall not focus on directing or manipulating public actions or opinion.

E1.1.17. Public Diplomacy. Those overt information activities of the USG designed to promote united foreign policy objectives by seeking to understand, inform, and influence foreign audiences and opinion makers and by broadening the dialog between American citizens and institutions and their counterparts abroad.

E1.1.18. Security Cooperation. Those activities conducted with allies and friends, in accordance with Secretary of Defense Guidance, to:

E1.1.18.1. Build relationships that promote specified U.S. interests.

E1.1.18.2. Build allied and friendly capabilities for self-defense and coalition operations.

E1.1.18.3. Provide U.S. forces with peacetime and contingency access.