Department of Defense
DIRECTIVE

NUMBER 3600.01
May 2, 2013
Incorporating Change 1, May 4, 2017

USD(P)

SUBJECT: Information Operations (IO)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues DoD Directive 3600.01 (Reference (a)) in accordance with the authority in DoD Directive 5111.1 (Reference (b)) and, pursuant to the authority and guidance in Secretary of Defense Memorandum (Reference (c)), updates established policy and assigned responsibilities for IO.

b. Updates IO definitions.

c. Directs the establishment of the Information Operations Executive Steering Group (IO ESG).

2. APPLICABILITY. This directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

3. POLICY. It is DoD policy that:

a. IO will be the principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of operations to effect adversaries' or potential adversaries' decision-making while protecting our own.

b. IRCs constitute tools, techniques, or activities employed within a dimension of the information environment (IE) that can be used to achieve a specific end at a specific time and place. IRCs can include, but are not be limited to, a variety of technical and non-technical activities that intersect the traditional areas of electronic warfare, cyberspace operations, military

information support operations (MISO), military deception (MILDEC), influence activities, operations security (OPSEC), and intelligence.

c. The development and management of individual IRCs will be the responsibility of various DoD Components and will be brought together at a specific time and in a coherent and integrated fashion for use against adversaries and potential adversaries in support of military operations.

d. DoD IO will be synchronized with information and influence activities of other U.S. Government (USG) organizations to ensure consistency across USG activities in the IE.

e. DoD IO will be coordinated and, as practicable, integrated with related activities conducted by allied nations and coalition partners.

f. Consistent with existing statutory requirements and manpower polices, Service and joint IO forces must be an appropriate and cost effective total force mix of active and reserve military personnel, government civilian personnel, and contracted support.

g. IO will be included across Active and Reserve Components, and government civilian professional education curriculums to foster an understanding of IO and IRCs across all ranks and positions within DoD.

h. IO tactics, techniques, and procedures (TTPs); technologies; and lessons learned will be shared among DoD Components and, as practicable, with allied nations and coalition partners to fully facilitate the synchronization, integration, and effectiveness of IO while reducing redundancies in capabilities across the DoD.

i. IO will be integrated into joint exercises and joint training, security cooperation guidance for theater planning, communication strategy, and deliberate and contingency planning.

j. DoD IO programs and activities will incorporate an explicit means of assessing the results of operations in relation to expectations.

k. DoD IO activities will not be directed at or intended to manipulate audiences, public actions, or opinions in the United States and will be conducted in accordance with all applicable U.S. statutes, codes, and laws.

l. DoD IO information gathering programs and activities will be coordinated and deconflicted with DoD intelligence activities as set forth in DoD Directive S-5200.37 (Reference (d)) and DoD 5240.1-R (Reference (e)). Human-derived information gathering activities in support of IO will remain separate from authorized HUMINT and related intelligence activities.

m. All DoD IO activities will be conducted in accordance with CJCS Instruction 3121.01B (Reference (f)).

n. The IO ESG will serve as the primary coordination forum within DoD to inform, coordinate, and resolve IO issues among the DoD Components and, as appropriate, deconflict IO issues as they are represented in established DoD policy and programmatic decision forums. The IO ESG's organization, membership, policies, and procedures will be established in a separate DoD Instruction.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. ~~**Unlimited**~~ ***Cleared for public release***. This directive ~~is approved for public release and~~ is available on ~~the Internet from~~ the DoD Issuances Website at http://www.dtic.mil/whs/directives.

6. EFFECTIVE DATE. This directive~~:~~ *is effective May 2, 2013.*

~~a. Is effective May 2, 2013.~~

~~b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (g)). If not, it will expire May 2, 2023 and be removed from the DoD Issuances Website.~~

Ashton B. Carter
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 3600.01, "Information Operations (IO)," August 14, 2006, as amended (hereby cancelled)
(b) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(c) Secretary of Defense Memorandum, "Strategic Communication and Information Operations in the DoD (U)," January 25, 2011
(d) DoD Directive S-5200.37, "Management and Execution of Defense Human Intelligence (HUMINT) (U)," February 9, 2009, as amended
(e) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982*, as amended*
(f) Chairman of the Joint Chiefs of Staff Instruction 3121.01B, "Standing Rules of Engagement /Standing Rules for the Use of Force for US Forces, and the Law of Armed Conflict (LOAC)," June 13, 2005
~~(g) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012~~
(~~h~~*g*) Secretary of Defense Memorandum, "Changing the Term Psychological Operations (PSYOP) to Military Support information Operations (MISO) (U)," December 3, 2010
(~~i~~*h*) "Trilateral Memorandum of Agreement signed by the Department of Defense, the Department of Justice and the Intelligence Community Regarding Computer Network Attack and Exploitation Activities," May 9, 2007
(~~j~~*i*) ~~Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition~~ *Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition*

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P):

a. Serves as the Principal Staff Advisor (PSA) to the Secretary of Defense for oversight of IO in the DoD. In this capacity, the USD(P):

(1) Is the primary coordination point of contact for DoD Components and other USG organizations for issues related to IO.

(2) Is the single point of fiscal and program accountability for IO.

(3) Links OSD, Joint, and Service IO policies, capabilities, and programs.

(4) Fully integrates IO with national and DoD strategy and planning functions.

b. Provides policy oversight, guidance, and advice for DoD IO to include providing policy guidance on IO force development and employment.

c. Coordinates within OSD, the Joint Staff, and the Military Services to address the Combatant Commanders' IO requirements, which includes the development of IRCs, ensuring adequate test and evaluation resources, and ensuring IRC integration across the CCMDs.

d. In coordination with the DoD Components responsible for the individual IRCs:

(1) Oversees, coordinates, and assesses the efforts of DoD Components to plan, program, and develop IRCs for use in the IE.

(2) Assesses the effectiveness of the IRCs as part of IO in operational applications.

e. Provides IO policy guidance for all phases of operations planning, including security cooperation.

f. Establishes DoD policy on MISO matters in accordance with Secretary of Defense Memorandum (Reference (~~h~~*g*)), and reviews and approves all CCMD MISO programs to be conducted during peacetime or in contingencies short of declared war.

g. Establishes and oversees DoD policy regarding the coordination of IO conducted by DoD Components with other USG organizations in support of U.S. national security strategy and policy in accordance with Reference (~~h~~*g*), so specific information objectives, target audiences, themes, and actions are synchronized. This specifically includes coordinating MISO policy, plans, and programs with other USG departments, agencies, and activities.

h. Establishes and oversees DoD policy regarding the coordination and, where practicable, the integration of IO efforts with allied and coalition partners.

i. Coordinates with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) on policies for the establishment and maintenance of professionally trained and educated Service and joint IO forces. These forces will consist of a total force mix as described in paragraph 3f above the signature of this directive.

j. Develops standardized fiscal methodologies for IRCs in accordance with Reference (c) and in coordination with the Under Secretary of Defense for Intelligence (USD(I)), the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (USD(C)/CFO), and the Director, Cost Assessment and Program Evaluation (DCAPE). As part of this responsibility, the USD(P) will maintain procedures to ensure fiscal accountability for IO as well as the individual IRCs.

k. Conducts programmatic assessments of DoD IO in coordination with DCAPE.

l. As one of the co-chairs of the IO ESG, establishes and maintains the IO ESG.

m. Assists in the development of Joint Electromagnetic Spectrum Operations (JEMSO) policy and coordinates with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and Commander, United States Strategic Command (USSTRATCOM) regarding the development, acquisition, and employment of JEMSO capabilities used to support IO.

n. Coordinates with the Assistant to the Secretary of Defense for Public Affairs to ensure that DoD IO is consistent with the policy established in this directive and that DoD IO is not directed at or intended to manipulate U.S. audiences, public actions, or opinions and is conducted in accordance with all applicable U.S. statutes, codes, and laws.

o. In coordination with the USD(I):

(1) Provides policy oversight for OPSEC; MILDEC; deconfliction of DoD IO and intelligence activities; and the development, acquisition, and integration of MILDEC capabilities used to support IO.

(2) Provides input to the DoD OPSEC program as required.

(3) Coordinates on intelligence related matters that support the integration of IRCs used during military operations.

(4) Assists in the development and maintenance of a DoD instruction on policy for intelligence support to IO, information gathering activities, and IE characterization.

2. USD(I). The USD(I):

a. Facilitates coordination of IO activities within the Intelligence Community consistent with Memorandum of Agreement (Reference (~~i~~*h*)).

b. Serves as the OSD program management lead for the DoD OPSEC and MILDEC programs.

c. In coordination with the USD(P):

(1) Develops and oversees the implementation of policy for intelligence support to IO, information gathering activities, and IE characterization.

(2) Establishes and oversees the implementation of policies and procedures for the conduct of DoD OPSEC and MILDEC as warfighting enablers and military competencies, and the coordination and deconfliction of DoD IO and intelligence activities.

(3) Coordinates on intelligence related matters that support the integration of IRCs used during military operations.

(4) Develops, approves, and maintains DoD instruction on policy for intelligence support to IO, information gathering activities, and IE characterization.

3. USD(AT&L). In partnership with the Secretaries of the Military Departments, the USD(AT&L) researches IRCs affecting IO and coordinates these activities with the USD(P).

4. USD(P&R). The USD(P&R):

a. Develops policies for the establishment and maintenance of professionally trained and educated Military Service and joint IO forces in coordination with the USD(P) and the Secretaries of the Military Departments. These forces will consist of a total force mix.

b. Develops and distributes polices for the establishment and maintenance of professionally trained and educated Military Service and joint IO forces in collaboration with USD(P).

5. USD(C)/CFO. The USD(C)/CFO:

a. In coordination with the USD(P) and DCAPE, develops standardized fiscal methodologies for IRCs when applied to support IO. Included in this activity is the maintenance of procedures to ensure fiscal accountability for IO as well as the individual IRCs when they are employed in support of IO.

b. Requires all organizations conducting MISO to capture costs for MISO as a separate and distinct entity from other IO-related costs.

6. DCAPE. The DCAPE:

a. As appropriate, reviews IO programs, costs, and effectiveness.

b. In coordination with the USD(P) and USD(C)/CFO, develops standardized fiscal methodologies for IRCs and IO activities.

7. DOD COMPONENT HEADS. The DoD Component heads:

a. Assign responsibilities and establish procedures within their respective DoD Components to implement this directive.

b. Support IO planning, coordination, operations, and deconfliction within DoD Components and other USG organizations.

8. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments:

a. In coordination with the USD(P) and CJCS, implement joint IO policy and doctrine and develop, plan, and program IO into the full spectrum of military operations.

b. Develop and implement Service component IO policy, doctrine, and TTPs that are compatible with DoD and joint IO policy and doctrine.

c. Provide education and training to meet IO military and civilian force development goals to meet joint IO requirements.

d. Provide intelligence oversight training to IO staffs and units in accordance with Reference (e).

e. Share IO TTPs and technologies with DoD Components and, when release of such information and technologies is permitted, allied and coalition partners.

f. Establish and oversee policies that provide for IO reporting and assessment as well as the integration of individual IRCs to meet Combatant Commanders' needs and objectives.

g. In accordance with Reference (c) and in coordination with the USD(P), USD(C)/CFO, and DCAPE, annually provide comprehensive Service inputs required to ensure fiscal accountability for IO as well as individual IRCs.

9. CJCS. The CJCS:

a. Serves as the joint IO proponent. Functions as the oversight authority for IO policy execution within the CCMDs and joint task forces.

b. Develops procedures for a professionally trained and educated joint IO force in coordination with the USD(P&R) and USD(P).

c. Emphasizes the importance of including IO as an instrumental part of military operations through the development and validation of joint IO doctrine.

d. Validates IO needs through the Joint Capabilities Integration and Development System.

e. Incorporates IO into all military planning efforts, including joint exercises and training.

f. Serves as the joint proponent for MILDEC and OPSEC.

g. Ensures all joint education, training, plans, and operations are consistent with joint IO policy, strategy, and doctrine.

h. Evaluates the joint IO education and training system and conducts assessments of IO to ensure the requirements of the Combatant Commanders are met.

i. Consistent with Reference (c), oversees the Joint IO Warfare Center as a Chairman's Controlled Activity.

j. As one of the co-chairs of the IO ESG, establishes and maintains Joint Staff participation in the IO ESG.

k. Ensures coordination and deconfliction of joint IO and intelligence activities in all operational planning and execution.

l. Establishes a framework for sharing TTPs as well as lessons learned among DoD Components and allied and coalition partners.

10. COMBATANT COMMANDERS. The Combatant Commanders:

a. Utilize IO as the principal mechanism to integrate, synchronize, employ, and adapt all IRCs in the IE to accomplish operational objectives against adversaries and potential adversaries.

b. Develop, plan, program and assess IO as well as IRC execution in support of IO during all phases of military engagement and at all levels of war.

c. In coordination with the USD(P) and CJCS, identify in advance and seek, as appropriate, the delegated authorities required for employing IRCs in support of IO across the full range of military operations.

d. Identify and prioritize IO needs on their respective integrated priority lists.

e. Integrate IO into joint exercises and training, security cooperation guidance for theater planning, and deliberate and contingency planning.

f. Develop and share IO lessons learned through written and oral assessments communicated to other DoD Components and allied and coalition partners as appropriate.

g. Ensure that joint IO staffs and units under CCMD command and control have received intelligence oversight training in accordance with Reference (e).

h. Ensure coordination and deconfliction of CCMD IO and intelligence activities in all operational planning and execution.

11. COMMANDER, USSTRATCOM. The Commander, USSTRATCOM, is the joint proponent for JEMSO and computer network operations. In addition to the responsibilities outlined in section 10 of this enclosure and in coordination with the USD(P) and through the CJCS, the Commander, USSTRATCOM, coordinates JEMSO, space operations, and cyberspace operations in support of IO.

12. COMMANDER, U.S. SPECIAL OPERATIONS COMMAND (USSOCOM). The Commander, USSOCOM, is the joint proponent for MISO. In addition to the responsibilities outlined in sections 8 and 10 of this enclosure and in coordination with the USD(P) and through the CJCS, the Commander, USSOCOM, coordinates joint force MISO in support of IO.

13. DIRECTORS OF THE DEFENSE AGENCIES. The Directors of the Defense Agencies:

a. Integrate IO into joint exercises, training, and deliberate and contingency planning.

b. Develop and share IO lessons learned through written and oral assessments communicated to other DoD Components and, as applicable, allied and coalition partners.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CAPE	Cost Assessment and Program Evaluation
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
DCAPE	Director, Cost Assessment and Program Evaluation
IE	information environment
IO	information operations
IO ESG	Information Operations Executive Steering Group
IRC	information related capability
JEMSO	Joint Electromagnetic Spectrum Operations
MILDEC	military deception
MISO	military information support operations
OPSEC	operations security
PSA	Principal Staff Advisor
PSYOP	psychological operations
TTP	tactics, techniques, and procedures
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USG	United States Government
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command

PART II. DEFINITIONS

These terms and their definitions are proposed for inclusion in the next edition of ~~Joint Publication 1-02~~ *the DoD Dictionary of Military and Associated Terms* (Reference (j)).

IE. An environment that is an aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

IO. The integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

IO force. A force consisting of units, staff elements, and individual military professionals in the Active and Reserve Components, and DoD civilian employees who conduct or directly support the integration of IRCs against adversaries and potential adversaries during military operations as well as those who train these professionals.

IRC. A capability that is a tool, technique, or activity employed within a dimension(s) of the information environment that can be used to achieve a specific end(s).