[redacted]

Department of Defense
DIRECTIVE

December 21, 1992
NUMBER TS 3600.1

ASD(C3I)

SUBJECT: Information Warfare (U)

References: (a) DoD Directive 3222.4, "Electronic Warfare (EW) and Command, Control, and Communications Countermeasures (C3CM)," July 31, 1992
(b) DoD Directive 5111.1, "Under Secretary of Defense for Policy," July 27, 1989

A. PURPOSE

(U) This Directive establishes Department of Defense (DoD) policy and assigns responsibilities for information warfare.

B. APPLICABILITY

(U) This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Combatant Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. DEFINITIONS

1. (U) Information. Data or knowledge relevant to a particular circumstance or task.

2. (U) Information System. The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In the context of information warfare, it includes the entire infrastructure that collects, processes, stores, and disseminates information regarding both one's own forces and opposing forces and the means to determine and display the status of one's own forces and to direct those forces.

3. (U) [redacted] Information Warfare. The competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information system through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own information system from such attacks. The objective of information warfare is to attain a significant enough information advantage to enable the force overall to predominate and to do so quickly.

D. POLICY

It is DoD policy that:

1. (U) [redacted] U.S. Armed Forces shall be organized, trained, equipped and supported in such a manner as to be able to achieve a distinct information advantage over potential adversaries in order to win quickly, decisively, and with minimum losses and collateral effects.

Classified by: [redacted] DODI O-3600.02, dated AUG 28, 2005
Declassify on: 20200602

See Def Cont Nr. X60614

[redacted]

Copy 65 of 69 Copies

OSD/WHS D-001
by 1

2. (U) Information warfare requires the interaction and the integration of command, control, communications (C3), intelligence, information systems countermeasures, and information systems security. This interrelationship shall be pursued vigorously, particularly with regard to requirements definition and validation, research and development, acquisition, plans, and operations.

3. (S) (b)(1)

4. (U) Intelligence collection against the information systems of potential adversaries shall be afforded sufficient priority to support the information warfare requirements of the Department of Defense.

5. (U) The Department of Defense shall vigorously pursue information system countermeasures, recognizing their significant role in attaining an information advantage. Reference (a) pertains.

a. (U) Particular emphasis shall be placed on the analytic effort requisite to ensuring the identification and development of highly effective countermeasures at reasonable cost.

b. (S) (b)(1)

c. (U) Dual use systems that can be used both to exploit adversary information systems as well as to corrupt those systems shall be acquired whenever practical and cost effective.

6. (S) (b)(1)

7. (S) (b)(1)

8. (U) Command and control of forces shall be planned and exercised in such a manner as to minimize the amount of information transfer required for effective direction and application of force to ensure our forces are able to operate successfully in degraded information and communications environments.

9. (U) Elements of the DoD information system critical to the transmission and use of minimum-essential information for the control and direction of forces shall be designed and employed in a manner that minimizes or prevents exploitation and denial or degradation of service. Training and exercise capabilities shall be built into the individual components of the DoD information system, as appropriate.

10. (U) Computer simulation technologies together with networked wargaming and exercises shall be developed and used to create realistic information warfare environments for training, exercise and planning purposes as well as the requirements definition portion of the acquisition process.

11. (U) [redacted] Sufficient training, including realistic training exercises that simulate wartime stresses, shall be conducted to ensure the commanders of U.S. forces are well-informed and well-versed in the trade-offs among exploitation, corruption, and destruction of adversary information systems; the varying capabilities and vulnerabilities of the various elements of U.S. information systems; and the interaction and interrelationship of the two.

12. (U) Information warfare plans and policies shall be integrated with overall national security objectives.

E. RESPONSIBILITIES

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

a. (U) Be the primary point of contact within the OSD and serve as the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for information warfare activities of the Department of Defense.

b. (U) Establish policy and provide guidance on information warfare.

c. (U) Review information warfare plans, programs, and requirements and monitor and evaluate program responsiveness to validated requirements.

d. (U) Provide for the centralized planning and coordination of information warfare matters to include policy development, broad strategy, program and budget review, technology development, security, and education and training, while maintaining decentralized execution.

e. (U) Provide security guidance for information warfare activities.

2. (U) The Under Secretary of Defense (Acquisition) shall:

a. (U) Review and approve information systems technology and tactical information warfare system developments.

b. (U) Ensure that adequate science and technology programs exist to provide technology for the development and acquisition of information warfare systems.

c. (U) Ensure electronic counter-countermeasures (ECCM) are considered during the development of information warfare systems.

3. (U) The Under Secretary of Defense (Policy) shall develop policies and review information warfare requirements, plans, and capabilities when information warfare matters concern the integration of DoD plans and policies with overall national security objectives, or when information warfare matters bear on or fall under his responsibilities and functions as defined in reference (b).

4. (U) The Secretaries of the Military Departments shall:

a. (U) [redacted] Develop information warfare doctrine and tactics; and organize and train to ensure that these are well-integrated into overall doctrine and tactics and become an essential element in our warfighting capability.

b. (U) Define information warfare requirements and develop and acquire systems in response to validated requirements.

c. (U) Keep the Director, National Security Agency (NSA) informed of developmental efforts consistent with subsection E.6., below.

d. (U) Review related Service programs for applicability to information warfare, advising the Assistant Secretary of Defense for Command, Control, Communications and Intelligence of reviews conducted.

5. (U) The Chairman of the Joint Chiefs of Staff shall:

a. (U) Validate information warfare requirements, as appropriate.

b. (U) Establish doctrine to facilitate the integration of information warfare concepts into joint warfare.

c. (U) Ensure plans and operations include and are consistent with information warfare policy, strategy, and doctrine.

d. (U) Coordinate with the commanders of the Unified and Specified Combatant Commands to ensure effective execution of information warfare activities.

e. (U) Ensure that exercises routinely test and refine information warfare capabilities, including the application of realistic wartime stress to information systems.

6. (U) The Director, National Security Agency, shall be kept informed of technology and system development efforts associated with the information warfare activities of the Department of Defense.

7. (U) The Director, Defense Information Systems Agency, as central manager of the Defense information infrastructure (DII), shall ensure the DII contains adequate protection against attack.

8. (U) 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 keep the Director, NSA informed of developmental efforts consistent with subsection E.6., above.

F. EFFECTIVE DATE AND IMPLEMENTATION

(U) This Directive is effective immediately. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence may issue instructions as may be necessary to implement this Directive. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments. Instructions to the Unified and Specified Combatant Commands shall be communicated through the Chairman of the Joint Chiefs of Staff.

D. J. Atwood

Donald J. Atwood
Deputy Secretary of Defense