(b)(3)

~~TOP SECRET/~~ [redacted] ~~NOFORN//X1~~

DOC (b)(3)

[redacted] (b)(3)

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 7/3

INFORMATION OPERATIONS AND INTELLIGENCE COMMUNITY RELATED ACTIVITIES (U)

(Effective 01 July 1999)

1. REFERENCES.

a) (U) DCID 5/1, "Espionage and Counterintelligence Activities Abroad," 19 Dec 1984

b) (U) NSCID 5, "U.S. Espionage and Counterintelligence Activities Abroad," 19 Dec 1984

c) (U) NSCID 6, "Signals Intelligence," 17 Feb 1972

d) (U) NSD 42, "National Policy for the Security of National Security Telecommunications and Information Systems," 05 Jul 1990

e) (U) Presidential Decision Directive/NSC-63 (PDD-63), "Critical Infrastructure Protection," 22 May 1998

f) (U) Memorandum of Agreement on Oversight Board for Private Sector Relationships, 05 Jun 1998

g) (U) Charter of the National Special Communications Working Group (NSCWG), 07 Jan 1997

h) (U) Memorandum of Agreement concerning Deconfliction of Computer Network Operations (CNO), 01 Jul 1999

i) (U) Charter of the Bilateral Information Operations Steering Group (BIOSG), 14 Apr 1998

j) (U) DCID 5/6, "Intelligence Disclosure Policy," 30 Jun 1998

k) (U) National Security Act (NSA) of 1947, as amended

l) (U) Title 10, U.S. Code (Armed Forces)

m) (U) MOA Between DoD and the IC Regarding the Information Operations Technology Center (IOTC), 04 Mar 1997

n) (U) Concept of Operations (CONOP) for the Information Operations Technology Center (IOTC), 04 Mar 1997

o) (U) Title 50, U.S. Code

2. PURPOSE.

(U) This directive sets forth the responsibilities of Intelligence Community (IC) components in the conduct and coordination of:

- (U) Information Operations (IO),
- (U) Intelligence and related support to IO, and
- (U//~~FOUO~~) Deconfliction of specific computer network operations (CNO) conducted by National Foreign Intelligence Program (NFIP) agencies.

3. AUTHORITIES.

(~~S//NF~~) This DCID does not affect the authorities, responsibilities, and restrictions relating to components of the IC and the Department of Defense (DoD) that are set out in existing statutes, executive orders, and policy directives such as Presidential Decision Directives (PDDs), National Security Council Intelligence Directives (NSCIDs), and other DCIDs, in particular the requirements under reference (a) for coordination of espionage and counterintelligence activities abroad. This DCID clarifies the DCI authorities under which IC elements may carry out computer network attack (CNA) and computer network exploitation (CNE) using NFIP funds.

4. DEFINITIONS.

A. (U//~~FOUO~~) The definition of information operations (IO) is: *"Actions taken to affect adversary information and information systems while defending one's own information and information systems."*

B. (U//~~FOUO~~) Information Operations is an integrating strategy. Although still evolving, the fundamental concept of IO is to integrate different activities to affect decision making processes, information systems, and supporting information infrastructures to achieve specific objectives, as well as to protect and defend friendly information and information infrastructures. IC IO-related activities include CNE and other supporting intelligence activities.

5. DISCUSSION.

A. (U//~~FOUO~~) The concept of Information Operations (IO) emerged against the backdrop of the explosive growth of information technology. IO has made use of electronic warfare (EW), psychological operations (PSYOP), military deception, operational security (OPSEC), and physical destruction. The rapid spread of computers and computer networks has led to their inclusion as instruments for attacking and influencing information infrastructures.

B. (U//~~FOUO~~) Computer network operations (CNO) comprises computer network exploitation (CNE) -- denoting a broad range of intelligence collection activity; computer network attack (CNA) -- denoting attacks on computer systems and networks; and computer network defense (CND) -- denoting actions taken to protect U.S. computer systems and networks and possibly those of allies and coalition partners. CNE is an intelligence collection activity and, while not viewed as an integral pillar of DoD IO doctrine, it is recognized as an IO-related activity that requires deconfliction with IO. There are interdependencies and relationships among CNE, CNA, CND, and other IC activities in support of IO which may require mechanisms to ensure proper deconfliction or coordination among those NFIP funded IC elements that engage in these activities.

 (b)(3)

C. (U//~~FOUO~~) IC IO activities include conducting, with proper authorization, covert action, including CNA. IC elements authorized to conduct CNA under DCI authorities in peacetime will be specified by a Presidential Finding.

D. (U//~~FOUO~~) IC IO-related activities include:

- (U) Collecting, processing, analyzing, and disseminating foreign intelligence and counterintelligence on IO.
- ~~(C)~~ Conducting CNE, in accordance with the authorities described in references (b) and (c).
- (U) Supporting other U.S. government organizations in the conduct of their IO missions.
- (U) Ensuring effective warning and defense against IO.
- (U) Performing computer network defense (CND) activities commensurate with established legal statutes or the technical direction provided by NSA/CSS, as specified in reference (d), or the National Infrastructure Protection Center (NIPC), as set forth in reference (e).

6. DECONFLICTION.

A. (U) While this DCID does not address every contingency, IO and IO-related activities specified in paragraphs 6.C and 6.D shall be deconflicted and mutually supporting. Deconfliction mechanisms shall be established to guarantee compatibility within areas of common concern.

B. (U) To support the establishment of deconfliction processes, it is important to initially identify the applicable authority for an action so that activities can be conducted within an appropriate legal context and oversight requirements can be satisfied. The nature and the context of an activity will determine the applicable legal authority for the activity (i.e., the authority under which an activity is conducted). The following guidelines shall apply:

1) (U) The criterion for identifying the applicable authority for a proposed activity shall be the "primary purpose" of the activity. For example, if the "primary purpose" of an activity is foreign intelligence (FI) collection, FI collection authorities shall prevail, notwithstanding the fact that the activity may have other purposes.

2) (U) The nature and context of the activity, and not the U.S. Government entity that conducts it, shall determine the applicable authority.

C. (~~TS~~/ /~~NF~~) The Oversight Board for Private Sector Relationships (reference f) and the National Special Communications Working Group (NSCWG) (reference g) exist to deconflict IO-related industrial relations and special communications, respectively. They shall be expanded to include new membership as appropriate. (b)(3)

D. (~~S//NF~~) CNA/E Deconfliction process. CIA and NSA will jointly manage, as an IC service of common concern, an Interagency Target Register (ITR) to deconflict IC CNA and CNE operations. IC elements conducting CNA or CNE operations under DCI authorities shall deconflict their operations within the ITR structure according to ITR procedures and appropriate access negotiated with the principal signatories to the MOA cited in reference (h). The IC recognizes a need to establish procedures for deconflicting CNE activities with other appropriate U.S. agencies.

(b)(1)
(b)(3)

 (b)(3)

(b)(1)
(b)(3)

7. IMPLEMENTATION.

(S//NF) Except where covered by existing policies, IC IO-related responsibilities are listed below.

A. (U) The Deputy Director of Central Intelligence for Community Management (DDCI/CM) shall:

1) (U) Serve as the IC focal point for IO strategic planning and policy coordination within the IC and with the Bilateral Information Operations Steering Group (BIOSG) (per reference i).

2) (U) Represent IC organizations that are not already represented on the BIOSG.

3) (U) Provide administrative and staff support to the Secretariat of the BIOSG (per reference i).

4) (U) Oversee implementation of this DCID.

B. (U) The Assistant Secretary of State for Intelligence and Research (I&R) shall:

1) (U) Support the Chiefs of Mission in their review of the implications of contemplated IO for foreign affairs and diplomatic relations pursuant to reference (a).

2) (U) Pursuant to reference (j), review the implications of contemplated sharing of intelligence on foreign IO programs with allies or other foreign entities.

C. (U) The National Intelligence Officers (NIOs) for Warning and for Science & Technology shall jointly provide the DCI and other IC elements with appropriate strategic warning against IO.

D. (U) Consistent with the National Security Act of 1947 (reference k), the DCI has assigned the following tasks, which, pursuant to 10 USC 113 (reference l), the Secretary of Defense has directed the DoD components listed below to execute.

1) (U) The Director, National Security Agency/Chief Central Security Service (DIRNSA/CCSS) shall:

i. (S//NF) Integrate CNA, CNE, and CND tools, techniques, and technology into the SIGINT and INFOSEC communities.

ii. (U) Train, equip, and organize the U.S. Cryptologic System to support the CNE, CNA, and CND requirements needs of its customers.

iii.(U) Provide IO-related military targeting support.

iv. (~~S~~) Provide intelligence gain/loss assessments in response to CINC IO targeting.

v. (~~S~~) Develop and support analytic modeling and simulation techniques to support CNA/CNE efforts.

2) The Director, Defense Intelligence Agency (D/DIA) shall:

i. (U) Ensure that DIA is postured to support the full range of IO activities, both offensive and defensive, including psychological operations, military deception, electronic warfare, computer network operations, operations security, and physical destruction.

ii. (U) Train and equip the Defense HUMINT Service (DHS) to support the IO requirements of its customers.

iii.(U) Provide IO-related military targeting support.

iv. (U) Perform all-source analysis, production, dissemination, and provision of military and military-related intelligence on foreign information infrastructures and foreign information threats for the Secretary of Defense, Joint Chiefs of Staff, other defense components, and, as appropriate, non-defense agencies.

v. (~~S//NF~~) Pursuant to existing DoD directives, instructions and other guidance, conduct Human Factors intelligence support for the full range of IO.

vi. (U) Pursuant to DoD requirements, provide strategic indications and warning for IO.

vii.(U) Provide political-military assessments in response to CINC IO targeting.

3) (U) The Director, National Imagery and Mapping Agency (D/NIMA) shall:

i. (U) Conduct imagery and geospatial analysis to identify critical foreign information infrastructures and assess their interdependencies.

ii. (U) In partnership with other IC elements, provide targeting support to IO. This includes identifying physical targets, developing targeting packages and preparing combat assessments.

iii.(U) With approved tasking, help identify vulnerabilities to key U.S. infrastructures (CONUS and OCONUS) in order to contribute to more effective defensive IO practices.

iv. (U) Provide other imagery and geospatial information support to IC and DoD IO efforts in a timely and effective manner.

v. (U) Ensure IO requirements are included in any delineation and assessment of future requirements.

4) [redacted] (b)(1) (b)(3)

5) (U) The Director of the Information Operations Technology Center (D/IOTC) shall execute responsibilities in accordance with references (m) and (n).

E. (U) The Director, Federal Bureau of Investigation (D/FBI) shall:

1) (U) Provide available, releasable information and operational support that may assist in the planning or execution of an IO activity by IC and DoD.

2) (U) Assist other agencies in assessing the risks of planned IO activities to the U.S. information infrastructure.

3) (U) Keep the U.S. private sector and Government at all levels informed of threats to the U.S. information infrastructure that may arise from IO activities without divulging U.S. plans or intentions.

4) (U) Develop and deploy tools to reduce the risk of penetration, corruption, and disruption of critical U.S. information systems and networks.

5) (U) Investigate IO intrusions and attacks against information networks and systems in the United States.

F. (U) All IC Element Heads shall:

1) (U) Provide the DDCI/CM with the information required to assist the DCI in implementing this directive.

2) ~~(S)~~ Cooperate closely with the IOTC to ensure consistency between the CNA and dual purpose (CNE) techniques contained in the Toolbox and any other

 (b)(3)

developing or employed capabilities.

3) (U) Take reasonable steps to protect their own systems from hostile CNA and CNE.

8. REVIEW.

(U) The DDCI/CM shall coordinate the IC's annual review of this DCID for currency and completeness.

George J. Tenet
DIRECTOR OF CENTRAL INTELLIGENCE

July 21, 1999
DATE

APPENDIX A

Definitions of Terms Used in this Directive

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

Computer Network Defense (CND): (U) Efforts to defend against the CNO of others, especially that directed against U.S. and allied computers and networks.

Computer Network Exploitation (CNE): (U) Intelligence collection and enabling operations to gather data from target or adversary automated information systems (AIS) or networks.

[redacted] (b)(1) (b)(3)

Computer Network Operations (CNO): (U) CNE, CNA, and CND collectively.

Covert Action: (U) Refer to Section 503 of the National Security Act of 1947, Title V (50 U.S.C. 413-413b) (references k and o) and related legislation. [Related legislation includes the 1991 Intelligence Authorization Act and 102d Congress Report SENATE First Session 102-85 and House Conference Report 102-166.] Section 503 refers to covert action as, ". . . an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include--

 (b)(3)

(U) . . . activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the security of United States Government programs, or administrative activities;

. . . traditional diplomatic or military activities or routine support to such activities; . . . traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or . . . activities to provide routine support to the overt activities . . . of other United States Government agencies abroad." (Special Activities is a euphemism for covert action; as such it is redundant to include it here.)

Deception: (U) 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.

(b)(1)
(b)(3)

Electronic Warfare: (U) The use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack an adversary.

Human Factors: (U) 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.

Information Operations (IO): (U) Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information System: (U) The organizations, personnel, and components that collect, process, store, transmit, display, disseminate and act on information.

Operations Security (OPSEC): (U) 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.

Physical Destruction: (U) Referred to in Joint military doctrine as one of the core disciplines of IO. Note: Not all physical destruction is IO nor related to it. Physical destruction can be used to further tactical, operational, and/or strategic IO objectives. Examples include destroying command and control facilities, communications links, and components supplying energy to power communications.

Psychological Operations: (U) 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 or PSYOPs is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.

Special Communications: (U//~~FOUO~~) The relay of U.S. government or allied signals from or into areas

 (b)(3)

typically characterized by an intense counterintelligence or operational security environment, usually in support of covert or clandestine intelligence or military operations, or sensitive overseas law enforcement activities.

(b)(3)

(b)(3)