~~SECRET~~

6288

THE WHITE HOUSE

WASHINGTON

October 23, 2000

PRESIDENTIAL REVIEW DIRECTIVE/NSC-

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
CHIEF OF STAFF TO THE PRESIDENT
DIRECTOR, CENTRAL INTELLIGENCE AGENCY
DIRECTOR, OFFICE OF SCIENCE AND TECHNOLOGY POLICY
CHAIRMAN, JOINT CHIEFS OF STAFF
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Subject: Computer Network Operations (CNO) (U)

I. Policy Objectives, Definitions and the Intent of this Presidential Review Directive

The increasing availability of information technologies and the dependence of every level of management and leadership on institutions and infrastructures that process, store, and communicate information are affecting the very nature of conflict and crisis management just as they are profoundly changing the international political and strategic environment in which the United States must act. (U)

A U.S. policy objective is to be able to employ the full spectrum of computer network operations (CNO) to achieve information superiority and shape the international environment to support our nation's national security strategy. It is also possible to use CNO to support and complement other, traditional military, peacekeeping, diplomatic, economic, law enforcement, and foreign intelligence and counterintelligence missions. ~~(C)~~

Computer network operations (CNO), as defined within this document, aggregates three separate, but interrelated, fields of activity:

~~SECRET~~
Classified by: Samuel R. Berger
Reason: 1.5 (a,b,c,d,e,g)
Declassify On: 1.6, X1, X2, X3, X4, X5, X6

- Computer network attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves;

- Computer network defense (CND): Efforts to detect and defend against the CNO of others, especially those directed against U.S. and allied computers and networks; and

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

The United States' ability to effectively attain and employ an information advantage will depend upon creating effective CNA, CND, and CNE capabilities which enable us to:

- Provide the United States the means and technologies necessary to affect the information systems and networks we target.

- Protect United States, allied, and coalition partner information systems and networks.

- Provide the United States the capability to obtain the intelligence and information necessary to identify and affect the information systems and networks our adversaries or competitor states rely upon. (S)

Potential adversaries who employ CNO include non-state actors such as terrorists, criminal organizations, and individual criminals as well as traditional nation-states. (U)

The intent of this review is to improve and institutionalize the United States' ability to employ CNO in support of existing strategy as put forward in the *National Security Strategy* and support the development of CNO capabilities within the U.S. Government, including the development of appropriate policy and legal oversight. As part of this effort a number of legal, privacy, policy, and structural issues surrounding the effective development of CNO policy warrant review, including an effort to determine how to integrate the use of CNO into existing decision-making and organizational structures. (U)

II. Study Process

To accomplish this review, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council (NSC) will chair a Computer Network Operations Interagency Working Group (CNO IWG). The CNO IWG will include

representatives from Office of the Secretary of Defense, Joint Staff, Office of the Deputy Director of Central Intelligence For Community Management, National Security Agency, Central Intelligence Agency, Defense Intelligence Agency, NSC, State, Justice, Federal Bureau of Investigation, National Infrastructure Protection Center (NIPC), Office of Science and Technology Policy and Office of Management and Budget, and other executive branch agencies as required. (U)

III. Issues to be addressed by Review

1. CNO Definitions and Broad Policy.

As part of the review the CNO definitions and broad policy statement articulated in section I above, and other CNO related definitions as required, shall be put to interagency review and evaluation. (U)

2. Declaratory Policy.

The review shall evaluate the utility of the United States Government adopting a declaratory policy on the use of CNO, and if recommended, what that declaratory policy would entail. (U)

3. Engagement Policy.

There is a need for an elaboration of current authorities and legal constraints and responsibilities for the conduct of CNO under uncertain or ambiguous circumstances short of actual hostilities. ~~(C)~~

The review shall examine current engagement policy and determine what changes, if any, are necessary to permit flexible employment of CNO and adequate response to CNE and CNA by an adversary. This review will include the issue of emplacement of CNO tools. The goal of this review is to permit the effective integration of CNO capabilities across the full spectrum of operations. This PRD is not intended to review the use of CNO on the battlefield. ~~(S)~~

4. Deconfliction of CNO.

EO 13526 1.4a, 1.4(c), 1.4(d)

EO 13526 1.4a, 1.4(c), 1.4(d)	There is a potential for mutual

interference and/or compromise of sensitive capabilities, methods, and sources as CNO increase and become more routine. ~~(S)~~

Deconfliction and, potentially, coordination of CNO activities by multiple agencies of the United States Government will be necessary to ensure appropriate legal oversight, command, and control of CNO activities. After study of current deconfliction and coordination processes, including the interagency target registries, political-military assessments, and intelligence gain/loss mechanisms, the review shall determine if there is a need for improvements or changes in the policy and processes that ensure coordination and deconfliction of CNO activities conducted by agencies/elements of the federal government during peacetime as well as crisis and conflict. ~~(S)~~

5. Relationships Among Response Mechanisms.

The review shall examine what processes, if any, are needed to support the newly created cyber incident groups (CIWG/CISG) and facilitate coordination among law enforcement, foreign intelligence, counterintelligence and infrastructure protection response mechanisms for CNO, in light of applicable law and existing Presidential Decision Directives. Specifically, the review shall study indicators such as the use of levels of damage, scope of impact, implications for sources and methods, and other specific conditions which would assist in the rapid evaluation of future cases as deserving law enforcement, foreign intelligence, counterintelligence or infrastructure protection emphasis. ~~(C)~~

6. Active Defense.

There is no definition for 'active defense' of computer networks. One interpretation of the term incorporates the concept of actively seeking out the source of CNA or CNE directed against U.S. systems, then using technical means to negate the perpetrator's ability to continue the attack or exploitation. We are challenged by the frequent inability to rapidly or definitively identify the perpetrator of a CNA or CNE against a U.S. computer network or system. Because identification is not specific or reliable, it is difficult to respond in support of national security decision making, or in legal proceedings. ~~(S)~~

The review shall examine and define the concept of 'active defense', and evaluate possible policy, legal, and process mechanisms to determine what 'active defense' measures are lawful and appropriate under which circumstances. This review shall also reflect the likelihood that the United States will not be able to firmly identify perpetrators. ~~(S)~~

7. Engagement with other Nation States.

Awareness of CNO as both a potential threat and a force multiplier is widespread, and in some countries CNO has been assimilated into warfare plans and operations. Given the U.S. leadership in information technology and CNO, allied nations may seek assistance in developing their own CNO programs. (U)

This review shall determine what areas of CNO could be made available to our allies and if specific policies are needed to ensure coordinated, appropriate response to requests from foreign nations for CNO collaboration, technical support, capabilities sharing, and information exchange. ~~(S)~~

Additionally, the review shall also consider what options for response the United States has upon the discovery of significant, highly compromising CNE conducted by a potential adversary. ~~(S)~~

8. Sharing of Vulnerability Information.

EO 13526 1.4a, 1.4(c), EO 13526 1.4g

The review shall study existing methods for evaluating computer network vulnerabilities and advising U.S. entities and other organizations of their effects. The review shall determine the need, if any, for further policy to support existing processes. ~~(S)~~

9. CNO Indications and Warning.

The review shall evaluate the current state of interagency organizational structures and relationships for CNO incidents, mutual support procedures, and resources applied to providing indications and warning of CNA or CNE by an adversary. ~~(S)~~

10. CNO Integration Into Existing Contingency Planning Efforts.

When an Executive Committee, as described in *PDD-56, Managing Complex Contingency Operations*, is established it is the primary interagency mechanism to conduct political-military planning and to coordinate day-to-day management of U.S. participation in

peace operations and foreign humanitarian assistance operations. The review shall explore the applicability of CNO to complex contingency planning operations under PDD-56. (C)

IV. Tasking

The CNO IWG will prepare a draft paper for review by participating agencies which addresses the policy and structural issues detailed above. Following agency comments and discussion, and within 180 days of the signing of this directive, the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism will prepare and coordinate a summary document for Deputies Committee review. An interim report will be provided on January 15, 2001. (U)

Samuel R. Berger
Assistant to the President
for National Security Affairs