Distributed by Penny Hill Press

BT-1017
Updated Dec. 9, 2003

Congressional Research Service
CRS

http://pennyhill.com

Cyberwarfare

Clay Wilson

Issue Definition

Military planning is shifting toward the view that combat power can be enhanced through increased use of computers, communications networks, and digital information. Several policy issues raised by cyberwarfare, or information warfare activities include (1) does reliance on computer technology and the civilian communications critical infrastructure create unacceptable vulnerabilities for the U.S. military; (2) should the U.S. engage in covert psychological operations affecting audiences within friendly nations; (3) does the use of cyber weapons by the military invite similar retaliation by others; and, (4) should the U.S. pursue international agreements to harmonize cyber crime legislation to help quickly identify and pursue cyber attackers?

As tools for cyberwarfare become available, appropriate and more effective, a key issue for Congress is whether the disabling effects of cyber weapons can be properly controlled to avoid damaging non-military critical computer systems or other systems belonging to friendly nations that may be near military targets.

Current Situation

The U.S. Department of Defense (DOD) uses the term "Information Operations" to describe military information warfare activities. Information Operations encompasses five capabilities: Psychological Operations, Military Deception, Operational Security, Computer Network Operations, and Electronic Warfare.

The Joint Information Operations Center (JIOC) within the U.S. Strategic Command (USSTRATCOM) manages information warfare activities. Computer Network Operations include offensive and defensive aspects of information warfare; however, most of the military's resources and efforts devoted to information warfare are focused on defensive measures.

National Security Presidential Directive 16, signed in July 2002, provides guidance for determining when and how the United States would launch computer network attacks against foreign adversary computer systems. It is intended to clarify circumstances under which an attack by DOD would be justified and would identify who has authority to launch a computer attack.

Policy Analysis

A large percentage of U.S. military administrative information is currently routed through the civilian Internet. Some observers believe that the increased flexibility and other short-term benefits offered by connections to the civilian Internet may outweigh the security threats to military administrative information systems.

DOD Directive 3600.1 provides guidelines for military psychological operations (PSYOPS). However, media reports have indicated that DOD personnel drafted an amendment to the Directive that described covert operations designed to influence public opinion, for example by publishing stories favorable to American policies. However, the new Office of Global Communications, established in 2003 by Executive Order 13283, is tasked to promote the spread of truthful and accurate messages to others about U.S. policy and avoid disinformation.

It is technically difficult to trace back to the source of a computer attack. A military cyber counterattack may be misdirected against a group or country that may itself have been falsely set up to appear as the attacker. Once launched, a DOD cyber attack may be interpreted as an unprovoked first strike and may invite similar retaliation against the U.S. critical infrastructure by unfriendly groups. It may also be difficult to prevent cyber weapons and electromagnetic weapons from damaging computers that are part of the civilian critical infrastructure in a foreign country, such as hospitals or the water supply system.

Traditional just war concepts of discrimination and proportionality have been raised in an increasing literature and debate concerning what some observers have begun to call an "electronic means of mass disruption" and the need to develop new international law conventions. However, other observers reportedly believe that U.S. attempts to harmonize international laws against cyber crime and cyber terrorism might actually hinder the research and development that supports some U.S. information warfare capabilities.

Role of Congress/Legislation

In a general sense, Congress can play a vital role in determining funding and exercising oversight of policy and programs dealing with cyberwarfare activities in the defense and intelligence community budgets. Congress might also be interested in international arms control fora that are starting to examine the issue of cyber warfare.

CRS Products

CRS Report RL31787(pdf). *Information Warfare and Cyberwar: Capabilities and Related Policy Issues.*

CRS Report RL32114(pdf). *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.*