Distributed by Penny Hill Press

BT-1017
Updated Sept. 10, 2002

Congressional Research Service

CRS

http://pennyhill.com

Cyberwarfare

Steven A. Hildreth

Issue Definition

In the search for an appropriate response to the terrorist attack of September 11, 2001, the United States possesses a number of political, economic, and military tools. One of the military tools available is the use of computers, computer networks, the Internet, and software to deny likely adversaries, including terrorists, the ability to attack or exploit computer networks and critical infrastructure, and their ability to communicate in planning and carrying out terrorist acts. The key issue in this context is the degree to which such tools might be available, appropriate, and effective.

Current Situation

U.S. Space Command has the military lead for defending Defense Department computers and networks-Computer Network Defense (CND). Computer Network Defense includes all the various forms of information assurance, information protection, 'cyber defense,' and the defensive aspects of information warfare. Most of the military's resources and efforts devoted to information warfare are focused on defensive measures.

U.S. Space Command also has responsibility, however, for developing, articulating, and supporting Computer Network Attack (CNA) requirements and policy for the various CINCs (Commanders in Chief). CNA military options are viewed as augmenting, not replacing, more conventional military tools. CNA options are developed in close coordination with the National Command Authority (NCA), the Joint Chiefs of Staff, and the regional CINC. CNA options are further developed in conjunction with civilian policy and legal review (i.e., whether such an option is appropriate and justified and is consistent with international obligations and the Law of Armed Conflict).

The exercise of CNA options, therefore, is apparently quite limited. The former head of Space Command, Gen. Richard Myers, now Chairman, Joint Chiefs of Staff, said in 2000 that CNA has been used on a "case-by-case" basis. It was considered for Kosovo operations, but opportunities were limited because Serbian armed forces were not heavily dependent on information systems. Currently, there are no reports of the use of CNA in the military operation against bin-Laden and the Taliban in Afghanistan or elsewhere.

However, Defense Department legal and policy review requirements may differ from possible covert cyber warfare options that might be pursued by other agencies.

Policy Analysis

Although most observers might agree that CND is a prudent investment of resources and an increasingly necessary requirement for military and national security networks, there is likely less agreement over the most appropriate role for CNA. The heart of the problem lies in the fact that networks are interwoven and interdependent; an attack on an adversary's network or computer capability could have both known and unforeseen consequences for innocent participants. For example, disruption of an electrical power grid, intended to paralyze impending military operations, could also harm civilian access to refrigerated food

stuffs and medical assistance. Traditional just war concepts of discrimination and proportionality have been raised in an increasing literature and debate concerning what some have begun to call an "electronic means of mass disruption" and the need to develop new international law conventions.

In this particular instance, where most observers agree the near-term military option remains focused on Afghanistan and Osama bin-Laden, CNA options may be somewhat limited given the terrorists' minimal reliance on technology. If the mission widens however, to include more modern states, such as Iraq, and terrorist groups more reliant on technology and electronic networks, CNA options may play a relatively larger role with potentially larger implications.

Options and Implications for U.S. Policy

The question at this junction is, in light of the considerations noted above, the degree to which possible use of U.S. cyberwar tools might play in the attempt to bring those responsible for the September 11th attack to justice. Currently, various options are likely being considered by the military, the White House, and perhaps other agencies. The use or not of these tools, as well as their results, will likely influence the long-term development of this new field for the military and other agencies.

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 cyberwar 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 RL30735. *Cyberwarfare.*