Greater transparency needed in development of US policy on cyberattack

April 29 2009

The current policy and legal framework regulating use of cyberattack by the United States is ill-formed, undeveloped, and highly uncertain, says a new report from the National Research Council. The United States should establish clear national policy on the use of cyberattack, while also continuing to develop its technological capabilities in this area. The U.S. policy should be informed by open national debate on the technological, policy, legal, and ethical issues of cyberwarfare, said the committee that wrote the report.

"Cyberattack is too important a subject for the nation to be discussed only behind closed doors," said Adm. William Owens, former vice chairman of the Joint Chiefs of Staff and former vice chairman and CEO of Nortel Corp., and Kenneth Dam, Max Pam Professor Emeritus of American and Foreign Law at the University of Chicago School of Law, who co-chaired the committee.

Cyberattacks -- actions taken against computer systems or networks -- are often complex to plan and execute but relatively inexpensive, and the technology needed is widely available. Defenses against such attacks are discussed, but questions on the potential for, and the ramifications of, the United States' use of cyberattack as a component of its military and intelligence arsenal have not been the subject of much public debate. Although the policy and organizational issues raised by the use of cyberattack are significant, the report says, "neither government nor society at large is organized or prepared to handle issues related to cyberattack, let alone to make broadly informed decisions."

The U.S. could use cyberattack either defensively, in response to a cyberattack from another nation, or offensively to support military missions or covert actions, the report says. Deterring such attacks against the U.S. with the threat of an in-kind response has limited applicability, however; cyberattacks can be conducted anonymously or falsely attributed to another party relatively easily, making it difficult to reliably identify the originator of the attack.

Employing a cyberattack carries with it some implications that are unlike those associated with traditional physical warfare, the report says. The outcome is likely to be more uncertain, and there may be substantial impact on the private sector, which owns and operates much of the infrastructure through which the U.S. would conduct a cyberattack. The scale of such an attack can be enormous and difficult to localize. "Blowback" to the U.S. -- effects on our own network systems -- is possible.

Clear national policy regarding the use of cyberattack should be developed through open debate within the U.S. government and diplomatic discussion with other nations, the report says. The U.S. policy should make it clear why, when, and how a cyberattack would be authorized, and require a periodic accounting of any attacks that are conducted, to be made available to the executive branch and to Congress.

From a legal perspective, cyberattack should be judged by its effects rather than the method of attack; cyberwarfare should not be judged less harshly than physical warfare simply by virtue of the weapons employed. The Law of Armed Conflict (LOAC), an international law regulating conduct during war, should apply to cyberattack. However, there are aspects of cyberwarfare that will not fit neatly within this structure. LOAC was designed to regulate conflict between nations, but cyberweapons can easily be used by non-state groups, making issues

such as determining appropriate targets for military retaliation difficult to address. Additional legal constructs will be needed to govern cyberattacks, and the framework of LOAC and the U.N. Charter on the use of armed force would be an appropriate starting point, the report says.

Source: National Academy of Sciences (news : web)