Report: US cyber warfare needs oversight, debate

April 30 2009, By LOLITA C. BALDOR , Associated Press Writer

(AP) -- Shrouded in secrecy, the U.S. government's policies on how and when to wage cyber warfare are ill-formed, lack adequate oversight and require a broad public debate, a new report by the National Research Council says.

The report warns that the "undeveloped and uncertain nature" of the government's cyber warfare policies could lead to them being used hastily and ill-advisedly during a crisis. That danger is compounded by secrecy and lack of oversight, the report's authors cautioned on Wednesday.

"Unsound policy formulated and implemented during crisis may prove difficult to change or reverse when the crisis has passed," concludes the report, the first to take a comprehensive look at American cyber war capabilities. The research council is the working arm of the National Academy of Sciences.

The U.S. government has spoken only broadly about cyber warfare in the past, noting its value as a national security tool. Officials routinely refuse to talk about computer attacks America has launched.

The 322-page report, prepared by an independent panel of academics and cyber security experts, comes as the Obama administration is on the verge of releasing its own review of the nation's cyber security.

That review, however, is expected to focus largely on defensive and

administrative measures, including who will lead the nation's cyber effort, and how the government can better manage and use technology to protect everything from the electrical grid to the stock market.

Officials have warned in recent months that the nation's computer and internet networks are at risk and are repeatedly probed by foreign governments, criminals or other groups.

U.S. offensive cyber war options could range from a more passive cyber intrusion such as listening in on a foe's communications to an attack that cripples an enemy's air defense systems to clear the way for a bomber attack.

A key challenge, however, may be determining who the enemy is, particularly if U.S. officials are considering a response to a cyber attack or intrusion against America.

Conducted from hundreds or thousands of miles away, a cyber attack can be over in a millisecond, with the press of a button. The perpetrator can be a single hacker looking to do mischief, a terrorist seeking to kill thousands, or a nation aiming to cripple the U.S. economy.

The council emphasized its call for greater public debate on the government's plans for cyber warfare, which to date has been clandestine. The council likened the need for further public airings to the debates that accompanied the use and testing of nuclear weapons more than 50 years ago.

"There needs to be a national debate, just as there was in the 1950s about nuclear weapons," said Kenneth W. Dam, co-chairman of the committee on offensive information warfare that put together the report. "The problem is, there is no national decision-making apparatus."

Earlier this month, Air Force Gen. Kevin Chilton, who heads U.S. Strategic Command, told reporters that the military has rules and procedures for cyber warfare, just as it does for armed conflict. He then declined to provide details, adding: "A good defense also depends on a good offense."

The Research Council's report warned that such secrecy surrounding the government's exploration of cyber warfare has "impeded widespread understanding and debate about the nature and implications of U.S. cyber attack."

It said that while the U.S. has highly developed and sophisticated capabilities to launch a cyber attack, it is difficult to determine the outcome of such a move compared to a traditional armed assault.

So far, said study director Herbert Lin, Americans have been focused more on defensive digital maneuvers - building firewalls, using anti-virus and other protective software and implementing safety procedures, such as the Pentagon's recent ban on the use of external computer flash drives.

Those efforts are important, he said. But he added that the U.S. cannot just continue to build bigger walls, particularly as cyber attacks grow and become increasingly easier to execute.

In its final recommendations, the report said the U.S. government must develop a clear decision-making process for cyber actions, require periodic accounting of cyber attacks at least in a classified form to those charged with oversight, and work with other nations around the world to establish a better legal and ethical framework for such attacks.

©2009 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Report: US cyber warfare needs oversight, debate (2009, April 30) retrieved 17 April 2024 from https://phys.org/news/2009-04-cyber-warfare-oversight-debate.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.