

Monday, September 29, 2008

U.S. urged to go on offense in cyberwar

Shaun Waterman, UNITED PRESS INTERNATIONAL

The United States needs to do more to develop an offensive cyberwar capability rather than just focus on defending its networks from attack, says the chairman of the House cybersecurity subcommittee.

"The best defense is a good offense and an offensive [cyberwar] capability is essential to our national defense," Rep. Jim Langevin told United Press International, calling it "a necessary deterrent."

"Warfare is forever changed. ... Never again will we see major warfare without a strong cyber component executed as part of it," the Rhode Island Democrat added, citing the assault on Georgian government Web sites that accompanied Russia's invasion last month.

Mr. Langevin, chairman of the House Homeland Security subcommittee on emerging threats, cybersecurity and science and technology and a member of the House Permanent Select Committee on Intelligence, also called on the White House to declassify much more of its Comprehensive National Cybersecurity Initiative (CNCI) and said the Department of Homeland Security should be stripped of its lead role in defending the nation's computer networks.

His call for a more robust offensive capacity in cyberwarfare highlights an ongoing debate in government about how best to address the complex challenges posed by U.S. dependence on the Internet and other computer networks - a vulnerability that the nation's enemies could exploit.

One issue that analysts highlight is the difficulty in determining the origins of cyber-attacks, which often are launched using "bot-nets" of compromised computers owned by innocent users anywhere on the planet.

The issue was raised earlier this month in two House hearings in which lawmakers heard testimony from members of a bipartisan, blue-ribbon panel - the Commission on Cyber Security for the 44th Presidency.

"We have a tremendous amount of trouble determining attribution ... where an attack actually came from, who was responsible, who might have been behind that computer. And we have a very, very long way to go on that," commission member Paul Kurtz, a former White House cybersecurity official, told the House intelligence committee.

"Until we start to get clarity in that piece, it's going to be very difficult to contemplate the military option, of responding appropriately," Mr. Kurtz added.

Another issue raised at the hearings was that, in order for any offensive capacity to be a deterrent for adversaries, it would have to be made public, whereas the U.S. military's cyberwar capacities are largely classified.

"Clearly, our offensive capabilities and sources and methods we probably do not want to disclose in any detailed way," AT&T executive John Nagengast, formerly an assistant deputy director at the National Security Agency, told the committee.

"But as part of an overall doctrine and strategy in cyberspace, we need to consider what are the deterrent factors. ... [What] do we want to make public, as part of that deterrence strategy, and what do we need to keep secret because most of our offensive capabilities should be kept secret?" he added.

Former intelligence official Suzanne E. Spaulding told the hearing that focusing on offensive capabilities and giving a lead role to the military might make it harder for the United States to work with other countries on cyber issues, where the lines separating crime, terrorism and warfare are often hard to draw.

"My concern is that [the Defense Department] has been so vocal about the development and deployment of cyberwarfare capabilities that it will be very difficult for that department to develop and sustain the trust necessary to undertake essential collaboration on defense cybersecurity efforts with the private sector and with international stakeholders," she said.

"There is a significant risk that these vital partners will suspect that the collaboration is really aimed at strengthening our offensive arsenal," she concluded.

Mr. Langevin told UPI that work on international treaties to deal with cyberwar offered no real alternative to developing an offensive capability.

"That discussion at the international level may be appropriate at some point," he said. "There are treaties on cybercrime that do exist, but it doesn't mean that cybercrime doesn't occur."