

## **Officials Lack Policy for Taking Offensive In Cyber War**

*Congress Daily*

**December 4, 2008**

The United States lacks a fully defined policy and legal framework for using offensive cyberwarfare capabilities against adversaries, making it difficult for policymakers to determine the origin of computer attacks and when pre-emptive action is justified against criminals, terrorists and hostile foreign nations, according to current and former government officials.

The information networks of U.S. government agencies and critical industry sectors, such as the nation's power and banking companies, are under persistent and increasing cyber attack from foreign foes, including major criminal organizations and countries like China, according to officials and recent high-level reports. Although the U.S. government has an arsenal of cyberwarfare capabilities at its disposal, policymakers are grappling with how and when to use them, along with what kind of privacy and civil liberties issues are raised in doing so.

Officials say the government needs to develop better policies and laws for cyberwarfare, similar to that developed for the use of nuclear weapons. "It is, in many ways, uncharted territory and I know the Policymakers are struggling with how and when to use our offensive capabilities," House Homeland Security Emerging Threats Subcommittee Chairman James Langevin, D-R.I., said in a recent interview.

"It's important for the government to have a clear understanding of what our offensive capabilities are and how best to employ them and when. There are a lot of questions that still need to be answered," Langevin added. "Should the U.S. include pre-emption action as part of its cyber doctrine? What are the thresholds for proportionality of response?"

### **Playing Offense**

The Bush administration launched the so-called Comprehensive National Cybersecurity Initiative this year to monitor Internet traffic and protect federal agencies against cyber attacks. The initiative is expected to cost billions of dollars over many years, and most of its details are classified. Although government officials have talked publicly about defensive measures being deployed for cyber security, the U.S. government also has offensive capabilities, officials said.

Steven Chabinsky, deputy director of the joint interagency cyber task force within the office of the director of national intelligence, hinted at the offensive aspects of the initiative in a speech at a security conference last week. "The CNCI brings the offense and defense together to try to achieve complete information awareness," he said. He did not give specific examples but added that the initiative will "blend the U.S. government's talents and expertise in computer network operations with such disciplines as information security, law enforcement, combat and counter intelligence."

That's where things get muddy, officials say.

"We don't have the doctrine yet that's codified" said Steven Bucci, former Pentagon deputy assistant secretary for homeland defense. "What is an act of war in the cyber realm?" Indeed, Pentagon officials told a cybersecurity commission established by the Center for Strategic and International Studies they need help clarifying existing doctrine for playing offense in the cyber realm, said James Lewis, director of the technology and public policy program at CSIS. "Modernize the laws; clarify the authorities," said Lewis, who serves as the commission's project director. "Clarify what your doctrine is for responding to attacks."

Chabinsky would not answer questions from reporters after his speech and directed inquires to the office of the director of national intelligence, which did not respond to questions.

### **Attribution vs. Retribution**

One of the most difficult issues for government agencies is determining the origin of cyberattacks because intruders can hide their identity by using remote servers or by installing malicious code on computers operated by innocent users, officials said. "Attribution is a very serious and complex troubling issue when you talk about deploying offensive capabilities for deterrence and for response," said Langevin, co-chairman of the cybersecurity commission.

Part of the challenge for policymakers is determining whether attacks require a law enforcement response, an intelligence response or a military response, Lewis said. "We were told the default is to use law enforcement authorities because often the circumstances are so unclear that you have to treat it as a crime rather than a military episode," he said.

And the scale of offensive action needs to be weighed against many factors. The U.S. government might be aware, for example, that relatively minor attacks against information networks in the United States are coming from a hostile foreign government, Bucci said.

But what happens if the United States learns that a large-scale cyber attack is going to come from that country, Bucci asked. The U.S. government will then be faced with whether to take pre-emptive cyber action against the information networks of that country, he said. Some organized crime syndicates also operate with the implicit support of adversarial foreign governments. "Do we attack those governments?" Bucci asked.

Such policy questions now await President-elect Obama, whose transition team declined to comment for this report. Langevin said the U.S. government must immediately define a national cyber strategy with a public component that communicates to adversaries what the United States is capable of doing and prepared to do. Such a strategy, he said, would

be equivalent to the policy of mutually assured destruction for nuclear weapons. Langevin said the government also must immediately train and equip a cybersecurity workforce. "This is something where the Congress and the administration need to work closely to determine when and how we will respond," Langevin said.

### **Growing Threats**

The need to clarify policies and laws for cyberwarfare was highlighted in recent high-level government and private industry reports that documented the growing cyber threat to U.S. agencies and companies. The congressionally chartered US-China Economic and Security Review Commission released its annual report last week, concluding that China is targeting U.S. government and commercial computers for espionage.

The Defense Science Board released a report earlier this month, saying in part that cyber attacks could have a crippling impact on space-based assets that provide surveillance, communication and navigation services.

And the board of directors of the Internet Security Alliance, a trade group that advocates greater public focus on and investment in cybersecurity, issued policy recommendations for President-elect Obama last week in a report documenting vulnerabilities and concerns of major firms in such sectors as technology, banking, defense, manufacturing and higher education. "Signature-based intrusion detection, firewalls, and anti-virus technologies are all deployed, but they do little to identify or prevent more sophisticated adversaries," said a section of the ISA report devoted to the defense industry. "Spam, spoofed e-mail addresses, multi-hopping exploits, and third party domain registration all serve to make internet crime and intellectual property theft all but impossible to prevent," the report said.

Questions also persist over whether, and when, the U.S. government should take offensive cyberwarfare action to protect a private company, given that most of the critical infrastructure in the United States is owned and operated by the private sector. "It's a great question. It's an important question," said J. Michael Hickey, Verizon's vice president of government affairs for national security policy, adding that he has not had discussions with the government about the issue. "I do think it's important for government and industry to address this issue given the ownership and responsibility for managing our nation's networks," he said. "If they are 90 percent privately owned, then there does need to be a considerable discussion about it."