

Former U.S. spy chief concerned it may take a crisis to create a new and improved cyber law

U.S. intelligence agencies have unique capabilities that can help protect American companies from cyber espionage and attack, but it will probably take a crisis to change laws to allow that type of cooperation, a former spy chief said on Monday.

Intelligence agencies like the National Security Agency are authorized to operate abroad but generally are restricted from working within the United States,

"Until we have a banking collapse or electric power goes off in the middle of a snowstorm for eight weeks, or something of that magnitude, we're likely just to talk about it and not do much," Mike McConnell, former director of national intelligence, said.

The Republican-controlled House of Representatives and the Democratic-controlled Senate have separate efforts under way on legislation aimed at improving cybersecurity.

The House intelligence committee in December approved a bill that would allow U.S. spy agencies to share cyber-threat intelligence with private companies.

Some critics worry that could lead to government surveillance of private data.

Senate Majority Leader Harry Reid has said the Senate will take up "comprehensive" cybersecurity legislation this year.

"There are unique things that the government can do. For example code-breaking. The private sector out there does not do code-breaking," McConnell, a former National Security Agency director, said. "How would you harness that capability and then make it available to the private sector in a way that their infrastructure could be better protected?"

A U.S. intelligence report last year pointed the finger at China and Russia as using cyber espionage to steal U.S. trade and technology secrets. McConnell gives an example that if NSA, which conducts electronic eavesdropping to detect foreign threats, observed a cyberthreat against the U.S. private sector, "NSA is powerless to do a thing other than issue a report."

He said in the area of cyber exploitation, such as reading an adversary's mail without leaving fingerprints, the United States, Britain and Russia are probably the best. The United States also has the ability to conduct cyber attacks, which would be to degrade or destroy an adversary's computerized system, and has used it.

Has the United States used its cyber attack capability? "Yes," McConnell said. Did it work?

"Yes." McConnell, now vice chairman at the Booz Allen Hamilton consulting firm in charge of cyber activities, did not elaborate on the use of a cyber attack capability. "Do we have the ability to attack, degrade or destroy? Sure. If you do that, what are the consequences? That is the question," he said.

McConnell said the priority is to protect the country's critical infrastructure such as the financial sector, the electric power grid and transportation from cyber attack and stop the theft of intellectual property through cyber espionage.

"There will be a thousand voices on what is the right thing to do," and it will probably require a crisis to reach consensus, he said. "All I'm arguing is the government has unique capability, figure out a way to harness the capability in the defense of the nation."

© Copyright (c) Postmedia News