Private networks vulnerable to cyber attack: Pentagon

Andrea Shalal-Esa, Reuters

(Reuters) - Privately-owned computer networks remain vulnerable to cyber attacks, and many U.S. companies are not doing enough to protect them, Deputy Defense Secretary Ashton Carter said on Wednesday.

"I hope this isn't one of those situations where we won't do what we need to do until we get slammed," Carter told the annual Air Force Association conference.

Attacks on American computer infrastructure by other countries and criminal gangs have soared in recent years, according to U.S. government officials.

Efforts to pass legislation to strengthen U.S. cyber security have met obstacles such as privacy issues, prompting the White House to consider an executive order to protect U.S. computer networks from attack.

Carter said the Pentagon was doing all it could to protect its own networks and develop offensive cyber weapons, but shoring up the nation's overall cyber infrastructure -- much of which is privately held -- was far more challenging.

"When it comes to the nation's networks there are many other forces and considerations that make it very complicated, and therefore very slow, and I'm concerned that it's moving too slowly," he told Reuters after his remarks at the conference.

"We're still vulnerable and the pace is not adequate," Carter told the conference, noting that many private companies either did not invest at all -- or invested too little in cyber security.

General Martin Dempsey, chairman of the U.S. Joint Chiefs of Staff, echoed his concerns about the vulnerabilities of U.S. computer systems and said cyberspace operations would be fully "integrated into the way we do business in the future."

"We better take seriously the threat in cyber space," Dempsey told Reuters after a speech at the conference. "We've got to get ourselves better prepared for the kind of activities in cyber that are happening all over the globe."

Congress' failure to pass cyber security legislation this summer was very disappointing, Carter told Reuters after the speech, noting that the proposed measure would have helped increase U.S. cybersecurity "tremendously".

As a result, he said, the Obama administration was trying to move ahead on its own, within existing legislative constraints.

"We're trying to do without legislation some of the things -- obviously we can't do everything -- that we need to do," he said.

White House homeland security adviser John Brennan last month said the White House was exploring whether to issue an executive order to protect the nation's critical computer infrastructure, but gave no details on the timing or possible content of such an order.

Senator Jay Rockefeller, who heads the Senate Commerce Committee, on Wednesday sent letters to the 500 biggest U.S. companies, challenging them to step up their computer security and blaming the defeat of the legislation on concerns raised by "a handful of business lobbying groups and trade associations."

He asked the companies to identify their own best practices and to spell out their concerns about government-conducted risk assessments that were part of the cybersecurity bill. He warned that the companies could face "reactive and overly prescriptive legislation" if nothing was done until some cyber disaster.

Carter told hundreds of industry executives and military officials at the conference that protecting the country's privately-controlled computer networks raised myriad antitrust and privacy questions that needed to be addressed more quickly.

Some of those questions center on the amount and type of data that can be shared among private companies and with the government, and to what extent the government can get involved in protecting private networks.

The Pentagon is facing mounting budget pressures, especially if Congress fails to avert an additional $500 billion in across-the-board defense cuts due to start taking effect in January.

Carter said the budget reductions would have a devastating effect on a number of Pentagon programs, but continued investment in offensive and defense cyber operations would continue, along with unmanned systems, space capabilities and electronic warfare.

General Mark Welsh, the Air Force's new chief of staff, on Tuesday told reporters that he planned to take a hard look at funding for cyber operations until the Pentagon more clearly spelled out its requirements for new "cyber warriors."

"Until we're all on board and under the same direction, I'm a little hesitant to commit wholeheartedly a major resource expenditure in an area that I don't completely understand," he said.

Debora Plunkett, of the secretive National Security Agency, whose responsibilities include protecting U.S. government computer networks, predicted earlier this month that Congress would pass long-stalled cybersecurity legislation within the next year.

She said other nations were increasingly employing cyber attacks without "any sense of restraint," citing "reckless" behaviors that neither the United States nor the Soviet Union would have dared at the height of Cold War tensions.

In July, NSA Director General Keith Alexander said the number of computer attacks from hackers, criminal gangs and foreign nations on American infrastructure had increased 17-fold from 2009 to 2011.

(Additional reporting by Joseph Menn Editing by Andrew Hay and Alden Bentley)

Source URL (retrieved on *12/09/2013 - 4:47am*):
http://www.ecnmag.com/news/2012/09/private-networks-vulnerable-cyber-attack-pentagon