Cybercom chief: U.S. unprepared for serious cyber attacks

Claudette Roulo, American Forces Press Service

ASPEN, Colo. (AFPS) -- The United States is not adequately prepared for a serious cyber attack, the commander of U.S. Cyber Command told the audience at the Aspen Institute's annual security forum today.

Army Gen. Keith Alexander, who also serves as the director of the National Security Agency and the chief of the Central Security Service, said that, in terms of preparation for a cyber attack on a critical part of its network infrastructure, the U.S. is at a three on a scale of one to ten.

The problem of defending the nation from a cyber attack is complicated, Alexander said. It's not just a question of preparing the Department of Defense or federal networks. Private industry also has to be defended.

"Industry has a variety of capabilities," Alexander said. While networks serving the financial community are well-defended, others sectors need help.

Key to developing a strong cyber security infrastructure is educating its users, Alexander said.

"We have a great program, it's jointly run by [the National Security Agency] and [the Department of Homeland Security] working with over 100 different colleges and universities to set up an information assurance/cyber security portfolio," he said.

Ensuring people who didn't grow up in the Internet age are security-aware is one of the major challenges facing those who secure the network, Alexander said.

The number of exploits of mobile technology has almost doubled over the past year, he said, and many people don't realize that phones are tied into the same digital network infrastructure as computers.

Alexander defined exploits as the means that a hacker uses to penetrate a system, including mobile phones or tablets, to potentially steal files and credentials or jump to another computer.

"The attack surfaces for adversaries to get on the internet now include all those mobile devices," Alexander said. And mobile security lags behind that of cyber security for landline devices like desktop computers.

Alexander said the Department of Defense, in concert with agencies like the Department of Homeland Security and the Federal Bureau of Investigation, works

together with industry to secure network devices.

"If we identify a problem, we jointly give that back to industry and say 'Here's a problem we found,'" Alexander said.

Using the nuclear model, or concentrating solely on major nation-states, to analyze the cyber threat is wrong, he said. Several nations are capable of serious cyber attacks, he explained, but anyone who finds vulnerabilities in the network infrastructure could cause tremendous problems.

Industry and government must work as a team to combat these threats, Alexander said.

"There are great folks in industry who have some great insights," he said. "That's the only way that we can prevent those several states from mounting a real attack on this nation's cyber."

In addition, deterrence theory worked for nuclear weapons in part because the decision time was much slower than it is for cyber threats.

"A piece of information can circumnavigate the globe in about 133-134 milliseconds," he said. "Your decision space in cyber [is] half that--60 seconds."

"My concern is...you've seen disruptions like in Estonia in 2007, in Georgia, Latvia, Lithuania, Azerbaijan, Kyrgyzstan, you could go on," he said. "We've seen them here in the United States... What I'm concerned about is the shift to destructive [attacks]. Those are the things that will hurt our nation."

Disruptive attacks, like distributed denial-of-service attacks, are aimed at interrupting the flow communication or finance, but aren't designed to cause long-term damage.

In contrast, destructive attacks are designed to destroy parts of the network infrastructure, like routers or servers, which would have to be replaced in order to resume normal operations, Alexander said. In some cases this could take weeks or months.

Congress is considering bills that would give the Department of Homeland Security a greater role in setting performance requirements for network industries. Alexander said this legislation is important to assist in setting network infrastructure standards.

Both parties have something to bring to the table, he said. Industry knows things that government doesn't, and government knows things that industry doesn't.

"If we were to be completely candid here, the reality is that industry is getting hacked [and] government is getting hacked," he said. "What we need to do is come together and form best practices."

Government-civil partnerships open up the possibility that the U.S. can accomplish things in cyber space that no other nation has the capability to accomplish, Alexander said.

"When we put together this ability for our nation to work as a team in cyber space, what that allows us to do now is do things that other countries aren't capable of doing in defending the nation," Alexander said.

Because attributing the source of a cyber attack is difficult, the focus is currently on defense rather than offense, Alexander said.

"Today, the offense clearly has the advantage," he said. "Get cyber legislation in there, bring industry and government together, and now we have the capability to say 'You don't want to attack us. We can stop it and there are other things that we can do to really make this hurt.'"

"The key is having a defensible capability that can survive that first onslaught," Alexander said.

Source URL (retrieved on *03/08/2014 - 7:19pm*):
http://www.ecnmag.com/news/2012/07/cybercom-chief-us-unprepared-serious-cyber-attacks?qt-video_of_the_day=0