

Experts warn of catastrophe from cyberattacks

by [Elinor Mills](#)

263

retweet

Share

26

Computer-based network attacks are slowly bleeding U.S. businesses of revenue and market advantage, while the government faces the prospect of losing in an all-out cyberwar, experts told Senators in a hearing on Tuesday.

"If the nation went to war today in a cyberwar, we would lose," said Michael McConnell, executive vice president of Booz Allen Hamilton's national security business and a former director of national security and national intelligence. "We're the most vulnerable. We're the most connected. We have the most to lose."

The U.S. will not be able to mitigate the risk from cyberattack until the government gets more actively involved in protecting the nation's network, which may not occur until after a "catastrophic event" happens, McConnell said in testimony during a [hearing of the Senate Committee on Commerce, Science and Transportation](#).

"The government's role will change to become more active," he said. "We're going to morph the Internet from '.com' to '.secure.'"

The subject of the hearing was the Cyber Security Act of 2009, which would regulate organizations and companies that provide critical infrastructure for the U.S., require licensing and certification for cybersecurity professionals, and provide funding for grant and scholarship programs. The U.S. House of Representatives passed its version of the Cyber Security Act [earlier this month](#).

The bill is necessary and overdue, said James Lewis, a senior fellow at the nonprofit Center for Strategic and International Studies (CSIS). The U.S. is "under attack every day, losing every day vital secrets. We can not wait," he said. "We need a new



Vice Admiral Michael McConnell, who works for Booz Allen Hamilton and used to be director of national security and intelligence for the U.S. government. (Credit: U.S. Senate)



James A. Lewis, senior fellow at the Center for Strategic and International Studies.

(Credit: U.S. Senate)

"I don't worry about terrorists (because)...terrorists are nuts. If they had the ability to attack us they would have used it," he said. "There are people who could attack us now: Russia, China, some others, our potential military opponents. And we know they've done reconnaissance on the electrical grid.

"Could they turn off the electrical grid in a conflict over Taiwan or Georgia? Sure. That's what it would look like," Lewis said.

Cyberattackers are stealing "massive" amounts of business information that is compromising U.S. companies and markets, according to Scott Borg, chief economist at the nonprofit U.S. Cyber Consequences Unit. "Cyberattacks are already damaging the American economy much more than is generally recognized," he said. "The loss is greater than losses due to identity theft and credit card fraud."

Mary Ann Davidson, chief security officer at Oracle, warned of the dangers of linking SCADA (Supervisory Control and Data Acquisition) systems for monitoring and controlling critical infrastructure [with the Internet](#).

"We know the SCADA protocols used in control systems were not designed to be attack resistant. They were originally used in electro-mechanical systems where you had to physically access the system, turn the knob, and so on," he said. "Now we are increasingly moving to the IP-based control systems and connecting them to corporate networks that are in turn connected to the Internet.

"We know some smart grid devices are hackable," she said. "We know there are PDAs, digital

framework for cybersecurity and this bill helps provide that."

"A cyberattack would be like being bled to death and not noticing it and that's kind of what's happening now,"

Lewis said when asked to define what a cyber attack is.

"The cyberattack is mainly espionage, some crime," he added, noting as an example an attack in which \$9.8 million was extracted from ATMs over a three-day weekend.

"I don't worry about terrorists (because)...terrorists are nuts. If they had the ability to attack us they would have



Mary Ann Davidson, chief security officer at Oracle.

(Credit: U.S. Senate)

assistants, that talk SCADA because it's just so expensive to send a technician to the plant. Dare I say move the control rods in and out of the reactor? There's an app for that."



Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. [E-mail Elinor](#).

Topics: [Criminal Hackers](#), [Security](#), [Privacy and data protection](#)

Tags: [cyber security](#), [government](#)

Share: [Digg](#) [Del.icio.us](#) [Reddit](#)  [Yahoo! Buzz](#) [Facebook](#) [Twitter](#)