



FB-17146-00

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit [www.djreprints.com](http://www.djreprints.com)

[See a sample reprint in PDF format.](#) [Order a reprint of this article now](#)

**THE WALL STREET JOURNAL**  
WSJ.com

TECHNOLOGY | NOVEMBER 19, 2009

## FBI Suspects Terrorists Are Exploring Cyber Attacks

By SIOBHAN GORMAN

The Federal Bureau of Investigation is looking at people with suspected links to al Qaeda who have shown an interest in mounting an attack on computer systems that control critical U.S. infrastructure, a senior official told Congress Tuesday.

While there is no evidence that terrorist groups have developed sophisticated cyber-attack capabilities, a lack of security protections in U.S. computer software increases the likelihood that terrorists could execute attacks in the future, the official warned.

If terrorists were to amass such capabilities, they would be wielded with "destructive and deadly intent," Steven Chabinsky, deputy assistant director of the FBI's Cyber Division, told the Senate Judiciary Committee Tuesday.

"The FBI is aware of and investigating individuals who are affiliated with or sympathetic to al Qaeda who have recognized and discussed the vulnerabilities of the U.S. infrastructure to cyber-attack," Mr. Chabinsky told the committee, without providing details.

Such infrastructure could include power grids and transportation systems.

The control systems of U.S. infrastructure as well as money transfers are now connected directly or indirectly to the Internet. Hackers have been able to penetrate computer systems running components of the U.S. electric grid as well as divert bank transfers.

In an interview Tuesday, former Homeland Security Secretary Michael Chertoff said al Qaeda already has some cyber-attack capability. "I don't think they're the most capable in the world, but they have some capability," he said.

Mr. Chertoff said he expects al Qaeda to develop more cyber-attack skills that would allow them to attack infrastructure that is less well protected, perhaps in the transportation and energy sectors. "It's only a matter of time," he said. "They're getting the capability to do some damage."

These descriptions reinforced concerns that former Director of National Intelligence Mike McConnell raised publicly last month about the potential for a terrorist attack on the computer systems and data underpinning the U.S. financial sector.

"I am worried about some terrorist group [with] the capability to destroy the U.S. money supply," Mr. McConnell said. The impact of such an attack would be "an order of magnitude greater" than the Sept. 11 terrorist attacks, he said.

At the Senate hearing, officials from the Homeland Security and Justice departments also told the panel that the country isn't fully prepared for a cyber-attack and current laws don't provide

an adequate framework for the government to fend off such attacks.

"We do need to step up our defensive game," said Philip Reitinger, a Homeland Security deputy undersecretary in charge of cybersecurity. He said U.S. systems are attacked every day by criminals and other adversaries who steal money to fund terrorist or criminal activities, as well as valuable information.

Among the chief areas of concern, Mr. Reitinger said, are vulnerabilities introduced when components of technology systems aren't properly vetted for security gaps before they are assembled into larger systems.

Officials also hinted at an internal battle brewing over whether laws that govern technology and surveillance need to be changed to better fend off cyber-attacks.

Associate Attorney General James Baker said the laws are not adequate, when pressed by Sen. Sheldon Whitehouse, a Rhode Island Democrat.

"We are definitely debating these kinds of issues inside the administration," Mr. Baker added.

Separately, the computer antivirus company [McAfee Inc.](#) issued a report by Paul Kurtz, who led the cyber-security review for the Obama transition team. He concluded that some cyber-attacks in 2007, including Israeli cyber-attacks on Syria and U.S. cyber-weapons employed in Iraq, constitute cyber-warfare.

The report is the first attempt to spell out characteristics of cyber-warfare and analyze how different attacks measure up.

**Write to Siobhan Gorman at [siobhan.gorman@wsj.com](mailto:siobhan.gorman@wsj.com)**

Printed in The Wall Street Journal, page A9

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit

[www.djreprints.com](http://www.djreprints.com)