

February 16, 2010 6:42 p.m. EST

Fact Check: Cyberattack threat

By **Jim Dexter**, CNN

STORY HIGHLIGHTS

- Most U.S. Internet executives in survey expect "major cyberincident" within two years
- Think tank's Robert Knake: Economic impact of major cyberincident may be limited
- Knake compares potential impact to that of 2003 Northeast blackout
- Knake: Nations that have ability to deliver devastating cyberstrike have much to lose

RELATED TOPICS

- [Computer Crime](#)
- [Computer Security](#)

(CNN) -- A Washington think tank staged a mock cyberattack on the United States on Tuesday in a bid to evaluate strategies for fighting cyberterrorists. Former senior government officials gathered at the Bipartisan Policy Center to play the roles of Cabinet members responding to a simulated attack on the nation's computer infrastructure.

In his annual threat assessment, National Intelligence Director Dennis Blair recently declared that a "successful cyberattack against a major financial service provider could severely impact the national economy, while cyberattacks against physical infrastructure computer systems, such as those that control power grids or oil refineries, have the potential to disrupt services for hours to weeks." After hearing Blair's testimony, Senate Intelligence Chairman Dianne Feinstein, D-California, responded, "The need to develop an overall cybersecurity strategy is very clear."

Fact Check: Is there consensus on the likelihood of a cyberattack against the United States?

-- According to the Center for Strategic and International Studies (CSIS), "Critical infrastructure owners and operators report that their networks and control systems are under repeated cyberattack, often from high-level adversaries like foreign nation-states." Sixty percent of U.S. Internet technology and infrastructure executives questioned in a recent CSIS survey expect to see a "major cyberincident" (an outage of at least 24 hours, a loss of life or a failure of a company) within two years.

-- Despite those concerns, the economic impact of a major cyberincident may be limited. Robert Knake of the Council on Foreign Relations compared the potential impact to the 2003 Northeast blackout, which cut service to 50 million people in the United States and Canada for up to four days. "Economists place the cost of that event between \$4.5 [billion] and \$10 billion," he writes, calling that "a blip in the \$14.2 trillion economy."

-- Knake also writes that "only a handful of sophisticated nation-states currently have the ability to carry out a devastating cyberstrike." He suggests that those nations would be reluctant to launch a major attack, saying that they "also have vulnerable systems, as well as a lot to lose, in any conflict, cyber or otherwise." Stewart Baker of CSIS, however, warns that as years go by, more and smaller countries will acquire the ability to launch serious attacks.

-- Professor Irving Lachow of National Defense University, which trains government and Pentagon leaders, defines cyberterrorism as a computer-based attack or threat made for political, religious or ideological reasons, and designed to generate fear comparable to that from a physical act of terrorism. He says under that definition, there has never been a single documented incidence of cyberterrorism against the U.S. government.

-- In a 2007 paper, Lachow and Courtney Richardson, also of National Defense University, argued that terrorists "prefer to inflict damage with physical means" because most cyberattacks "are not going to cause the levels of fear desired by most terrorists."

Bottom Line: While many experts agree that the risk of a cyberattack against the United States is real, there is no consensus as to how likely that attack might be.

CNN's Erin Levin contributed to this report.

Find this article at: <http://www.cnn.com/2010/TECH/02/16/fact.check.cyber.threat/index.html?hpt=Sbin>