

washingtonpost.com

## Cyber Attack Data-Sharing Is Lacking, Congress Told

Intelligence Experts Urge Coordinated Strategy for Private Sector

By Ellen Nakashima  
Washington Post Staff Writer  
Friday, September 19, 2008; D02

U.S. intelligence agencies are unable to share information about foreign cyber attacks against companies for fear of jeopardizing intelligence-gathering sources and methods, cyber security expert [Paul B. Kurtz](#) told lawmakers yesterday.

Kurtz, who served on the [National Security Council](#) in the Clinton and Bush administrations, spoke at the first open hearing on cyber security held by the House Permanent Select Committee on Intelligence. He and other experts discussed [President Bush's](#) Comprehensive National Cybersecurity Initiative, disclosed in January, which focuses on cyber espionage against government systems and, they said, does not adequately address the private sector. There is no coordinated strategy or mechanism for sharing intelligence about intrusions with companies, nor is there a systematic way for companies to share information with the government, said the panelists, who are members of the [Center for Strategic and International Studies](#) commission on cyber security, set up last year to advise the next administration.

While certain information must remain classified, "the government needs to do better" at sharing unclassified information about cyber attacks, said Rep. [Silvestre Reyes](#) (D-Tex.), who chairs the intelligence committee. "Everyone stands to benefit from an improved two-way information flow."

Ross Feinstein, deputy press secretary for the [Office of the Director of National Intelligence](#), countered the panelists' testimony. "The intelligence community works closely with law enforcement on cyber intrusions to share knowledge that might assist in their investigations and with the [Department of Homeland Security](#) to assist with their infrastructure protection efforts," he said in an e-mail after the hearing. "Through established channels, information is also provided to the victims to help them understand potential vulnerabilities and help protect their systems."

Industry representatives pushed for cooperation. "We would certainly want to participate in any government effort that gives us a view of what's happening in the broader cyber network, using the government as a hub for sharing, if there's a benefit to us," panelist John C. Nagengast, director of national information systems at AT&T, said after the hearing. "We know what's happening in our network. Qwest knows what's happening in its network. [Verizon](#) knows what's happening in its network."

Telecom companies may monitor and collect data to protect their own networks, but they cannot share that information freely with the federal government absent a court order, said [James A. Lewis](#), the [CSIS](#) commission program manager.

Rep. Jim Langevin (D-R.I.), a member of the intelligence committee who chairs the Homeland Security subcommittee on cyber security, said inconsistent federal policies leave the energy grid vulnerable to cyber attack.

Advertisement



3G LaptopConnect Card

WORKS ON THE NETWORK WITH THE BEST COVERAGE\*

CONNECT NOW

FREE after mail-in rebate

ROLL OVER FOR DETAILS

\*based on global coverage

More bars in more places™

at&t

Kurtz expressed concern about the breadth of the attacks. "American industry and government are spending billions of dollars to develop new products and technology that are being stolen at little to no cost by our adversaries," he said. "Nothing is off limits -- pharmaceuticals, biotech, IT, engine design . . . weapons design."

A key issue for policymakers is how the government can effectively monitor private networks for intrusions without infringing on the privacy rights of Americans whose data flow through those networks.

Industry's annual loss of intellectual property has been estimated at more than \$200 billion a year, Kurtz said. One defense contractor recently spent up to \$15 billion to repair the damage caused by a cyber attack, said Melissa Hathaway, a senior adviser on the [White House](#) cyber security initiative.

### Post a Comment

[View all comments](#) that have been posted about this article.

You must be logged in to leave a comment. [Login](#) | [Register](#)

Submit

Comments that include profanity or personal attacks or other inappropriate comments or material will be removed from the site. Additionally, entries that are unsigned or contain "signatures" by someone other than the actual author will be removed. Finally, we will take steps to block users who violate any of our posting standards, terms of use or privacy policies or any other policies governing this site. Please review the [full rules](#) governing commentaries and discussions. You are fully responsible for the content that you post.

© 2008 The Washington Post Company