

washingtonpost.com

## Partnering for Cyberspace Security

By Walter Pincus

Monday, November 3, 2008; A19

In two recent speeches that have attracted little notice, Donald Kerr, principal deputy director of national intelligence, has called for a radical new relationship between government and the private sector to counter what he called the "malicious activity in cyberspace [that] is a growing threat to everyone."

Kerr said the most serious challenge to the nation's economy and security is protecting the intellectual property of government and the private sector that is the basis for advancements in science and technology.

"I have a deep concern . . . that the intelligence community has still not properly aligned its response to what I would call this period of amazing innovation -- the 'technological Wild West' -- by grasping the full range of opportunities and threats that technology provides to us," he said at the annual symposium of the Association for Intelligence Officers on Oct. 24.

"Major losses of information and value for our government programs typically aren't from spies . . . In fact, one of the great concerns I have is that so much of the new capabilities that we're all going to depend on aren't any longer developed in government labs under government contract."

Calling for "a fundamental rethinking of our government's traditional relationship with the private sector," Kerr said that "a high percentage of our critical information infrastructure is privately owned, and both government and industry must recognize that an individual vulnerability is a common weakness."

Hackers steal proprietary information, shut down systems and corrupt the integrity of information by inserting erroneous data, he said. He described "supply-chain attacks" in which adversaries plant vulnerabilities in communications hardware and other high-tech equipment "that can be used later to bring down systems or cripple our infrastructure."

Kerr offered some far-reaching solutions in a talk Wednesday during another symposium, sponsored by the Office of the National Counterintelligence Executive, which is part of his organization.

One approach would have the government take equity stakes in companies developing technical products, in effect expanding the practice of In-Q-Tel, the [CIA](#) entity that invests in companies.

Another proposal is to provide the same protective capabilities applied to government Web sites, ending in .gov and .mil, to the private industry's sites, ending in .com, which Kerr said have close to 98 percent of the nation's most important information.

He also suggested that the government ask insurers whether they cover "a failure to protect intellectual capital." That way, Kerr said, the insurers, through their premiums, "provide an incentive for companies, in fact, to pay attention to protecting their intellectual property."

Advertisement



In the past, Kerr said, when the director of central intelligence or the [FBI](#) chief faced similar problems, they would meet privately with leaders of companies involved in new technologies, seeking cooperation and perhaps access to their products. "What's the modern equivalent of what used to be done?" Kerr asked.

"We have a responsibility . . . to help those companies that we take an equity stake in or those that are just out there in the U.S. economy, to protect the most valuable assets they have, their ideas and the people who create them," he said.

*National security and intelligence reporter Walter Pincus pores over the speeches, reports, transcripts and other documents that flood Washington and every week uncovers the fine print that rarely makes headlines -- but should. If you have any items that fit the bill, please send them to [fineprint@washpost.com](mailto:fineprint@washpost.com).*

### 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

#### Ads by Google

##### [Managed Network Firewall](#)

World-Class Perimeter Defenses With 24/7 Security Monitoring & Mgmt.

[DedicatedServer.com/Manage-Firewall](http://DedicatedServer.com/Manage-Firewall)

##### [PCI DSS Solutions](#)

Level 1 PCI DSS Certified Provider GPCI Certified Professionals

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

##### [PCI Compliant Solutions](#)

PCI Compliance w SIEM, IPS & DAM Free Compliance Whitepaper

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