

## CYBERSECURITY

## U.S. must craft cyberwarfare battle strategy

- By [William Jackson](#)
- Feb 18, 2009

America has to face up to the realities of cyberwarfare with tactical and strategic planning, Kurtz says

The intelligence community and the military have crucial roles to play in protecting cyber space, former presidential adviser Paul E. Kurtz said Wednesday, and a clear command and control structure is needed to ensure that our information infrastructure can survive and recover from major disruptions.

In his opening address at the Black Hat Federal security conference being held in Arlington, Va., Kurtz, who served on the National and Homeland Security councils under presidents Bill Clinton and George W. Bush, said the nation has been reluctant to consider the proper role of government in regulating and defending cyberspace. He said it is important that these decisions be made openly after public discussion rather than allowed to happen behind closed doors.

"To those who object to the militarization of cyberspace, I would say, it's too late: We're already there," Kurtz said.

Kurtz, who recently served as cybersecurity adviser on President Barack Obama's transition team, steered clear of discussing his advice to the new administration. But he praised the [60-day review](#) of federal cybersecurity initiatives announced by the president on Feb. 9 and called Melissa Hathaway, the Bush administration official tapped to conduct it, "exceptionally capable."

He said the United States should apply some of the lessons learned during the Cold War to cyber conflicts now simmering online. Cyber warfare is not as simple as the bipolar confrontation between the Western democracies and the Soviet bloc, Kurtz said. It is multilateral standoff involving multiple nations, shadowy organizations, and individual hackers and criminals.

"But I do think a number of concepts from the Cold War may apply, and one of these is deterrence," he added.

A clear policy of deterrence by the United States and its allies helped to avoid the use of nuclear weapons. But no similar policy has been established for battles fought over networks. There is no definition of cyberwarfare, no policy on how and when cyber weapons should be deployed and used, and we do not have a clear idea of who our enemies are.

"We must begin by addressing the question of attribution," Kurtz said. The ability to collect, share and analyze data in order to tailor responses to a threat is "the beginning of a deterrence policy."

That ability will require the efforts of the intelligence community, in cooperation with law enforcement and the private sector, he said. Each of these sectors now collects large amounts of data, but the same inability to share and "connect the dots" that led to the 2001 terrorist attacks still plague our cybersecurity, he said.

"There is a reluctance to play ball with the intelligence community," Kurtz said. This is partly because of the federal government's unwillingness to share its data with others. Policies are needed to enable and encourage [information/data] sharing, with proper government oversight to ensure privacy and civil liberties are not violated, he said. He envisioned a cyber security fusion center that would incorporate the capability of existing organization such as the Homeland Security Department and National Security Agency, without replacing them. Such a center would be able not only to collect and analyze data, but also to control responses.

These polices need to be extended to other countries, and clear command and control structures set up to guide the government's response to advanced and persistent attacks that pose a threat to our infrastructure. Such policies and controls for the use of cyber weapons could help avoid the escalation of conflict with the use of physical weapons, Kurtz said.

[Replay](#)**IBM System x3350 Express**

\$1,849 or \$48/month

[Learn more.](#)ibm express  
advantage™**IBM**

The country has yet to adequately address how the nation would respond to a serious disruption of the Internet.

"I am exceptionally concerned about 'cyber-Katrina,'" he said, referring to the botched federal response to the 2005 hurricane. "Is there a FEMA for the Internet? No. Who would be in charge of restoring the infrastructure? We don't have an answer for that today."

He said he would like to see a triumvirate of the Homeland Security and Defense departments and the Federal Communications Commission assume this task, with help from other agencies as needed. But more important than coming up with final answers to such questions is beginning a public discussion so the answers can be arrived at transparently and with proper oversight, he added.

#### About the Author

William Jackson is a senior writer for GCN.



© 1996-2009 1105 Media, Inc. All Rights Reserved.