


Switch to **SUSE® Linux Enterprise** and save up to 50% over Red Hat support.
[Learn more →](#)



Novell
Making IT Work As One™

www.internetnews.com/security/article.php/3839241

[Back to Article](#)

U.S. Reviewing Cyber Threat to Power Grid

By Larry Barrett

September 15, 2009

Officials at the U.S. Department of Homeland Security Tuesday said they are reviewing a startling report by a Chinese research scientist that outlines just how vulnerable information systems responsible for maintaining the grid powering the entire West Coast are to a possible cyber terrorism attack.

The report, which has been available online since March, was something of a pet project for Jian-Wei Wang, a network analyst at China's Dalian University of Technology. His study confirmed the fears of many technologists and government officials: a technology-assisted attack on just one subnetwork supporting the power grid would likely have a catastrophic impact on the entire West Coast.

"At this point, our command and control folks are looking into the report and making every effort to protect the nation's power grid infrastructure," DHS spokesman John Verrico said in an interview with *InternetNews.com*. "Right now I can tell you we're in the process of rolling out new technology that addresses this threat."

In 2003, the devastating Northeast blackout essentially shutdown New York City and a wide swatch of the East Coast and Midwest, resulting in more than \$10 billion in economic loss. Recent intelligence reports compiled by DHS and the CIA claim that hackers based in China have compromised the U.S. power grid twice in the past decade.

Some officials have suggested that hackers may have been responsible for the 2003 blackout despite initial reports that an Ohio generation plant operated by American Electric and Power (AEP) sent a surge into the system that caused a massive, cascading failure. A worm in the plant's non-power systems was said to be coincidental.

The Obama administration is taking the threat seriously and plans to invest up to \$200 million on so-called smart grid technologies to create a digitally connected power grid to help insulate the nation's electrical supply from terrorist attacks and innocent mistakes alike.

However, most of the nation's power grid and equipment hasn't been updated since the 1940s. And the prospect of connecting such a crucial component of the nation's security and economy to the Internet raises as many potential problems as it solves.

"Energy and power supply systems do have vulnerabilities," Tiffany Jones, Symantec's director of public policy and government relations, told *InternetNews.com* in March after



CLICK HERE
to find out more

Copyright © 2009 CA. All rights reserved.

ca Software

government officials confirmed that spies had twice compromised the U.S. power grid in the past decade.

At the time, Jones said challenge for technologists is that most power systems and their supporting software and hardware were not designed to be connected to the Internet. "Adding security onto these systems can slow things down," she said. "We need more research and development."

Opening up the electrical grid as a distribution system for the Internet and communications could open up the entire power system to greater risk. Utilities have already opened their closed networks and current Supervisory Control and Data Acquisition (SCADA) systems to largely unsecure systems connected to public networks. Adding greater uses for two-way communications, IP packet transmissions and control systems will only increase risk exposure, experts say.

"On the infrastructure side, we've made cyber security a priority," DHS' Verrico said. "Software is a very important part of this because it channels the flow of power and reroutes it."

For now, Verrico said, DHS will examine the doomsday model proffered by Wang to determine just how realistic it is and what can be done to safeguard against the potential vulnerability.

Meanwhile, the DHS has developed what it calls self-limiting, high-temperature superconductor technology that is designed to prevent unwanted power surges that, in turn, affect surrounding subnetworks in the grid—exactly the scenario depicted in Wang's theoretical model.

"We're hoping to launch a pilot of this new technology in New York City in 2010," Verrico said.

WebMediaBrands.



Search:

[WebMediaBrands Corporate Info](#)

Copyright 2009 WebMediaBrands Inc. All Rights Reserved.

[Legal Notices](#), [Licensing](#), [Reprints](#), [Permissions](#), [Privacy Policy](#).

[Advertise](#) | [Newsletters](#) | [Shopping](#) | [E-mail Offers](#) | [Freelance Jobs](#) **new!**

Solutions

Whitepapers and eBooks

The IBM Global CIO Study 2009

Article: Avaya AE Services Provide Rapid Telephony Integration with Facebook

Intel Video: Are Netbooks OK for Business?

Microsoft Article: Make Designer/Developer Collaboration a Reality

Whitepapers: Manage Your Business Infrastructure with IBM

Whitepaper: Maximize Your Storage Investment with HP

Internet.com eBook: Becoming a Better Project Manager

Internet.com eBook: Web Development Frameworks for Java

Microsoft Article: Stress Free and Efficient Designer/Developer Collaboration

Hot List Article: Intel Delivers Security and Manageability for Business PCs

Whitepapers: APC IT InfraStruXure Resource Center

Internet.com eBook: Developing a Content Management System Strategy

MORE WHITEPAPERS, EBOOKS, AND ARTICLES

Webcasts

SAP BusinessObjects Webcast: Unlock the Power of Reporting with Crystal Reports

Ipswitch Video: A Closer Look--WS_FTP Server

MORE WEBCASTS, PODCASTS, AND VIDEOS

Downloads and eKits

[Iron Speed Designer Application Generator](#)

[MORE DOWNLOADS, EKITS, AND FREE TRIALS](#)

Tutorials and Demos

[Demo: Microsoft Virtualization - Data Center to Desktop](#)

[Internet.com Hot List: Get the Inside Scoop on the Hottest IT and Developer Products](#)

[MORE TUTORIALS, DEMOS AND STEP-BY-STEP GUIDES](#)