



## Critical infrastructure central to cyber threat

By **Ben Bain**

Published on April 24, 2008

The United States is increasingly vulnerable to cyberattacks that could have catastrophic effects on critical physical infrastructure, and severely damage the country's economic, military and strategic interests, cybersecurity specialists said today.

The conventional strategic thinking that has driven defense efforts over the past century is becoming irrelevant in today's networked world, according to specialists from the U.S. Cyber Consequences Unit (US-CCU), who spoke at the GovSec, U.S. Law and Ready Conference and Exposition today in Washington.

US-CCU is an independent, nonprofit research institute, set up at the request of the government. Its reports are supplied directly to the government, critical infrastructure industries and the public.

"The change here is so profound that almost all of our previous defense categories are breaking down," said Scott Borg, US-CCU's director. "There is not a clear line there anymore."

Borg said the distinction between physical and information attacks is disappearing, and he cited the lasting effects the terrorist attacks of 2001 had on the information technology infrastructure. Borg said Industrial-era distinctions between the local and the remote, personal and public communications, and military and economic targets are fading and very sophisticated cyberattacks could damage major nations.

Scalable cyberattacks could physically destroy large numbers of electricity generators that would take years to replace, Borg said, adding that if a sizable region's electricity was shut down for an extended period, a majority of that economy would shut down and people likely would die.

Security experts worry that last spring's denial-of-service attacks on facilities in Estonia may be a precursor. Developed countries are considered to be most susceptible to the threats.

"Looking at the many wake-up calls that the international community has had over the past decade...I would say that we have entered an era of cyberterror and perhaps even an era of cyberwar," said Lauri Almann, Estonia's Permanent Undersecretary of Defence, at the conference.

Also, cybersecurity specialists warned that a cyberattack could cause greater economic and physical damage than the United States has suffered.

"We are talking about things much bigger than the Great Depression," said Borg. "We are talking about consequences that are only exceeded by use of nuclear weapons."

His colleague at US-CCU, John Bumgarner, said attacks that could cripple an entire industry can be carried out by a handful of knowledgeable people.

The specialists said the primary target of cyberattacks presently is business information that has been consolidated in a company's information system. This can allow thieves to open a new factory with the exact specifications and settings it took the business they victimized years to perfect.

Borg said he is concerned that although the federal government's efforts to consolidate access points to the government's systems could mitigate information leaks, more consolidation can also make systems more susceptible to damage from attacks. He said that cybersecurity and military efforts should be expanded from focusing on perimeter defenses to also stress resiliency, robust systems and protecting critical infrastructure.

Sponsored By

IBM System x3550 Express  
\$2,454 or \$63/MONTH

Learn more.

Replay.

IBM

ibm express advantage™

intel  
Xeon  
POWER  
Powerful.  
Efficient.

Homeland Security Department officials who have been rolling out the Bush administration's new classified cyberinitiative so far have stressed beefing up intrusion detection and improving coordination between federal agencies and the private sector, which owns approximately 85 percent of the country's critical infrastructure.

Homeland Security Presidential Directive 7, issued in December 2003, designated DHS as the lead agency for protecting critical infrastructure. DHS' 2006 National Infrastructure Protection Plan designated the roles that several agencies have in protecting different sectors of critical infrastructure.

US-CCU has developed a list of critical infrastructure groups based on how significant they are to the country's economy. The defense industry ranks only as the fourth most economically significant group.

The study ranks the Critical Infrastructure Groups (CIG) in the following order:

- Electric power, oil and gas fuel, telecommunications/Internet, banking.
- Chemical industries, water and sanitation, air and ground transport.
- Hospitals and health care, police and fire departments.
- Electronic, automotive and defense industries.
- Food processing, agriculture and national monuments, icons.

Almann said another challenge is that authorities are often unable to attribute attacks because of legal and technological challenges.

"Never prepare for the last war," Almann said. "We should prepare for the next war and let me tell you, next time when an attack like this occurs against any country it will be more painful, it will be more sophisticated."

*1105 Media, Federal Computer Week's parent company, sponsored the GovSec, U.S. Law and Ready Conference and Exposition.*

**Network, TIC and Beyond:**  
**Connecting the Dots**

Hear From These Government Experts:

May 13<sup>th</sup> • Hilton McLean Tysons Corner

Register Today!

© 1996-2008 1105 Media, Inc. All Rights Reserved.