http://www.forbes.com/2008/05/22/cyberwar-breach-government-tech-security_cx_ag_0521cyber.html

Security

Congress Alarmed At Cyber-Vulnerability Of Power Grid

Andy Greenberg, 05.22.08, 3:00 AM ET

Last June, the Department of Homeland Security leaked a video documenting a disturbing experiment. Using only digital means, researchers hacked into a power plant's generator and caused it to cough and shake before shutting down in a cloud of black smoke.

That clip, demonstrating what has since become known as the Aurora vulnerability, served as a wake-up call for regulators, highlighting the need to guard against cyber-security threats to critical infrastructure like power plants and the telecom system. But at a hearing Wednesday, members of the House Committee on Homeland Security warned that those regulatory bodies aren't moving fast enough.

"I think we could search far and wide and not find a more disorganized response to a national security issue of this import," said Rep. James Langevin (D-R.I.), chairman of the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology. He pointed a finger to several groups: the DHS for giving scanty details of its video-taped simulation; the power industry for working too slowly to mitigate the threat; and the North American Electric Reliability Corporation, an industry group, for failing in its role as the self-regulatory body assigned to ensure a consistent national power supply. "Everything about the way this vulnerability was handled … leaves me with little confidence that we're ready or willing to deal with the cyber security threat," he said.

The House's criticisms focused primarily on the electric utility industry group, NERC. They argued that the advisories issued by NERC are ineffective and that it has repeatedly misled the House in its investigation of the Aurora vulnerability.

Rep. Bill Pascrell (D-N.J.) recalled that in a subcommittee hearing last October on the Aurora vulnerability, a NERC representative told him that 75% of the nation's power plants had made progress in securing their systems against cyber threats. But when the subcommittee requested that survey, Pascrell said, it became clear that NERC had only performed the research two days after the subcommittee hearing.

"You are not going to sit there and waste my time telling us you're doing the job you're supposed to do," Pascrell said. "Who do you think we are, a bunch of jerks?"

In response to the committee's attacks, NERC Chief Executive Richard Sergel argued that his organization had made progress by putting in place a formal mechanism for issuing alerts to 1,800 owners and operators of the national power grid. He also pointed to a new set of security guidelines created in

cooperation with the Federal Energy Regulatory Commission. Those guideline begin to take affect in July but will not become mandatory until 2010. At that time, FERC will have the power to charge power companies as much as $1 million a day for violating the standards.

But FERC itself argued in the hearing that those measures weren't enough. NERC, argued FERC Chairman Joseph Kelliher, only has the power to issue voluntary advisories, not binding requirements. FERC, on the other hand, can create binding regulations like the ones that will take effect in 2010, but not quickly enough to protect against a fast-moving cyber-threat.

Kelliher argued that FERC needed new laws to expand its powers beyond those granted in the Federal Power Act, which he claimed was designed to protect the power grid against the threat of tree branches falling on power lines more than malicious hackers. "A process designed to guard against poor vegetation management is not well suited to guard against national security threats," Kelliher said.

The subcommittee hearing also highlighted a new example: a report by the Government Accounting Office released Wednesday reveals a litany of cyber-security vulnerabilities in the systems of **Tennessee Valley Authority** (nyse: TVC - news - people), the nation's largest public power company. The GAO report said that that TVA had failed to implement simple security measures like updated firewall and anti-virus software. Many access points to the company's network lacked password protection, and some insecure systems connected to TVA's systems for controlling power generation, GAO director of information security Greg Wilshusen told the subcommittee.

TVA's chief operating officer, William McCollum, responded that the company was in the process of complying with the fixes outlined in the GAO's report. He said that TVA had begun addressing 17 of the 19 recommendations even before the GAO began its investigation. McCollum added that the company had even hired an outside "penetration testing" team to probe the system for vulnerabilities, and that the hired testers had failed to access the company's power control systems.

Not every cyber-attack on critical infrastructure has been so successfully thwarted. Last August, SANS Institute Director Alan Paller told Forbes.com that cybercriminals had successfully penetrated and extorted hundreds of millions of dollars from multiple critical infrastructure companies in the previous two years. (See " America's Hackable Backbone") In January, a CIA official revealed that a power outage affecting multiple cities outside the U.S. had been caused by hackers hoping to extort money from the plants' owners. (See: " Hackers Cut Cities' Power")

http://www.forbes.com/2008/05/22/cyberwar-breach-government-tech-security_cx_ag_0521cyber.html

Incidents like these, along with discussion of the Aurora tape, may already be affecting national security policy. In January, President Bush signed a classified document authorizing a plan to spend as much as $30 billion over the next five to seven years to secure government networks, a joint project shared by the DHS, the Office of the Director of National Intelligence and the National Security Agency. At the RSA security conference in San Francisco in April, DHS Secretary Michael Chertoff suggested that the so-called cyber initiative would also ask for the participation of the private sector. "We can't be serious about national security or national cyber security without engaging with the private sector, and not just those in IT, but power plants,financial systems and transportation," he said. (See " Bush's Cyber Secrets Dilemma")

In Wednesday's subcommittee hearing, chairman Langevin expressed a similar desire to extend government cyber-security to critical parts of the private sector. He echoed FERC's argument that new legislation is needed to protect against cyber threats, and that critical infrastructure owned by the private sector should be held to standards outlined by the National Institute of Standards and Technology, (NIST) which defines cyber security regulations for the government.

"Clearly, this is an area where I believe stronger, more comprehensive authorities are needed," Langevin said. "The sooner we can move towards NIST standards, the better off we'll be."