STATEMENT OF SENATOR JON KYL
CHAIRMAN
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY
SENATE JUDICIARY COMMITTEE

"VIRTUAL THREAT, REAL TERROR — CYBERTERRORISM IN THE 21ST CENTURY"

24 FEBRUARY 2004

Overview

On January 27, the Subcommittee on Terrorism, Technology, and Homeland Security examined the security of our seaports, and their vulnerability to terrorist attacks. Today, we will examine the security of cyber infrastructure, and its vulnerability to cyberterrorist attacks.

As the world has grown more connected through the Internet and cyberspace, the dangers associated with attacks on that technology have also increased. The quantity and quality of cyber attacks are on the rise. The number of computer security intrusions increased from 84,000 in 2002 to 137,000 in 2003.[1] Computer viruses are spreading at much faster rates and causing more damage than ever before. While it took 26 hours for a virus in 2001 to infect 300,000 machines worldwide, a virus in February 2003 infected 300,000 machines within only 14 minutes.[2] As Secretary Ridge stated in December, "anywhere there is a computer . . . whether in a corporate building, a home office, or a dorm room . . . if that computer isn't secure, it represents a weak link. Because it only takes one vulnerable system to start a chain reaction that can lead to devastating results."[3]

---

[1] CERT Coordination Center, *CERT/CC Statistics 1988-2003*, available at http://www.cert.org/stats/cert_stats.html.

[2] Fiona Harvey, *Online Crime Set to Rise: Cyberspace: The Fight Against Hackers Is a Big Burden*, FIN. TIMES (London), Dec. 3, 2003, at 3.

[3] Secretary Tom Ridge, Remarks at the National Cyber Security Summit (Dec. 3, 2003).

Since 1997, the Subcommittee has held seven hearings on cyber attacks and critical infrastructure protection. During the most recent of these hearings,[4] witnesses expressed concerns about terrorists conducting cyber attacks against the United States. Terrorists already use cyber tools to raise funds and organize physical attacks; they could use those same tools for conducting cyberwarfare. In 2000, FBI Director Louis Freeh testified before the Subcommittee that cyberterrorism was "a very real, though still largely potential threat."[5] Today's hearing will focus on the status of that threat now, and what we are doing to reduce that threat.

Terrorists are targeting our cyber infrastructure, and we must educate the public about the threat of cyberterrorism. According news reports, data from al Qaeda computers found in Afghanistan show that the group had scouted systems that control critical U.S. infrastructure systems.[6] An attack on these systems could have devastating results, especially if done in conjunction with a physical attack. A study by the National Infrastructure Protection Center concluded that the effects of September 11 would have been "far greater" if launched in conjunction with a cyber attack disabling New York City's water or electrical systems.[7] An attack on these systems would have inhibited

---

[4] *See Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 1st Sess. (July 25, 2001) (S. Hrg. 107-366, Serial No. J-107-22); *Cyber Attack: Improving Prevention and Prosecution: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (Apr. 21, 2000) (S. Hrg. 106-838, Serial No. J-106-79).

[5] *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (Mar. 28, 2000) (S. Hrg. 106-839, Serial No. J-106-72), at 28 (written statement of Hon. Louis Freeh).

[6] David McLemore, *On the Cyberterror Front Lines; San Antonio Carving a Niche by Helping Protect Vital Systems*, DALLAS MORNING NEWS, Sept. 21, 2003, at 31A.

[7] National Infrastructure Protection Center (NIPC), *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption*, at 7 (July 2002). NIPC's functions have since been assumed by the Department of

emergency services from dealing with the crisis, and turned many of the spectators into victims.

Witnesses

The Subcommittee will hear from five witnesses, three experts from the federal government and two experts from the private sector.

Assistant Attorney General John Malcolm, DOJ

John Malcolm is the Deputy Assistant Attorney General in the Criminal Division of the Department of Justice. He oversees the Computer Crime and Intellectual Property Section, the Child Exploitation and Obscenity Section, the Domestic Security Section, and the Office of Special Investigations. An honors graduate of Columbia College and Harvard Law School, Mr. Malcolm served as a law clerk to judges on both the United States District Court for the Northern District of Georgia and the 11th Circuit Court of Appeals.

Deputy Assistant Director Keith Lourdeau, Cyber Division, FBI

Keith Lourdeau is the Deputy Assistant Director of the FBI's Cyber Division. He had previously served as Assistant Special Agent in Charge of the St. Louis Division, where he was responsible for the daily operation of the Division. Mr. Lourdeau entered the FBI in 1986 and has served in the Chicago, Little Rock, and St. Louis field offices. While serving at FBI Headquarters, Mr. Lourdeau was detailed to the CIA to assist in establishing a new initiative between the CIA and the FBI in targeting international organized crime groups.

Homeland Security's Information Analysis and Infrastructure Protection Directorate (IAIP), which is under the direction of the DHS witness, Director Amit Yoran. NIPC was formerly part of the Department of Justice.

Director Amit Yoran, National Cyber Security Division, DHS

Amit Yoran is the Director of the National Cyber Security Division for the Department of Homeland Security. Previously, he served as the Vice President for Managed Security Services at Symantec Corporation where he was primarily responsible for managing security infrastructures in 40 different countries. Before working in the private sector, Mr. Yoran was the Director of the Vulnerability Assessment Program within the Computer Emergency Response Team (CERT) at the Department of Defense and the Network Security Manager and the Department of Defense where he was responsible for maintaining operations of the Pentagon's network.

Dan Verton, Author

Dan Verton is the author of *Black Ice: The Invisible Threat of Cyberterrorism*, a book analyzing al Qaeda's ability to conduct cyber attacks and U.S. vulnerability to cyberterrorists. He is also a senior writer on the staff of Computerworld, covering national cyber security and critical infrastructure protection. Mr. Verton is a former intelligence officer in the U.S. Marine Corps, where he served as senior briefing officer for the Second Marine Expeditionary Force and analyst in charge of the Balkans Task Force from 1994 to 1996.

Howard Schmidt, eBay

Howard Schmidt is the Vice President and Chief Information Security Officer for eBay. Prior to that, Mr. Schmidt served as the Chair of the President's Critical Infrastructure Protection Board in 2003, and as the Special Adviser for Cyberspace Security for the White House from 2001 to 2003. Mr. Schmidt has also worked as the chief security officer for Microsoft and as the head of the Computer Exploitation Team at the FBI's National Drug Intelligence Center. And from 1983 to 1994, he was an officer for the Chandler Police Department in Arizona.

Conclusion

Although the United States has not suffered a major cyberterrorist attack, we must continue to improve the security of our critical infrastructure systems. The more dependent we become on technology, the more we must protect it.

We have a distinguished panel of witnesses before us today. I am interested in examining with them the threats and vulnerabilities that we face, and what Congress can do to help prevent cyberterror and prosecute cybercriminals in the United States and abroad.

I would like to thank Senator Feinstein for her hard work in putting together this hearing. We have always had an excellent working relationship, and I look forward to examining this issue with her.

###