Testimony of

Mr. Keith Lourdeau

February 24, 2004

Testimony of FBI Deputy Assistant Director Keith Lourdeau, Cyber Division
Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security
Hearing on Cyber Terrorism
February 24, 2004

Good Morning Chairman Kyl, and other distinguished Members of the Subcommittee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in combating Cyber Terrorism.

As our nation's economy becomes more dependent on computers, and the Internet becomes an increasingly more integral part of our society, new digital vulnerabilities make U.S. networked systems potential targets to an increasing number of individuals including terrorists. The Director of the FBI has established new priorities protecting the U.S. from terrorist attack as its #1 priority and protecting the U.S. against cyber-based attacks and high-technology crimes as its #3 priority. The FBI's Cyber Division's #1 priority is designated Counterterrorism related computer intrusions.

Within the past several years, the U.S. has been the target of increasingly lethal terrorist attacks which highlight the potential vulnerability of our networked systems. These attacks were carried out by terrorists wanting to harm U.S. interests in order to forward their individual cause. Our networked systems make inviting targets for terrorists due to the potential for large scale impact to the nation. The vulnerabilities to our networked systems arise from a number of sources, such as: easy accessibility to those systems via the Internet; harmful tools that are widely available to anyone with a point-and-click ability; the globalization of our nation's infrastructures increases their exposure to potential harm; and the interdependencies of networked systems make attack consequences harder to predict and perhaps more severe.

It is also crucial to understand the interrelationship between physical and cyber security in the current technological environment. Coordinated attacks on multiple regions could achieve a national effect. The most elaborate boundary control program of firewalls, intrusion detection, and virus filtering will be of little help if an intruder is able to gain physical access to servers, networks, or sensitive information.

Terrorist groups are increasingly adopting the power of modern communications technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fund raising and funds transfer, information gathering, and the like. However, mere terrorist use of information technology is not regarded as cyberterrorism. The true threat of "Cyberterrorism"

will be realized when all the factors that constitute a terrorist attack, coupled with the use of the Internet, are met.

Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda.

To date, cyber attacks by terrorists, or persons affiliated with them, have largely been limited to relatively unsophisticated efforts such as the email bombing of ideological foes or the publication of threatening content. However, increasing technical competency in these groups is resulting in an emerging capability for network-based attacks. Terrorist groups have proven themselves capable of carrying out acts of violence against our nation on a grand scale. The more familiar they become with computers and their potential as a viable weapon against us, the more likely they will try to acquire the skills necessary to carry out a cyberterrorist event.

The FBI assesses the cyberterrorism threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise. Terrorist groups have shown a clear interest in developing basic hacking tools and the FBI predicts that terrorist groups will either develop or hire hackers, particularly for the purpose of complimenting large physical attacks with cyber attacks.

If a terrorist lacked the technical sophistication to conduct a computer attack, and chose to recruit a hacker, potential damage would be increased if that hacker was an insider. Insider attacks originate from a variety of motivations (e.g., financial gain; personal grievances; revenge; recruitment; or coercion). It is not necessarily the motivation that makes insiders dangerous, but the fact that they may have unfiltered access to sensitive computer systems that can place public safety at risk. Moreover, there is an increasing concern over the prevalent trend to outsource, even to foreign conglomerates, for services which were previously handled domestically.

Attacks against regional targets could have a significant effect on computer networks, while coordinated attacks on multiple regions could achieve a national effect with severe repercussions. There are numerous control systems whose destruction would have a far-reaching effect. Large-scale distribution systems, such as those involving natural gas, oil, electric power, and water, tend to use automated supervisory and data acquisition (SCADA) systems for administration. SCADA systems tend to have both cyber and physical vulnerabilities. Poor computer security, lack of encryption, and poor enforcement of user privileges lead to risks to SCADA systems. Poor physical controls can make the disruption of the SCADA system a realistic possibility.

A major method used in preventing cyberterrorism is the sharing of intelligence information. The FBI routinely passes intelligence received in active investigations or developed through research to the intelligence community. Throughout the FBI field offices, Special Agents serve on cyber task forces with other agencies. The FBI is a sponsor/participant in the InterAgency Coordination Cell (IACC) at FBIHQ. This environment of information sharing and cooperation is expanding to include foreign governments such as the "5 Eyes."

Cyber programs are unique in nature. However, taking proactive investigative measures with tools such as Honey Pots/Nets and Undercover Operations enhances our ability to prevent a cyberterrorist attack. The FBI has undertaken the following initiatives to combat cyberterrorism: Cyber Task Forces, Public/Private alliances, International Cyber Investigative Support, Mobile Cyber Assistance Teams, Cyber Action Teams, Cyber Investigators Training, a Cyber Intelligence Center, and Cyber Tactical Analytical Case Support. These programs provide a strategic framework and program management tool for all FBI computer intrusion investigations.

The Computer Intrusion program provides administrative and operational support and guidance to the field offices investigating computer intrusions, assists other FBI programs that have a computer dimension, and coordinates computer intrusion investigations by various criminal investigative and intelligence components of the Federal Government.

The Special Technologies and Applications program supports FBI Counterterrorism computer intrusion-related investigations with all necessary equipment and technical investigative tools.

The Cyber International Investigative program creates the ability to conduct international cyber investigative efforts through coordination with FBI Headquarters Office of International Operations, Legal Attache offices, and foreign law enforcement agencies.

The Cyber Specialized Training Program coordinates with the Engineering Research Facility, Laboratory Division, Training Division, National White Collar Crime Center, private industry, academia and others to deliver training to FBI cyber squads, Task Forces, International Law Enforcement Officers, and others.

In the event of a cyberterrorist attack, the FBI will conduct an intense post-incident investigation to determine the source including the motive and purpose of the attack. In the digital age, data collection in that investigation can be extremely difficult. The computer industry is also conducting research and development involving basic security, such as developing cryptographic hardware which will serve to filter attempts to introduce malicious code or to stop unauthorized activity. Continued research in these areas will only serve to assist the FBI in its work against cyberterrorism.

While the following two incidents were not cyberterrorism, they are an indication of the ability of individuals to gain access to our networked systems and the possible damage that can result.

In 1996, an individual used simple explosive devices to destroy the master terminal of a hydroelectric dam in Oregon. Although there was no effect on the dam's structure, this simple attack completely disabled the dam's power-generating turbines and forced a switch to manual control. A coordinated attack on a region's infrastructure systems (e.g., the SCADA systems that control Washington D.C.'s electric power, natural gas, and water supply) would have a profound effect on the nation's sense of security. This incident demonstrated how minimal sophistication and material can destroy a SCADA system.

In 1997, a juvenile accessed the Generation Digital Loop Carrier System operated by NYNEX. Several commands were sent that disrupted the telephone service to the Federal Aviation Administration Tower at the Worcester Airport, to the Worcester Airport Fire Department and to other related entities such as airport security, the weather service, and various private airfreight companies. As a result of this disruption, the main radio transmitter and the circuit which enabled aircraft to send an electronic signal to activate the runway lights on approach were disabled. This same individual then accessed the loop carrier system for customers in and around Rutland, Massachusetts and sent commands that disabled the telephone service, including the 911 service, throughout the Rutland area.

On May 3, 2003, an e-mail was sent to the National Science Foundation's (NSF) Network Operations Center which read, "I've hacked into the server of your South Pole Research Station. Pay me off, or I will sell the station's data to another country and tell the world how vulnerable you are." The e-mail contained data only found on the NSF's computer systems, proving that this was no hoax. NSF personnel immediately shut down the penetrated servers. During May, the temperature at the South Pole can get down to 70 degrees below zero Fahrenheit; aircraft cannot land there until November due to the harsh weather conditions. The compromised computer systems controlled the life support systems for the 50 scientists "wintering over" at the South Pole Station.

The FBI determined that the hackers were accessing their e-mails from a cyber café in Romania. One of the hop points utilized by the intruder was a computer system in Pittsburgh owned and operated by a trucking company. A hop point is a computer system, usually compromised by the intruder, that is utilized to conceal the true location and identity of the intruder. Joint FBI investigative efforts with the Romanian authorities, in this matter, resulted in the seizure of documents, a credit card used in the extortion scheme, and a computer that contained the very e-mail account that was used to make the demands of the National Science Foundation. On June 3, 2003, two Romanian citizens accused of hacking into the NSF South Pole Research Station were arrested in a joint FBI/Romanian police operation. The two are currently scheduled to stand trial in Romania. A trial date has not been set.

The unique complexity of protecting our nation's networked systems is a daunting task. The key to prevention is effective attack warning and the education of the owners and operators of those systems. The protection of our networked systems is a shared responsibility and partnership between the private sector, state and local law enforcement agencies, U.S. Federal Law Enforcement agencies, the Department of Homeland Security, and the Intelligence Community, both domestic and foreign. The FBI encourages international cooperation to help manage this increasingly global problem.

Defending against a cyber attack also requires the integration of operational, physical, communication and personnel security measures. This involves a full range of matters such as: installing effective passwords, firewall protection, avoidance of unprotected and unnecessarily opened entry points, installation of default configuration and passwords; minimization of placing servers in unprotected areas; and vigilance against disgruntled employees. System administrators must be both vigilant and serious about cyber security.

Synopsis: According to how we have defined cyberterrorism, no cyberterrorist attack has occurred to date. However, in the future cyberterrorism may become a viable option to traditional physical acts of violence due to: its perceived anonymity, the proliferated number of networked targets, its low risk of detection, its low risk of personal injury, low investment requirements, and increased ease and access from various locations. The protection of our networked systems requires the integration of many components and is a shared responsibility between all sectors of our society. The FBI can not do this alone.