Testimony

PREPARED STATEMENT OF SENATOR FRED THOMPSON
CHAIRMAN COMMITTEE ON GOVERNMENTAL AFFAIRS

JUNE 24,1998

"CYBER ATTACK: IS OUR NATION AT RISK?"

The Governmental Affairs Committee today is holding its second in a series of hearings on the security of federal computer systems. Today's hearing will focus on the intelligence community's assessment of the threats to our Nation's information systems.

During our hearing last month, we heard that the foundation of our nation's information infrastructure is riddled with security vulnerabilities and flaws. The LOpht, a hacker think tank which testified at our earlier hearing, stated that they "could very trivially make the Internet unusable for the entire nation." This has serious implications when considering how dependant our society has become on the Internet. LOpht also testified that, given enough resources, a very small group of skilled hackers could wreak havoc on our country -- ranging from shutting down communication systems and utilities to causing unstable financial markets. Dr. Neumann, a renowned computer security expert who also testified, agreed with this, stating that "massive coordinated attacks on our infrastructure are possible; however, it may take a Chernobyl-scale event to raise awareness levels adequately, perhaps bringing several of the national infrastructures to their knees simultaneously."

We cannot wait for an electronic Pearl Harbor or Oklahoma City to recognize there Is a problem. At risk are the systems that control national security, air traffic, finances, power, and communications.

To date, the mainstream media has focused on unsophisticated hacking of government systems. This doesn't accurately represent the seriousness of the threat. We often read about the hackers that have been caught, but what about the sophisticated hackers that aren't detected or caught? What gives me grave concern is that we simply don't know what we don't know. According to a 1996 estimate by the Defense Information Systems Agency, as many as two hundred and fifty thousand attacks occurred on defense systems in 1995. How many of those were actually detected? How many of the perpetrators were caught? How many viruses were left behind? How much critical data was compromised? Unfortunately, we cannot answer these questions.

As the American way of life becomes increasingly dependant on computer systems and the uninterrupted flow of information, the use of information technologies as a tool of warfare and terror is becoming increasingly likely. Instead of confronting us head-to- on the traditional battlefield, adversaries will confront the U.S. at its point of least resistance - that is our information infrastructure. Cyberspace is the battlefield of tomorrow.

This Is well understood by our potential adversaries, whether it be other nations, terrorists, drug cartels, or organized crime groups. They can reach deep into our homeland from the sanctity of their's This is not just a theory. We know for a fact that terrorist and organized crime groups are developing information weapons. A recent Newsweek article claims there are about ten countries, in addition to China and Russia, with Information warfare programs, including Libya, Iraq and Iran -- none of which are considered friends of the U.S., and all of which sponsor anti-American terrorists.

I do not believe that this is a futuristic threat as some portray it -- the threat is real, it Is serious, and it is here today. Cyber weapons are being developed, countries are incorporating strategies into their doctrine, our computer systems are being probed to identify vulnerabilities, and our defenses are weak.

I believe that protecting our nation against cyber attack represents one of the greatest challenges we've faced as a country. We must act NOW to develop the policies, plans, programs, and strategies to deter this threat.

Today we will hear from the leaders of our intelligence community -- the Honorable George Tenet, Director of Central Intelligence, and Lieutenant General Ken Minihan, Director of the National Security Agency. Mr. Tenet will provide an assessment on the threats to our information infrastructure and what is being done to address these threats. General Minihan will testify on the findings from the military exercise "Eligible Receiver" which Identified serious vulnerabilities of our Nation's computer systems.

Return to the Main Page

footer

[Committee Members] [Subcommittees][Special Investigation]
[Jurisdiction] [Hearings] Press Releases] [Sites of Interest