



News from . . .

Senator Dianne Feinstein

of California

Statement of Senator Dianne Feinstein On The Threat of Cyberterrorism February 24, 2004

Washington, DC - The U.S. Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security today convened a hearing to assess the current cyberterror threat and examine how well federal agencies and companies are prepared for it.

Following is the statement of subcommittee ranking member U.S. Senator Dianne Feinstein (D-Calif.):

“You only have to look at the MyDoom virus that recently spread like wildfire across the Internet to understand the threat of cyberterrorism.

MyDoom was responsible for sending 100 million infected emails in its first 36 hours, and accounted for one-third of all emails sent worldwide on one evening.

The virus shut down the website of SCO Group and also attacked the Microsoft website. Damages worldwide ran into hundreds of millions of dollars.

Denial-of-service attacks offer only a small glimpse of the cyberterror threat. A terrorist could theoretically use a computer to:

- open up the flood gates of a dam;
- disrupt the operations of an aircraft control tower;
- shut down the New York Stock Exchange or other important businesses or government agencies; or
- disrupt emergency communications of law enforcement and safety officials.

We’ve been fortunate so far. There are only a couple of historical examples of cyberterrorism.

One oft-cited example is an April 2000 incident in Australia where a disgruntled consultant sabotaged the electronic controls to a sewage system, letting loose million of gallons of sewage on a town.

But the threat of cyberterrorism is uniquely insidious. In contrast to attacks on our ports or biological or chemical weapons, cyberterror does not have to be launched within the U.S. geographical confines.

I would also note that 85 to 90 percent of our nation's cyber-infrastructure remains under the control of the private sector.

The Administration has so far embraced a voluntary market-based approach to cybersecurity.

In December 2002, Governor Gilmore criticized this voluntary approach:

'So far, pure public/private partnerships and market forces are not acting ... to protect the cybercommunity.'

I am concerned that we remain under-prepared for a cyberattack, and, like Governor Gilmore, that market forces and public/private partnerships are inadequate.

Here are some questions I hope the panel can address:

- How real is the cyberterror threat?
- Has the Department of Homeland Security placed a high enough priority on defense against cyberterrorism?
- Are we better prepared today to defend against a cyberattack today than on 9/11?
- Is the current voluntary private sector and government collaboration working?
- Is there more we can or should do to defend ourselves?"

###