Internet 'biggest threat' to the US

LOLITA C BALDOR

http://news.smh.com.au/breaking-news-world/internet-biggest-threat-to-the-us-20091005-gi1v.html

October 5, 2009

The Obama administration wants to convey clear and concise guidance about one of the biggest national security threats in homes and offices - the computer.

The administration wants Americans to think before they click. Know who's on the other side of that instant message. What someone says or does in cyberspace stays in cyberspace - for many to see, steal and use against people and their government.

The internet, said former national intelligence director Michael McConnell, "is the soft underbelly" of the US today. Speaking recently at a new cybersecurity exhibit at the International Spy Museum in Washington, McConnell said the internet has "introduced a level of vulnerability that is unprecedented".

The Pentagon's computer systems are probed 360 million times a day, and one prominent power company has acknowledged that its networks see up to 70,000 scans a day, according to cybersecurity expert James Lewis.

For the most part, those probes of government and critical infrastructure networks are benign. Many, said McConnell, are a nuisance and some are crimes. But the most dangerous are probes aimed at espionage or tampering with or destroying data.

The attackers could be terrorists aiming at the US culture and economy, or nation-states looking to insert malicious computer code into the electrical grid that could be activated weeks or years from now.

"We are the fat kid in the race," said Lewis. "We are the biggest target, we have the most to steal, and everybody wants to get us."

And if, for example, the US gets into a conflict with China over Taiwan, "expect the lights to go out", he said.

The exhibit at the Spy Museum - Weapons of Mass Disruption - tries to bring that threat to life.

A network of neon lights zigzags across the ceiling. Along the walls computer screens light up with harrowing headlines outlining the country's digital dependence. Drinking water, sewer systems, phone lines, banks, air traffic, government systems, all depend on the electric grid, and losing them for weeks would plunge the country into the 1800s.

Suddenly, the lights go out and the room is plunged into silent darkness.

Seconds later as the sound system crackles, a video ticks off a pretend crisis: no food, no water, system shutdown.

That faux threat has become a prime concern for the government, but fully protecting the grid and other critical computer systems are problems still waiting a solution.

Federal agencies, including the Pentagon and the Department of Homeland Security, are pouring more money into hiring computer experts and protecting their networks.

But there are persistent questions about how to ensure internet traffic is safe without violating personal privacy.

One answer, experts said last week, is to begin a broader public dialogue about cybersecurity, making people more aware of the risks and how individuals can do their part at home and at work.

Some will find it easier than others.

Much of the younger generation has grown up online and are more likely to know about secure passwords, antivirus software and dangerous spam emails that look to steal identities, bank accounts and government secrets.

Older people moved into the digital universe as it began to evolve and most have not grown up thinking about how to protect themselves online.

"Detection and prevention are fast, but crime is still faster," said Phil Reitinger, director of the National Cybersecurity Centre.

The key, he said, "is to make sure that we're all getting the word out about not only the seriousness of the threat, but the fairly simple steps that people can take to help secure their systems and their lives and families from the threats that are out there."

Those steps include:

-using antivirus software, spam filters, parental controls and firewalls.

-regularly backing up important files to external computer drives.

-thinking twice before sending information over the internet, particularly when using wireless or unsecured public networks.