

China's Cybertooth Tigers

National Defense: America's electrical grid may have been implanted with cyber-"bombs" waiting to go off. Russia and China are preparing for a new kind of warfare. Where will you be when the lights go out?

On April 1, as part of our "Inside The Stimulus" series, we said the proposed "smart grid" designed to monitor electrical use and distribution would make it easier for hackers to break in and possibly disable parts or all of it. Turns out this was no April Fool's joke.

A few weeks ago the Pentagon released its 2008 report to Congress titled "Military Power of the People's Republic of China." It dealt with more than tanks, planes and missiles. It also dealt with China's capabilities in what's known as "asymmetrical" warfare, specifically cyberwarfare.

The report noted that China's armed forces and other entities "continue to develop and field disruptive military technologies, including those for . . . cyberwarfare." Chinese military doctrine has long emphasized exploiting opponents' weaknesses as much as attacking their strengths.

Since then, Homeland Security has acknowledged reports that foreign hackers had in fact penetrated the U.S. electrical grid and other systems and had left behind embedded software programs that could later be activated to disrupt these systems.

These reports come while the Obama administration is conducting an extensive review of the nation's cybersecurity situation. That report was due April 17 and expected to repeat the recommendations of a study done by the Center for Strategic and International Studies at the request of President Bush.

The Pentagon review listed several examples of Chinese hacking into foreign systems.

A year ago, the computer network at India's Ministry of Internal Affairs was attacked by Chinese hackers as were the government of Belgium's computers a month later.

A cyberattack in June 2007 crippled Secretary of Defense Robert Gates' computer system, leaving some 1,500 Pentagon computers offline for weeks. Among the military units that have been successfully "hacked" are the

Army's 101st and 82nd Airborne Divisions and the 4th Infantry Division.

The Canadian research group Information Warfare Monitor reports that a cyberespionage network based in China had infected 1,295 computers in 103 countries and penetrated systems containing sensitive information in top political, economic and media offices.

China uses cyberwarfare to shut down internal dissent as well as penetrate foreign systems. It employs 39,000 full-time Internet police who double as hackers.

China is not alone. Before the tanks rolled into Georgia, Moscow attacked that tiny country's cyberinfrastructure and rendered useless the command and control systems of Georgian President Mikhail Saakashvili.

In 2007, Russia unleashed a monthlong cyberattack on Estonia after it removed a Soviet-era war monument. That attack shut down Estonia's cyberinfrastructure.

CIA senior analyst Tom Donahue said in January 2008 that the agency had evidence of successful cyberattacks against various countries' critical national infrastructures.

"We have information that cyberattacks have been used to disrupt power equipment in several regions outside the U.S.," he said. "In at least one case, the disruption caused a power outage affecting multiple cities."

A March 2007 video of a test by the Idaho National Laboratory shows what kind of damage can be done by a cyberattack. The video showed a power turbine spinning out of control until it became a smoking hulk and shut down as a result of the test cyberattack.

Smart grids make security against cyberattacks more difficult. They require the extension of two-way digital communications right down to "smart meters" in our homes. Each extra "node" on a network is an extra doorway to spies and hackers.

"The severity of what we're seeing is off the charts," said Tom Kellermann, vice president of security awareness for Core Security Technologies and one of those advising President Obama. "Most of the critical infrastructure in the U.S. has been penetrated by state actors."

Despite engagement with Russia and China, they continue to develop new ways to attack us. As we've noted, unless we are prepared our next Pearl Harbor may not begin with an ominous "Tora, Tora, Tora," but with the innocent-sounding, "You've got mail."

Investors Business Daily 20 April 2009 p A15