Friday, August 13, 2010

A Threat Worse Than 9/11

By: Robert Maginnis - Human Events

Two new reports—one secret and one little noticed—confirm America faces a threat far worse than 9/11. We must demand immediate action before the nation is literally thrown back to the Stone Age.

Cyber attacks, the subject of the new reports, are responsible for "the biggest transfer of wealth through theft and piracy in the history of mankind," according to Sen. Sheldon Whitehouse (D.-R.I.). The senator also warns the nation's total dependence on our automated infrastructure—electric grid, air traffic control, manufacturing, and business—and our national defense networks are dangerously vulnerable to this accelerating and insidious threat.

The U.S. Senate Intelligence Committee's cyber task force chaired by Whitehouse filed its secret report last month. The senator said, "The public knows very little about the size and scope of the threat their nation faces." He claims the transfer of wealth attributable to cyber theft and piracy is "perhaps as high as $1 trillion" and he added if the American people "knew how vulnerable America's critical infrastructure is and the national security risk that has resulted, they would demand action."

Whitehouse's alarming comments are reinforced by a little noticed Energy Department report released July 22 which found the computer networks controlling our electric grid are plagued by widespread security flaws that allow our cyber enemies to manipulate the grid and steal critical data. The report, "NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses," was prepared by the Idaho National Laboratory.

The alarming information from both reports is no surprise to our intelligence community. James Clapper, President Obama's nominee to be director of National Intelligence, testified to the far-reaching impact of the cyber threat. "Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication," Clapper testified."

Steven Chabinsky, deputy assistant director of the FBI's cyber division, warns that our vulnerability and the expanding cyber security threat could "challenge our country's very existence." Consider the following evidence and what we must do about it.

Our critical infrastructure is vulnerable. Electric power utilities, for example, are vulnerable because of their growing reliance on Internet-based communication which makes their industrial control systems easy targets for spies and hackers.

In 2008, senior CIA official Tom Donohue told a meeting of utility company representatives in New Orleans that "we have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

Most cyber intrusions are not detected by the utilities but by intelligence agencies. U.S. intelligence officials worry cyber attackers will take control of electrical facilities or even a nuclear power plant, a potentially catastrophic event.

Last year, the Wall Street Journal reported cyber spies penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system. The spies, according to the Journal, were on a mission to navigate the U.S. electrical system and its controls. So far, according to officials, the intruders

haven't sought to damage our power grid or other key infrastructure.

Our Defense Department is a cyber target. Gen. Keith Alexander, the leader of the new U.S. Cyber Command, said the Defense Department systems are probed by unauthorized users roughly 250,000 times an hour, or more than six million times a day. Alexander said the potential for sabotage and destruction is "something we must treat very seriously."

In 2007, a cyber attack forced the Defense Department to take as many as 1,500 computers offline and, according to the Financial Times, the Chinese military cracked into a Pentagon network serving the office of Defense Secretary Robert Gates.

Gen. Kevin Chilton, who heads the U.S. Strategic Command, said "The important thing is that we recognize that we are under assault from the least sophisticated—what I would say the bored teenager—all the way up to the sophisticated nation-state, with some pretty criminal elements sandwiched in-between," said Chilton.

The scope of the state-sponsored threat is sobering. Deputy Defense Secretary William Lynn wrote in the Wall Street Journal that more than 100 intelligence agencies and foreign militaries are actively trying to penetrate U.S. systems and weapons-system blueprints.
State-sponsored cyber intrusions are the worst of our threat. Russia and China stand out as the most persistent at targeting the U.S. and the most dangerous because they have harnessed cyber technology as a military weapon.

In 2007, Moscow orchestrated a massive cyber attack against the small country of Estonia in the wake of a dispute over the relocation of a World War II memorial. That attack shutdown Estonia's economy and government.

Russia used a cyber attack a year later to shutdown the Republic of Georgia's government. That attack coincided with Moscow's ground invasion into South Ossetia making it the first time a cyber attack had coincided with a shooting war.

But the Chinese are our most dangerous cyber foe. The Pentagon's 2006 Military Power of the People's Republic of China report exposed Beijing's growing computer network attack capabilities. That report states "China is developing the ability to launch pre-emptive attacks against enemy computer networks in a crisis."

The report continues, "During a military contingency, information warfare units could support active PLA [People's Liberation Army] forces by conducting 'hacker attacks' and network intrusions, or other forms of 'cyber' warfare, while helping to defend Chinese networks."

The Pentagon's 2009 China report identifies Beijing for serious cyber intrusions. "It remains unclear if these intrusions were conducted by, or with the endorsement of the PLA or other elements of the PRC [People's Republic of China] government" states the report. But the Pentagon acknowledges these intrusions are consistent with China's military writings. It identified suspected Chinese attacks on India, Belgium, and the U.S.

The Pentagon's 2010 China report is now mysteriously five months late. It's possible the update is being held-up because it once again exposes evidence that China is becoming more dangerous in areas like cyber warfare, a concept that is politically inconvenient to the Obama Administration.

The cyber threat is very serious, but to date all the U.S. government seems capable of doing is passing laws, creating organizations, and wringing its rhetorical hands. What we need is real leadership to address four specific challenges.

First, President Obama must rally public awareness to this threat and outline what citizens must do.

Second, the private sector must begin to counter cyber threats. Businesses must train their people and upgrade their computer networks against cyber intrusions. The private sector managing critical infrastructure have no higher priority than closing the security gaps identified in the recent Department of Energy report.

Third, the Justice Department must aggressively stop cyber criminals no matter where they are and put them behind bars.

Finally, the Pentagon's new cyber command must have the authority, means, and approval to take offensive action against state-sponsored cyber attacks but must not violate American civil liberties in the process.

The President must make fighting the cyber war a top priority. Failing to take immediate and appropriate actions such as those outlined above could result in a cyber catastrophe that "challenges our very existence."