

Cyber Warfare

Article submitted by Alex Berta, Jedburgh Information Warfare Director.

Imagine waking up in the morning and your electricity is out. No lights, no heat and no computers. You try to turn on your cell phone but the network is down and so is your access to the Internet. You suddenly feel alone and afraid with no contact to anyone. An army of foreign computer hackers has brought down America's power grid and government operations.

According to cyber security advisors this kind of scenario is very real and the U.S. is unprepared to defend itself.

Cyber sieges do happen and can have a crippling effect on national defense. In August of 2008, Russia launched a cyber attack on the national websites of Georgia, its neighboring country. These attacks coincided with Russia's military campaign in the South Ossetia region. The attacks debilitated Georgian news and government websites and marked one of the first cyber/military wars in modern history.

The U.S. is anticipating the cyber wars of the future and is gearing up to respond and retaliate to the looming threats of both rogue states and powerful nations. Today, at the Mandarin Oriental Hotel in Washington, DC, an independent group of former DHS, CIA and national security advisors launched a three hour cyber attack simulation.

The "Cyber ShockWave" event and was hosted by the Bipartisan Policy Center, a Washington based nonprofit organization. Their mission was to test the U.S. response to a coordinated, international attack on America's technological infrastructure.

The group hired experts in cyber warfare to compose a simulated scenario where a virus attaches itself to a "March Madness" college basketball phone application. In the simulation, the virus replicated and spread through smart phone contact lists until it eventually brought down cellular service for most Americans. Included in the exercise were a number of private companies, such as PayPal and General Dynamics, which have a vested interest in bolstering U.S. cyber defense capabilities.

So how did America fare against a such a strike?

Epic Fail.

“The general consensus of the panel today was that we are not prepared to deal with these kinds of attacks,” said Eileen McMenammin, vice president of communications at the Bipartisan Policy Center. “Whether these threats come from individual hackers, state organizations or terrorist groups, they are very real and something we really need to be prepared for.”

Participants indicated that a large challenge in reacting to a cyber attack is identifying who the attackers are and how to find them. This concern has dogged U.S. cybersecurity experts throughout the modern era.

“It’s very easy for hackers to hide in other people’s computers and servers,” said Lou Von Thaer, a top security expert with General Dynamics, a defense firm based in Falls Church, Va. “We spent a lot of time today trying to figure out who did it and it created a lot of chaos.”

Von Thaer said that the biggest take away from the exercise was that the U.S. government needs to do more work on the policy side and pass better legislation to protect American interests.

“What we’re suggesting is the seat belt analogy,” said Von Thaer. “These days we wouldn’t imagine driving across town without wearing a seat belt. And that’s because now there are laws and regulations that have made seat belt use a standard way of life. We need to have similar standards in the cyber world.”

Don’t train on what you want. Train on what you need. Jedburgh Corp has developed the most innovative information security training available anywhere. Contact us at info@Jedburgh-USA.com to provide feedback on the blog, or discuss your training needs. Also, feel free to post your comments.

Scott Watson
President, Jedburgh Corp
Scott.Watson@Jedburgh-USA.com

