

# Cyber Defenses Get Physical

## Security Intelligence Advisory

On Thursday May 7<sup>th</sup>, 2009 a day that may be written about in the history books of tomorrow, Air Force Gen. Kevin P. Chilton, head of U.S. Strategic Command, told reporters that, "The Law of Armed Conflict will apply to this domain," (meaning cyber space). The U.S. now stands ready to respond with physical military force to acts of cyber aggression. As the frequency, complexity and sophistication of cyber attacks increase, hostile cyber operations continues to grow at an unprecedented rate. "This is not unexpected," said Brian a cyber warfare subject matter expert from Spy-Ops. "It is easy to see how a smart bomb, torpedo or laser guided missile could be used to sever a telecommunications cable, switching complex or even data center as a defensive measure to halt an attack!" He went on to explain that it is not just the military and the government that are at risk. He quoted the following numbers from managed security services provider Solutionary that were used in testimony before the U.S. China Economic and Security Commission hearing last week. "Last month (March 2009) there were 128 acts of cyber aggression each and every minute against their 300+ clients. That's more than two attacks a second! If those numbers were not enough to concern you, the Defense Department said that on one 24 hour period in 2008, the Pentagon was attacked more that 6 million times in one 24 hour period." That is more than 4,100 times a minute or over 69 times a second! In addition, DoD stated they spent more than \$100 million in the last six months responding to and repairing damage from cyber attacks and other computer network problems.

One of the military's greatest concerns of late is that our enemies could or would break into our Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) systems, and intercept or even alter orders being sent to field commanders. He went on to say even though most of the C4ISR systems are classified and isolated from the Internet, the attack on the Pentagon last Novembers showed clearly they are still at risk! At this point, every computer is a potential cyber weapon waiting to be loaded and used by criminal enterprises, terrorist organizations and rogue nation states. Until we accept that fundamental construct and build our defenses capabilities with that construct in mind, our information infrastructure, business systems, government networks and military capabilities are at risk from acts of cyber aggression. The rules of engagement for cyber space are gray or non-existent. Military, governmental and legal authorities need to thoroughly review situation like this and provide guidance on these issues. Furthermore, a full cyber doctrine around acts of cyber aggression must be created now to reduce the possibly of accidentally triggering an international cyber conflict. The question of what constitutes an act of cyber war has been asked multiple times and so far, there is no answer.

### Recent Attack

A new, sophisticated cyber attack was discovered that circumvented advanced security measures. The security measures required two-factor authentication by two separate individuals within the organization. The attack covertly collected the login and authentication information for both parties and then proceeded with its malicious activities.

### Actions

Given the increased cyber threat activity, organizations must remain vigilant. They should:

- Check Firewall Settings
- Review Mobile Device Security
- Apply Software Patches
- Update Security Software
- Reinforce Security Policies
- Update Awareness Training
- Monitor & Spot-check Financial Transactions
- Monitor & Spot-check High Volume Transmission to Specific IP Addresses.

Organizations and governments around the world must increase their cyber security efforts or face the threat of compromise and disruption as well as the possible isolation from the electronic economy!

### Technolytics

4017 Washington Road  
Mail Stop 348  
McMurray, PA 15317  
P 888-650-0800  
F 412-291-1193  
I [www.technolytics.com](http://www.technolytics.com)

**technolytics**