

North Korean

Cyber Capabilities Estimate

As of March 2009

Designation: Unit 121

Established: 1998

Force Size: 12,000 declining with 500 to 1,000 being actual hackers.

Cyber Budget: \$56+ million.

Goal: To increase their military standing by advancing their asymmetric and cyber warfare capabilities.

Experience: Hacked into South Korea and caused substantial damage; hacked into the U.S. Defense Department Systems had moderate impact.

Threat Rating: North Korea is ranked 8th on the cyber capabilities threat matrix developed in August 2007 and updated February 2009.

Offensive Cyber Weapons: North Korea now has the technical capability to construct and deploy an array of cyber weapons. They have moderately advanced distributed denial of service (DDoS) capabilities with moderate virus and malicious code capabilities. Hacking capabilities are moderate to strong with an experience rating of limited to moderate.

Cyber Espionage: Basic to moderately advanced weapons with significant ongoing development into cyber intelligence.

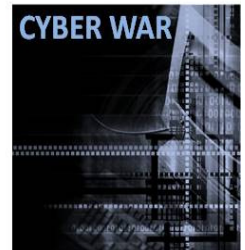
Technolytics warned that North Korea would respond to sanctions imposed by the United Nations back on April 20th on the DefenseTech.org Cyber Warfare Blog (see below).

North Korea warned the United Nations Security Council on April 7th, 2009 that it would take "strong steps" if the fifteen nation body took any action in response to Pyongyang's launch of a long-range rocket three days earlier. The United States voiced its displeasure calling the launch a "provocative act" that violated a 2006 Security Council resolution prohibiting Pyongyang from conducting ballistic missile launches. On April 13th, 2009 the United Nations Security Council in a "Presidential Letter" condemned North Korea's April 5th rocket launch and demanded that Pyongyang not conduct further tests, saying that it would expand existing sanctions against North Korea. The 15 member Security Council voted unanimously for the statement. This response was one level below a formal resolution.

On April 17th, 2009 Washington increased pressure on North Korea by warning of "consequences" for its recent rocket launch and the latest decision to kick out nuclear inspectors. A State Department spokesperson said that "North Korea has not listened to the will of the international community, and therefore it's going to have to face the consequences from its unwillingness to meet the international community's requirements."

North Korea quickly responded saying any sanctions or pressure to be put upon it as a declaration of undisguised confrontation and a declaration of a war against the DPRK. The North Korean spokesman reportedly said, "There is no limit to the strike to be made by the revolutionary armed forces of the DPRK." North Korea has reacted to the criticism with more than just words. They expelled all nuclear weapons inspectors and declared that they will resume work on nuclear weapons.

Most military strategists agree that cyber attacks are an excellent first strike weapon. In these specific circumstances, cyber attacks might be considered by Pyongyang as an appropriate and proportional response to the U.N. Security Council's condemnation and reinforcement of existing sanctions. High probability targets if DPRK launches cyber attacks include South Korea and the fifteen countries that make up the current U.N. Security Council that include -- permanent members-China, France, Russian Federation, the United Kingdom and the United States -- and ten non-permanent members Austria, Japan, Uganda, Burkina Faso, Libyan Arab Jamahiriya, Vietnam, Costa Rica, Mexico, Croatia and Turkey. This calls for increased vigilance by cyber security professionals guarding the critical infrastructure of those targets identified above.



Cyber Security Briefing

The Associated Press obtained a list of the targets in a coordinated attack last weekend on US networks. Included on the list are the White House, the Department of State, the National Security Agency, the Department of Homeland Security, the State Department, the Nasdaq stock exchange, the Treasury Department, the Secret Service, the Federal Trade Commission, the Transportation Department and other organization. Johannes Ullrich, Chief Technology Officer for the private SANS Internet Storm Center said, "It was a pretty massive (*we disagree*) attack." Many of the organizations appeared to have successfully blunted the sustained computer assaults after several hours. There are unconfirmed reports that South Korean intelligence sources have obtained documents ordering a North Korean army units to start the attack. If true, this could be the smoking gun!

Asia has become the most active cyber war battle front. China and North Korea are well understood to have set up a computer warfare unit in the late 1990s making substantial investment in cyber warfare capability. These recent cyber attacks linked to North Korea is just a glimpse of how much damage can be done by cyber weapons. Security analysts are missing the main point and that is the concern about what the attacks accomplished! They are caught in "bugs in the code and the limited nature of the attack. The fact that these attacks were so well-coordinated, used only the compromised computing resources they needed, lasted so long and were able to bring down a number of sites says more about the state of our defenses than the moderate level of sophistication of the attacks that were launched!

The well coordinated DDoS attacks that swamped U.S. and South Korea Web sites over the past several days is a harbinger and will seem minor compared to things to come. Another issue that has arisen is the report "some defense officials complained privately that the Department of Homeland Security was taking the lead on protecting government agencies from cyber attacks, and yet the Pentagon wasn't informed about the attacks until Wednesday — by hearing about it from the media." This clearly indicates a big communication and coordination problem among all those that should be in the loop when a cyber attack against the United States occurs. This also serves to justify the use of liaison officers under the three cyber command branches that appear on the organizational chart in the Cyber Command & Infrastructure whitepaper authored by Technolytics. We should learn from this attack! The coordinated attacks that swamped Web sites in the U.S. and South Korea in the past several days and our reaction has not been what it should be. We are left with the old question - What constitutes an act of cyber war? This is a question that was posed in the DefenseTech.org cyber warfare blog over a year ago that remains unanswered today. Given our response on this minor attack, the United States is currently ill prepared to respond to a significant cyber attack. It is not wise to develop this definition or international cyber warfare doctrine during the heat of a cyber attack. These recent events illustrate the need for the United Nations to set-up and create a cyber attack doctrine that all of its members abide by and cooperate in the investigations. At this time 16 countries were thought to be unwillingly involved in the generation of the attack traffic.

Attack Statistics

At least 35 government and commercial Web sites in South Korea and the United States came under major attack.

DDoS attack capacity is estimated at between 30 and 40 million computers for the South Korea thrust and between 55 and 65 million for the U.S. thrust. They used only 10% of their estimated capacity—86 IP addresses in 16 countries.

South Korean intelligence officials told South Korean lawmakers that North Korea or its sympathizers were prime suspects in the attacks.

North Korea was indeed behind the cyber attacks that targeted dozens of Web sites in the U.S. and South Korea over the past week, a U.S. defense official told Fox News.

South Korea is one of the world's most wired countries, with broadband access in more than 90 percent of homes and Internet data-transfer speeds that are much faster than in most of the United States.

Key Analysis

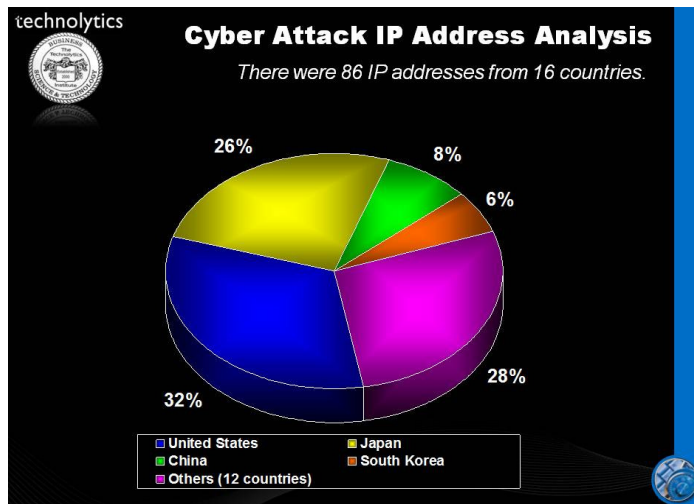
This was not a major strike! North Korea's cyber attack demonstrates the accuracy of the capabilities assessed and documented back in March of 2009 and provided on page 1 in the left hand column.

Give the July 4th holiday and what that represents coupled with the April 20th advisory, proactive measures should have been taken.

One (so called) expert described the software used in the attacks as "amateurish," and full of programming errors. This demonstrates how uninformed most so called experts are. This type attack is a throw-away cyber weapon. It is more about the impact than proper code etiquette or quality. Whatever gets the job done is the only design criteria that matters for this style attack.

Cyber Security Briefing

South Korea's intelligence agency briefed their lawmakers on circumstantial and technical evidence behind their belief that North Korea was behind the recent cyber attacks. Other intelligence sources stated that Kim Chong Un, the third son of North Korean dictator Kim Jong Il, has been accused of being the mastermind of the recent cyber attacks that have plagued government computers in the United States, South Korea and other some 14 other countries. Foreign intelligence sources have also reported that the North Korean government sent a cyber contingent of 10 people across the border into China to conduct some of the operations and that Kim Chong Un actually was in command of that unit. Also sources have speculated that North Korean Research and Development Unit (110 or 101) and Cyber Warfare Unit 121 were the primary military units involved in the planning and execution of the DDoS style cyber attack.



Rep. Peter Hoekstra (R-Michigan) said that North Korea needed to be "sent a strong message." The lead Republican on the House Intelligence Committee has also reportedly called for President Obama to launch a cyber attack against North Korea in retaliation. Given the very limited information infrastructure in North Korea coupled with the very limited number of computer connected to the Internet, this type of retaliation would be very ineffective.

Observations and Recommendations

1. This is a sign of things to come and in all likelihood the attacks will be much worse.
2. The current defenses against cyber attack are woefully inadequate against even moderate level attacks as we have just experienced.
3. International agreements of cooperation are critical to investigating cyber attacks, proper attribution and any response - legal or military.
4. Ignoring old cyber weapons such as MyDoom has proven to be a significant flaw in cyber security. A few modifications and MyDoom snuck past even the most up-to-date current defenses.
5. Coordination between DOD, DHS, DOJ and other government organizations as well as the private sector is critical in times of cyber attack and therefore must be improved and maintained.
6. A panel should be assembled and convened to review, assess and learn from this event.
7. Liaisons should be assigned by each cyber team organization and resident inside the other team members incident command centers.

Key Analysis

(continued)

A U.S. official familiar with the attacks said they were significant in the sense that they were widespread and well-coordinated.

Foreign Intelligence sources said to have reported to the lawmakers that the malicious codes were distributed by a total of 86 Internet protocols (IPs) addresses in 16 countries, including 28 in the United States, 22 in Japan, 7 in China and 5 in South Korea. North Korea is not included among those countries.

The malware associated with the cyber attack is a derivative of the MyDoom worm. The cyber weapon was designed to download a payload from a specific set of Web servers. The payload included a Trojan program that overwrites the data on the hard drive with a message that reads "memory of the independence day," followed by as many "u" characters as it takes to write over every sector of every physical drive attached to the compromised system. South Korea's Computer Emergency Response Team (KR-CERT) has confirmed that machines which participated in this attack are now self-destructing. A dropper program called W32.Dozer that contains the other components is sent by W32.Myto!gen to email addresses it gathers from the compromised computer, the Symantec Response Blog says. If a user executes the attachment, W32.Dozer drops Trojan.Dozer and W32.Mydoom.A@mm on the system. The Dozer Trojan serves as a backdoor and connects to IPs through certain ports, allowing it to update itself and to receive instructions on sites to attack.

Contact Information

The Technolytics Institute
4017 Washington Road
Mail Stop #348
McMurray, PA 15317 USA
P 888-650-0800
F 412-291-1193
I www.technolytics.com