

JOURNAL OF LAW AND CYBER WARFARE

- I. North Korea: The Cyber Wild
Card.....1
Rhea Siers
- II. Hack, Attack or Whack; The Politics
of Imprecision in Cyber Law 13
James E. McGhee
- III. A Brave New World: Applying
International Law of War to Cyber
Attacks 42
Noah Simmons
- IV. Strengthening Director Duties of Care for
Cybersecurity Oversight: Evolving
Expectations of Existing Legal
Doctrine.....109
Brad Lunn

Editor-in-Chief

Daniel B. Garrie, *Partner, Law & Forensics*

Associate Editors

Siddartha Rao, *Special Counsel, Law & Forensics*

Samantha Tucker, *Analyst, Pulse Advisory*

Michael Mann, *Associate, Law & Forensics*

Radhika Tiwari, *Analyst, Pulse Advisory*

Tarique Collins, *Associate, Zeichner, Ellman & Krause*

Editorial Board

Christopher Burgess

Founder & CEO, Prevendra

Jean-Claude Knebel

*Consul General of Luxembourg to
New York*

Jack Dever

*Director, Business Intelligence Unit,
General Electric*

Dr. Larry Ponemon

Chairman, Ponemon Institute

Jeremy Kroll

CEO, K2 Intelligence

John Dever

*General Counsel of Defense Firm
Major Reserve, US Army*

Dr. Joseph Weiss

*Managing Partner, Applied Control
Solutions*

Shane Reeves

*Associate Law Professor, US
Military Academy, West Point*

Mitchell Silber

*Executive Managing Director, K2
Intelligence*

Noah Bledstein

*IT Data Privacy Leader at GE
Healthcare*

Retired Major U.S. Airforce

Robert Clark

Cyber Attorney, Army Cyber Institute

Robert Bair

*Lieutenant Commander,
United States Navy*

Ryan Lasalle

*Global Managing Director, Security
Transformation Services, Accenture*

William Spernow

Chief of Security, Virus Inspector

Eric Jensen

Law Professor, BYU

Uma Chandrashekar

*Global Information Security and Privacy
Leader at Edwards Life Sciences*

Vincent Scott

*GBS-ITS Cybersecurity, Proctor &
Gamble Company*

Rhea Siers

*Senior Associate at the GWU Cyber
Security Initiative*

Richard Borden

*Assistant General Counsel, Bank of
America Merrill Lynch*

Professor Michael Schmitt

*Director, Stockton Study of International
Law at the US Naval War College*

NORTH KOREA: THE CYBER WILD CARD

By Rhea Siers, J.D.¹

Note: This article was written in large part prior to the recent cyber actions against SONY.

If you're worried about North Korea's nukes, you probably should be even more concerned about Pyongyang's cyber weapons. Much has been made of the alleged attribution of North Korea for the cyber attacks against SONY. But even prior to the SONY fracas, there was considerable concern about North Korea's recent attacks against on several South Korean institutions involved in security research.² In fact, following these security related incidents, Hewlett Packard provided a detailed analysis of North Korea's cyber apparatus and capabilities. Certainly, the North Korean attacks against the South demonstrate a degree of cyber capability but the real question is whether North Korea sees cyber attack against the US, specifically targeting U.S. economic and business institutions, as a viable and destructive weapon. The Democratic People's Republic of

¹ Rhea Siers, J.D. is currently a Senior Associate of the George Washington University (GWU) Cybersecurity Initiative and a member of the adjunct faculty at the Elliott School of International Affairs, GWU as well as Johns Hopkins University.

² Lucien Constantin, *Cyberspies attack key South Korean institutions, North Korean Hackers suspected*, PC WORLD, <http://www.pcworld.com/article/2048580/cyberspies-attack-key-south-korean-institutions-north-korean-hackers-suspected.html>.

Korea's (DPRK) motivations need to be carefully compared to the PRC, their cyber enabler and sponsor, which uses its cyber capability for espionage and commercial advantage, but not to directly damage the US economy.

I. The Growth of North Korea Cyber Capabilities

In its annual report to Congress regarding the capabilities of the DPRK, the Department of Defense shares the view that North Korean cyber capabilities pose a serious threat beyond the immediate region:

Given North Korea's bleak economic outlook, OCO may be seen as a cost-effective way to develop asymmetric, deniable military options. Because of North Korea's historical isolation from outside communications and influence, it is also likely to use communications and influence, it is also likely to use Internet infrastructure from third-party nations. This increases the risk of destabilizing actions and escalation on and beyond the Korean peninsula.³In fact, the state-run North Korean newspaper, Minju Joson, has criticized the US cyber operations policy (Presidential Policy

³ "Military and Security Developments Involving The Democratic People's Republic of Korea", Office of the Secretary of Defense, Annual Report to Congress, 2013, 11, http://www.defense.gov/pubs/North_Korea_Military_Power_Report_2013-2014.pdf.

Directive 20) as “a declaration of cyber war” and noted “the cyber attack in internet network may bring irrevocable financial and material damage to the opponent side in a moment”.⁴ The realization of the cyber threat to its own critical infrastructure has led the North Koreans to build their program and develop a solid cyber cadre – their first generation of “cyber warriors” and to build beyond defensive capabilities. In his article on North Korean cyber development, Christian Science Monitor reporter Mark Clayton discussed the details of the North Korean program with several experts, including Alexandre Monsourov of the Johns Hopkins’ US-Korea Institute, who noted that the North Koreans are on a clear path to develop cyber capabilities targeting their perceived primary adversaries – “South Korea, the US, and Japan”.⁵ Clayton writes that several experts see current North Korean efforts as “a kind of cyber-sword sharpening”. Further, like DoD, he notes that cyber is the ideal weapon for a “cash strapped” nation.⁶

⁴ *North Korean Newspaper hits out at U.S. cyber warfare policy*, NORTH KOREAN TECH, Aug. 12, 2013, <http://www.northkoreatech.org/2013/08/12/north-korean-newspaper-hits-out-at-u-s-cyber-warfare-policy/>.

⁵ Mark Clayton, *In Cyberarms race, North Korea emerging as a power, not a pushover*, THE CHRISTIAN SCIENCE MONITOR, Oct. 19, 2013, <http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover>.

⁶ *Id.*

In its extensive report on North Korean capabilities, Hewlett Packard (HP) notes that the DPRK is “remarkably committed” to the development of its cyber capabilities, including training up a new generation of cyber warriors.⁷ The HP report notes an extensive cyber structure and cites South Korean estimates of a cyber offensive corps that may be the third largest in the world.⁸ The North Korean cyber units, known as Office No. 91 and Unit 121, operate under the authority of the DPRK’s Reconnaissance General Bureau, which oversees both conventional intelligence and cyber operations. Most interesting is the fact that these two units are actually resident in the PRC, not in North Korea.⁹ This is due to the fact of North Korea’s heavy Internet restrictions limiting outgoing connections which necessitates DPRK’s reliance on other nations for their networks and botnets.¹⁰ North Korea’s “digital deprivation”¹¹ forces its dependence on the PRC as well limits, for now, the vulnerability of the DPRK’s own networks.

While a large cyber corps does not guarantee sophisticated or broad impact

⁷ HP Security Research, *Profiling an enigma The mystery of North Korea’s cyber threat landscape* (Aug. 2014), http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

⁸ Charlie Osborne, *North Korea cyber warfare capabilities exposed*, ZDNET, Sept. 2, 2014, <http://www.zdnet.com/article/north-korea-cyber-warfare-capabilities-exposed/>.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *North Korean Cyber Rattling*, THE ECONOMIST, May 17, 2013, <http://www.economist.com/blogs/babbage/2013/05/digital-warfare>.

immediately, one can see the gradual development in the efficacy of North Korean cyber attacks in the last ten years. According to Hewlett Packard, the DPRK was able to successfully penetrate 33 of 80 South Korean Military wireless communications networks in 2004. South Korea attributed this attack to their northern neighbor as well as an intrusion later that same year into the US State Department computers.¹² Of course, given the difficulties in proving attribution, these reports are not definitive but certainly reflect available evidence.

McAfee's analysis of attacks against South Korean government and banking sites in 2011 and 2009 also concludes that there was a definite improvement in capabilities by the perpetrator, which they attribute to North Korean elements. The McAfee report concluded "the combination of technical sophistication juxtaposed with relatively limited execution and myopic outcome to bringing a Lamborghini to a go cart race". Why use advanced capabilities for a rather low-level attack? According to McAfee, "the motivations appear to outweigh the attack, making this truly seem like an exercise to test and observe responses".¹³

Isolated and impoverished, how did North Korea improve its status among cyber actors during

¹² *Id.*

¹³ McAfee, *Ten Days of Rain Expert analysis of distributed denial-of-service attacks targeting South Korea*, <http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf>.

such a short period? While Pyongyang certainly benefitted from the cyber expertise of its patron in Beijing, it also clearly views its cyber capability as a key national resource perhaps gradually approaching the level of its nuclear aspirations. North Korea is developing its youngest students, pushing computer science, and recruiting the “best and the brightest” among university students, including programs sending them overseas for advanced training.¹⁴ This cyber cadre is then directed to two cyber units. In 2009, it is believed that Kim Jong Il expanded the cyber units by 200% to 3000.¹⁵ The PRC continues to play a key role in the development of cyber capability by North Korea and it is probable that the PRC actually hosts North Korean cyber warriors on their servers.¹⁶

II. Cyber and Crime – The Future of North Korea’s Limited Economic Lifeblood

Criminal activity is one of the few locomotives that drive the very limited North Korean economic engine, as well, of course as military technology sold to other state and non-state actors. In a recent Brookings institute report, North Korea was depicted as utilizing criminal

¹⁴ Mark Clayton, *In Cyberarms race, North Korea emerging as a power, not a pushover*, THE CHRISTIAN SCIENCE MONITOR, Oct. 19, 2013, <http://www.csmonitor.com/World/Security-Watch/2013/1019/In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover>.

¹⁵ Youkyoung Lee, *North Korea Cyber Warfare Hacking Warriors’ Being Trained in Teams, Experts Say*, HUFF POST, Mar. 24, 2013, http://www.huffingtonpost.com/2013/03/24/north-korea-cyber-warfare-warriors-trained-teams_n_2943907.html.

¹⁶ *Id.*

activity to obtain hard currency and moving towards a “Criminal Market Economy”.¹⁷ The criminal activity, which was initially sponsored and encouraged by the DPRK regime, has expanded to criminal “elites” in the population who expanded distribution networks of drug smuggling and several types of counterfeiting, including currency and pharmaceuticals.¹⁸

Just as other transnational criminal syndicates have moved into cyber crime, so is North Korea expected to use some of its increasing hacking expertise to diversify its criminal enterprises. However, it is unclear whether the regime would be willing to relinquish its strict control of networks to criminal syndicates in the same way that it has “delegated” other criminal activity. South Korea has already suffered massive data breaches, including the theft of thousands of credit card numbers¹⁹ attributed to different possible perpetrators, including North Korea, as well as the loss of proprietary information by several of its key industries. The industrialized south, whose economy is highly dependent on credit cards as well, makes a tempting target for criminal as well as political purposes.

¹⁷ Parameswaran Ponnudurai, *North Korea Moving Towards a 'Criminal' Market Economy*, Apr. 15, 2014, <http://www.rfa.org/english/news/korea/illicit-04152014015031.html>.

¹⁸ *Id.*

¹⁹ Choe Sang-Hun, *Theft of Data Fuels Worries in South Korea*, N.Y. TIMES, Jan 20, 2014, http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html?_r=0.

III. Key Questions

Three questions emerge in assessing North Korean intentions and capabilities: (1) Should we assume that since the PRC actively hosts and enables DPRK cyber operations that the Chinese can inhibit North Korean offensive cyber intentions as they continue to build an independent capability? (2) Under what circumstances would North Korea consider a destructive cyber attack against key US economic and financial interests? (3) Given North Korea's proclivity to provide other destructive technologies and military assistance to rogue states and non-state actors, would the DPRK also assist them with destructive cyber capabilities?

IV. Can China Inhibit North Korean Intentions?

There is no question that the China-DPRK relationship is a very strong alliance across all sectors. But as the Council on Foreign Relations notes, this alliance does not mean control by the PRC, including in the nuclear arena.²⁰ Control may become even less likely in the cyber realm where expert cyber operators can diminish the possibility of clear and/or immediate attribution. If North Korea moves away from the necessity of Chinese cyber platforms, it can perform more independently and in concert with its own strategy and economic needs. However, North Korea remains dependent

²⁰ Jayshree Bajoria & Beina Xu, *Backgrounders: The China-North Korea Relationship*, COUNCIL ON FOREIGN RELATIONS, Feb. 21, 2013, <http://www.cfr.org/china/china-north-korea-relationship/p11097>.

on these platforms at the current time and it is unclear as to whether North Korean cyber operations are partitioned from their Chinese patrons. One can assume there is significant oversight over any Chinese platforms being leveraged by DPRK cyber operators.

It should be noted as an isolated and sanctioned state, North Korea does not have any compelling interest in avoiding disruptions to the world economy. What would be the impact on Pyongyang of a major disruption to the Western banking system? Even the Bank of China has terminated its relationship with North Korean financial institutions.²¹ North Korea's relationship with foreign banks is severely limited due to sanctions and while it has successfully circumvented sanctions and increased some trade, Pyongyang uses small Chinese regional banks and other underground methods to move money internationally. Having been exiled from major world banks, North Korea has adopted many of the same money laundering and movement techniques as criminal and terrorist organizations – using money brokers or trading in gold for hard currency.²² In other words, this is not a state that would necessarily hesitate at cyber attacks on US

²¹ Keith Bradsher & Nick Cumming-Bruce, *China Cuts Ties with Key North Korean Bank*, N.Y. TIMES, May 7, 2013, http://www.nytimes.com/2013/05/08/world/asia/china-cuts-ties-with-north-korean-bank.html?_r=0.

²² Leon Sigal, *How North Korea Evades Financial Sanctions*, 38 NORTH: INFORMED ANALYSIS OF NORTH KOREA, May 3, 2013, <http://38north.org/2013/05/lsigal050313/>.

financial centers out of a need to protect its own economy, investments and trading capabilities.

Then there is the issue of North Korea becoming a “cyber hired gun” – paid to conduct attacks or provide plausible deniability for other cyber “have nots” – from other states to terrorist or criminal organizations. If it is true that the global missile or nuclear market is no longer as successful or lucrative for Pyongyang due to successful international interdiction efforts²³, North Korea must find yet another way to circumvent sanctions and bring in hard currency. While some have suggested that North Korea is working with Iran in this area, there is little concrete evidence to suggest this is true. The analogy to North Korean nuclear cooperation with Iran has not yet been indicated except in one claim that Israel may have such evidence.²⁴ Both countries have made considerable progress in their cyber capabilities, but one wonders whether Iran truly has a need for North Korean assistance in this area, unless it is serving as a conduit for Chinese support.

All of which leads us back to North Korea’s cyber inclinations. Obviously, Pyongyang realistically views itself as a key target by the US,

²³ Joshua Pollack, *North Korea’s Shrinking Role in the Global Missile Market*, 38 North: Informed Analysis of North Korea, Jul. 29, 2011, <http://38north.org/2011/07/jpollack072911/>.

²⁴ Thom Shanker & David Sanger, *US Allies Trying to Battle Iranian Hackers*, N.Y. TIMES, Jun. 8, 2013, http://www.nytimes.com/2013/06/09/world/middleeast/us-helps-allies-trying-to-battle-iranian-hackers.html?pagewanted=1&_r=0&smid=tw-share.

Japan, South Korea and others so it initially focused on building its defensive capabilities. Having accomplished some limited degree of defensive capacity, Pyongyang must understand that it can use computer network exploitation of others to build both a defense and attack capability. There are strong indications that it is using its cyber capability against South Korea with some success. There are two risks here – that attacks against South Korea will impact beyond these borders, a clear danger in any cyber attack scenario and of equal, if not greater concern, that North Korea, devoid of any other effective tools in its arsenal, will lash out specifically against those countries that have intensified its isolation.

In testimony before Congress, Frank Cilluffo of the Homeland Security Policy Institute stated:

“Precisely because North Korea has fewer constraints, I would underscore that it poses an important ‘wildcard’ threat, not only to the United States but also to the region and broader international stability.”²⁵

Sometimes the threats we should prepare for and consider are those that come from entities

²⁵ Frank Cilluffo, *Cyber Threats from China, Russia and Iran Protecting American Critical Infrastructure*, TESTIMONY BEFORE THE US HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY, Mar. 20, 2013, http://www.gwumc.edu/hspi/policy/Meehan_Cilluffo%20Testimony%20March%202013.pdf.

considerably less powerful and capable than us, particularly those that could cause negative economic impact in a matter of minutes.