North Korea's Cyber Attacks and Cyber Peace in Northeast Asia

Duk Ki Kim (金德起)

Professor, Kongju National University

Abstract

A long and challenging negotiation process is still going on by the United States and North Korea. The focus is North Korea's illicit nuclear weapons capability as well as other weapons of mass destruction (WMD) and their delivery means, including ballistic missiles. To understand the full scale of challenges that faces any nation that must work with North Korea, one must understand North Korea and its military capabilities as well as cyber power. Although North Korea's conventional forces operate obsolete tanks and aircraft with limited proficiency, its army is still invested in areas that make it a force to be reckoned with. First, in addition to maintaining a garrison nation and a standing army of over one million troops, North Korea maintains a fitter and better-equipped ground force that it views as special force.

Second, North Korea has been investing in GPS-jamming capabilities and the use of cheap disposable drone's reconnaissance, jamming and weapons delivery to include biological and chemical agents. Up to this point, South Korea has had difficulty detecting these drones, let alone shooting them down. This will be another form of North Korean military

capability that is hard to react to them because of counter capability and the potential for misunderstanding and escalation.

The last and alarming threat is North Korea's cyber capability. North Korea is the 4th strong cyber power followed by the U.S., China and Russia. North Korea's cyber capability stems from its ability to recruit from its entire population. Talented and gifted people can be directed to work as cyber warriors without factoring any personal considerations. Because the North Korean government operates without any moral or legal inhibitions, it can experiment with and execute operations that provide its cyber operators more experience and expertise. North Korea's cyber recruitment and training programs have been going on for at least 20 years. Security analysts have verified that North Korea is involved in international cyber theft activities and capable of cyber intimidation, sabotage and direct attacks on infrastructure, including nuclear facilities.

Keywords: Cyber Capability, Cyber Attack, Cyber Warrior, Electronic Warfare, Psychological Warfare, North Korea, South Korea, U.S., China

I. Introduction

The Democratic People's Republic of Korea(or DPRK) (hereinafter North Korea) has one of the smallest internet presences in the world, and the bulk of its limited internet access is routed through China.[1] The DPRK has a national intranet called 'Kwangmyong Intranet' that offers email and websites and connects domestic institutions, but appears to be disconnected from the World Wide Web.[2] Currently, it is known that North Korea coopetes with China to replace Kwangmyong Intranet to Huawei system. Elites and foreign visitors have access to the broader internet, but usage is heavily monitored by the regime.[3] The North Korean government has devoted significant resources to develop its cyber operational capabilities and has grown increasingly sophisticated in its ability to attack targets. Among governments that pose cyber threats to the United States, some analysts consider the North Korean threat to be exceeded only by those posed by China and Russia.[4] North Korea appears to be engaging in increasingly

---

[1] Jose Pagliery, "A Peek into North Korea's Internet," *CNN Tech*, 23 December 2014.

[2] Sparks, Matthew, "Internet in North Korea: Everything You Need to Know," *The Telegraph*, 23 December 2014.

[3] "How the Internet 'Works' in North Korea," *Slate.com*, 26 November 2016.

[4] Will Edwards, "North Korea as a Cyber Threat," *The Cypher Brief*, 1 July

hostile cyber activities including theft, website vandalism, and denial of service attacks. Some cybersecurity analysts, however, question whether the country has developed the technical capability to conduct large-scale destructive attacks on critical infrastructure.

The Republic of Korea (or ROK) (hereinafter South Korea)—among the most wired countries in the world—has been the victim of suspected North Korean hacks for years, but Pyongyang's cyber activities appear to have expanded to include other countries, particularly targeting the banking sector. As in North Korea's accelerating missile program, even the failures reveal the growing capability and ambition of the Pyongyang regime. In early 2017, North Korean hackers reportedly attempted to break into several Polish banks. Although unsuccessful, the hackers' techniques reportedly were more advanced than many security analysts had expected. Researchers also uncovered a list of other organizations that North Korean hackers may have intended to target, including large U.S. financial institutions, the World Bank, and banks in countries from Russia to Uruguay.[5]

North Korea has employed cyber attacks for several decades. These began as primitive disruptions and have since

---

2016.

[5] "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, 25 March 2017.

increased in sophistication. From this record of experience, analysts have drawn conclusions that can help shape analysis of this new military capability. Firstly, countries use cyber attacks in a manner consistent with their larger national strategies. Secondly, the physical damage they cause is easy to overstate: a cyber attack is not a WMD. Thirdly, while cyber attacks can produce effects similar to kinetic weapons, there is an informational aspect that is equally important. Some analysts consider cyber attack as a tool of asymmetric warfare, but this can obscure important operational distinctions in its use. A cyber attack does not require 'an act of violence to force the enemy to do our will.'[6] Violence through cyber means is possible, but its more common effect is to manipulate information, create uncertainty and shape opinion. Cyber attacks are attractive in that they offer varying degrees of concealment and their treatment under international law remains ambiguous: it is unclear whether they qualify as an 'armed attack' that would make retaliation legitimate.[7] Public data suggests that North Korea has used some form of cyber attacks like other countries. Pyongyang has developed a range

[6] Clausewitz's definition of war. See Carl von Clausewitz, *On War*, ed. and trans. by Peter Paret and Michael Howard (Princeton, NJ: Princeton University Press, 1976), p. 90.

[7] Under Article 51 of the UN Charter, which recognizes states' inherent right to self-defense.

of unconventional military capabilities, to the extent that it's limited economic and technological resources allow, but cyber attack has a special place in that it is 'operational' and the North has used cyber attacks against the regime's opponents, such as South Korea and the U.S.

Cyber capabilities can serve to provide adversaries with a degree of parity in what may otherwise be an unequal contest. North Korea seeks to avoid confrontation with the opponent's main force. It is useful to note the similarities between North Korea's behavior and that of Iran: both are developing asymmetric capabilities such as cyber weapons and ballistic missiles because of similarities in their strategic thinking. Both states wish to deter a powerful opponent and maintain an operational space in which they can still conduct offensive action, even if those actions provide only symbolic effect aimed at a domestic audience. Cyber attacks give these countries a means to take action against what they perceive to be their primary opponent, such as the U.S. The purpose of this paper is to analyze North Korea's cyber capabilities and cyber attack cases and to suggest countermeasures focusing on the impact of cyber attacks in Northeast Asian security.

II. North Korean Cyber Attacks as Source of Advantage

Kim Il-sung—the regime's founder and grandfather of current leader Kim Jong-un—North Korea's military strategy was intended to achieve forced reunification with the South by

employing surprise, speed and overwhelming firepower.[8] By Kim Il-sung's final years, it was clear that this was no longer realistic. Invasion would greatly harm the South, but it would be suicidal for the North. Efforts by Pyongyang to compensate for the growing military imbalance, by developing alternatives to conventional military forces, were first intended to support reunification by military force. Since then, the rationale for acquiring these capabilities has changed significantly.[9]

North Korea's armed forces provide a variety of benefits to the regime, but a realistic option for conquering the South is not one of them, even when reinforced by other asymmetric capabilities. Assuming that this is acknowledged by Pyongyang, this would influence the development of cyber capabilities. The North's military goals are now to deter invasion or aggression, maintain internal security and provide coercive capabilities that support the regime's broader political and economic goals. As such, its efforts to develop military

---

[8] Homer T. Hodge, "North Korea's Military Strategy," *Parameters*, vol. 33, no. 1 (Spring 2003).

[9] Axel Berkofsky, "North Korea's Armed Forces: All Dressed Up, with Places to Go?," *ISN, Center for Security Studies* (ETH Zurich), 7 February 2013 and Bruce E. Bechtol, Jr, "Maintaining a Rogue Military: North Korea's Military Capabilities and Strategy at the End of the Kim Jong-il Era," *International Journal of Korean Studies*, vol. 31, no. 1 (Spring 2012).

capabilities will focus on strengthening deterrence, coercion and political effect. Asymmetric capabilities are developed in order to circumvent an opponent's areas of strength and attack areas of relative weakness. Combining new technologies and novel tactics—such as in blitzkrieg—can provide unexpected advantage, but it is easy to overvalue this. Asymmetric capabilities are rarely decisive (nuclear weapons, given their destructiveness, are unique). Their effect lies in shifting the direction of warfare, strategy and tactics, and in accommodating new technologies.

North Korea has developed a range of military technologies to compensate for its conventional weaknesses, including cyber attack, chemical weapons, electronic warfare, nuclear weapons and ballistic missiles, but these efforts are hampered by its relative technological backwardness. Its unmanned air vehicles (UAVs), for example, are still rudimentary models, and the North has no real precision or stealth capabilities. While it does have WMD, their use would face severe political constraints, even for the North.[10] Of all the new military technologies that might provide advantage, cyber attack poses the lowest 'cost of entry' in both resource and political terms.

[10] Duk-ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy: Lessons from ROKS Cheonan and Yeonpyeong Island," *Naval War College Review*, vol. 65, no. 1 (Winter 2012).

However, it is a mistake to interpret cyber-attack capabilities solely from the perspective of kinetic military action. Advanced cyber attacks can produce results equivalent to kinetic attack, but the manipulation of software, data, knowledge and opinion to degrade performance and produce political or psychological effect is equally important. For instance, introducing uncertainty into the minds of opposing commanders or political leaders is a valuable outcome, as is manipulating public opinion to damage an opponent's national or international legitimacy and authority with both domestic and international audiences. Like other nations, North Korea is exploring how best to both produce and benefit from cyber effects, within the framework of its own military and strategic doctrine.

North Korea began to develop cyber capabilities in the mid-1990s, initially stemming from efforts in the area of electronic warfare (EW).[11] Pyongyang sent Koreans overseas for training in programming and began to acquire computer technology, both legally and illicitly. Some of the motivation was economic, part of an effort to revitalize and expand the

[11] Joseph S. Bermudez Jr, "SIGINT, EW, and EIW in the Korean People's Army: An Overview of Development and Organization," in Alexandre Y. Mansourov (ed.), *Bytes and Bullets: Information Technology Revolution and National Security on the Korean Peninsula* (Honolulu, HI: Asia-Pacific Center for Security Studies, 2005), pp. 234–275.

country's flagging economy. Kim Jong-il made it a goal to create a national information-technology industry. But it is likely that acquiring new espionage tools and military capabilities also drove North Korean efforts. China was building a military cyber capability at the same time and this may have had some influence on North Korean thinking.

North Korea uses its cyber-attack capabilities in three principal ways: for 'coercive diplomacy', for state-sponsored criminal acts to acquire hard currency, and to prepare for disruptive actions in the South (and perhaps the United States), in the event of a major conflict. These goals reflect broader changes in North Korean strategy. The North appears to have given up on forced reunification of the peninsula, although it is important for its strategy to continue to emphasize the threat of conventional assault against the South. Indeed, in comparison to the era of Kim Il-sung— who actively pursued reunification thorough the use of force—North Korea is on the defensive strategically. Its goals are to deter US and South Korean military action, prevent absorption by South Korea, preserve the rule of the Kim's family, and also improve negotiating positions and influence over the future of Korea. These goals and other trends suggest that the use of cyber-attack capabilities for coercive purposes will remain an attractive option for the North – one that it may exercise when it judges

the risk of retaliation to be acceptable.[12]

The risk from cyber attack needs to be put in the context of North Korean provocations, the most important being the 2010 sinking of the corvette Cheonan and the shelling of Yeonpyeong Island. Both incidents resulted in fatalities—46 in the case of the Cheonan, and four (two of whom were civilians) in that of the artillery attacks. While the North has used cyber attacks (as opposed to espionage) a number of times, including WannaCry and the Bangladesh Bank heist, none rose to the levels of these earlier incidents in terms of effect.

The dilemma in this asymmetric attack is the risk of miscalculation by North Korea's leaders, who may take action to gain influence with the assumption that they can manage escalation. However, there is a lack of reliable and publicly available insight into the North's strategic thinking or decision-making processes. North Korea is a xenophobic state for which South Korea is an increasingly alien culture.

III. North Korea's Cyber Power and Command and Control

1. Organization of North Korean Cyber Operations

[12] Victor D. Cha, "Korea: A Peninsula in Crisis and Flux," in Ashley J. Tellis and Michael Wills (eds), *Strategic Asia 2004–2005: Confronting Terrorism in the Pursuit of Power* (Washington DC: National Bureau of Asian Research, 2005), pp. 139–164.

North Korea's cyberwarfare should not be ignored. The North perceives cyber warfare tactics to be as important as WMDs and has concentrated on their development. The regime selects young students of ages twelve and thirteen, enrolls them in computer courses for the gifted at the First and Second Geumseong Senior-Middle Schools, and then matriculates them in either Kim Il-sung University(金日成大學) or the Command Automation University (指揮自動化大學)(formerly known as Mirim University) after graduation. The Command Automation University selects around a hundred talented students for an intensive five-year course and then sends graduates to cyber-related institutions and military units.

Most sources report that North Korean cyber operations are headquartered in the Reconnaissance General Bureau (RGB), specifically under Unit 121.[13] The RGB appears to serve as the central hub for North Korea's clandestine operations and in the past has been blamed for attacks such as the 2010 sinking of the Cheonan, a South Korean Navy corvette, killing 46 sailors.[14] The North Korean People's Army (KPA) General Staff is responsible for operational planning, and its cyber units may coordinate with RGB as well.

---

[13] "North Korea's Cyber Operations," Center for Strategic and International Studies Korea Chair, December 2015.

[14] Joseph Bermudez, "A New Emphasis on Operations against South Korea," *38 North Special Report*, June 2010.

Also, as illustrated in Table 1, the Unit 121, originally under the KPA's General Staff RGB, was reorganized in 1998[15] into technical reconnaissance teams, with a mission that includes infiltrating computer networks, hacking secret information, and planting viruses to paralyze enemy networks.[16] According to a report by Reuters, Unit 121 is staffed by some of North Korea's most talented computer experts and is run by the KPA.[17] A North defector indicated that the agency has about 1,800 specialists.[18] Many of the bureau's hackers are hand-picked graduates of the Command Automation University, Pyongyang and spend five years in training.[19] While these specialists are scattered around the world, their families benefit from special privileges at home. The alleged cyber attacks by the Unit 121 are 2013 South Korea cyberattack, November 2014 Sony Pictures hack,

[15] David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks before Sony Attack, Officials Say," *New York Times*, 20 January 2015.

[16] Samuel Gibbs, "Did North Korea's notorious Unit 121 cyber army hack Sony Pictures?," *The Guardian*, 20 January 2015.

[17] Ju-Min Park and James Pearson, "In North Korea, hackers are a handpicked, pampered elite," *Reuters*, 18 December 2014.

[18] *Ibid*.

[19] James Waterhouse and Anna Doble, "Bureau 121: North Korea's elite hackers and a 'tasteful' hotel in China," *BBC News*, 27 April 2017.

February 2016 Bangladesh Bank robbery, 2015–2016 SWIFT banking hack and May 2017 WannaCry ransomware attack. Other such organizations—the 204th Unit, under the Operations Department of the Unification Propaganda Bureau (UPB), and the Psychological Operations Department of the North Korea Defense Commission—are primarily focused on cyber-psychological warfare.

<Table 1> North Korea's Cyber- and Cyber-Psychological Warfare Unit

Institution/Unit	Composition	Mission and Activities
Unit 121 (RGB)	Approx. 1,800 specialists, 10 combat teams, 13 Technical support teams	Hacking, virus-planting in military units related to cyber warfare
Central Party Investigative Group	Approx. 500 persons, 10 technical teams	Technical education and training
Unification Propaganda Bureau (UPB)	50 persons	Cyber-psychological warfare, organizational espionage and propaganda
204 Cyber-Psychological Unit (Operations Dept. of the UPB)	Approx. 100 persons, Five espionage teams	Cyber-psychological warfare planning, execution, and research on its techniques and technology

Source: Kim, *op. cit.*, p. 68.

North Korea is known to operate and manage directly websites—for instance, The North Korea Official Page, in collaboration with pro-North and civil organizations within the South—that execute psychological warfare and organized espionage.[20] According to a report submitted to parliament by the National Police Agency in September 2008, the agency had by that date blocked forty-two foreign-based, pro-North websites out of a total of seventy-two that propagandize juche ideology(主體思想) and the North's unique socialist state while at the same time inciting anti-South and anti-American sentiments. North Korea has also utilized websites operated by sympathizing parties in order to initiate espionage. By the end of 2008 North Korea possessed twenty-four websites, including 'Gugukjeonseon' (救國戰線), and the numbers continue to increase. Recently, pro-North civil organizations digitized posters and leaflets used in the 1980s by activist students and uploaded them to their websites, where they have been highly effective.[21]

North Korea has liked many statistics on North Korea, publicly available estimates of its cyber capabilities are

[20] The North Korea Official Page, available at www.korea-dpr.com; Gugukjeonseon (救國戰線), available at www.ndfsk.dynds.org.

[21] Yoon Kyu Lee, "The Essence of North Korea's Cyber-Psychological Warfare and Appropriate Counter-measures," *The ROK Army* (monthly magazine), August 2009, pp. 1–6.

imprecise and prone to exaggeration. The Reconnaissance General Bureau, a relatively new intelligence organization formed through the consolidation of several North Korean intelligence agencies, likely has between 1,800 and 3,000 cyber operators, although some South Korean press sources put the figure as high as around 8,000.[22] It is the 4th largest cyber power followed by the U.S., China and Russia in the world.

The size of North Korea's cyber force has been estimated to be between 3,000 and 6,000 hackers trained in cyber operations, with most of these "warriors" belonging to the RGB and the KPA's General Staff.[23] North Korea identifies talented students and trains them at domestic universities such as Kim-Il-Sung University, Kim Chaek University of Technology, and the Command Automation University.[24]

---

[22] Egle Murauskaite, "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment," *38 North*, 12 September 2014; US Department of the Treasury, "2010 Recent OFAC Actions," August 30, 2010, http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20100830.shtml.aspx; and Joseph S. Bermudez Jr, "A New Emphasis on Operations against South Korea?," *38 North*, 11 June 2010.

[23] Ken Gause, "North Korea's Provocation and Escalation Calculus: Dealing with the Kim Jong-un Regime," *Center for Naval Analyses*, August 2015.

[24] "N. Korea Bolsters Cyberwarfare Capabilities," *The Korea Herald*, 27

Some research suggests that some students train internationally in Russia and China.[25] North Korean hackers often live overseas—a freedom only afforded to a few elite citizens—to take advantage of other countries' more advanced infrastructure.[26]

2. Command and Control of Cyber Force

Cyber operations are thought to be a cost-effective way for North Korea to maintain an asymmetric military option, as well as a means to gather intelligence; its primary intelligence targets are South Korea, the United States and Japan. North Korea's armed forces are experimenting with how to organize, train and equip their forces to prosecute cyber attacks like other countries. There is no doubt that the addition of cyber-warfare capabilities produces military advantage, and will increasingly be as vital for survival and success in combat as the deployment of EW capabilities.

Many countries could simply adapt existing approaches to EW to manage and plan military cyber capabilities. North

---

July 2014.

[25] Donghui Park, "North Korea Cyber /Attacks: A New Asymmetrical Military Strategy," *Henry M. Jackson School for International Studies Post*, 28 June 2016.

[26] "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, 25 March 2017.

Korea, however, seems to have separated EW and cyber for operational purposes, with the KPA having lead responsibility for EW, while cyber actions are undertaken by the RGB, the intelligence agency responsible for both espionage and covert action,[27] and with a history of paramilitary operations against the South.[28] Currently, North Korea's organizational approach seems to be to create a single, large unit for cyber actions under the auspices of the RGB, but it remains to be seen if cyber units will appear in operational elements of the North's army.

In North Korea, any decision to launch a cyber-attack is likely made by Kim Jong-un. This would be consistent with North Korea's strategic culture and its centralized and compartmentalized decision-making structure. It is also consistent with the practice in other nations where, as far as we know, attacks require the consent of the head of state (in contrast to cyber-espionage activities, which are usually carried out under a blanket authorization from political leaders). North Korea's cyber-attacks are carefully orchestrated to fit its larger political and diplomatic agenda and, although this may be opaque to outsiders, these involve rational decisions about risk and rewards in the North's strategic context and culture.

---

[27] Park Sung Kook, "Tasks of the General Bureau of Reconnaissance," *Daily NK*, 7 May 2010.

[28] Bermudez, *op. cit.*, pp. 234–275.

That there have not been more cyber-attacks against South Korea can in some way be explained by improvements in the South's cyber-defenses. It is also possible that the North faces the trade-off that confronts all cyber powers, in deciding when the loss to cyber-espionage collection will outweigh the benefits of an attack. It may also be the case that Chinese remonstrations about the destabilizing effect of such actions could check North Korea's cyber ambitions.[29] These factors, combined with uncertainty over US attribution capabilities, may have reshaped the North's calculus in relation to cyber-attack, but the pace of cyber-attack is dictated by what

[29] China is concerned about the stability and survivability of North Korea. See Julian Ryall, "China Plans for North Korean Regime Collapse Leaked," *Telegraph*, 5 May 2014; Jane Perlez, "Chinese Annoyance with North Korea Bubbles to the Surface," *New York Times*, 20 December 2014; and Richard C. Bush, "China's Response to Collapse in North Korea," *Brookings Institution*, 3 January 2014. Nonetheless, reports emerged in late 2016 alleging that North Korean cyber operators had penetrated South Korean military networks and, according to some reports, had exfiltrated information including on operational plans. See "N. Korea likely hacked S. Korea cyber command: military," *Yonhap News*, 6 December 2016; "North Korea 'hacks South's military cyber command," *BBC News*; and Sang-hun Choe, "North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says," *New York Times*, 10 October 2017.

the North sees as the requirements of its international agenda—and, until it renounces provocation as a diplomatic tool, cyber-attacks will likely continue when required.

All of these attacks, it should be noted, take place against a backdrop of Pyongyang's threats to incinerate, annihilate, or otherwise obliterate South Korea and the U.S., in retaliation or deterrence. This propaganda is not persuasive to Western audiences and is more likely aimed at North Korea's own population. This may also be the case with cyber-attacks; largely symbolic actions whose effects may be pleasing to Pyongyang, but are also overestimated by it. The psychological advantage gained from these actions may not be in weakening the South but in strengthening the North's view of itself.

IV. North Korea's Cyber Attacks to Other Counties

1. North Korea's Cyber Attacks to South Korea

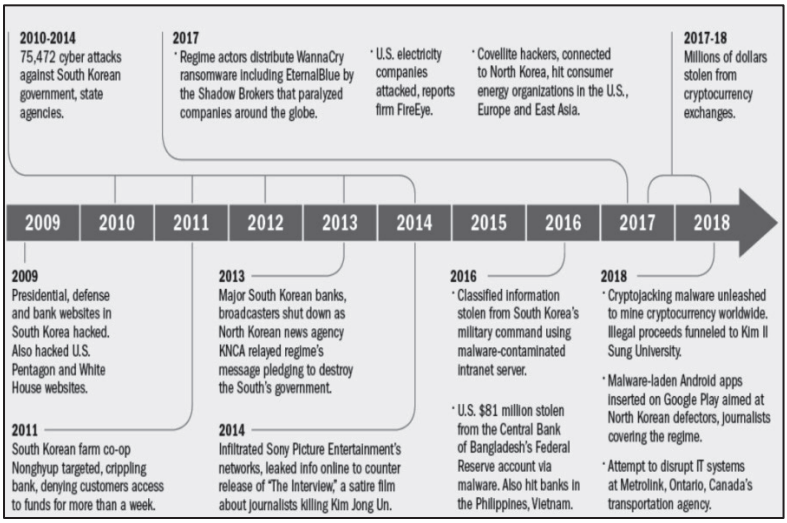
North Korea has been implicated in a number of major cyber-attacks over the past few years, primarily against South Korea. Criminal investigators have investigated a host of cyber-attacks worldwide to North Kore hackers, sponsored by the regime. Sometimes the hackers steal money and information; other attacks aim to disable infrastructure such as electricity systems and nuclear power plants. Still others target perceived detractors of Kim Jong-un.

The first known North Korean use of cyber techniques for coercive purposes occurred in 2009 as shown in Figure 1, but

the state's use of cyber-espionage techniques predates this. The 2009 incident saw unsophisticated denial-of-service attacks against 27 US and South Korean government agencies. Little damage resulted, and the attack failed against many targets. The perpetrators were not identified and no one has claimed responsibility. Other denial-of-service attacks against South Korean targets, including Incheon International Airport, took place between 2009 and 2011, and were attributed to North Korea by South Korean sources.

In 2009, the North Korea hacked the Presidential, defense and bank websites in South Korea. The North also hacked U.S. Pentagon and White websites. In 2010-2014, Pyongyang 75,472 cyber attacks against South Korean government and state agencies.

<Figure 1> North Korea's Cyber Attacks in a Decade



Source: In-bum Chen, "Another Long Challenge shared by the Indo-Pacific Region," *IDF Forum*, vol. 44, no. 1 (2019), p. 18.

In April 2011, a cyber attack on the National Agricultural Cooperative Federation (Nonghyup Bank) left customers unable to use ATMs or online services for several days. The attack also destroyed data and deleted customer accounts and files, while removing evidence of the attack from the bank's computers.[30] April is significant for the North, being the

[30] Chico Harlan and Ellen Nakashima, "Suspected North Korean cyber attack on a bank raises fears for S. Korea, Allies," *Washington Post*, 29 August 2011.

month in which the deified Kim Il-sung was born – leading to what appear to be commemorative attacks on South Korean targets. Similar attacks took place against banks and media outlets in March 2013, likely in response to a perceived slight against Kim Jong-un, with data erased and services disrupted. Despite these cyber actions, life in Seoul continued normally and there was no panic over cyber attacks. When asked about the attacks, one senior South Korean official said this was a normal practice for the North to signal a desire to negotiate.

In March 2013, several South Korean banks and news broadcasters experienced network disruption at a time when American and South Korean military forces were conducting major combined exercises. In this attack, malware previously identified as 'DarkSeou' evaded South Korean cybersecurity software and rendered computers unusable.[31] The Korea Communications Commission said that the disruption originated at an Internet Protocol address in China but that it was not known who was responsible. Some observers suspected North Korean involvement, particularly as the attacks reportedly were less sophisticated than those that have been linked to China.[32]

---

[31] Sang-Hun Choe, "Computer Networks in South Korea Are Paralyzed in Cyberattacks," *New York Times*, 20 March 2013.

[32] "Cyberattack Shakes South Korea: Could North Korea Have Pulled it Off?," *Christian Science Monitor*, 20 March 2013.

Previous attacks that had been linked to North Korea mostly involved a less sophisticated method of attack known as a denial of service, in which Internet traffic targets and overwhelms a particular site, causing it to become temporarily unusable. A denial of service attack on the National Agricultural Co-operative Federation bank in 2011 caused a three-day outage that left customers unable to access their accounts, and also deleted some credit card records.[33] A wave of denial of service cyberattacks beginning on July 4, 2009, temporarily slowed or disabled targets in both South Korea and the U.S. The South Korean National Intelligence Service said that the attacks appeared to have been carried out by a hostile group or government, and a Korean news service reported that the agency had implicated North Korea or pro-North Korean groups.[34] Similar malware code reportedly was used in these latter two attacks, and some of the Internet Protocol addresses were traced to computers in North Korea. South Korean officials claim that North Korea has conducted more than 6,000 cyberattacks since 2010, costing nearly $650 billion in repairs and economic losses.[35]

---

[33] Nicole Perlroth and Michael Corkery, "North Korea Linked to Digital Attacks on Global Banks," *New York Times*, May 26, 2016.

[34] "North Korea 'Behind South Korean Bank Cyber Hack,'" *BBC News*, 3 May 2011.

[35] Alex Hern, "North Korean 'Cyberwarfare' Said to Have Cost South Korea £500m," *The Guardian*, 16 October 2013.

2. Case Studies of Suspected North Korean Cyber Attacks to Other Countries

One of the aims of the North Korea's cyberattack other countries is to steal money. North Korea has generated an estimated $2 billion for its weapons of mass destruction programs using 'widespread and increasingly sophisticated' cyberattacks to steal from banks and cryptocurrency exchanges, according to a confidential UN report in 2019. The UN experts said North Korea's attacks against cryptocurrency exchanges allowed it 'to generate income in ways that are harder to trace and subject to less government oversight and regulation than the traditional banking sector.' The Security Council has unanimously imposed sanctions on North Korea since 2006 in a bid to choke funding for Pyongyang's nuclear and ballistic missile programs. The council has banned exports including coal, iron, lead, textiles and seafood and capped imports of crude oil and refined petroleum products.

(1) WannaCry Cyber Attack in 2017

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency as shown in Map 1. The worm is also known as WannaCrypt, Wanna

Decryptor 2.0,[36] WanaCryptor 2.0,[37] and Wanna Decryptor. It propagated through EternalBlue,[38] an exploit developed by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called the Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems.

The attack was stopped within a few days of its discovery due to emergency patches released by Microsoft, and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars.[39] Security experts believed

---

[36] Jakub Kroustek, "Avast reports on WanaCrypt0r 2.0 Ransomware that infected NHS and Telefonica," *Avast Security News, Avast Software, Inc*, 12 May 2017.

[37] Fox-Brewster, Thomas, "An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak," *Forbes*. 12 May 2017.

[38] Bruce Schneier, "Who Are the Shadow Brokers?" *The Atlantic*, 23 May 2017.

[39] Initial reports placed the number of affected computers at 200,000. See

from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country. In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.[40]

<Map 1> Map of the Countries initially Affected by WannaCry Attack

Source: "Cyber-attack: Europol says it was unprecedented in scale," *BBC*, *13 May 2017.*

According to Kaspersky Lab, the four most affected

Russell Goldman, "What We Know and Don't Know About the International Cyberattack," *New York Times*, 12 May 2017.

[40] Thomas P. Bossert, "It's Official: North Korea Is Behind WannaCry," *The Wall Street Journa*, 19 December 2017.

countries were Russia, Ukraine, India and Taiwan.[41] A new variant of WannaCry ransomware also forced Taiwan Semiconductor Manufacturing Company (TSMC) to temporarily shut down several of its chip-fabrication factories in August 2018. The virus spread to 10,000 machines in TSMC's most advanced facilities.[42]

(2) Bangladesh Central Bank Cyber Attack in 2016

In February 2016, a series of cyberattacks on banks in Bangladesh and Southeast Asia, including the Philippines and Vietnam, resulted in the theft of approximately $81 million.[43] Some researchers have linked these attacks to North Korea, citing similarity between the code used in this incident and that used in previous attacks in which North Korea was implicated. In this theft, hackers used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) global messaging service to the Federal Reserve Bank of New York to transfer money from the Bangladesh Central Bank to accounts in the Philippines. This reportedly was achieved by network intruders inserting malware into a SWIFT terminal used by Bangladesh's

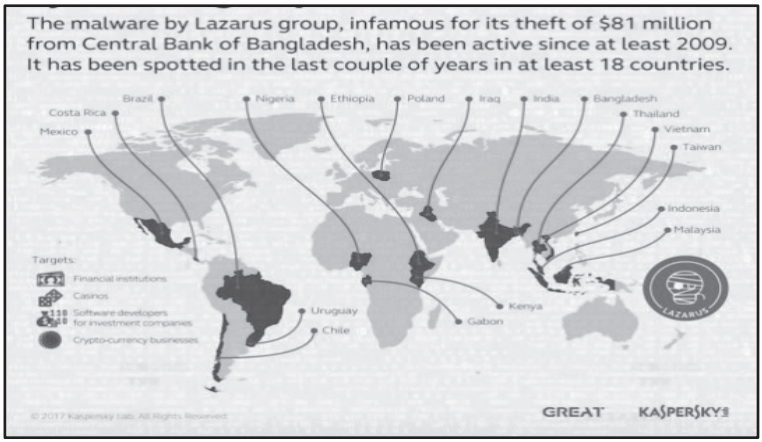
[41] Sam Jones, "Global alert to prepare for fresh cyber attacks," *Financial Times*, 14 May 2017.

[42] "TSMC Chip Maker Blames WannaCry Malware for Production Halt," *The Hacker News*. 7 August 2018.

[43] Aruna Viswanatha and Nicole Hong, "U.S. Preparing Cases Linking North Korea to Theft at N.Y. Fed," *Wall Street Journal*, 22 March 2017.

central bank. Bangladesh's network may have been particularly vulnerable, as it reportedly lacked a firewall to protect against outside intrusion. The hackers sent fraudulent SWIFT messages between the banks in New York and Bangladesh, and altered the printed confirmation of transactions in order to obscure the activity. The hackers had requested nearly $1 billion from one bank to the other, but the U.S. central bank rejected most of the requests.

<Figure 2> The Geography of Financial Attacks by Lazarus Group



Source: Source: Kaspersky Lab, "Lazarus Under the Hood," accessed at https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf.

On March 21, 2017, Deputy Director of the National Security Agency Richard Ledgett noted research that "forensically" tied this incident to the cyberattacks on Sony, and said that if North Korea's role in the bank robbery was confirmed, it would represent a troubling new capability.[44] Reportedly, some investigators believe that Chinese intermediaries aided North Korea in conducting the theft, while others have outright accused Chinese hackers of being the perpetrators.[45]

In addition to the Bangladesh Bank, hackers reportedly attacked other banks using SWIFT. According to one report,[46] North Korea is now being linked to similar attacks on banks in as many as 18 countries.[47] The SWIFT system is used by some 11,000 banks and companies to transfer money from one country to another and is considered the backbone of global finance. Yet cyberattacks on banks have not been limited to the

---

[44] Jonathan Spicer and Joseph Menn, "U.S. May Accuse North Korea in Bangladesh Cyber Heist: WSJ," *Reuters*, 22 March 2017.

[45] Karen Lema and Manuel Mogato, "Bangladesh Bank Hackers 'Possibly Chinese,' Says Philippines Senator," *Reuter***s**, 5 April 2016.

[46] Kaspersky Lab, "Lazarus Under the Hood," accessed at https://securelist.com/files/2017/04/Lazarus_Under_The_Hood_PDF_final.pdf.

[47] Jose Pagliery, "North Korea-linked hackers are attacking banks worldwide," *CNN*, 4 April 2017.

use of SWIFT; other bank attacks were said to have employed a "watering hole" technique in which hackers lurk around a highly trafficked website in order to redirect the website's visitors to a page containing malicious software. Security researchers at Symantec believe that the same hackers were behind both of these attack methods.[48]

(3) Sony Pictures Entertainment Cyber Attack in 2013

In the run-up to the scheduled Christmas Day 2014 release of The Interview, a film depicting the fictional assassination of North Korean leader Kim Jong-un, North Korea's Foreign Ministry called the film 'the most blatant act of terrorism and war' and threatened a 'merciless countermeasure.'[49] On November 24, Sony Pictures Entertainment experienced a cyberattack that disabled its information technology systems, destroyed data, and accessed internal emails and other documents that were then leaked to the public. North Korea denied involvement in the attack, but praised hackers, who called themselves the 'Guardians of Peace,' for having done a "righteous deed."[50] Hackers then sent emails, threatening

[48] Paul Mozer and Sang-Hun Choe, "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, 25 March 2017.

[49] "Hackers' Threats Prompt Sony Pictures to Shelve Christmas Release of 'The Interview,'" *Washington Post*, 17 December 2014.

[50] "North Korea: Sony Hack a Righteous Deed but We Didn't Do It," *The Guardian*, 7 December 2014.

'9/11-style' terrorist attacks on theaters scheduled to show the film, leading some theaters to cancel screenings and for Sony to cancel its widespread release; U.S. officials claimed to have 'no specific, credible intelligence' of such a plot.[51]

The FBI and the Director of National Intelligence (DNI) attributed the cyberattacks to the North Korean government.[52] During a December 19, 2014, press conference, President Obama pledged to "respond proportionally" to North Korea's alleged cyber assault, 'in a place, time and manner of our choosing' and called the incident an act of 'cyber-vandalism.'[53] On December 20, cyber analysts and news media reported that the North Korean network providing access to the Internet went offline for approximately 10 hours. Many cyber analysts said the disruption pointed to a network attack, although they could not rule out either an overload or a preventive shutdown by North Korea.[54] U.S. officials would not comment on

---

[51] "U.S. Weighs Options to Respond to Sony Hack, Homeland Security Chief Says," *Wall Street Journal*, 18 December 2014.

[52] FBI National Press Office, "Update on Sony Investigation," 19 December 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

[53] Andrew Grossman, "U.S. Weighs Options to Respond to Sony Hack, Homeland Security Chief Says," *Wall Street Journal*, 18 December 2014.

[54] Cory Bennett, "Did the US Take Down North Korea's Internet?" *The*

whether this constituted the 'proportional response,' saying only that some elements of the response would be seen while others would not. Although elements of the U.S. intelligence community publicly claimed to have compelling proof of North Korean involvement in the attacks on Sony, some information security experts questioned whether North Korea had the capability to conduct destructive attacks and whether the malware involved contained markers that would definitively indicate North Korean origin.[55]

The Sony incident differs from other cyberattacks in that it had a destructive element; in this incident, many of the work stations targeted were damaged beyond repair and had to be replaced. Previously, much of the cyber activity that stemmed from North Korea had been limited to being disruptive, such as denial of service or website defacement. For example, the South Korean government accused North Korea of a December 2014 cyberattack on the computer systems of the Korea Hydro and Nuclear Power Ltd (KHNP), which runs South Korea's

---

Hill, 23 December 2014.

[55] See FBI National Press Office, "Update on Sony Investigation," 19 December 2014, https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation and Paul Szoldra, "A Hacker Explains Why You Shouldn't Believe North Korea Was Behind the Massive Sony Attack," *Business Insider*, 10 June 2016.

nuclear power plants.[56] In December 2014 and again in March 2015, hackers published designs, manuals, and other information that had been obtained through a phishing attack on employee email accounts, prompting heightened cybersecurity measures. Investigators said that the hackers intended to cause a malfunction at atomic reactors, but failed to break into their control system, which is not connected to the Internet.[57]

Sony was also likely an unpleasant surprise for the North Koreans, as they had assumed a high degree of – if not anonymity – plausible deniability. Advances in US attribution capabilities stripped this away. Pyongyang likely underestimated Washington's ability to determine the source of the attack. The hope was that this would influence the likelihood of such an incident being repeated, leading North Korea to recalculate the risk of more action against the US driven not only by concern over possible US retaliation but also over Chinese displeasure at destabilizing actions that would affect its interests.[58] A wholly successful US response

[56] "S. Korea Accuses North of Cyber-Attacks on Nuclear Plants," *Phys.org*, 17 March 2015.

[57] "South Korea Says Nuclear Reactors Safe After Cyber-Attacks," *Security Week*, 25 December 2014.

[58] James A. Lewis, "North Korea and Sony: Why So Much Doubt and What about Deterrence?," *38 North*, 7 January 2015.

to the Sony attack would have changed the basis on which North Korea made such decisions, by demonstrating that the leadership in Pyongyang had underestimated the risk (at least the risk of detection and attribution) involved in actions against the US and US-based entities. North Korean attacks would still be possible, but the threshold for deciding to carry them out would likely be higher. However, North Korea had changed the rationale for its cyber operations, turning the capabilities it had developed for intelligence purposes to a new task: cyber crime.

V. Conclusion

The South Korea's security will be seriously threatened should it lose the battle to control cyberspace. However, it has not been easy to devise innovative counterstrategies, because of the special conditions of cyberspace and the substantial investment and effort required. The best policy available at this point is, first, to upgrade, as a strategic matter, the ROK Cyber Command, established in early 2010. This command will open the way for cooperation among existing national cyberwarfare institutions and for collaboration in new policies and connections. It can also formulate a system that will enable cyberwarfare operations led by the military in time of war; connect and conduct integrated intelligence and regular operations; and design an overall cyberwarfare structure, including the concepts, doctrine, requirements, education, and training methods needed for the command to operate

effectively.

Countermeasures at the government level are also necessary. South Korea is an information-technology powerhouse. Its world-class 'cyber geniuses,' technological abilities, investment capital, and infrastructure make it asymmetrically superior to the North. The problem lies with the government's lack of effort and will to organize and systemize such potential for effective use in the field of national security. It is urgent that we resolve such an ironic contradiction. At a policy level, solutions may include establishing norms for the cyber realm, obliging real-name usage, creating a cyber 'shinmungo' (신문고, a big drum that was struck by petitioners against the government during the Joseon dynasty, 1392–1897) to allow the people to report suspicious activities, formulating a voluntary cyber reserve force and a mobile civil-defense unit, commending regions that have greatly contributed to cyber protection, and holding cyber-protection technology competitions.

Furthermore, the ROK must establish and strengthen legal and systematic devices that can block North Korea's unusual cyber-infiltration tactics and sever its connections with sympathizers within the South. Although it is important that the government protect its citizens' freedom in cyberspace, irresponsible, antisocial, and antinational behavior must be constrained. Cyberspace has now become the fifth battlefield, where an important 'nonwar' must be fought and victory won

through a ‘minimal damage’ strategy.

As North Korea improves its ability to conduct more aggressive cyber operations, the South Korea’s executive branch and National Assembly face pressure to counter such attacks like the United States. Response in the cyber arena is mostly classified, heightening the need for relevant national assembly committees to engage with the intelligence and defense communities. For preventing and countering North Korean cyber attacks, we try to find the answers to the following questions.

- ✓ How secure is our financial system?
- ✓ Should we develop legislation to regulate the network security of the financial sector?
- ✓ Are more regulations needed to prevent traders from unwittingly exposing their systems to infiltrators?
- ✓ Should our direct resources toward securing weak links in international finance systems?
- ✓ What are government agencies’ roles and responsibilities in responding to a cyber incident on private networks?
- ✓ What offensive capabilities is South Korea employing to respond to North Korean hackers?
- ✓ What is the administration’s strategy to deter

cyberattacks from North Korea?

- ✓ What pressure can South Korea, the United States and other countries put on countries that host North Korean overseas hackers?
- ✓ How should South Kore and the United States weigh North Korean cyber intrusions against other more conventional threats emanating from the regime?
- ✓ How should the sanctions regime address North Korean cyber operations?

On balance, the global nature of cyber operations requires multiple committees with varying jurisdictions to share information, oversight, and authority. International finance, foreign affairs, homeland security, armed services, law enforcement, and information technology infrastructure committees may all have equities in this area. Developing legislation may require disparate members and committees to adequately address the complex nature of the challenge.