An Assessment of North Korean Cyber Threats and the Republic of Korea's Policy Responses: An Update

Hyeong-Wook Boo

Research Fellow

Center for Security and Strategy, Korea Institute for Defense Analyses (KIDA)

Kyung-Roak Kang

Research Assistant

Center for Security and Strategy, KIDA

Abstract

Recent cyber threats from North Korea and its transformations since 2009 are introduced and analyzed in this present study. There is a clear difference in North Korea's recent behavior in cyberspace, compared to prior years. Currently refraining from continuing any saber-rattling cyber attacks against South Korea and the world, North Korea's recent cyber operation cases are regarded as primarily motivated by financial objectives. This crucial development is relevant to the rapidly transforming geopolitical situation of the Korean Peninsula, and represents a strategic overturn of Kim Jung Un's national strategy. This, in turn, will cause cyberwar logic in the Peninsula to eventually lose its existential rationales in the future. Thus, it is necessary to develop a multidimensional approach towards existing North Korean cyber threats, in both domestic and international policy. Such efforts should include renewing domestic cyber-response systems, securing international cooperation to restrict the mobility of North Korean hackers, and even lifting international sanctions to some extent, in order to provide incentives to discourage North Korea's cyber activities in the pursuit of financial resources.

Keywords*: cybersecurity, North Korean, cyber capabilities, geopolitical situation, international sanctions*

An Assessment of North Korean Cyber Threats

北韓網路威脅評估與大韓民國政策回應：最新觀察

Hyeong-Wook Boo

韓國國防研究院安保戰略研究中心 研究員

Kyung-Roak Kang

韓國國防研究院安保戰略研究中心 研究助理

本文闡述並分析北韓近期網路威脅與 2009 年以來之演變。近年來北韓的網路行為模式與過去存在明顯差異。目前北韓透過網路攻擊對韓國與世界發動文攻武嚇的行為有所節制，其近來網路行動目的多半被認為已轉為金融目標導向。這個關鍵發展與韓半島上快速轉變的地緣政治局勢息息相關，同時也反映了金正恩的戰略轉變。此轉變將使得大規模網路戰爭在韓半島最終失去存在的理由。為了應對新型北韓網路威脅，（韓國）勢必要發展貫穿國內外政策在內的全方位網路政策，包括更新國內網路應變系統、透過國際合作抑制北韓駭客的機動能力，甚至將其納入制裁標準以嚇阻北韓透過網路行動來攫取金融資源。

關鍵詞：網路安全，北韓，網路能力，地緣政治，國際制裁

Introduction

As of December 2018, we are witnessing a renewed strategic environment on the Korean Peninsula, which is unprecedented for those accustomed to the decade-long confrontations between the two Koreas. The South and North Korean leaders met three times in the course of six months, and the world is looking forward to seeing the second US-DPRK summit in a month or two. People around the world are waiting for the remarkable news of North Korea's submission of a denuclearization roadmap to the international community. Suddenly, the advent of permanent peace on the Korean Peninsula seems inevitable.

However, many skeptics still believe that North Korea's announcement of denuclearization is just a show or another deception tactic. According to an official from the United States Department of Defense (DoD), North Korea has made more than five nuclear warheads in 2018, despite the progress of peace talks.[1] Thus, we need to maintain dual perspectives and take a cautious approach in handling the current situation of the Peninsula. This attitude is necessary because concrete results that will ensure peace are not yet in our grasp, despite the burgeoning prospect of peace in the Peninsula. This supports us to support the rationale of delving into North Korean cyber threats assessment without making this case a political issue.

In 2018, however, we have not heard of cyber activities that might have had a huge impact on the military and other means of security. North Korean cyber threats became an important issue last September when the US Department of Justice prosecuted the North Korean hacker, Jin-Hyok Park, for launching several cyber attacks.[2] The FBI field officer's criminal complaint submitted to the US District Court does not deal with his activities in 2018. It concerns Park's activities in the years of 2017, 2016 and 2014.[3]

---

[1] Kube, Courtney and Andrea Mitchell, "North Korea is Still Producing Ballistic Missiles after Summit," *NBC NEWS,* August 1, 2018. https://www.nbcnews.com/news/north-korea/north-korea-still-producing-ballistic-missiles -after-summit-n896331.

[2] The U.S authority has tracked the North Korean hackers' activities with clues detected when the hackers used the G-mail. While the investigation of other hackers that colluded with Mr. Park is still going on, the Interpol reveals the plan for issuing the 'Red Notice (to seek the location/arrest of a person wanted by a judicial jurisdiction)', if asked by the U.S.

[3] Shields, Nathan, "Criminal Complaint (U.S. vs. Park, Jin Hyok)," *US. District Court for*

Meanwhile, cyber threats posed by North Korea became an issue when cyber money began drawing attentions starting last year. Some newspapers printed several articles implicating North Korean hackers for exchanging encrypted cyber money.[4] Those arguments were not validated by authorities, but experts in the cybersecurity field are keeping an eye on the situation. It also has been suggested that some parts of the government may be working on this as well.[5]

In any case, it can be argued that North Korean hackers have been relatively quiet in 2018. While it is possible that the world simply has not uncovered North Korea's hacking activities, North Korea does not seem eager to disrupt the peace-oriented mood on the Peninsula with any hacking attempts. As many commentators have stated, Kim Jung Un wants to obtain a reputation from the world that he is sincere in his participation in the peace talks and that he is trustworthy. From another perspective, analysts have postulated that North Korea may be focusing more on the financial side of its cyber operations than the military and security related side. This speculation reflects a highly plausible scenario because North Korea needs new financial sources to maintain both its economy, and Kim Jung Un's luxurious lifestyle. The regime continues to talk with South Korea, the United States and others, hoping that the economic sanctions will be lifted. However, this presents a struggle, as the international community does not want to lift the sanctions over North Korea until North Korea's denuclearization presents visible progress. Whatever the case may be, we need to carefully look at North Korea's cyber capabilities and assume that it poses a very serious threats until North Korea clarifies its intention to terminate cyber attacks. Thus, for now, we must ensure that the dual stances toward North Korea and North Korean cyber issues be maintained for a while. Under these considerations, in this article, North Korea's activities in cyberspace and its characteristics will be

---

the Central District of California, June 8 ,2018. https://www.justice.gov/opa/press-release/file/1092091/download.

[4] Min-seo Kim, "More Than 7,000 Cyber Warriors in North Korea, Earning 1 Trillion Won Annually," *Segye Ilbo*, November 23, 2017. http://www.segye.com/newsView/20171123005037.

[5] Seon-mok Lee, "US reveals that, North Korea will continue to focus on cyber activities, to secure Funds for the WMD Development," *Chosen Ilbo,* September 10, 2018. http://news.chosun.com/site/data/html_dir/2018/09/10/ 2018091000625.html.

reviewed. In the following section, recent cases of North Korean cyber threats and their major differences from the past will be analyzed in a comparative perspective. Then, South Korea's policy responses including recent developments and limitations will be briefly reviewed. Lastly, policy implications and suggestions will be proposed.

Cases of North Korean Cyber Attacks[6]

In this section, the author of this article argues that the focus of North Korean cyber operations is moving toward profit seeking, contrary to the past motivation of saber rattling cyber attacks. The premise is that North Korea and its cyber strategy is rapidly changing. In 2018, as mentioned above, the North Korean cyber strategy has proved to be less militaristic than before-even though this strategy is still dangerous and poses preponderance of threats to free and safe transactions in cyberspace. While some evaluate that North Korea has reset its national strategy, there is a general consensus that North Korea wants to be seen as a normal country and to claim membership in the international community. This is why Kim Jung Un changed his strategic stance earlier this year. It also seems that the strategic turnover has been reflected in North Korea's behavior in cyberspace. Reviewing the short history of North Korea's cyber provocations will reveal the validity of the argument. To begin, cases of the 2000s will be discussed.

The social discourse regarding cybersecurity has a relatively short history in South Korea. The 7.7 DDoS attacks in 2009 marked a watershed moment in raising the general public's awareness regarding cyber threats posed by North Korea. Compounding traditional security threats with non-traditional threats was a remarkable feature of the 7.7 DDoS attacks. North Korea coordinated cyber-attacks with the second nuclear test on May 2009 and missile launches on the July 4, 2009 and others, with the primary intention of shattering South Korean minds. Similar cyber attacks having occurred after the 7.7 DDoS attacks include the DDoS attack on July 7, 2010. North Korea sank the Cheon-an corvette in March 2010 and scheduled a

[6] Please see Boo, Hyeong-wook, "An Assessment of North Korean Cyber Threats." *The Journal of East Asian Affairs*, Vol. 31, No. 1, 2017, pp.97-117.

cyber-attack after a major military provocation. On April 12, 2011, North Korea caused the paralysis of the Nonghyup Internet banking system. In that month, South Korea and the United States carried out their annual combined military exercises which North Korea had always condemned. On March 20, 2013, about one month after the third nuclear test, North Korea launched the Master Boot Record (MBR) wiper attacks which shut down 32,000 computers of banks and media agencies.[7] North Korea also increased cyber attacks after the fourth nuclear test on January 4, 2016. As many commentators argued, North Korea had deliberately chosen the date of the cyber attack because it wanted to sound an alarm in South Korea. In other words, North Korea seemed to cause psychological damage to the South Korean society by using its cyber capabilities.

In 2014 and 2016, there were many cyber attack cases that were considered serious incidents in military perspectives. It seemed North Korea was trying to prove that it could cause real, physical damage in wartime through cyber attacks. In 2014, there were hacking attempts on Seoul Metro, the city's subway system. North Korea intended to compromise the mass transportation management system which would result in widespread chaos. It also sent an ominous sign to the general public of South Korea, which forecast a transportation disaster to be triggered by a cyber attack. In December 2014, there were cyber-attack attempts against the information system of the South Korean nuclear power plant corporation, Korea Hydro & Nuclear Power (KHNP). North Korea even hacked South Korea's Ministry of National Defense (MND) in 2016. North Korean hackers infiltrated the MND intranet using a malware-implanted USB stick and eventually stole South Korea's War Plan 5027 material. This was an extremely shocking incident because the MND Intranet, which operated separately from the Internet, had seemed highly secure and safe from hacking attempts. There was also a hacking attempt on defense-related corporations in 2016. The hackers stole the maintenance manuals of F-16's, photos of South Korean drone parts, and other sensitive documents. Authorities estimated that 42,600 documents were

[7] Kwang-hyung Cho, "Malicious Code Penetration Aginst Network of KBS, North Korea's Deed." *New Daily,* March 20, 2013. http://www.newdaily.co.kr/site/data/html/2013/03/20/2013032000061.html.

stolen. This was a new phenomenon that once again conveyed an impression of North Korean hackers as being more military-oriented in the purposes of their attack.

Meanwhile, there were different types of North Korean cyber behavior that seemed to have financial motive. These kinds of behavior can be observed from 2015. In 2015, North Korean hackers had penetrated the Vietnamese and Philippino banks. They had created bank accounts that were used as money-laundering accounts for the Bangladesh Bank penetration later in 2016. In February 2016, North Korean hackers infiltrated the Bangladesh Bank and stole USD 81 million. According to a FBI field officer, "Approximately 81 million dollars was routed to accounts in the Philippines, and 20 million dollars was routed to an account in Sri Lanka. But the 20 million dollars sent to Sri Lanka was stopped by the recipient bank." The money sent to the Philippinn bank was laundered in various ways, and this became the largest successful cyber theft from a financial institution.

In Korean history, 2017 will likely be remembered as one of the most dangerous years from the perspective of North Korean military provocations, while being marked as a turning point in North Korean cyber strategies. Kim Jung Un rushed to finish nuclear weapons and intercontinental ballistic missiles (ICBM) developments. On average, there had been a North Korean military provocation once every two weeks. However, in cyberspace, there had not been saber-rattling cyber attacks in 2017, targeting transportation networks, nuclear power plants and Internet banking systems. However, North Korean hackers did launch the Wannacry ransomware attacks and tried to hack crypto-currency markets. Arguably, the primary motivations of those cyber operations were monetary.

When the Wannacry ransomware attacks occurred, the *New York Times* conducted an interview and wrote the following; "Boo Hyeong-wook said the scale of the attack was large enough that it was likely to have been supported on a national level. He also said it would be a logical extension of growing boldness of North Korean hackers to exploit their abilities to raise much-needed funds for the government, which has been starved of cash by

international sanction."[8] A recent FBI complaint submitted to US District Court confirmed that the Wannacry ransomware attack was orchestrated by North Korean hackers, also known as Lazarus. The complaint designated Park, Jin Hyok as a member of Chosun Expo, which is a North Korean company operating in Dalian, China.[9] Chosun Expo is affiliated with the North Korean hacking organization, Lab 110 and is suspected to have launched many cyber attacks across the world, with the intention of obtaining cash for the government at that time. According to Dune Lawrence of *Bloomberg Businessweek*, three Wannacry bitcoin wallets had received 277 payments by May 17, 2017, at a value equivalent to USD 82,000.[10]

North Korean hacker groups, especially Lazarus, have broken into crypto-currency exchanges all over the world. This is a recent development in North Korean cyber operations. Most of these recent North Korean cyber operations concerning crypto-currency are under investigation and the details have yet to come to light. Some of the penetrations known to the public occurred in 2017 and 2018. For example, in June 2017, the Coinrail and Bithumb exchanges were compromised owing to hacking and estimated losses were equivalent to USD 50 million.[11] In September 2017, North Korean hackers seemingly affiliated with the 121 Bureau under the General Bureau of Reconnaissance broke into Coinis, a South Korean crypto-currency exchange and stole crypto-currencies equivalent to about 1.5 million dollars. In December 2017, Youbit, another South Korean crypto-currency exchange was compromised by alleged North Korean hackers, resulting in a loss of crypto-currency worth more than USD 14 million. In January 2018, authorities found malware that had the command

---

[8] Sang-Hun Choe et al, "Focus Turns to North Korea Sleeper Cells as Possible Culprits in cyber attack," *The New York Times,* May 16, 2017. https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper- cells-ransomware.html.

[9] David Sanger and Katie Banner, "U.S. Accuses North Korea of Plot to Hurt Economy as Spy is Charged in Sony Hack," *The New York Times*, September 6, 2018. https://www.nytimes.com/2018/09/06/us/politics/north- korea-sony- -wannacry-indictment.html

[10] Dune Lawrence, "North Korea's Bitcoin Play: Cut off from the hack world economy by sanctions, Pyongyang is looking for ways to get its hands on cryptocurrency," *Bloomberg Businessweek*, December 15, 2017. https://www.bloomberg.com/news/articles/2017-12-14/north-korea-s-bitcoin-play.

[11] *"*North Korea Cyber Activity,*" Recorded Future Insikt Group*, June 14, 2017. https://go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

lines to mine Monero, a crypto-currency, and transferred funds to a Kim Il-sung University bank account. In March 2018, Lazarus launched spear-phishing[12] attacks across the world by using Falcon coin accounts which are similar to the Falcon coin of the Turkish crypto-currency exchange. Research presented by McAfee, an international security firm based in California, has revealed that Lazarus reused the code used in previous hackings when attacking Falcon accounts.[13] In August 2018, Lazarus penetrated the Cosmos Bank in India, compromised the alarm system and stole USD 13 million. They created a fake debit card and successfully made ATM deals through which they can transfer money to other places.

Policy Response to North Korean Cyber Threats: A Brief Overview

In review of North Korean cyber activities since 2009, security experts have consistently suggested that the primary feature of North Korean cyber attacks are characterized as an implementation of asymmetric strategy. This strategy provides less-developed countries with scarce resources the opportunity to damage information and communications technology (ICT) environments of developed counterparts at low costs.[14] As South Korea may be at particular risk due to developed ICT, the high frequency of cyberspace usage and immature awareness of cybersecurity among South Koreans, a few attacks on core infrastructure may cause catastrophic confusion in the society.[15] As a world-renowned information technology (IT) giant, these

[12] Spear phishing sends malicious e-mail to a specific person, which infects the computer and takes information when the attachment file is opened.

[13] Jay Rosenburg and Christiaan Beek, "Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families." McAfee, August 9, 2018. https://securingtomorrow.mcafee.com/mcafee-labs/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/.

[14] Jong-In Lim et al., "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The* Quarterly *Journal of Defense Policy Studies,* Vol. 29, No. 4, 2013, p.32. (in Korean)

[15] Hyeong-wook Boo, "Issues of Cyber Security and Policy Directions: Discussions for the Establishment of Defense Ministry's Cyber Policy," *Journal of National Defense Studies*, Vol. 56, No. 2, 2013, p.106. (in Korean)

reasons are precisely why South Korea has been targeted by major North Korean cyber attacks for more than a decade. Moreover, South Korea's increasing network dependency has exposed some system vulnerabilities, despite enhanced societal cybersecurity measures. Networks are compromised due to their own vulnerabilities, compounded by North Korea's improved cyber capabilities. These two factors are not only interconnected, but also expected to trigger devastating societal effects once a cyber attack occurs.

Faced with the abovementioned cases, the South Korean government has developed a variety of policy efforts in the cybersecurity area. The establishment of Cyber Command in 2010 was an important initial measure by the Ministry of National Defense. In order to foster experts in cybersecurity, the government also sponsored the introduction of cybersecurity programs at universities and various public competition events. In 2011, the government announced a Cybersecurity Master Plan, which was significant as it marked the first plan to serve as a foundation for future national cyber -security strategies. The plan, aiming for a thorough defense of national cyberspace from cyber threats, emphasized the specific roles of each ministry, along with their cooperation.

Following these developments, the National Cyber Threat Joint Response Team was established within the National Cyber Safety Center to promote information sharing and multi-level cooperation. Their underlying principles were to achieve early detection of cyber attacks while establishing an essential response system. Importantly, the Plan also included efforts to enhance citizens' cybersecurity awareness throughout society. It proposed to enact "The Information Security Day," a statutory anniversary on the second Wednesday of every July, to raise awareness of cybersecurity and information protection. The plan also promoted private-sector campaigns to protect personal information from zombie personal computers (PC) and strengthening education in information security in primary and secondary schools. However, it has been suggested that palpable effects of these countermeasures in the early 2010's seem to be negligible, likely due to the constant development of cyber threats over time.

These efforts led to the National Cybersecurity Strengthening Plan in

2015, which was proposed following the hacking of the Korea Hydro & Nuclear Power (KHNP) in December 2014.[16] First, the government planned to establish and expand the role of government organizations dedicated to cybersecurity, enabling improvement of security capabilities in central administrative agencies. The Presidential Secretary for Cybersecurity was established, and in May 2015, a meeting was held with the Office of National Security. The aim of this meeting was to gather the National Intelligence Service (NIS), military, police, and senior officials from various government ministries to discuss cyber-attack countermeasures. The government also announced a plan to expand its professional manpower, strengthening its capacity to cope with cybersecurity affairs. At the same time, the government has also been actively sponsoring relevant industries, such as anti-hacking and security technology companies, to maintain major information and communication networks. Lastly, the government revealed a plan to cooperate closely with the international community regarding hacking cyber incidents.

The most recent example, according to the *White Paper for National Information Protection* published in May 2018, is the Office of National Security's designation as the sole control tower of cybersecurity. This is a part of a "five-year plan for state affairs," announced immediately after the Moon Jae-in administration assumed office in 2017.[17] The National Assembly Advisory Planning Committee, which drafted the proposal, announced that the proposal is a part of an "enhancement of the cybersecurity control tower," balancing the organizational capabilities in cybersecurity areas that was once concentrated in the NIS.[18] This settles the controversy over which organization should play the leading role in cybersecurity affairs, while also partially resolving security experts' concern that the NIS was previously overgrown with an information monopoly. Such prevention of organizational inefficiency in cyber countermeasures is consistent with plans specified in the

[16] Sea Min, "Strengthening National Cyber Security Significantly," *Boan News*, March 18, 2015. https://www.boannews.com/media/view.asp?idx=45697&kind=2.

[17] Jae-woon Lee, "The Government's New Cyber Security 'Center' is The National Security Office." *E-Daily,* May 21, 2018. http://www.edaily.co.kr/news/read?newsId=02660086619211216&mediaCodeNo=257&Out LnkChk=Y.

[18] *Ibid.*

Defense Reform 2.0, released on July 2018; this is an expansive initiative to restructure and modernize South Korea's defense capacity.[19] The cybersecurity section of the initiative specified a plan to establish a cyber response team, ensuring an increasingly responsive cyber defense operation. It has been reported that the organization will concentrate on 'cyber operations' after completely abolishing the function of "cyber psychological-operations," the central topic of recent political controversy.

South Korea's responses to North Korean cyber activities have been gradually evolving. However, despite the various efforts undertaken, several experts consistently identify loopholes within the response system, still fragmented and highly complicated, that impact the provision of effective responses in the face of rapidly evolving cyber threats. This problem is aggravated by the fact that the Blue House recently abolished the position of Presidential Secretary for Cybersecurity, which was established in 2015 as part of an organizational restructuring.[20] Moreover, the additional bill responding to North Korean cyber attacks has been pending in the National Assembly for a long time, making active and responsive countermeasures infeasible. It is of little surprise that successive government-wide meetings to discuss countermeasures against cyber threats have ended fruitlessly. This may be due to several reasons, including a lack of adequate legislation and legal basis, as well as the absence of coordination between related organizations. Experts state these problems repeat due to insufficient system management regarding cyber threats.[21] For example, the role of the control tower for cybersecurity has still not been clearly defined, and the division of roles by government agencies remains vague.[22] Another problem is sparse

[19] Sung-young Jang, "How Will 'Defense Reform 2.0 Change South Korea's Defense? A Closer Look at Moon Jae-in's Ambitious Defense Modernization Plan,'" *The Diplomat*, August 27, 2018. https://thediplomat.com/2018/08/how-will-defense-reform-2-0-change-south-koreas-defense/.

[20] Young-dong Son, "Stop Acting! The United States Gives a Red Card to the North Korean cyber attacks." *Choong-Ang Daily*. September 14, 2018. https://news.joins.com/article/22970263.

[21] Hyeong-wook Boo, "An Assessment of North Korean Cyber Threats," *The Journal of East Asian Affairs*, Vol. 31, No. 1, 2017, p.110.

[22] A specific implementation schedule of the plan specified in "A five-year plan for state affairs" and the details of the responsibility sharing among related government organizations still remains unclear.

debate regarding how to share the costs between the public and the private sectors for cybersecurity projects, which is a significant responsibility. No viable plan for how the government should build and develop a flexible regulatory system for cybersecurity has been suggested. The outcome of such shortcomings, combined with the absence of endeavors to forge social consensus on cybersecurity issues, has resulted in reactive measures only, focusing on minimizing damage following an attack taken, rather than any preemptive measures.

Given the above-mentioned situations, responses to cyber threats in South Korea can be evaluated as insufficiently discussed, with limited strategic consideration. Compared to the intensity of North Korea's cyber threats, the South Korean government and the public's interests in cybersecurity are limited. According to the recently published article of Lee et al.,[23] the current national cybersecurity system demonstrates difficulties in preventive detection of cyber attacks from North Korea, which conducts simultaneous attacks on various parts of society. Inconsistent political support for sustainable budget allocation for cybersecurity affairs and nascent efforts to develop international cooperation are other important factors that impede further development. Due to this array of obstacles, vulnerability is still pervasive within the South Korean response system against North Korean cyber threats. In 2013, experts evaluated the cybersecurity system, which was current at the time, by sharing Delphi results representing South Korea's cyber preparedness. The results stated their level of goal sharing, organizational process and culture for cooperation were below average.[24] More recent policy development of cybersecurity does not support much improvement at the time of this article's writing, However, most importantly, the response system needed to be adequately updated to reflect the swift transformation of North Korean cyber activities; this will be discussed in the following section.

---

[23] Yong-joon Lee et al., "The Countermeasure Strategy Based on Big Data against Nor th Korean Cyber Attacks," *The Korean Journal of Defense Analysis*, Vol. 30, No. 3, 2018, p. 445.

[24] Hyeong-wook Boo et al., "A Study on Future Directions of Defense Cyber Policy," *KIDA report,* 2013 (in Korean).

Changing Trends and Policy Implications

There is a qualitative change in North Korea's cyberspace behavior in recent years. A review of the recent behavior of North Korean hackers in cyberspace reveals North Korea is abstaining from launching saber-rattling cyber attacks against South Korea and the world. With recent strategic changes in both the Peninsula and North Korean cyber operations especially in 2017 and 2018, it seems North Korea does not want to be viewed as plotting a future cyber warfare. Cyberwar logic does not match with Kim Jung Un's strategic overturn and does not have solid grounds considering North Korea's behavior in 2018. This situation, in turn, will eventually render cyberwar logic in the Peninsula obsolete in the future, which is an important and radical development.

Interpreting North Korea's intentions requires a review of their radically changed national strategy. Professor Hwang Il-do of the Korean National Diplomatic Academy argued North Korea established a two-year plan for the completion of nuclear weapons and ICBM in 2015.[25] He estimated that North Korea secured ICBM technologies and a RD-250 engine from Ukraine in 2015, and with these technologies, Kim Jung Un became confident that North Korea would eventually obtain the ICBM in less than two years. The reason for establishing this two-year plan, according to Professor Hwang, is due to the presidential election in December 2017 (it was for the impeachment of the former president Park in May 2017).[26] Thus, the North Korean leader thought he could make a deal with the newly elected president regarding his nuclear warheads and ICBMs. North Korea also wanted to aggrandize their nuclear capacities, making the Trump administration interested in dealing with North Korea. In so doing, however, North Korea had to prepare for possible reinforcement international sanctions given their needs to test missile engines and nuclear explosions for the completion of nuclear-tipped ICBMs by the end of 2017.

Evading international sanctions is not an easy task and we percive that North Korea viewed cyber activities as a means of obtaining financial

[25] Il-do Hwang, "North Korea's 'Guam Enemy Shooting' Threat: Intention and Calculation." *Institute of Foreign Affairs and National Security FOCUS*, 2017 (in Korean).
[26] *Ibid.*

resources. It should be noted that, compared to other financial sources such as laborer dispatching, US-dollar forgery, and drug trafficking, cyber operations are not a reliable source of finances. However, the cyber bureau of North Korea and Kim Jung Un's policy orientation can be clearly considered "all-in" for the completion of nuclear weapons and ICBMs. Thus, the cyber bureau should assume any kind of role for the policy. Since they have obtained technologies from Ukraine, locating sources of money to help in furthering Kim's policy became a essential choice. Through this method, they could claim their raison d'etre in the North Korean regime. We think that this candidate scenario has been guiding North Korea's policy transformations in cyber operations.[27]

Though North Korea would not be expected to pose meaningful military threats via cyber, this does not necessarily indicate that North Korea is a reliable and trustworthy player in cyberspace. Following this, evaluation of the danger of North Korea's cyber threats should be provided. North Korea still uses its cyber capabilities in siphoning money from various sources and, by doing this, poses a marked threat in cyberspace. As reviewed earlier, recent cyber activities of North Korean hackers include compromising Internet banking systems, crypto-currency exchanges, e-mail service providers, and other financial systems. If these activities continue in the future, they may bring about a devastating impact on world financial systems and the virtual economy. In some respects, this may be as dangerous as a cyberwar, from a military point of view. The difficulty of cybersecurity is that defenders are much more vulnerable than attackers. Attackers have freedom of choice. Their behavior cannot be detected on time due to attribution issues. Several months of hard work would be needed in confirming who the attackers were and how they completed their mission. Further, North Korea would seek to take advantage of the attacker's merits to the greatest extent.

After the third Inter-Korean Summit, the prospect of complete denuclearization and the establishment of permanent peace in the Korean Peninsula seems more probable than ever. This shift in prospect provides

[27] Anonymous research from LogRhythm Labs posits North Korean Cyber activity for financial resources will continue to escalate in 2018; they speculate the public impact of this will rise as well.

significant incentives for the Kim Jung Un regime to behave properly. Thus, South Korea, and the world, do not need to worry about cyberwar-like provocations in the near future. However, the ability of North Korean hackers to compromise financial systems and other money-making cyber business systems remains a worry. North Korea needs financial resources and the authorities might overlook their cyber warriors' illicit operations. Because of the precise restraints made by international sanctions, North Korea's illicit operations in cyberspace will continue despite peace talks and denuclearization negotiations.

Along with updating domestic policy responses and countermeasures management, two additional efforts can be suggested. First, international sanctions may need to be lifted in accordance with the progress of North Korea's efforts in denuclearization. This should provide breathing room for the North Korean economy, which might alter the incentive calculations of the regime's cyber operations. That is, if Kim Jung Un considers compliance with international norms will bring more profits than illicit cyber operations, there remains no reason to continue cyber hacking for financial resources. Second, interested parties should put joint pressure on North Korea to not employ additional illicit cyber operations. For example, international communities should ask the candidate countries where North Korean hackers freely travel and launch cyber attacks using that countries' cyber infrastructure, to follow regulating measures. These countries include China, South Asian countries, and countries in the Middle East and Africa. China, especially, should take this seriously; cities such as Dandong, Shenyang, Beijing and Shanghai are frequently visited by North Korean hackers and presumably have hosted North Korean cyber operation base camps.

Conclusion

This article analyzes the recent cyber threats of North Korea and discussed its break with past performance. North Korea recently discarded saber-rattling cyber attacks against South Korea and adopted cyber activities mainly driven by financial objectives. These transformations are relevant to the radically changing strategic topology in the Korean Peninsula. Thus, a

new approach is needed for North Korea and its cyber threats. Considering this, South Korea and the international community may need a flexible strategy to tame North Korean cyber threats. For now, lifting some of the international sanctions and reinforcing self-regulations and responsibilities of interested states in cyberspace would be the corresponding way of action to North Korea's strategic change. Meanwhile, President Moon of South Korea ascertained it is not yet known how the results of North Korea's denuclearization will unfold, as he expected a number of turmoil and challenges in the process. In some potential scenarios, the denuclearization process may take longer than initially expected. Thus, South Korea and the international community should continue to monitor possible illicit behavior of North Korean hackers, since, as President Moon stated, it is not yet known how long the process of denuclearization may take. Therefore, a cautious and reserved approach toward North Korea's cyber threats should continue to be taken by both the domestic South Korean and international policy communities.

Bibliography

Boo, Hyeong-wook, "Issues of Cybersecurity and Policy Directions: Discussions for the Establishment of Defense Ministry's Cyber Policy," *Journal of National Defense Studies*, Vol. 56, No. 2, 2013, pp.97-122. (in Korean)

Boo, Hyeong-wook et al., "A Study on Future Directions of Defense Cyber Policy," *KIDA Report,* 2013. (in Korean)

Boo, Hyeong-wook, and Choi, Suon., "Crisis Pattern Change and Its Implication for National Crisis Management System," *Journal of Defense Policy Studies*, Vol. 30, No. 1, 2014, pp.123-152. (in Korean)

Boo, Hyeong-wook, "An Assessment of North Korean Cyber Threats," *The Journal of East Asian Affairs*, Vol. 31, No. 1, 2017, pp.97-117.

Chanlett-Avery, Emma et al., "North Korean Cyber Capabilities: In Brief," *Congressional Research Service Report*, August 3, 2017, https://fas.org/sgp/crs/row/R44912.pdf.

Cho, Kwang-hyung, "Malicious Code Penetration Aginst Network of KBS, North Korea's Deed," *New Daily,* March 20, 2013, http://www.newdaily.co.kr/site/data/html/2013/03/20/ 2013032000061.html.

Choe, Sang-Hun et al., "Focus Turns to North Korea Sleeper Cells as Possible Culprits in cyber attack," *The New York Times,* May 16, 2017, https://www.nytimes.com/2017/05/16/world/asia/north-korea-cyber-sleeper-cells-ransomware.html.

Comfort, L. K, "Rethinking Security: Organizational Fragility in Extreme Events," *Public Administration Review*, Vol. 62, No. 1, 2002, pp.98-107.

Han, Hee, "Cyber Threat by North Korea: Capability and Intention,", presented at the 6th RINSA-KAS Joint International Conference (2016).

Hwang, Il-do, "North Korea's 'Guam Enemy Shooting' Threat: Intention and Calculation," *Institute of Foreign Affairs and National Security FOCUS,* 2017. (in Korean)

Jang, Sung-young, "How Will 'Defense Reform 2.0 Change South Korea's Defense? A Closer Look at Moon Jae-in's Ambitious Defense Modernization Plan," *The Diplomat*, August 27, 2018, https://thediplomat.com/2018/08/how-will-defense-reform-2-0-change-south-koreas-defense/.

Kim, Min-ho, "An Assessment of North Korean Cyber War Threats," *KIDA Presentation*, 2016. (in Korean)

Kim, Min-seo, "More Than 7,000 Cyber Worriers in North Korea, Earning 1 Trillion Won Annually," *Segye Ilbo*, November 23, 2017, http://www.segye.com/newsView/20171123005037.

Kube, Courtney and Mitchell, Andrea, "North Korea is Still Producing Ballistic Missiles after Summit," *NBC NEWS*, August 1, 2018, https://www.nbcnews.com/news/ north-korea /north-korea-still-producing-ballistic-missiles-after-summit-n896331.

Lawrence, Dune, "North Korea's Bitcoin Play: Cut off from the hack world economy by sanctions, Pyongyang is looking for ways to get its hands on cryptocurrency," *Bloomberg Businessweek*, December 15, 2017, https://www.bloomberg.com/news/ articles/2017-12-14/north-korea-s-bitcoin-play.

Libicki, Martin, C., *Cyberdeterrence and Cyberwar* (Santa Monica, California: RAND, 2009).

Lim, Jong-In, et al., "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *The Quarterly Journal of Defense Policy Studies,* Vol. 29, No. 4, 2013, pp.10-45. (in Korean)

Lee, Seon-mok, "US reveals that, North Korea will continue to focus on cyber activities, to secure Funds for the WMD Development," *Chosen Ilbo,* September 10, 2018, http://news.chosun.com/site/data/html_dir/2018/09/10/2018091000625.html.

Lee, Jae-woon, "The Government's New Cybersecurity 'Center' is The National Security Office," *E- Daily,* May 21, 2018, http://www.edaily.co.kr/news/read? newsId=026600 8661921 1216&mediaCodeNo=257&OutLnkChk=Y.

Lee, Yong-joon et al., "The Countermeasure Strategy Based on Big Data against North Korean Cyber Attacks," *The Korean Journal of Defense Analysis*, Vol. 30, No. 3, 2018, pp.437-454.

Mahnken, G, Thomas, "Cyberwar and Cyber Warfare," in Lord M., Kristin and Sharp, Travis ed(s)., *America's Cyber Future: Security and Prosperity in the Information Age,* Vol. 2 (Washington, DC: Center for a New American Security, 2011).

Min, Sea, "Strengthening National Cybersecurity Significantly," *Boan News*, March 18, 2015, https://www.boannews.com/media/view.asp?idx=45697&kind=2.

"North Korea Cyber Activity," *Recorded Future Insikt Group*, June 14, 2017, https:// go.recordedfuture.com/hubfs/reports/north-korea-activity.pdf.

Rosenburg, Jay and Beek, Christiaan, "Examining Code Reuse Reveals Undiscovered Links Among North Korea's Malware Families," *McAfee*, August 9, 2018, https:// securingtomorrow.mcafee.com/mcafee-labs/examining-code-reuse-reveals-undiscover ed-links-among-north-koreas-malware-families/.

Sanger, David and Banner, Katie, "U.S. Accuses North Korea of Plot to Hurt Economy as Spy is Charged in Sony Hack," *The New York Times*, September 6, 2018, https:// www.nytimes.com/2018/09/06/us/politics/north-korea-sony--wannacryndictment.html.

Shields, Nathan, “Criminal Complaint (U.S. vs. Park, Jin Hyok),” *U.S. District Court for the Central District of California,* June 8, 2018, https://www.justice.gov/opa/press-release/file/1092091/download.

Son, Young-dong, “Stop Acting! The United States Gives a Red Card to the North Korean cyber attacks,” *Choong-Ang Daily*, September 14, 2018, https://news.joins.com/article/22970263.