Chapter 2
An Assessment of North Korean Cyber Threats

Hyeong-wook Boo

I. Introduction

North Korea is one of the hardest intelligence targets for a government. It is a chauvinistic country endorsing the Ju-che ideology. It is one of the poorest counties in the world. Its cyber infrastructure seems to be very rudimentary and one can hardly expect public Wi-Fi or cloud services in North Korea. When Eric Schmidt, CEO of Google returned from North Korea in 2013 after his short visit, he said there were only a few thousand computers connected to the internet in North Korea. Even from the perspective of cyber, North Korea is surely a hermit kingdom.

Meanwhile, we have witnessed that North Korea launched very sophisticated cyber attacks against South Korea and the United States. Starting from simple DDoS attacks on popular websites and e-mail hacking, their cyber offensive operations adopted advanced technologies called APT[1] (Advanced Persistent Threat). Recently, North Korean hackers tried to expand their playing fields from PC platforms to mobile platforms as in the recent attack that compromised smartphones of several influential politicians.

Witnessing North Korean cyber attacks and its infrastructure, people raised many questions. How can a country like North Korea pose such serious cyber threats?[2] Some skeptics argued that the computer security industry exaggerated North Korea's cyber capabilities and the magnitude of the threats for the promotion of their business. With these questions in mind, there is a growing need to assess North Korea's cyber capabilities and the reality of the threat correctly. However, it is a very hard task to assess North Korea's cyber capabilities and its intent. Even though we have analyzed North Korean

---

1 An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term.

2 Professor Libicki, a renowned cyber security expert, responded to the question in e-mail communications with me. His position is as follows: "North Korea is poor but North Koreans are not primitive (people starve because North Korea's leaders prefer to pursue many other goals that compete with making sure people are fed). It did develop atomic weapons, something primitive countries cannot do. Developing the cyberwar capability (of the sort that North Korea has) is not surprising for a country that can develop atomic weapons."

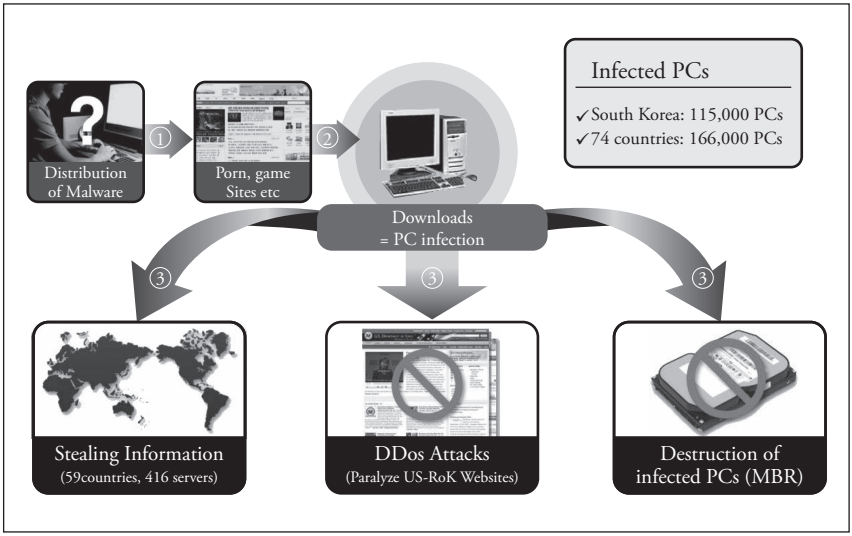
made malwares and human intelligence[3], we don't know much about what is happening in North Korea.

In this study, I tried to aggregate information about North Korea's cyber capabilities and assess them objectively. To do this, analyses of North Korean cyber attack cases, discussions of findings in the area of North Korean cyber threats, and responses against North Korea's cyber threats will be evaluated in the following sections.

II. North Korean Cyber Attack Cases

Even though cyber terrorism and cyber warfare became buzzwords these days, the social discourses on cyber security have a very short history in South Korea. Experts see that North Korean cyber attacks began around 2004; however, it was the 7.7 DDoS attack in 2009 that triggered the general public's concerns regarding the cyber threats posed by North Korea. Most of the cyber attacks before 7.7 DDoS were e-mail hacking incidents employing basic techniques.

Figure 1. 7.7 DDoS Cyber Attack



[3] Currently, there are almost 30,000 North Korean refugees in South Korea and some of them provide valuable information about North Korean cyber capabilities.

After the 7.7 DDoS attack, North Korea launched cyber attacks against South Korea more often, and the impacts of attacks have been getting worse. In this context, journalists like Baek (2015) of *Monthly Chosun* introduced a speculation that there seemed to have been a relationship between the increase of North Korean cyber attacks and the debut of heir-apparent, Kim, Jung-Un at that time. Despite some criticisms for the argument[4], it is evident that there has been a surge of North Korean cyber attacks in the Kim, Jung-Un era.

Several well-known incidents after the 7.7 DDoS incidents are as follows. On July 7, 2010, North Korea launched a DDoS attack on the RoK government and private-sector websites. They disseminated malwares through P2P sites, chat-rooms, web-hards, and free vaccine programs sites. The malwares infected PCs and made them into zombie PCs. North Korean hackers took control of the resources, thousands, if not millions, of zombie PCs around the world. When they decided to launch cyber attacks, those zombie PCs sent a huge amount of data packets to designated websites and inundated capacities of the website servers. Sometimes DDoS attacks caused severe damage to a society; however, this kind of cyber attack just caused paralysis of websites and other esthetic damages to websites such as defacement of websites. It didn't require advanced technologies even though North Korean technical sophistication of DDoS attacks got better and sometimes they erased the data of servers as they paralyzed websites.

In 2011, North Korean hackers demonstrated enhanced cyber attack capabilities. On March 4, North Korea launched DDoS attacks on 40 RoK public, government, military, and private websites including USFK. About a month later, North Korea caused the paralysis of the Nonghyup internet banking system. Servers of the bank were disrupted and data were erased. This incident happened on April 12, 2011. After a close evaluation of the attack, experts concluded that North Korean hackers seemed to have employed APT against the technician for the internet banking system's maintenance. It seemed that North Korean hackers spent a lot of time and energy to identify the maintenance technician and injected malwares into his PC. Without knowing this, the technician connected the PC to the Nonghyup internet banking system for routine check-ups and the malware was simultaneously injected into the system. And that was the beginning of

[4] Experts like M. Libicki argues that it's hard to say whether the increase in cyber-activity from North Korea has resulted from the new ruler's accession. They see that all the trend lines everywhere else are going up except that China's visible activity, particularly against corporations, seems to be going down. In this regard, the frequency of North Korea's cyber attacks seems to be a part of the recent trends. However, it seems that the frequency of North Korea's cyber attacks has been way over the general trends of cyber attack cases in other parts of the world.

the whole story.[5]

Other notorious cyber attacks happened in 2013. On March 20, 2013, MBR (Master Boot Record)[6] wiper attacks shut down 32,000 computers of banks and media agencies. Banks include Nonghyup, Shinhan Bank, and Jeju Bank. Media agencies include YTN, KBS, and MBC. This incident was named the 3.20 cyber terror of 2013. Five days after the 3.20 cyber terror, North Korean cyber warriors also attacked DailyNK, Free North Korea Radio, and NKnet. These are public media agencies run by defected North Korean intellectuals trying to disseminate the wrongfulness of the North Korean regime via those media agencies. Another cyber attack organized by North Korea happened on June 25, 2013. It was DDoS attacks on 16 government and media agency websites. North Korean hackers also targeted DNS servers of those websites.

In November 2014, North Korea got even more audacious and they launched an MBR wiper attack against Sony Pictures Entertainment. The Sony Pictures hacking incident drew extraordinary concerns and anger against the North Korean cyber threat. In December 2014, there were cyber attack attempts against the information system of the South Korean nuclear power plant corporation, Korea Hydro and Nuclear Power. They intended data theft, extortion, and MBR wiper attack. This incident was also considered a serious one because it seemed that North Korea was trying to be seen as capable of causing real and physical damages through cyber attacks.[7]

The year of 2015 was a relatively quiet period in terms of North Korea's cyber attacks even though there were so many 'physical' military provocations. Entering 2016, however, North Korean cyber threats became an issue again. According to Min-ho Kim of Jetco Technology, North Korea launched at least ten cyber attacks during the first half of 2016. North Korea increased cyber attacks after the fourth nuclear test. As of the end of June 2016, South Korea identified sixteen attack servers in Ryukyung-dong, Pyongyang. Analyses of 33 malwares which were allegedly used by North Korean hackers in those cyber attacks are underway.[8]

---

5 It took Nonghyup for a month to normalize banking services (http://www.itworld.co.kr/news/73444?page=0,1; retrieved Aug 25, 2016).

6 A master boot record (MBR) is a special type of boot sector at the very beginning of partitioned computer mass storage devices.

7 It also triggered widespread concerns regarding nuclear power plant safety in South Korea. In this regard, it caused psychological damages. (http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150317160750&type=det&re=; retrieved Aug 25, 2016)

8 Experts said that there are repeated command lines in malwares that North Korean hackers developed. Many North Korean made malwares are named 'Kimsuky series' because 'kimsuky' is repeatedly used in malwares' codes.

Reviewing North Korean cyber attack incidents, one can find several features that draw our attention. First, it became their usual attack patterns, compounding traditional security threats with non-traditional threats. It seems that elites of North Korea's hacking organizations got an order from the above to coordinate cyber attacks with other military provocations such as the fourth nuclear test. North Korea's intent is shattering the minds of South Koreans and, to attain this goal, hackers disseminated misinformation and propaganda, etc. Some e-mails were sent with malign contents of President Park. For example, North Korean hackers sent mass e-mails and criticized the current government's approaches to the North Korean nuclear issues. They tried to make those e-mails more reliable by sending them from stolen accounts of influential scholars or broadcasting companies (for example, MBC and SBS).

Second, North Korean cyber warriors expanded their domain of operations to the mobile area as in the incidents that North Korea hacked smartphones of several politicians and high level military personnel. They tried to intercept text messages, recorded telephone conversations, and obtained contacts information. The third aspect is that North Korea had intent to compromise the mass transportation management system which would end up with large scale chaos. Indeed, there were hacking attempts on Seoul Metro, a subway system of Seoul. It rendered an ominous sign to the general public of South Korea foreshadowing a transportation disaster triggered from cyber. Lastly, there was a hacking attempt on defense related corporations in 2016. They stole maintenance manuals of F-16, photos of South Korean drone parts, and other sensitive documents. Authorities estimated 42,600 documents had been stolen. It is a new phenomenon and it renders an impression of North Korean hackers being more of military oriented purposes.

III. North Korean Cyber Threats: Some Findings

Entering the 2010s, many South Korean security experts participated in the discussion of cyber warfare and cyber terrorism. Many experts looked at the issues from various perspectives and here are some of the important arguments. First, one of the most popular topics is analyzing the intent of North Korean cyber attacks. Experts see North Korean cyber attacks as its implementation of asymmetric strategy. In fact, cyber threats have become a synonym of asymmetric threats. It enables poor countries to have chances to harm a rich nation's ICT (information and communications technology) assets with low costs. If a nation is highly wired with advanced ICT networks as in the case of South Korea, attack on the target infrastructure of the nation can cause cascading confusion.

With the decades-long economic hardships, North Korea had to give up the arms

race with South Korea especially in the area of conventional weapons. Thus going nuclear was a bold attempt to offset its inferiorities, and developing sophisticated cyber weapons was the other option. We can name it North Korea's offset strategy[9] and cyber is an important part of it. With the employment of cyber means, North Korea can cause widespread chaos in the networked society as in the case of the Seoul Metro cyber attack. In the military sense, North Korean hackers will try to encroach military networks, such as sensors-shooters complex and integrated command-control systems of the US and South Korean military. Therefore, RoK-US combined forces may face difficulties conducting network-centric warfare if North Korea's cyber warriors are successful.

Second, North Korea has employed cyber attacks as a political means that can turn security situations of the Korean peninsula into a grey zone, a zone where threats are significant and evident, but there is almost no way to normalize the situation by using military measures. That is, North Korea tried to shatter the political terrains of the peninsula by adopting various means such as missile tests, nuclear tests, limited military attacks to remote islands or DMZ, and cyber terrors. Moreover, North Korea usually mixed different types of provocations, resulting in good tactical moves. This is why experts including myself have tried to find out the regularities of North Korean cyber attacks from the perspective of compound crisis, a situation mixed with different kinds of crises. A preliminary finding is that cyber terrors, if compounded with other provocations, can be used as good tools for generating greater tension and North Korea always takes advantage of them. (Boo and Choi 2014). Indeed, North Korea has used cyber threats as a means of enhancing the political impact of its military provocations and its propagandas. North Korea usually launched cyber attacks before or after major military provocations such as long-range missile tests and nuclear tests. Experts also see the utility of cyberspace in that North Korea can take advantage of cyber means in fulfilling its intent of dividing the South Korean society into two extreme opinions regarding how to deal with North Korea.

Another hot topic is the evaluation of the technological level of North Korean cyber threats. Researchers and writers have evaluated North Korean capabilities and tried to compare its capabilities with other countries. There were some findings. Even though some experts even estimate that North Korea's cyber warfare ability would be almost equal to that of CIA, North Korea's cyber attack capacity seems to be in

[9] An offset is some means of asymmetrically compensating for a disadvantage. Offset strategy is usually understood as game-changing strategy.

middle-level[10]. However, its defending capacity is very high since there is almost no way to penetrate the North Korean system because of its lack of internet connections. This ironic situation makes the North Korean cyber threat formidable.[11]

Table 1. Comparison of Cyber War Capabilities among Nations

Nations	Cyber Offense	Cyber Dependence	Cyber Defense	Total
U.S.	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

Source: Richard A. Clarke and Robert K. Knake, "*Cyber War: The Next Threat to National Security and What to Do About It*", ECC 2010 p. 149.

Table 2. Coleman's Comparison Results

Nations	Intent	Offensive Capabilities	Intelligence Rating	Total
China	4.2	3.8	4.0	4.0
U.S.	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India	4.0	3.5	3.5	3.7
Iran	4.1	3.4	3.4	3.6
North Korea	4.2	3.4	3.3	3.6
Japan	3.9	3.3	3.5	3.6
Israel	4.0	3.8	3.0	3.6
South Korea	3.5	3.0	3.2	3.2
Pakistan	3.9	2.7	2.6	3.1

Source: Coleman, K., The Weaponry and Strategies of Digital Conflict, in Armstead, E. L (eds.), *The Proceedings of the 5th International Conference on Information Warfare and Security*, (The Air Force Institute of Technology, Ohio; 2010). p. 498.

[10] When it comes to attack behaviors, the North Korean hackers are exceptionally aggressive. When we have a discussion regarding North Korean cyber attack capacities, professor Libicki said "While most other nations break into computer systems to steal information, the North Koreans also break into computer systems to break them."

[11] According to Professor M. Libicki of the United States Naval Academy, North Korea is more sophisticated than many other countries (e.g., Spain, Lebanon) in terms of cyber capabilities. He sees that North Korea is probably as sophisticated as many cybercrime organizations are (and such organizations specialize in going after soft targets). It is not that hard for a moderately competent hacking group to break into a system that is open to the outside world, and runs normal Windows machines.

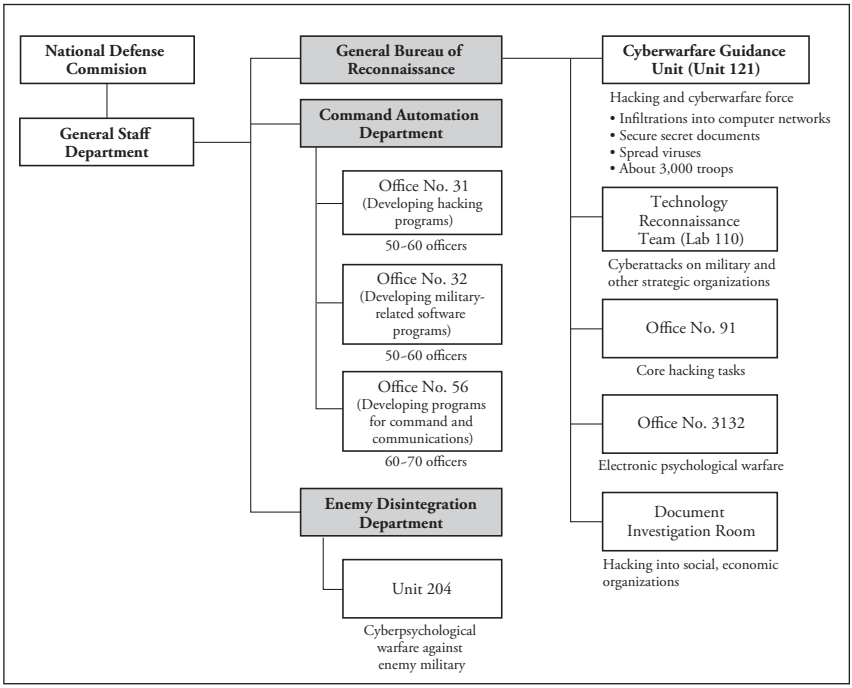
Even though there is not much information about North Korean organizations for cyber warfare or institutions for education, we came to know that the General Bureau of Reconnaissance (GBR) has deeply been related with the cyber attacks against South Korea. Kim, Heung-kwang, a defected North Korean intellectual and chair of NKnet, provided information about core North Korean cyber units; he argued that Unit 121 was established in September 1998 by Kim, Jung-il and launched more than 30,000 cyber attacks against South Korea ever since. Many news sources reported that Kim Jung-il himself stressed to enhance the ability of waging cyber war. For example, he said, "the 20th century's war was a war of oil and bullets, but the 21st century's war is an intelligence war." Experts think that North Korea's notion of intelligence war includes cyber war. Reflecting this, the Korean People's Army tried to enhance cyber warfare capability under the concept of "electronic intelligence warfare" which encompasses disrupting networks, destructing infrastructure and paralyzing the enemy's military command-and-control systems.

As for ways of launching cyber attacks, Kim, Heung-kwang of NKnet designated several secrete operation sites for cyber attack in China, such as Chilsung-gak, a North Korean restaurant in Shenyang. Sometimes, according to Kim, Heung-kwang, North Korean hackers launched cyber attacks in PC cafes in Shenyang, Dan-dong, Beijing and other Chinese cities. Sometimes they sneakily put jumpers on the backbone of Chinese telecommunication corporations, such as China Unicom, and launched cyber attacks using the compromised communication lines. Some cyber terrorists of Unit 121 even traveled to Japan, Southeast Asia, Africa and European countries for state-sponsored cyber attack activities.

In order to raise future hackers, the North Korean government has established a set of institutions that are solely for cyber warriors. North Korea has enhanced its cyber attack capabilities by training professional hackers since the mid-1980s. News sources found that North Korea established Mirim College, Moranbong College and other higher education institutions for the purpose of educating cyber warriors. These schools are closely related to the People's Armed Forces of North Korea and allegedly educate hundreds of professional hackers every year. They are estimated to be top class hackers and appointed as military officials to hacking units after graduation. As for North Korea's cyber warfare organizations, experts' estimations and defected North Koreans' witnesses were used in building the organizational diagram seen

in Figure 2.[12] The most important thing to shed light on regarding North Korea's cyber warfare organizational diagram is that hacking units are attached under GBR[13] which is controlled by the National Defense Commission. As mentioned earlier, South Korea's Prosecution Service and National Intelligence Service have designated Unit 121 of GBR as a major suspect of numerous cyber attacks. Meanwhile, the estimated total number of North Korean cyber warriors reached 6,800 and, according to Kim, Heung-kwang and other news sources, it would reach 10,000 sooner or later.

Figure 2. North Korea's Cyber Warfare Organizations



Source: Boo, Hyeong-wook *et. al*. 2013. *A Study on Future Direction of Defense Cyber Policy*. KIDA report (*in Korean*). p. 94.

[12] Even though I collect information as much as I can, there should be some inaccuracy because of limited information. However, Figure 2 very closely reflects the reality of North Korea's cyber warfare organization.

[13] GBR is one of North Korea's intelligence agencies and is responsible for secrete operations against South Korea.

Meanwhile, it is a rather recent finding that shows North Korea is quite successful in getting profits by the use of its cyber capabilities. According to You, Dong-ryul of the Korea Institute of Liberal Democracy (KILD), North Korea earns 1 billion dollars per year through cyber activities.[14] North Korean hackers established illegal cyber gambling sites, engaged in online games selling rare game items to players, and dismantled the online banking system as in the case of Bangladesh, etc. According to Dr. You, North Korea acquires a huge amount of foreign currencies from these kinds of activities.

IV. Responses against North Korean Cyber Threats and New Threat Assessments

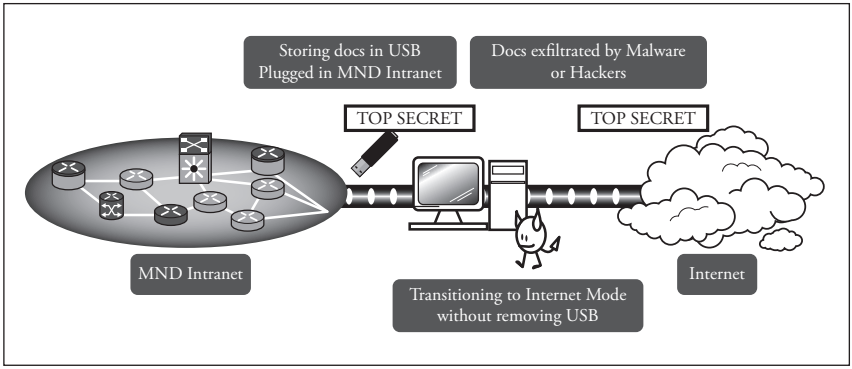
South Korea has been under North Korean cyber attacks for more than a decade as it has progressed to be one of the world's IT powers. Even though the society has strengthened cyber security, the growing network dependency of South Korea inevitably exposed some vulnerability as in the cases of free and democratic societies of the world. Networks are compromised because of their own vulnerabilities and the enemy's enhanced offensive cyber capacities. These two factors are intertwined and have demonstrated catastrophic effects in South Korea. With North Korean cyber attacks, sometimes the damages were confined to the freezing of certain websites but there were many incidents that caused substantial societal costs. The latter cases include paralysis of internet banking, exfiltration of OPLAN 5027 from the military, theft of sensitive documents from defense related industries, and the hacking of influential politicians' smartphones. Among these, OPLAN 5027 exfiltration, an incident of exfiltration of documents containing major contents of OPLAN, was the most surprising incident. The following diagram shows how the data was extruded from the military's intranet.[15]

---

[14] One billion dollars is a lot of money to North Korea considering their official trade volume to the outside world is less than 10 billion dollars per year. The amount of money suggested by Dr. You is somewhat surprising. However, experts including myself raised questions about the amount of money Dr. You suggested, even though they understand the fact that North Korea is getting some amount of money from those activities.

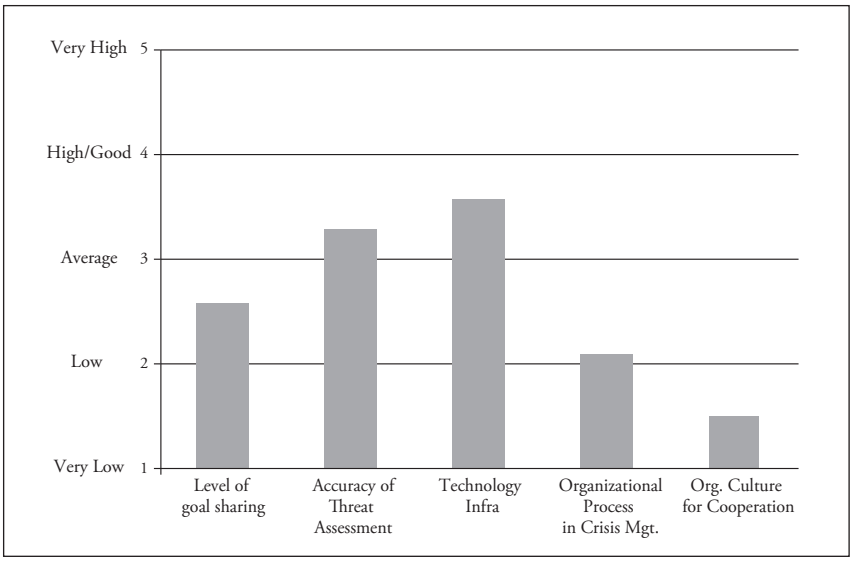
[15] In a sense, using the title of "OPLAN 5027 exfiltration" may be misleading because it is not exfiltration of whole OPLAN 5027 documents but exfiltration of a summary of OPLAN which was a Powerpoint file used for a briefing. It happened from using a USB stick in a Dual PC. Dual PC is a PC that has two hard drives with an individual operating system respectively used for MND (Ministry of National Defense)'s intranet and internet. Thus, one needed to reboot a computer for MND intranet connections from the internet connection and vice versa. In fact, Dual PC is two PCs sharing every component of the computers except the hard drive. OPLAN 5027 exfiltration happened when an officer rebooted the system connected with the MND intranet for the use of the internet connection without removing the USB stick from the system. Again, the USB stick stored the summary of OPLAN 5027. After the incident, MND banned the use of Dual PCs (http://www.hani.co.kr/arti/politics/defense/394238.html retrieved Aug. 25. 2016).

Figure 3. OPLAN 5027 Exfiltration



Faced with growing cyber threats, South Korea exerted multi-faceted efforts; for example, the government established Cyber Commands in 2010, sponsored cyber security related departments in universities and educated young students, and announced the Cyber Security Master Plan. However, experts argued that the government and military should do more and proposed multi-faceted approaches in responding to North Korean cyber attacks. In this context, practitioners and researchers have showed their urgency and tried to make a momentum for the establishment of a solid cyber defense posture in South Korea. Despite the efforts of government and opinion leaders, systems are still fragmented and very complex. Also, political support for enhancing anti-terrorism posture has been inconsistent, and international cooperation efforts are just emerging. Moreover, the general public is prone to value privacy rather than to impose limitations and regulations over cyberspace. Meanwhile, North Korea always tries to achieve its goal out of these conundrums. Because of various reasons, the current status of the South Korean response system against North Korean cyber threats has much vulnerability. Boo *et. al.* (2013) tried to vividly demonstrate the current status of the anti-terrorism system and showed experts Delphi results. As seen in Figure 4, technology infrastructure and the accuracy of threat assessment scored well while other factors were assessed to be below average.

Figure 4. Expert Delphi Results in Evaluating South Korea's Cyber Preparedness



Source: Boo, Hyeong-wook *et. al.*. 2013. *A Study on Future Direction of Defense Cyber Policy*. KIDA report (*in Korean*). p. 19.

Despite the relative high scores in technology infrastructure and accuracy of threat assessment, the scores were low in goal sharing, organizational process and culture foreshadow difficulties in enhancing resilience of cyber preparedness in South Korea. Meanwhile, there are some experts who argued that even threat assessment went wrong. They argue that South Korea needs to re-assess cyber threats posed by North Korea. This is somewhat surprising because people generally accepted that the South Korean government's threat assessment is quite accurate. However, scholars like Han, Hee (2016) argued that MND of South Korea needs to pay attention to the invisible parts of North Korean cyber capabilities. He argues that there is a tendency within MND to see 6,800 hackers as the entirety of the North Korean cyber threat. He rejected this view, stating that MND needs to focus on the potentials behind the wall. Since North Korean hackers gained control over more than thousands, if not millions, of zombie PCs, their capacity would not be reduced to the number of hackers in North Korea. With several clicks, they can launch concerted cyber attacks from all over the world. From this perspective, he argued that we need to have a refreshed perspective regarding North Korean cyber forces; it would be the mixtures of 6,800 cyber warriors, zombie PCs, and malwares that

are floating in the web.

According to Dr. Han, it is important to recognize the fact that North Korea has deceived the cyber security policy community in South Korea. North Korea has tried to be seen as having elementary cyber technology. Experts argue that North Korea launched cyber attacks with rudimentary offensive techniques because they want to test the capacity of the South Korean society and military in responding to their cyber attacks. Since North Korea's intent is deception, it can be argued the worst scenario has not come yet. It is true considering tactics in waging cyber war; when a cyber weapon or a malware is released, the item has no value as a cyber weapon or a malware. It is because responders will analyze it and find ways of neutralizing it. Moreover, responders will produce antidotes and provide them as countermeasures. Therefore, it would be a natural conclusion that North Korea's most valuable and potent cyber weapons were not used yet in the real world.

V. Conclusion

General Brooks who was recently inaugurated the USFK commander said that North Korea has one of the world's most well-organized and able cyber forces, if not the world's best.[16] With this capacity, North Korea has launched serious cyber attacks against South Korea and the outside world. During the Kim, Jung-Un era, there has been a surge of cyber attack incidents. Sophisticated technologies adopted for attacks and the objective of cyber operations seemed to move from random exfiltration of information to planned and well-orchestrated attacks on critical infrastructure of South Korea. Also, North Korean cyber warrior sign-ups on many SNS sites try to manipulate public opinion and fan the flame of colliding perspectives within the South Korean society, which can be seen as an act of waging psychological warfare. Recently, North Korea uses cyber capacity as a means of earning foreign currency and they did a good job.

For almost 60 years, an arms race between North Korea and South Korea had taken place in the area of conventional weapon systems; the military focused on acquiring tanks, artillery, fighter jets, destroyers, submarines, etc. Entering the 2010s, however, things changed drastically. North Korea developed nuclear weapons and other WMDs and this changed the military balance in the Korean peninsula. The importance of modernizing conventional weapon systems became less crucial in the face of WMDs.

[16] General Brooks commented like that at the Senate hearings for his nomination as Combined Forces Commander in April 2016 (http://news.chosun.com/site/data/html_dir/2016/04/20/2016042002453.html ; retrieved on Aug. 25. 2016).

North Korea's another strategic move has been made in the area of cyber. Developing WMDs and cyber weapons is considered as instituting asymmetric strategy.

In this article, North Korea's cyber attack incidents were analyzed, and findings from previous studies regarding North Korean cyber capabilities were aggregated. Also, South Korea's responses and lessons learned from the response efforts were evaluated. Having discussed these issues, one can conclude that the North Korean cyber threat should be regarded seriously. Cyber weapons are cheap and pose a serious threat to network-dependent South Korea. The worst scenario has not happened yet. Thus, researchers and practitioners should think the unthinkables and provide analyses to the government and the military.

Reference

Baek, Seung-koo. 2015. Evolving North Korean Cyber Terrorism. *Monthly Chosun*. (https://monthly.chosun.com/client/news/viw.asp?nNewsNumb=201509100013 accessed 2016. 7. 23)

Boo, Hyeong-wook and Choi, Suon. 2014. Crisis Pattern Change and Its Implication for National Crisis Management System. *Journal of Defense Policy Studies*. Vol. 30. No. 1.

Boo, Hyeong-wook and Lee, Kang-kyu. 2012. Cyber War and Policy Suggestions for South Korean Planners. *International Journal of Korean Unification Studies*, Vol. 21, No. 2.

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

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

Clarke, Richard A. and Robert K. Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. ECC 2010

Coleman, K. 2010. The Weaponry and Strategies of Digital Conflict, in Armstead, E. L (eds.). *The Proceedings of the 5th International Conference on Information Warfare and Security*, (The Air Force Institute of Technology, Ohio; 2010)

Comfort, L. K. 2002. Rethinking Security: Organizational Fragility in Extreme Events. *Public Administration Review.* pp. 98-107.

Deibert, Ronald. "Militarizing Cyberspace", *Technological Review*, (Boston, MA: MIT, 2010), (http://www.technologyreview.com/notebook/419458/militarizing-cyberspace;

retrieved Aug 25, 2016)

Dennis C. Blair. 2010. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence.

Han, Hee. 2016. *Cyber threat by North Korea: capability and intention*. Paper presented at The 6th RINSA-KAS Joint International Conference.

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

Mahnken, Thomas G. 2011. Cyberwar and Cyber Warfare in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age Vol. II* (Washington, DC: Center for a New American Security). pp. 55-64.

Manjikian, Mary McEvoy. 2010. From Global Village to Virtual battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly.* Vol 54. Issue 2. pp. 381-401.

Nye, Joseph S. Jr. 2011. Power and National Security in Cyberspace. in Kristin M. Lord and Travis Sharp (eds.) *America's Cyber Future: Security and Prosperity in the Information Age Vol.II.* (Washington, DC: Center for a New American Security). pp. 5-23.

Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke. 2011. On Cyber Warfare. *A Chatham House Report*

Singer, Peter W. and Noah Schactman. 2011. *The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive*. Brookings Institute. (http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman; retrieved Aug 25, 2016)

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