Before Dark Seoul Becomes Destroy Seoul

Ye Ra Kim

February 14, 2014

Draft working paper in the Cyber Law and Policy Program. The views expressed are those of the author.

Contents

INTRODUCTION

Guarding national security in cyberspace has become a core interest for many nations connected to the Internet. Indeed, the growing dependence on ever evolving information technology and the continuous occurrence of cyber-attacks against nations demonstrate the need for solid security strategy in cyberspace. South Korea is not an exception in this regard. Notwithstanding cybercrimes of varying severity, South Korea has been the target of major cyber-attacks in recent years. The directed denial of service (DDoS) attacks of July 7, 2009 and March 4, 2011 temporarily took down public websites including those of the Presidential Office and the National Assembly, and were followed by another attack against Nonghyup Bank, a major bank of South Korea, on April 20, 2011 which shocked the nation by paralyzing financial transactions over the bank's networks. Between these highly publicized attacks, South Korea suffered a slew of smaller scale attacks including GPS jamming and spear-phishing attempts targeting particular social groups.[1]

Indeed, cyber-attacks against South Korea are intensifying. In 2013 alone, the nation has already been the victim of two significant cyber-attacks occurring on March 20 and June 25. In particular, the severity of the March 20 attack which simultaneously targeted major banks and broadcasters in the country, spread panic through the nation. The malware used in the attack was later nicknamed "DarkSeoul" because of the repetitive use of the term in the malware programming source.[2] DarkSeoul's simultaneous attack implies that the action was the work of the same culprit, prepared over a long period of time. Inaction or any response falling short of

[1] These include a class of graduate students from the National Military School and the Graduate School of Information Security, Korea University.

[2] Beom-jin Lee. "Warning for a mutant DarkSeoul virus" *The Weekly Chosun*. 1 April 2013. <http://weekly.chosun.com/client/news/viw.asp?nNewsNumb=002250100007&ctcd=C04>

appropriate countermeasures from South Korea will undoubtedly bring about the advent of "DestroySeoul," a future cyber-attack that will be more destructive than DarkSeoul. Thus, South Korea should place a special emphasis on efforts to prevent and combat attacks in cyberspace.

Throughout the series of past cyber-attacks, the South Korean government has remained consistent on pointing the accusatory finger at North Korea. Technically, the two Koreas have remained in a state of war since the 1953 Korean War Armistice Agreement which ended hostilities in the Korean War. Since then, inter-Korean relations have gone through notable changes ranging from the Cold War era confrontation, and the reconciliatory moves brought about by the Sunshine Policy, to the limited scale military collisions of the North's surprise attacks against the South's naval warship, Cheon-an and the artillery attack against the civilian inhabited island of Yeonpyeong in 2010. If the attacks did indeed come from the North, the recent incidents in cyberspace will illustrate the changing nature of the conflict on the Korean Peninsula, reflecting the need for a new concept of national security in which cyberforce plays a critical role.

Accurate assessment of the techniques and strategic calculations of the North shown in the past attacks will help South Korea prepare proper countermeasures. Among the series of cyber-attacks from the North, the March 20 attack will be the focus of this analysis, not only because it is one of the most recent such attacks, but also because it reveals much about the pattern of North Korea's aggressive activities in cyberspace. Overall, the analysis serves two purposes: First, to provide concrete and factual explanation as to the nature, intent and technical characteristics of the March 20 attack. Second, to gauge possible attacks in the future and propose recommendations to South Korean policymakers. As James Lewis has argued, conflicts in

cyberspace, despite its groundbreaking nature, have not yet set new rules for strategic calculations different from the classical understanding of state behaviors in international relations. [3]

NORTH KOREA'S EVOLVING CYBER CAPABILITIES

Shortly after 2:00 pm on March 20, 2013 in South Korea, the computer networks of Nonghyup Bank and Nonghyup Life Insurance suddenly crashed along with those of three major media networks, KBS, MBC and YTN. About an hour later, Shinhan Bank and Jeju Bank reported similar problems on their networks. The media networks' websites were taken offline while bank clients were prevented from accessing online and mobile banking applications as well as the ATM services. In total, the attack resulted in the damage of 48,700 computers, servers and ATMs affiliated with the targeted organizations.[4]

South Korean institutions were not the only victims in the attack. On the same day, the Washington-based Committee for Human Rights in North Korea also reported its website had come under cyber-attack and that documents had been stolen. Interestingly, the attacks occurred a day before the voting on the resolution for the establishment of an independent investigation of North Korean human rights abuses took place at the United Nations Human Rights Council.[5]

---

[3] James A. Lewis "Conflict and Negotiation in Cyberspace" *Center for Strategic and International Studies*. February 2013. < http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf >

[4] Eun-jae Lee. "3.20 cyber-attack and its malwares (PPT)" *Korea Internet and Security Agency (KISA)*. June 27, 2013. <http://www.oas.org/cyber/events/KISA.pdf >

[5] Sang-hun Choe. "Computer Networks in South Korea Are Paralyzed in Cyber-attacks" *The New York Times*. March 20 2013. < http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=0 >

TECHNICAL CHARACTERISTICS OF THE MARCH 20 ATTACK

The nickname "DarkSeoul" refers to the specific type of malware used in the March 20 attack. "KillMBR-FBIA and Dropper-FDH" and "Mal/EncPk-ACE" are the technical names given to this malware by the computer security software companies, McAfee and Sophos respectively. Initially discovered in 2012, the malware commonly disguises itself as an antivirus program and penetrates into the operating system of affected computers.[6] The malware used in the March 20 attack had the same data structure as DarkSeoul, but the exact commands executed were slightly different.[7] Destruction of hard disk drives and remote controlling of compromised devices were the two main functions of the malware, and the build path for both functions was identically "Make Troy" known to have been in development since June 2012.[8] Some remarkable technical characteristics displayed in the attack are as in the following.

Shift from DDoS to APT

In the past, a number of South Korean institutions were the victims of distributed denial of service attacks, commonly known as DDoS, which flood targeted websites with overloaded traffic that eventually make them inaccessible. Two major DDoS attacks occurred on July 7, 2009 and March 4, 2011 against South Korean government institutions. These types of attacks cause annoyance and inconvenience at worst, but does not leave any lasting damage to the victim once the massive net traffic has been cleared.

---

6 *The Weekly Chosun*. 1 April 2013.

7 Guilherme Venere. "South Korean Banks, Media Companies Targeted by Destructive Malware" *McAfee*. Mar 20 2013. <http://blogs.mcafee.com/mcafee-labs/south-korean-banks-media-companies-targeted-by-destructive-malware >

8 *KISA*. June 27, 2013.

In contrast to the mere irritation caused by DDoS attacks, attacks classified as the advanced persistent threat or simply APT, often damage the targeted system to a level beyond a simple denial of access. APT attacks are elaborated over a long period of time executing various activities such as information collecting, malware installation and disruption of operations on the targeted system.[9] It requires more effort and patience from the hacker than a DDoS attack because the process usually involves a chain of complicated operations ranging from social engineering to initially break into the network, remaining undetected over a long period of time while mapping the network's defense system for another attack, and to accessing vulnerable parts of the system to steal data and disrupt the operations.

As the malware continuously sends back the data it has gathered from inside, the hacker retains an unauthorized access to secret information from the target as long as the malware remains undetected.[10] Nevertheless, the March 20 attack in 2013 did not mark the first known APT attack against South Korea. In April 2011, an APT attack had already wiped out files on Nonghyup Bank's computer networks. The increasing shift from DDoS to APT suggests a grim reality for future cyber-attacks that will be harder to detect, for which the consequences will be more destructive and the recovery markedly more laborious.

Destruction of Master Boot Records (MBR)

Another significant technical characteristic of the March 20 attack can be found in the massive destruction of master boot records or MBRs. A MBR plays a critical role in booting a computer to start an operating system. It is the information in the first sector of any hard disk that identifies how and where

[9] Symantec "Advanced Persistent Threats: How They Work" 1995 - 2013 *Symantec Corporation* < http://www.symantec.com/theme.jsp?themeid=apt-infographic-1 >
[10] *Ibid.*

an operating system is located so it can be loaded into the computer's main storage.[11] Therefore, its destruction means disabling the entire computer system. In the past DDoS attacks against South Korea, hackers destroyed MBRs of the zombie computers at the final stage of the attack in order to delete the traces of routing.

When Nonghyup Bank came under cyber-attack in April 2011, however, hackers deliberately ordered MBR destruction as the means to cause direct damage to the bank's networks. In the March 20 attack in 2013, hackers further maximized the impacts of MBR destruction by differentiating the destruction methods according to the specific operating systems used in each targeted institution's computers.[12]

MBR destruction in the 2011 and 2013 incidents suggests a strong linkage between the two, because such attack would not have occurred had the hackers merely sought financial gain or the spread of a political message.[13] In relation to this point, McAfee has stated that the only goal of the hackers was making the targeted computers unusable noting that the malware did not make any other changes in the system such as dropping files or changing registry keys.[14]

Malware targeting MBR is not only difficult to detect, but also the restoration is almost impossible.[15] MBR infection may go unnoticed until hackers order visible actions analogous to self-destruction as in the cyber-

---

[11] Margaret Rouse. "Definition: Master Boot Record (MBR)." *Search Cio-Midmarket*. April 2005. <http://searchcio-midmarket.techtarget.com/definition/Master-Boot-Record >

[12] Seon-mi Jeong. "Damage caused by 3.20 cyberterror, 40 times more serious than 2011 attack" *Chosun Biz*. March 1, 2013. <
http://biz.chosun.com/site/data/html_dir/2013/03/21/2013032102342.html >

[13] Yong-seok Kim, Ho-jae Jeong, Yeong-il Son. "Destruction of hard disks suggests link to 2011 attack" *Dong-A Ilbo*. March 22 2013.
<http://news.donga.com/3/all/20130322/53885761/1 >

[14] *McAfee*. Mar 20 2013.

[15] Hyunmok Lee. "[Threat Analysis] Fearful bootkit affects MBR" *AhnLab*. June 3, 2011.
<http://m.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=17907 >

attacks against South Korea. Programming this type of malware requires advanced knowledge of the complicated MBR structure and patient labor over a long period of time for a successful execution. This aspect leads one to believe that the March 20 attack was the work of an organized hacker group, specifically desiring to cause damage to the nation of South Korea as opposed to individuals.[16]

Malware Penetration Through a Patch Program

According to an analysis published by Symantec, an American computer security software company, in the wake of the March 20 attack, the suspected malware was identified as Trojan Horse/Trojan.Jokra.[17] Once inside the targeted system, Trojan.Jokra took following actions in sequence: create a file referencing itself with "JO840112-CRAS8468-11150923-PCI8273V"[18]; map the object; end the antivirus processes provided by two local security companies, AhnLab Policy Agent's "pasvc.exe" and Hauri ViRobot ISMS' "clisvc.exe"; enumerate all drives; and finally overwrite the MBRs with one of these strings: "PRINCPES", "PR!NCPES" or "HASTATI." At the end of the process, all contents in the affected hard disks were wiped out. Finally, the malware forced the computers to restart by executing "shutdown -r -t 0", the

[16] Tae-hyeong Kim. "Cyberterror, similar to previous North Korean attacks" *BoanNews*. Mar 20 2013. <http://www.boannews.com/media/view.asp?idx=35307 >

[17] Symantec. "South Korean Banks and Broadcasting Organizations Suffer Major Damage from Cyber-attack" *Symantec Official Blog Security Response*. Created on Mar 20 2013 and undated on June 26, 2013. <http://www.symantec.com/connect/blogs/south-korean-banks-and-broadcasting-organizations-suffer-major-damage-cyberattack >

[18] The hacker differentiated malware identifiers for the execution of the commands "destroying hard disk drives" and "remote control." JO840112-CRAS8468-11150923-PCI8273V mentioned here was the destroying hard disk drives malware identifier whereas the remote control malware identifier was later found to be "JO840112-TONG8468-KSI82076-PCI8273T."

action that rendered the computers unusable as the MBRs and the contents in the drives had already been corrupted.

Before executing the actions, the malware must have found an entry point that let it into the matrix of massive inner corporate networks. It was later found that compromised Patch Management System (PMS) servers served as the malware installation vector. The constant automating patching operation of PMS on public or corporate networks is intended to ease security administrators' burden associated with security optimization. [19] Once penetrated into the system through PMS, the malware quickly spreads to the entire network when PMS sent out next patching updates.

The sophisticated nature of the malware and the massive disk wiping on a simultaneous basis both hint the existence of a same entity behind the scene. An accurate identification of the hackers will help determine their ultimate objectives and conjecture likely attacks in the future.

NORTH KOREA GOING CYBER OVER DECADES

North Korea turned its attention to cyberwarfare in the mid-1980s when economic difficulties began in earnest, much in contrast with the increasing prosperity that its Southern neighbor was going through. The dire situation prevented the North from revamping its conventional arms and further forced it to reduce military intelligence resources and networks against the South. Undergoing such a difficult period, cost-effective cyberwarfare provided an attractive option to North Korea in its effort to narrow the growing military and economic gaps with South Korea.[20]

---

[19] Jude Chao. "Patch Management System Best Practices" *Enterprise Networking Planet*. June 6, 2013.
<http://www.enterprisenetworkingplanet.com/netsecur/patch-management-system-best-practices.html >

[20] Cheol Baek, "The Truths about North Korea's Cyberwarfare Capabilities", *Kyeonghyang Shinmun*, April 13, 2013 <http://news.zum.com/articles/6409296?cm=popular>

The pace accelerated as the North witnessed the strategic use of advanced information systems by U.S. forces during the Gulf War.[21] After a period of gradual development, North Korea's cyberforce experienced significant growth when the regime created the Reconnaissance General Bureau in 2009. Under the Bureau's supervision, a division known as Unit 121 specializes in penetrating into foreign servers to steal data and install malware.[22]

Several other specialized departments also work systematically to enhance the nation's offensive cyber capabilities. These include the Central Party's Investigations Department and Enemy Secret Department Cyber Psychological Warfare Unit, each responsible for stealing secret information from foreign governments' networks and spreading rumors favorable to the North Korean regime respectively.[23]

In fact, contrary to what many outsiders would imagine, North Korea is not completely disconnected from the Internet. North Korea owns a network connected to the World Wide Web, but that is mainly used to spread pro-regime propaganda through its more than 440 newspapers, websites, social media accounts and other outlets.[24] In the era when the North still lacked its own Internet provider, only a few members from the highly privileged class were allowed to access the Internet via Chinese networks.

---

[21] Tae-il Jeong. "Surprising capabilities of North Korean cyber warriors" *Herald Kyeongjae*. April 10, 2013. < http://m.heraldbiz.com/view.php?ud=20130410000705&ntn=0 >

[22] Ibid.

[23] Seok-ho Ahn. "Cyberspace, the 5th battlefield" *Segye Ilbo*. September 5, 2011. <http://www.segye.com/content/html/2011/07/06/20110706003962.html >

[24] Hyon-hee Shin,"Seoul Faces Growing Cyber Warfare Challenges" *Korea Herald*, March 21, 2013, <http://m.koreaherald.com/view.php?ud=20130321000980&ntn=0>

North Korea has gradually expanded its presence on the web. In 2009, it established a joint venture with Thailand's Loxley Pacific Company [25] to introduce a network service in North Korea through an Internet provider named "Star Joint Venture." The company reportedly administers the North's "kp" domain.[26] As of December 14, 2009, the company has registered 1,024 IP addresses from 175.45.176.0 to 175.45.179.255 to the Asia Pacific Network Information Center (APNIC).[27] A number of official North Korean websites including the Korean Central News Agency, Rodong Shinmun and the national portal Nae-nara, use IP addresses registered at this company.

At the same time, some North Korean websites still use IP addresses based in Shenyang, China, which include the official propaganda website "Uri-minzok-kkiri". [28] Furthermore, intranets such as Gwang-myeong-mang are available to North Korea's privileged elite, providing only extremely limited information approved by the state.[29] Some estimate the number of the official North Korean cyber army, counting only those considered as "strategically trained elite unit" under the direct control of leader Kim Jong-un, to be at least 3,000.[30] When operating abroad, notably in China, North Korean state hackers

---

[25] Mathew J. Schwartz. "How South Korea Traced Hacker To Pyongyang", *Information Week*, April 11, 2013. <http://www.informationweek.com/security/attacks/how-south-korea-traced-hacker-to-pyongya/240152702>

[26] *Ibid.*

[27] "Attackers' IP Based in Ryugyong-Dong" *E-Today*, April 11, 2013 <http://money.joinsmsn.com/news/article/article.asp?total_id=11197682&ctg=1100>

[28] "3.20 Cyberterror IP address traced back to Pyongyang's Ryugyong-Dong " *Donga Ilbo*, April 11, 2013. <http://news.donga.com/List/PoliticsNK/3/000301/20130411/54354257/1>

[29] *Korea Herald*, Mar. 21 2013.

[30] Jeong-gyu Lee. "Realities of North Korean Cyber Troops" *Economy Segye*. August 30, 2011. <http://economysegye.segye.com/articles/View.html?aid=20110826001828&cid=711308000 0000 >

usually disguise themselves as software developers and animation producers.[31]

Broadly speaking, three main components form the North Korean cyberforce: manpower, equipment and system. The manpower consists of state hackers who have mastered network related theories and are able to deliver sophisticated cyber-attacks. As to the equipment, North Korea imports high tech computers, mainframes and other network facilities from countries including China in order to provide an ideal training and operational environment for the state hackers. Further, the system refers to an organized set of command, control and monitoring mechanisms designed for North Korean state hackers' systematic execution of an order. Once an order is delivered under the system, various hacker units move in a shipshape manner over a period of time to develop attacking malware, exploit the target's security vulnerabilities, hack the administrator's account, set an attack plan based on the reconnaissance and finally launch an attack from a third country such as China.[32]

Because state hackers are easily exposed to the affluence of outside world through their activities on the web, the North Korean regime allegedly offers a competitive rewards package in order to ensure that the hackers remain loyal to the regime.[33] Although the extent of North Korea's cyber capabilities are yet to be known, an official from South Korean intelligence service has stated that North Korean hackers have shown superior skills in hacking and

---

[31] Rak-in Jeong, "North Korean Hackers' Dangerous Deals", *Sisa Press*, August 24, 2011. <http://m.sisapress.com/articleView.html?idxno=55919>

[32] Heung-kwang Kim. "North Korean Cyberterror and our response" *NK Vision*. October 10, 2011. <http://www.nkvision.com/read.php?quarterId=NKV7&ca_item=4&num=165 >

[33] Ho-yeol Choi, "North Korea's Full Scale War in Cyberspace Could Devastate South Korea", *Donga Ilbo*, April 21, 2013, <http://m.donga.com/Politics/BestClick/3/all/20130421/54559246/1>

programming whereas they seem slow with absorbing fast developing new information technologies.[34]

NORTH KOREAN LINKAGE IN THE MARCH 20 ATTACK

Hackers usually showcase their skills by intentionally leaving clues to their identity. The culprits of the March 20 attack, however, were extremely careful not to leave anything behind that might help to uncover their identity. Investigation later revealed that the March 20 attack had required over eight months of preparation. Individual hackers are unlikely to organize themselves and endure time-consuming and labor-intensive tasks only to leave their attack anonymous. Despite the lack of clues, comparing the March 20 attack with the intent and technical similarities discovered in the past attacks can provide a useful piece of evidence. After an extensive investigation, taking both aspects into account, North Korea again appears to be the culprit behind the March 20 attack.

Symantec Analysis: Connection Between the 2011 and 2013 Attacks

If the culprits behind the series of cyber-attacks against South Korea turn out to be same, it will then imply the existence of a politically motivated group, likely another nation state that has a strategic interest in damaging South Korean infrastructures and intimidating the public. Following the March 20 attack, Symantec published on its blog a technical analysis indicating possible connections between the 2011 and 2013 attacks. Malware named "Trojan.Koredos" and "Trojan.Jokra" were used in the March 4 attack in 2011 and the March 20 attack in 2013 respectively. [35]

---

[34] *Sisa Press*, Aug 24 2011.

[35] "Are the 2011 and 2013 South Korean Cyber-attacks Related?" *Symantec (official blog)*. March 29, 2013. < http://www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related >

In the Trojan.Koredos investigation, Symantec identified a sophisticated backdoor "Backdoor.Prioxer" that infected files in a discreet manner. A modified version of this backdoor (named "Backdoor.Prioxer.B" by Symantec) resurfaced during the Trojan.Jokra attack in 2013. Although the newer version of Backdoor.Prioxer did not proxy Internet Relay Chat (IRC) communications as in the older one, they shared the same command and control base protocols.

In the 2013 Trojan.Jokra attack, hackers also used the Jokra packer to obfuscate both Trojan.Jokra samples and a downloader. So far, the Jokra packer appears to be rare: Its use has been limited to Korea. Moreover, the packer has only covered Jokra, the downloader, and the back door Trojan containing the "Z:" build string.[36] Given this low prevalence, the packer seems to be in use by only one group, confirming the link between Backdoor.Prioxer.B and Trojan.Jokra. They shared the same build path shown in the following strings:

A sample of Trojan.Jokra malware:

Z:\Work\Make **Troy**\3RAT Project\3RATClient_Load\Release\3RATClient_Load.pdb

A sample of Backdoor.Prioxer.B:

Z:\Work\Make **Troy**\Concealment Troy\Exe_Concealment_Troy(Winlogon_Shell) \Dll\Concealment_Troy(Dll)\Release\Concealment_Troy.pdb

Again, the common build path "Z:\work\Make Troy" proves not only the link between Trojan.Jokra and Backdoor.Prioxer.B, but also connections

[36] Packers are wrappers put around pieces of software to compress and/or encrypt their contents, usually with the view of minimizing download times and storage space or to protect copyrighted coding. Oftentimes, they are used in malware to disguise the contents of malicious files form malware scanners. (Source: Virus Bulletin <http://www.virusbtn.com/resources/glossary/packer.xml >)

between the 2013 Trojan.Jokra and the 2011 Trojan.Koredos attacks as almost identical backdoors surged during both incidents.

In addition to the aforementioned analysis, the Symantec analysis further suggests possible involvement of a professional hacker group employed in order to carry out attacks against South Korea. The malware build path starts with "Z:\work", an indication that the hackers created a work folder to develop a Trojan. This contrasts with the general understanding that independent hackers would hardly store a Trojan in a "work" folder, as they would do it for "fun" rather than for "work."

Investigation by the South Korean Government

Soon after the March 20 cyber-attack, the South Korean government opened an investigation by a team composed of military, civil and government experts. On April 10, 2013, South Korea's Ministry of Science, ICT and Future Planning released the mid-term results[37] of the investigation holding North Korea responsible. The investigation team collected a total of 76 samples of malware and found that 9 of them were used for destructive purposes and the remaining 67 for penetration and monitoring purposes. The team also analyzed military and intelligence data on North Korea's previous cyber-attacks against South Korea and concluded the March 20 attack had required more than 8 months of preparations. The four main reasons cited as evidence for North Korean responsibility in the attack are as follows:

Suspicious access to the targeted servers

Beginning from June 2012, at least 6 computers from North Korea had accessed the targeted firms' networks as many as 1,590 times to spread malware

[37] "Mid-term Release of Civil-Government-Military Joint Team's Investigation into 3.20 Cyberterror" *Ministry of Science, ICT and Future Planning*. April 10, 2013 <http://www.msip.go.kr/Board_detailForm.action?bbsId=72&bbsNo=182 >

and steal data. Some of these computers even reconnected to the servers on the next day of the attack in an attempt to delete remaining traces of evidence which may have helped to disclose their identity.

Exposure of an IP address based in Pyongyang

On February 22, 2013, an IP address identified as "175.45.178.xx" accessed South Korean routes, probably to conduct a remote controlled test prior to the attack. South Korean investigators later retraced the geographical location of the IP address to the North Korean Start Joint Venture based in Ryugyong-dong residential district of Pyongyang. The IP address exposure is believed to have occurred accidentally. As for the possibility of IP spoofing by a third party intending to bring a false charge against North Korea, the chances are rather slim. IP spoofing is only possible in a situation where hacker sends out a unilateral command such as in DDoS attack. However, APT attacks like the March 20 attack require continuous bidirectional communication between the hacker and the compromised computers.[38] Thus, the possibility of IP spoofing is highly unlikely as this would prevent the hacker from receiving a reply.

Routing points similar to those in the past attacks

Among the 49 IP addresses (25 South Korean, 24 overseas) through which the culprits routed their attacks, 22 of them (18 South Korean and 4 overseas) were identical to the ones discovered in the past cyber-attacks attributed to North Korea. Other IP addresses used in the attack were based in more than 10 countries including the US, Hong Kong and Australia, reflecting the North's growing technical ability to diversify its routing points. This is in contrast with the past attacks in which North Korea mostly used Chinese IP addresses for

[38] "Evidence for North Korean implications in March 20 attack" *Halos*. April 10, 2013. <http://www.halos.co.kr/community/notice/view.do?noticeCode=124 >

routing. The increasingly diversified routing points further illustrate the growing difficulty associated with investigations into future cyber-attacks.

Reuse of malware

Of the 76 samples of malware used in the March 20 attack, at least 30 had been used by the North Koreans in the past attack. South Korean investigators also found an 8-digit identification code used exclusively by North Korean hackers for distinguishing compromised computers.

Based on these findings, the South Korean government placed the blame for the March 20 attack on North Korea. In preparation for the attack, the North Koreans were keen to exploit security vulnerabilities in the networks of South Korea's private institutions, notably administrators PCs, corporate intranet servers, and antivirus software.[39] Collecting security data one by one from a broad range of institutions involves a great deal of work over a long period of time. Yet, the North Koreans were able to execute the task, suggesting that the March 20 attack was part of carefully planned tactics rather than an impulsive act.

Apart from the technical aspects, North Korea had previously warned of upcoming strikes against major institutions in South Korea though it did not specify the methods. About a year earlier, North Korea's Ministry of the People's Armed Forces condemned KBS, MBS and YTN, among the victims of the March 20 attack, as the South Korean media outlets unjustly reporting biased news against North Korea. It further threatened that they would have to "pay the price for their acts."[40] Coincidence alone cannot fully explain that

[39] Young-jeon Kwon. "Intellectualization of North Korean cyberwarfare". *Financial News*. April 11, 2013.
<http://www.fnnews.com/view?ra=Sent0701m_View&corp=fnnews&arcid=130411061140 54&cDateYear=2013&cDateMonth=04&cDateDay=11 >

[40] "North Korea behind cyber-attack? Previous cyber-attacks against South Korea" *Yonhap News Agency*. March 20, 2013

these media firms were simultaneously attacked on March 20. The attack indeed proved that the North mated its words and deeds.

Then, other questions arise. Why has North Korea increasingly opted for cyber-attacks in recent years? What are the strategic calculations behind these provocations?

STRATEGIC CALCULATIONS BEHIND THE MARCH 20 ATTACK

In international relations, nations are willing to bear different costs in exchange for benefits. North Korea's underpinning foreign policy remains as regime survival and the perpetuation of the Kim dynasty descending down to the current young leader Kim Jong-un, the third generation of the Kims to accede to the throne. Accordingly, North Koreans are willing to sacrifice more in exchange for strategic means helping regime survival. Lewis also concluded the North is "clearly willing to take greater risks than most nations" and despite international pressure to stop them, it is "willing to spend scare resources to gain asymmetric advantages" including nuclear and missile programs.[41]

Given that a well-prepared cyber-attack can cause considerable damage and chaos to highly wired South Korea, the North has chosen to develop cyberforce as a strategic weapon. Its development does not require costly investment in installments and materials as does a nuclear program. Moreover, the development of nuclear weapons and missiles makes North Korea face pressure from external actors for their discontinuation, whereas covert cyberweapons mitigate such consequences. Indeed, when accused of

<http://www.yonhapnews.co.kr/northkorea/2013/03/20/1801000000AKR20130320193051014.HTML >

[41] James A. Lewis. "Who Is "Whois"?" *Foreign Policy*. March 21, 2013. <http://www.foreignpolicy.com/articles/2013/03/21/who_is_whois >

the cyber-attack which took place against South Korea on March 20, 2013, the North reacted angrily by denying its involvement.

On April 12, Radio Pyongyang termed the accusation a "calculated provocation" to exacerbate the already tense situation on the Korean Peninsula. [42] No matter how the North Koreans reacted, the strategic advantages brought about by cyberweapons seem to outweigh the potential costs North Korea has to bear.

REPLACING CONVENTIONAL PROVOCATIONS

Hackers generally target civil or financial organizations seeking financial gains or confidential corporate information. However, no evidence was found to link the primary objective of the March 20 attack with such types of gains. Investigators instead categorized the motivation as a political one.[43]

The unanimous adoption of United Nations Security Council Resolution 2087 on January 22, 2013 condemned North Korea for the launch of Kwangmyongsong-3 and broadened already existing sanctions on North Korea. A series of subsequent actions and rhetoric from North Korea escalated tensions on the Korean Peninsula. The North conducted a nuclear test on February 12 and informed China of its intention to conduct two more nuclear tests in 2013. UN Security Council Resolution 2094, adopted on March 7, 2013, marked another international condemnation against the nuclear test. In response to the UN resolution, the North Korean government closed its joint border and cut off the hotline to South Korea.

Later, the North confirmed it had nullified the 1953 Korean Armistice Agreement. Declaring the North-South non-aggression agreement void, North

[42] Radio Pyongyang. April 12, 2013 Rpt. in "Internal Affairs on North Korea" *Korean Institute for National Reunification*. March/April 2013, volume 7, number 2.
[43] *Foreign Policy*. March 21, 2013.

Korea warned of an upcoming "merciless" military retaliation against its enemies. Against this backdrop, annual South Korea-U.S. joint military exercises took place amid heightened tensions. Historically, the North has displayed hysterical defiance to the South Korean and U.S. annual joint military exercises Key Resolve and Foal Eagle.

The 2013 Key Resolve exercises were scheduled from between March 11 to March 21 and the cyber-attack broke out on the eve of their termination. In fact, North Korea's denunciation of this year's exercises went far beyond the level of criticism it has expressed in the past. Indeed, the 2013 Key Resolve marked another significant development in the military cooperation between South Korea and the US. With the view of showing its resolve in deterring the North Korean nuclear threat and enhancing its strategic posture in the Asia-Pacific regions, the US mobilized B-52 bombers from Anderson Air force base in Guam to carry out simulated nuclear bombing raids on North Korea.

The sortie of the B-52 was believed to pose a considerable threat to North Korea as the bomber was equipped with both precision-guided conventional and nuclear ordnance.[44] The overwhelming cyber-attack just before the end of Key Resolve raised strong suspicion that North Korea condemned this year's overtly clear military posture against its nuclear ambition through the cyber-attack. Moreover, a conventional provocation would have been too risky during the joint exercises when South Korea-U.S. forces were ready to carry out large-scale operations.

In fact, cyber-attack often works to the advantage of the attacker by delaying or reducing retaliatory actions from the victim. Nations targeted by

[44] Bill Gertz. "U.S. B-52 bombers simulated raids over North Korea during military exercises" *The Washington Times*. March 19, 2013. <http://www.washingtontimes.com/news/2013/mar/19/us-b-52-bombers-simulated-raids-over-north-korea-d/?page=all >

cyber-attack avoid taking rash countermeasures until concrete evidence unveils the identity of the culprit. But the process of reaching the conclusion may take up to a few months if hackers leave little or intentionally wrong traces obfuscating their identity. Even if the evidence is clear, no legal basis exists to justify a state-level cyber counterattack or define the extent to which the principle of proportionality should apply. The March 20 cyber-attack did not cause any kinetic damage or human loss unlike North Korea's conventional military provocations in 2010 that sank the South Korean naval ship Cheon-an and shelled Yeonpyeong Island.

Thus, it was not as clear how to respond to the North Korean cyber provocation even after investigation concluded North Korean's guilt months after the incident. Planning counterstrike against computer networks in North Korea would have been meaningless given the destitute nation's extremely limited network systems. To make matters worse, consensus had not yet been formed among South Koreans as to whether the findings of the government investigation was convincing enough to attribute the attack to North Korea. Faced with the unprecedented scale of cyber-attacks, South Korea was left with a dearth of options to choose from.

The attack demonstrated North Korea's strategic use of cyberforce in the midst of heightened political and military tensions. Due to the lack of hard evidence in the cyber-attacks, North Korea successfully stoked the fears of South Koreans and damaged important networks while officially denying its implication to minimize the risk of retaliation. Consequently, North Korea is likely to launch more cyber-attacks against South Korea in replacement of conventional military provocations.

CAUSING SOCIAL CHAOS

Major victims of the March 20 attack were South Korea's well-known media and financial companies. What could be the gains for the North by disrupting the nationwide networks of broadcasters and financial institutions? Interestingly, closely tied to the daily activities of people, abnormalities in the functioning of both sectors can be noticed immediately. TV and radio stations occupied by a hostile side may broadcast manipulated contents which dramatically increases public fears. Even worse, people become gripped with panic if access to their personal bank accounts is suddenly denied. Though the culprits of the March 20 attack did not cross the red line by actually carrying out such actions, this observation suggests that they at least had in expectation that their malicious activities would cause an immediate chaos in South Korea.[45] By hacking into the nation's biggest broadcasters and banks, the hackers wanted to magnify the impacts of the attack.

In addition, media and financial firms can maximize confusion in a war time. Broadcasting stations act as the central channel of information transmission in emergency situations. Paralyzing or spreading false information across the targeted nation will bring invaluable advantages to the attacker. From this perspective, the cyber-attack against South Korean broadcasters on March 20 may also be understood as North Korea's trial-run to measure the extent of the damage caused to South Korea's communications infrastructure and observe the readiness of the South's cyber defense system. In fact, some believe that North Korea has acquired cyberforce well beyond the level shown during the March 20 attack and the attack only partially revealed the North's cyber capabilities, far less than its actual strength.

---

[45] "Who's behind simultaneous hacking into broadcasters and financial sector?" *SBS*. March 20, 2013. <http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1001690871 >

There is a fair chance that North Korean cyberforce is already capable of bringing down South Korea's critical infrastructures.[46] In the March 20 attack, however, the North intentionally avoided deploying the full forces of its cyber-arsenal. If North Korea's goal was limited to arousing public fear, there would have been little use of deploying excessive forces beyond what appeared sufficient. Doing so would only have increased the risk of being caught if the attempt had failed.

ASYMMETRIC AND COVERT, YET SUBSTANTIVE

In the middle of chronic economic hardships, confronting the South with conventional weapons is not viable nor does it appear economically sustainable. Under such circumstances, the North is naturally attracted to unconventional weapons with asymmetrical advantages, among which are nuclear, missiles and cyber weapons.

When used against South Korea, asymmetric weapons are able to transform the perceived advantage of the South into weakness. Facing cyberwarfare, the South's advanced computer infrastructures would become the vulnerable potential targets from the North Korean perspective, while South Korea would have a difficulty identifying targets in unwired North Korea.

The advantage brought by well-developed cyberforce is significant even in comparison with nuclear weapons, another asymmetric weapon that North Korea has been eager to develop. North Korea's pursuit of nuclear weapons calls forth tightened sanctions from the UN Security Council which restrict the North's weapons trade or any materials that can be used for weapons production. The sanctions also set barriers to financing missiles and nuclear

[46] Interview with Prof. Lim.

programs by freezing North Korean assets abroad. Nuclear weapons are further likely to be a burden on the back of China, the traditional ally of North Korea which now wants to become an influential member of the international community.

For North Korea, the recent leadership transition in China adds uncertainty to the geopolitics surrounding the Korean Peninsula. Different from the Cold War during which solid North Korea-Chinese ties guaranteed friendly bilateral relationships, current Chinese approach to North Korean issues do not always work in favor of North Korea's interest. New Chinese President Xi Jinping appears to prefer practical foreign policy promoting Chinese interest internationally rather than turning a blind eye to the misbehaviors of the communist ally.[47]

North Korea can no longer fully rely on Chinese support to go against international norms if doing so means pushing China to handle additional pressure from other countries to foil North Korean nuclear ambitions. Further deterioration of diplomatic ties with China will only deepen North Korea's international isolation. Therefore, it is more viable for the North to use the nuclear programs as a bargaining chip while deploying cyberforce to cause covert, yet substantive damage to South Korea.

CYBER BASES IN CHINA

Regardless of its real intention, China has provided North Korea with necessary materials and operational bases to test and launch cyber-attacks. Over the past years, North Korea has established IT subcontract companies in China mostly in the northeastern provinces where geographical proximity

[47] Jonathan D. Pollack. "Obama, Xi and North Korea: The Long Overdue Conversation" *Brookings*. June 4, 2013. <http://www.brookings.edu/blogs/up-front/posts/2013/06/04-north-korea-obama-xi-jinping-meetings-pollack >

facilitates North Korean business activities in the regions. North Korean software engineers work for Chinese or North Korean IT companies in normal times to earn foreign currency. To make additional money, they sometimes develop illegal software for South Korean criminal groups.[48] These IT workers transform into state hackers when an order is dispatched from the Reconnaissance General Bureau in Pyongyang.

Referring to the March 20 attack, not only was the attack launched using IP addresses based in China, but also about a month before the attack, a large number of North Korean IT workers on one month visa suddenly flowed across the border to Shenyang and Hunchun. The owner of a local inn that accommodated some of the workers later reported seeing them using strange equipment similar to an antenna.[49] If this reporting is accurate, then some North Korean hackers crossed the border to carry out a cyber-attack with North Korean workers already present in China. In China, North Korean software engineers are perceived as skillful workforce available at a relatively low cost. Although Chinese public security bureau is known to be aware of the malicious cyber activities against foreign governments, no concrete measures have been taken against them.[50]

Additionally, North Korean cyberforce present in China poses a constant long-term threat to South Korea. In collaboration with South Korean criminals in China, North Korean workers develop illegal software called "auto programs" that collect online game items convertible into cash. In the process of the development, North Korean workers intentionally install malware in the software which is then sold to South Korean brokers.[51] Ultimately, the

[48] *Sisa Press*. August 24, 2011.
[49] Sang-min Park, "North Korea behind Illegal Games" *KBS*, April 19, 2013. <http://news.kbs.co.kr/news/naverNewsView.do?SEARCH_NEWS_CODE=2646300>
[50] *TV Chosun*. March 31, 2013.
[51] *KBS*, April 19, 2013.

malware spreads across the game users once it penetrates into South Korean servers. Recently, North Korean hackers have focused their activities on developing and distributing smartphone applications, so the South Korean users unconsciously download the malware installed in the applications.

The malware not only collects the users' sensitive personal information stored on their smartphones but also compromise the devices for potential cyber-attacks.[52] Clearly, South Korean computer networks remain unguarded against malicious activities of North Korean IT developers in China.

The particularly vulnerable Internet security conditions in China further exacerbate the situation. Illegal software and files downloads which commonly occur on Chinese websites help dissemination of malware, some of which planted by North Korean hackers.[53] As a result, Chinese computers are easily compromised which can be later used for North Korean hackers' cyber operations against South Korea.

North Korea reportedly brought in 12 LAN cables from China in 2010 to command and control cyber operations directly from Pyongyang.[54] However, China still serves as the main attack base for North Korea, in part to avert possible operational mistakes which may reveal the North Korean involvement. Thus, South Korea should always take the complicit role of China into account when examining North Korean cyber operations.

THE NEXT CYBER-ATTACK?

Those developing cyberforce ultimately aim at taking control of a target's critical infrastructures. In the past, controlling critical infrastructures

---

52 *Sisa Press*, August 24, 2011.
53 Interview with Prof. Lim.
54 Eun-seo Shin. "China increases regulations against North Korean hackers" *TV Chosun*. March 31, 2013.
<http://news.tv.chosun.com/site/data/html_dir/2013/03/31/2013033190007.html >

from a distance was often regarded as an imaginary scenario. However, the discovery of Stuxnet in 2010, which sabotaged centrifuges at Natanz nuclear site in Iran, marked the advent of cyber-attacks causing direct kinetic damages from a distance. Such moves will only intensify as national critical infrastructures are increasingly connected to the Internet. In line with this trend, North Korea also aims at damaging South Korea's critical infrastructures when it deems such action necessary.

South Korea's major infrastructure usually include telecommunications, media, finance, energy, and transportations. The March 20 attack demonstrated a successful mobilization of North Korean cyberforce against South Korea's major finance and media infrastructures. As for the ensuing attack, South Korean cybersecurity experts argue transportation systems and nuclear power plants are likely to be the next targets.[55, 56] If North Korean hackers somehow manage to plant malware in the command and control system of South Korea's nuclear power plants, a variety of its operations will cause dire consequences for South Korea's national security.

The malware may operate in concealment and collect secret nuclear management data from inside. In the worst case, it may even manipulate the South Korean nuclear power plants against South Korean citizens in the event of war on the Korean Peninsula. As for the transportation system, the derailment of a KTX train that carries hundreds of thousands of passengers on a daily basis would cause disastrous human and material losses for South Korea.[57] There is a high probability that North Korea has already acquired the

[55] Interview with both Prof. Lim and the South Korean police inspector.
[56] Hyuk-jin Park. "Interview with Son Yeong-dong, former president of National Security Research Institute". *Weekly Chosun*. 1 April 2013. <http://weekly.chosun.com/client/news/viw.asp?nNewsNumb=002250100006&ctcd=C07>
[57] Korea Train Express, referring to South Korea's high speed rail system.

technology to put such plans into action, except it has not yet felt compelled to do so.[58]

Moreover, the next stage of cyberwarfare will be replete with intense psychological operations. As it can be inferred from the term "psychological", the operations are invisible but take the form of pro-North Korean propaganda and intrusions onto South Korean websites on a constant basis. They were first commanded by the late North Korean leader Kim Jong-il who defined the Internet as a particularly vulnerable space where South Korean national security laws are emasculated. Distinctive from the attacks exploiting the target's technical vulnerabilities, psychological operations convey selected information to large audiences of the targeted country's citizens to influence their emotions, motives, objective reasoning and ultimately the behavior of the government of the targeted country, organizations, groups and individuals.[59]

Through the omnidirectional psychological operations, the North Koreans aim to cultivate favorable public opinion in South Korea towards North Korean policies. More important, they seek to cause serious disunity among South Koreans, because fiercely divided public opinion will prevent prompt decision-making and its effective implementation by the government. Therefore, the real danger of cyber psychological operations comes from its ability to encroach surreptitiously on the South Korean population to limit the nation's response against the threats from North Korea.[60]

---

[58] Interview with Prof. Lim. During the interview, he said North Korea has already developed the skills to hit South Korea's critical infrastructures and some malware possibly has begun operation in the infrastructures.

[59] DoD. Joint electronic library [online, cited: May 28, 2012]. <http://www.dtic.mil/doctrine/>. Retrieved on Steve Winterfeld and Jason Andress. "The Basics of Cyber Warfare" Chapter 6. Psychological Weapons. Syngress. December 28, 2012 < http://my.safaribooksonline.com/book/ethics/9780124047372/chapter-6dot-psychological-weapons/chp007_html >

[60] *Weekly Chosun*. 1 April 2013.

Taking these aspects into account, the following scenario can be formulated as a hypothesis of the next cyber-attack from North Korea. Through psychological operations in normal times, North Korea enervates South Korea's defensive posture against North Korean provocations. Once a war breaks out, pre-planted malware neutralizes considerable parts of South Korea's response capability by paralyzing its major military facilities, communications systems, and critical infrastructures.[61]

South Korea, already devastated by the pre-assault cyber operations, is now easily brought down by North Korea's final strike with conventional arms. Although this only provides a hypothetical case, South Korea should prepare itself against the worst possible scenarios with regards to the growing cyber threats from North Korea.

HOW SHOULD SOUTH KOREA PREVENT DESTROYSEOUL?

Over the eight months during which the attack was under preparation, North Korean malware successfully escaped detection which lays bare South Korea's insufficient cyber capabilities, North Korea's sophisticated cyber techniques, or both. In reality, "perfect security" in cyberspace is a flawed concept.[62] Hackers are there to make unreal things happen. The notion of cyberwarfare itself was unfamiliar to many only a few years ago. In 2012 alone, however, the web security company Kaspersky found that about 200,000 new malicious programs were made on a daily basis.[63]

---

61 *Ibid.*

62 Interview with Prof. Lim.

63 Virus News. "2012 by the numbers: Kaspersky Lab now detects 200,000 new malicious programs every day" *Kaspersky Lab*. December 10, 2012. <http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day >

Facing the unending emergence of new malware at an exponentially growing speed, the effectiveness of the existing security measures are destined to fade away quickly. Indeed, relying solely on technical solutions cannot guarantee lasting advantages in cybersecurity and this is why South Korea should build its cyber strategy at multiple levels.

NEED FOR A NATIONAL CONSENSUS ON GROWING CYBERTHREATS FROM NORTH KOREA

Within South Korea a nationwide consensus exists on the existence of the threat and support for government actions are prerequisite for building effective security frameworks. Therefore, any effort to strengthen national cybersecurity should begin by revisiting this concept.

Whenever a major security incident sweeps across South Korea implying a linkage with North Korea, South Koreans tend to question the veracity of information due to the ideological division deeply rooted in the South Korean politics. In the wake of the March 20 attack, the official investigation results could not convince the entire South Korean public of the North Korean responsibility. Some remained skeptical of the findings which implicated North Korea in the attacks. Others speculated that perhaps North Korea was chosen as a scapegoat in an attempt to conceal the weakness of the South Korean government's cybersecurity policies.[64] In fact, the divided public opinion was a blunt reflection of public distrust and criticism against the government's failure to prevent cyber-attacks from reoccurring. Given that public opinion can exercise a significant influence on national agendas, the South Korean government needs to take appropriate measures to address the problem.

---

64 Jae-jin Lee "Suspicion raises against investigation" *Media Today*. April 10, 2013. <http://www.mediatoday.co.kr/news/articleView.html?idxno=108679 >

Making matters worse, inept government responses in the past did not help to quell the South Korean public's distrust of the results of official investigations. In the aftermath of the Nonghyup Bank hacking in April 2011, for example, inconsistent positions taken by investigating authorities only fuelled confusion in the hearing before members of the National Assembly. While the National Intelligence Service (NIS) and the Public Prosecutors Office attributed the attack to North Korea, the Financial Supervisory Service stood indecisive regarding the North Korean responsibility.[65] In the recent March 20 attack, the government put public confidence at stake when it prematurely held the North accountable for the attack. When compared against the three months taken before releasing the results of the 2011 Nonghyup incident, it becomes evident that the release of the results of the 2013 attack investigation after a mere 20 days was premature.

Because an investigation usually take up to a few months due to long and tedious IP retracing work, some were skeptical of the thoroughness of the March 20 attack's investigation. Furthermore, the Ministry of Science, ICT and Future Planning made the announcement at the instigation of NIS while the National Police Agency[66] opted out of the press conference.[67] In fact, the Police Agency had already accumulated a similar amount of data comparable to the Ministry and NIS. Nevertheless, the Police Agency decided to wait until they could collect supplementary evidence through overseas C&C servers in cooperation with foreign police agency.[68]

---

[65] In-sung Kim. "So it's North Korea again?" *OhMyNews*. April 10, 2013. <http://www.ohmynews.com/nws_web/view/at_pg.aspx?CNTN_CD=A0001853270 >

[66] The police officer interviewed admitted concluding on the North Korean responsibility was considered too premature at that time, although additional investigation later confirmed the North Korean implication in the March 20 attack.

[67] *Media Today*. April 10, 2013.

[68] Interview with the South Korean police inspector.

The Police Agency's decision was based on the belief that ensuring consistency and transparency throughout the process of investigation is particularly important in gathering virtual evidence, so the results of the investigation can be readily trusted by the public. In any case, the controversy surrounding investigation into the March 20 attack reveals the lack of both unity and consistency in South Korea's national approach to a major cyber-attack. Rather than executing the investigation in a comprehensive national framework under the leadership of a strong coordinating entity, the investigating authorities tackled the same incident separately. In order to enhance efficiency in the investigating process, South Korea needs a well-coordinated inter-ministerial framework that can bring about prompt and efficient investigation into cyber-attack. A unified approach to the investigation and consistency in the findings will naturally earn more public trust.

Solid cybersecurity strategy should be built on a firm national consensus on the existence of a valid threat. As the first step toward enhancing cybersecurity, the South Korean government should demonstrate to the nation that the North Korean threat is real. It is only through this process that future cybersecurity measures will be implemented successfully.

REVISITING THE CYBER CONTROL TOWER

Following the two major cyber-attacks in 2011, the South Korea government made public its decision to create a National Cyber Security Master Plan (Master Plan). The plan addressed fundamental problems that South Korea must overcome to enhance national cybersecurity and include the following as the main course of actions:

- Establishment of a joint response system comprised of the private, public and military sectors;

- Protection of critical infrastructures;
- Systemic national level response to cyber-attack including protection, detection and resistance to assault;
- Developing deterrence mechanisms through international cooperation; and
- Building a national cybersecurity control tower.[69]

Nevertheless, the outbreak of the March 20 attack demonstrated that the fundamental weakness of South Korea's current cybersecurity strategy is not the nation's lack of policies, but that of viable implementation mechanisms for their successful execution. It is apparent that the government could not prevent another major cyber-attack, nor could it reduce the damage and public controversy in the aftermath of the attack. Indeed, good policy alone cannot result in the intended benefits if not implemented in a way that maximizes those benefits.

A main pillar of the Master Plan contains the establishment of a National Cybersecurity Control Tower (Control Tower) with the view of enhancing prompt coordination among relevant government agencies against cyber-attacks. Government agencies forming the Control Tower are responsible for the implementation of policies that are specific to their own area of expertise. For example, the Korean Police Agency, NIS, the Korea Information Security Agency and the Ministry of National Defense ensure cybersecurity in the areas of crimes and terrors, the public sector, the private sector and defense respectively.

Although the South Korean Presidential Office, Cheong Wa Dae, officially heads the Control Tower, it is the NIS that plays the pivotal role of its

[69] "Strategic Discussion on National Cybersecurity in Response to 3.20 Cyber-attack" *Ministry of Science, ICT and Future Planning*. April 11, 2013 <http://www.msip.go.kr/Board_detailForm.action?bbsId=72&bbsNo=219 >

operations by acting as the de facto working-level chief and manages the inter-agency coordination. This structure, however, might prevent the Control Tower from realizing its goals as originally intended.

As mentioned earlier, the creation of the Control Tower envisages a prompt and coordinated response from government agencies in charge of national cybersecurity. The inter-agency coordination can be notably enhanced by a vertical command structure with a command office on the top that can exercise sufficient authority over others. In normal times, the office should plan and oversee the nation's general cybersecurity strategies and their executions based on the periodic reports of trends in cyberthreats submitted by individual agencies. Once a cyber-attack raids the country, the office should quickly assign a specific role to each agency in order to bring out a coordinated national level response against the attack.

Therefore, the ideal functioning of the Control Tower should be based on a hierarchical structure that facilitates centralized information gathering on one hand and a powerful command structure on the other. Given that the Control Tower should also act as a coordinator mediating possible frictions among the agencies and give them directions to follow, it is not viable to confer such authority on one specific agency over others as a working-level chief.

Instead, it is recommended that Cheong Wa Dae proactively expands its competency in cybersecurity. Already acting as a powerful executive organ of the nation, integrating the Control Tower into the full competence of Cheong Wa Dae will create a unified channel of communication without overlap.[70] Additionally, using its far-reaching relations with foreign governments, Cheong Wa Dae will be able to facilitate smooth flow of information exchange

[70] Jongbin-Seo "Interview with Prof. Seung-joo Kim, cybersecurity expert at Korea University" *Pyonghwa Bangsong*. March 28, 2013. <http://bbs2.pbc.co.kr/bbs/bbs/board.php?bo_table=open&wr_id=6552 >

on cybersecurity with foreign governments and promote international cooperation.[71]

It is time for Cheong Wa Dae to prioritize cybersecurity in its agendas. In addition, to derive the desired outcomes from the Control Tower, it needs to expand its role as both the official and de facto command office of the Tower.

INTERNATIONAL COOPERATION ON CYBERSECURITY

The transnational nature of cyber operations stresses the need for cooperation at the international level. For South Korea, it should consider a variety of measures including notably opening bilateral cooperation with China, creating global governance for cybersecurity, enacting cybersecurity laws, and building partnership with countries in the process of developing IT infrastructure.

As previously mentioned, North Korean hackers, normally working as IT workers, are physically present in China. Although most of them may have arrived in China through due process, their malicious operations to disrupt another country's cyber infrastructures should be subject to regulations. Due to the operations taking place under the jurisdiction of China, however, there is little room for South Korean authorities to act against these activities unless China agrees to provide support.

If China agrees to cooperate, it can officially ban the activities of foreign hacking organizations within its territory. Although the difficulty associated with proving the crime and possible diplomatic frictions with North Korea might set practical barriers to the actual punishment of the hackers, the official prohibition itself will demonstrate China's will to confront illegal abuse of its

[71] Interview with Prof. Lim.; also from Jisung-Noh "Cheong Wa Dae should preside cyber control tower" *Korea Advanced Institute of Science & Technology.* 2013. <http://mshelp.kaist.ac.kr/Essay/Essay_2013/7.pdf >

Internet infrastructures by foreign agents and rid China of the indirect responsibility of being complicit in North Korean cyber operations. Ultimately, such moves should gradually pave the path for bilateral cooperation between South Korea and China for the investigation into North Korea's cyber-attacks launched from China.

Introducing an international legal framework guarding cybersecurity is another crucial area for consideration. Questions critical to confronting rising cross-border cyber operations require appropriate legal approach. These questions may include, among others, deciding on the internationally agreed threshold to determine the scale of cyber-attack justifying a counterattack; international regulations on belligerent cyber actions; legal basis for a third party to mediate a cyberconflict involving more than two nations.

Currently, these questions remain largely unanswered. In practice, any law may be imperfect to control malicious acts in the virtual world. Nevertheless, it does not mean that cyberwarfare should be neglected and left as a lawless area. In the case of chemical weapons, countries internationally agreed on the need to ban their use by signing the Chemical Weapons Convention despite their different approaches to the complex mechanisms of the regulations. A similar principle can be applied to the regulations of cyberwarfare.[72]

The moves calling for the imposition of legal limits on cyber operations will eventually emphasize the need for creating global cyber governance in which nations gather, build cooperation frameworks and introduce the basic norms to be respected in pursuing cybersecurity.

There is nevertheless a long way to go before the above recommendations can come to the fruition. In promoting international

[72] Interview with Prof. Lim.

cooperation regarding cybersecurity, a number of practical difficulties still lay ahead. For example, following the March 20 attack, few countries except the US and Hong Kong, responded positively to the request of cooperation on investigation from the Korean Police Agency.[73]

The reasons for this reservation vary but may include, among others, the lack of precedents in their countries, less critical use of IT technologies and the fear of creating constraints that might trap their own cyber activities in the future. Despite the difficulties, South Korea should concentrate efforts to build a cooperation framework with like-minded countries. For example, South Korea recently took the initiative to join the EU Cyber Convention.[74]

Such moves should be welcomed and promoted further. Another possibility comes from partnership with the US. Being the frontrunner in cybersecurity and a long-time ally of South Korea, the US can lead the global discussion on cybersecurity with South Korea. Starting from relatively small projects, the cooperation should gradually expand to other areas such as personnel exchanges between cybersecurity departments of the two nations and the establishment of strategic information exchange channels.

In the long-term, providing technical assistance to countries in the process of developing IT infrastructure will bring another strategic advantage to South Korea. North Korea has already made such a move. For example, it signed an IT cooperation treaty with Laos in March 2013 in addition to the one signed with Syria earlier.[75] Although details of the cooperation are only vaguely known, it could potentially provide another unguarded base for North Korean cyber operations in addition to its base in China. It is therefore in South

[73] Interview with the South Korean police inspector.
[74] *Ibid.*
[75] Jeong-woo Park "North Korea-Laos strengthened cooperation in IT" *Radio Free Asia*. March 21, 2013. <http://www.rfa.org/korean/in_focus/laos-03212013163148.html >

Korea's interest to establish and strengthen partnership with countries wishing to improve IT infrastructure. Although doing so may require heavy investment from South Korea in the initial stages, it will eventually help win the support of partner countries regarding cooperation on future cyber-related investigation. Ultimately, it will also enhance these countries' capacity to prevent and apply regulating measures against illegal cyber activities taking place in their territories against South Korea.[76]

Given the borderless characteristics of cyberwarfare, international cooperation is the key to protecting nations against future cyber-attacks. South Korea should be creative in exploring various opportunities in this field. At the same time, it should also prepare itself to use the next cyber-attack, highly likely to reoccur, as a momentum to call for the establishment of global governance on cybersecurity.

IN SEARCH OF DYNAMIC DEFENSE WITH THE PRIVATE SECTOR

Under North Korea's totalitarian regime, state hackers are not merely skillful technicians, but fierce combatants who are obliged to fight vehemently to win cyber-battles against the South. Facing attacks from North Korean cyber soldiers, South Korea must develop strategies leading to dynamic defense. Here, the term "dynamic defense" can be understood as maintaining up-to-date technological innovations in the field of national cybersecurity and reducing damage from potential cyber-attacks through active participation from the private sector.

In cyberwarfare, defense and offense are inseparable: Only a nation with an acute knowledge of an enemy's offensive capabilities is able to strengthen its defensive capabilities accordingly. Given that the most dynamic driving

[76] Interview with the South Korean police inspector.

force of computer technologies is humans themselves, government needs to build its cybersecurity strategy around discovering and training those with special talents in computer technologies. Nevertheless, training state hackers is only part of the dynamic defense scheme. As in the March 20 attack, cyber-attacks not only targeted public institutions, but also private institutions that provide vital services to the population. Therefore, by no means can the government alone successfully fend off well-prepared cyber-attacks.

In fact, technological agility, essential for developing antivirus and other innovative computer techniques, is better pursued by the creative private sector. In the end, both the government and the private sector should work together: The former providing the general picture of national cybersecurity and policy guidelines, with the latter taking part in efforts to back the government with innovative technologies. In other words, the South Korean government guides the nation to stay alert against external cyberthreats, equips it with the most advanced defense and offensive cyber technologies and supports private IT companies in their development of cutting edge technologies. Such interactive mechanisms will allow contributions from the private sector to refine the nation's overall cybersecurity.[77]

Active participation from the private sector also plays a significant role in preventing the spread of malware. Unlike conventional military arms, cyber weapons are deployed in a cunning manner and individual users are constantly exposed to the danger. An Internet user's incautious click on a website affected by virus can serve as the entry point of fatal malware later attacking the nation's critical systems. This establishes another reason why the government should promote cybersecurity in close cooperation with the private sector.

[77] *Ibid.*

One possibility is to require schools to teach mandatory cybersecurity courses, so the students become familiarized with core issues of cybersecurity from a young age and take due caution in surfing the web. Another possible option for the South Korean government is to provide incentives to college students to take internships in computer security software companies that will give them opportunities to acquire working level knowledge in cybersecurity.[78]

From the perspective of national security, future cyberspace will be a battlefield where conflicting goals of different nations come into collision. Against this backdrop, only nations working closely with the private sector will be able to take advantage of the human talents and realize dynamic defense in cybersecurity.

These recommendations provide basic steps that South Korea should take, but are no way exhaustive. As continuous cyber-attacks from North Korea have made cyberwarfare one of the most alarming security issues for South Korea, the South should actively improve available measures against the North Korean threat through various creative means.

CONCLUSION

South Korea, a country keen to explore benefits brought by the Internet, has suffered a heavy blow from a series of North Korea's cyber-attacks in the past. Among the series of the cyber-attacks, this paper analyzed the 2013 March 20 cyber-attack in detail and shed light on the fast developing cyber capabilities of North Korea.

Unquestionably, cyber-attacks from North Korea are on the rise more than ever causing increasingly grave consequences. From a different point of view, however, incessant North Korean cyber-attacks provide South Korea

[78] *Ibid.*

with the opportunity to review its preparedness for cyberwarfare and enhance its national cybersecurity system. In doing so, the South Korean government needs to prioritize a few strategies in the agenda. These notably include building a national consensus on the existence of the cyberthreats from North Korea, improving current cyberstrategy by restructuring the Cyber Control Tower, promoting international cooperation in cybersecurity and lastly, cooperating closely with the private sector to realize dynamic defense in cyberspace.

In the end, the direction South Korea is about to take at this stage, after undergoing the latest major cyber-attacks in 2013, will determine if it can repulse future attempts for another DarkSeoul, or unwittingly leave the nation to face the advent of DestroySeoul.

REFERENCES

1. **Interviews:**

   Prof. Lim Jong-In, Dean of the Graduate School of Information Security, Department of Cyber Defense, Korea University.

   South Korean Police Inspector (interviewed on the condition of anonymity), Cyber Terror Response Center, South Korean National Police Agency.

2. **Web sources:**

   Ahn Lab: http://m.ahnlab.com/

   Boan News: http://www.boannews.com/

   Brookings Institute: www.brookings.edu

   Chosun Ilbo : www.chosun.com

   CSIS: http://csis.org/

   Dong-A Ilbo: http://news.donga.com/

   Financial News: www.fnnews.com/

   Foreign Policy: www.foreignpolicy.com

   Information Week: www.informationweek.com

   Kaspersky Lab: www.kaspersky.com

   KBS: www.news.kbs.co.kr

   Korea Advanced Institute of Science & Technology: www.kaist.ac.kr

   Korea Herald: www.koreaherald.com

   Korean Institute for National Reunification: www.kinu.or.kr

   Korea Internet and Security Agency: www.kisa.or.kr/

   Kyeonghyang Shinmun: www.khan.co.kr

   McAfee: http://blogs.mcafee.com

   Media Today: www.mediatoday.co.kr

   Ministry of Science, ICT and Future Planning: www.msip.go.kr

New York Times: http://www.nytimes.com/

NK Vision: www.nkvision.com/

Pyonghwa Bangsong: www.bbs2.pbc.co.k

Radio Free Asia: www.rfa.org

SBS: http://news.sbs.co.kr

Segye Ilbo: www.segye.com/

Sisa Press: http://m.sisapress.com/

Symantec: http://www.symantec.com/

Washington Times: www.washingtontimes.com

Yonhap News Agency: www.yonhapnews.co.kr