issue BRIEF

The Evolution of North Korean Cyber Threats

2019-03

Chong Woo Kim, Senior Fellow
The Asan Institute for Policy Studies
Carolina Polito[1]
University of Bologna
2019.02.19

Introduction

In North Korea, only a few people are allowed access to Kwangmyong, the national intranet service, as global internet access is restricted to a group of selected people, and the country has one of the weakest internet infrastructures in the world.[2] Nonetheless, North Korea is a formidable cyber power, standing alongside major players like the United States, China, Russia, the United Kingdom, Israel and Iran.[3] North Korea has been increasing resources to enhance and expand its cyber capabilities, as testified by the intensification of the regime-sponsored attacks that the world has witnessed in the last 10 years. Amongst the most blatant offensive cyber-attacks allegedly linked to hacker groups close to North Korea are the Sony Pictures attack, the WannaCry attack, and the DarkSeoul attack, despite the North's constant denial of any involvement with these attacks or the damage suffered by them. North Korea's cyber army consists of approximately 7,000 hackers,[4] performing a wide range of activities including theft, denial of service (DDoS), espionage and sabotage.[5] These types of operations have proved to be very useful as part of North Korea's asymmetric strategy towards the ROK-U.S. Combined Forces Command. Cyber operations are low-cost and low-risk, allowing North Korea to counter countries which have highly computer-dependent infrastructure, with little fear of retaliation. Due to their low-intensity, these attacks often lie beneath the threshold of an armed attack, reducing the risk of escalating the conflict to an unaffordable level. Pyongyang has consistently been using cyber-attacks with its political and strategic agenda. These attacks have been instrumental in supporting its espionage strategy, retaliating against competitors and sustaining its economy through financial thefts. There is no reason to doubt that cyber operations will continue to be an integral part of the regime's national strategy. Hence, they should be amenable to analysis as any other offensive behavior in the kinetic field.

The wide variation of the regime's activity throughout the years has often been perceived as chaotic, making the analysis of North Korean actions in cyberspace difficult. Therefore, a broad and general evaluation of the scope of the attacks would be helpful to infer meaning to this apparent randomness. This paper aims to ascertain how North Korea's cyber operations against South Korea have evolved in the period between 2009 and 2018. Through understanding its behaviors hitherto we can strengthen our strategies for the future. Broadly two main shifts in Pyongyang's cyber operations are observed: (1) an increase in cyber-attacks aimed at financial gain, (2) a decrease in the visibility of cyber operations at espionage and information gathering. One can only speculate as to the reasons behind the shifts.[6] It could be that Pyongyang has shifted its target, thus concentrating more of its efforts on hacking financial institutions in order to reduce the impact of international sanctions.[7] North Koreans could have also improved its deception capabilities, making it more challenging for South Korea to detect its espionage activities. This means that both types of activities are being carried out. It appears that North Korea's interests in demonstrating its cyber capabilities through blatant cyber-attacks have diminished, and over the years, its attacks have become increasingly subtle and sophisticated.

Given the changing nature of cyber-attacks, it is possible to outline three different strategic goals: at first, the main strategic goal was to cause disruption with Distributed Denial of Service (DDoS), then it turned to espionage and finally to financial gain. This classification can be subject to variations in minor attacks but it helps to clarify the general trends in the time frame considered. Also, it must be borne in mind that North Korea has always denied its involvement in cyber-attacks and proving its guilt conclusively can be very challenging. However, there are usually some indicators that point the finger at North Korea.

The Distributed Denial of Services (DDoS) Attacks

A DDoS attack is defined by the Council of Foreign Relations as "The intentional paralyzing of a computer network by flooding it with data sent simultaneously from many individual computers."[8] It is one of the most disruptive operations that can be carried out in cyberspace. Blocking all of the targeted computer system at once, DDoS attacks are striking. They tend to be brief in duration even though the length of an attack can vary widely depending on the ability of a server provider to recover its system as well as on the severity of the attack.

- **2009** - The first recorded DDoS attack carried out by Pyongyang's regime, known as the"4th of July" campaign[9], targeted both South Korea and the U.S. in July 2009. The sites of the South Korean Presidential Office, the Ministry of National Defense and the National Assembly were saturated with access requests generated by malicious software, while the White House, the Pentagon, and the Washington Post were among the high-level institutions targeted in the U.S.[10]

- **2011** - The "Ten Days of Rain" attack and the attack on the Nonghyup Bank were executed in March 2011. The targets of the first attack included the South Korea's Presidential Office,

the Foreign Ministry, the National Intelligence Service, and some major South Korean financial institutions. Attackers injected malware into two peer-to-peer file-sharing websites, infecting up to 40 websites and 11,000 personal computers.[11] The Nonghyup Bank attack destroyed 273 of the bank's 587 servers.[12] The hackers infiltrated the bank's personal computers for over 7 months, during which time they were able to place malicious code throughout its network, allowing them to crash hundreds of servers at a set time.

- **2013** - Thirteen days after the UNSC Resolution 2094 imposed new sanctions on North Korea following its third nuclear test, the regime carried out the notorious "Dark Seoul Attack" on March 20th 2013. Public broadcasters KBS, MBC, and YTN shut down at 2 p.m. local time. Concurrently, the Shinhan Bank and the Nonghyup Bank computers were temporarily shut down, and the Jeju Bank also reported network shutdowns at some of its branches. It took weeks for them to fully recover their systems, and only 10 percent of the targeted websites were working within two days.[13] The attack was considered to be one of the most severe cyber-attacks suffered by South Korea. It affected 48,000 machines,[14] and contributed to the international diffusion of terms such as Advanced Persisted Threat (APT) or cyber terrorism.[15]

- The last DDoS attack examined here dates back to June 25th 2013 on the 63rd anniversary of the outbreak of the Korean War. The intruders targeted the Presidential Office's website and several official media sites, affecting 69 machines in total.[16] It collected files containing personal data of U.S. and South Korean military personnel, among whom were members of the U.S. Army's 3rd Marine Division, 25th Infantry Division, and 1st Cavalry Division. The data was later uploaded to text-sharing websites.[17]

The hacker group responsible for most of the cyber-attacks listed is known as the "Lazarus Group". It was also behind the Sony attack and the Wanna Cry attack, which makes it undoubtedly the most famous group operating on behalf of the North Korean regime.[18] Its activities are allegedly carried out under the control of Bureau 121, a branch of the North Korean intelligence agency, the Reconnaissance General Bureau.[19] As the nature of North Korean attacks evolved, the structure of the Lazarus group also adapted creating new branches to support other activities required by the regime.

During this first sequence of offensive cyber operations, Pyongyang seemed generally inclined to display its cyber capabilities and project its cyber power in the international arena. This period also coincided with a renewed aggressiveness in North Korea's military policy as the regime carried out its second nuclear test in 2009. Given the circumstances, an offensive cyber strategy would suit the regime with little fear of retaliation. North Korea's infrastructure is far less computer-dependent than those of its adversaries. Moreover, the boundaries of the attribution were much vaguer during these years, and it was unclear to what extent and how rapidly states would have been able to detect attackers and retaliate against them. These factors have likely influenced North Korea to take such a vehement stance in the cyberspace during this period.

The Espionage Attacks

North Korea's cyber activities became increasingly oriented towards information gathering especially related to South Korea's strategies and military capabilities during the period between 2013 and 2016. North Korea has a long history of espionage; spy boats have been crossing Korean waters since the Korean War,[20] and with the advent of the internet, this new means proved to be extremely effective for gathering information. Cyber espionage activities were the most frequent during this period. North Korea performed at least six major espionage attacks against South Korea alone. Those attacks displayed a greater degree of technical capabilities than the first DDoS attacks.

- **2013** - The first attack, named "Kimsuky" after the hacker group, took place in September 2013. It targeted South Korean think tanks including the Sejong Institute, the Korea Institute for Defense Analyses, the Ministry of Reunification and the Hyundai Merchant Marine shipping company.[21] The nature of attack was complex and multifaceted with separate modules consisting of a keystroke logger,[22] a directory listing collector,[23] an HWP document theft, a remote control download & execution and a remote control access. The malware was distributed in the system using spear-phishing emails with personalized messages designed to steal password and other security details. One notable espionage operation targeted three computers belonging to National Assembly members.

- **2014** - Only a month after Sony Pictures cyber-attack, Korea Hydro and Nuclear Power (KHNP), South Korea's nuclear power plant operator, was targeted. The details of 10,000 KHNP workers and the documents containing reactor designs and manuals were stolen. 5,986 phishing emails were sent out to spread the malicious code within the power plant's IT system, which bears all the hallmarks of the Kimsuky attack. This technique is much more discrete than the blatant DDoS attacks even though stolen information was disclosed by the hackers later. This shows that there was not yet a concrete effort to cover up the offensive cyber-attacks. This attack on KHNP has raised concerns about Pyongyang's ability to cripple South Korea's infrastructure. It has contributed to the diffusion of the "Cyber Pearl Harbor" narratives. However, while such concerns should not be taken lightly, North Korea's strategy hitherto suggests that it is not in the regime's interest to target the infrastructure.

- **2015** - One notable espionage operation targeting three computers belonging to National Assembly members and eleven computers belonging to government aides occurred.[24]

- **2016** - In March, forty South Korean officials' smartphones were hacked, accessing their phone conversations, text messages, and other sensitive information.[25] North Korea has expanded its domain of operations to mobile technology. In April, Daewoo Shipbuilding & Marine Engineering Co., Ltd was targeted. Nearly 40,000 documents including 60 classified files were leaked during this attack.[26] The stolen documents contained information on construction technology, blueprints, weapons systems, and evaluations of ships and submarines. South Korea was not able to detect this operation immediately. In September, it was discovered that OPLAN 5015 had been leaked while investigating an unrelated cyber-attack. It contains operational procedures for the "decapitation" of the leader Kim Jong-un. It was a successor to OPLAN 5027 jointly developed by the U.S. and South Korea in the event of a resumption of hostilities on the Korean peninsula. A part of OPLAN 5027 and

OPLAN3100 had also fallen into the hands of North Koreans.[27] 2016 marks the year of increased tensions with two nuclear tests and a new round of UN sanctions against North Korea. Unsurprisingly, North Korea's offensive cyber operations became very aggressive in light of these events and increased political instability in South Korea.

These cyber-attacks highlighted the vulnerabilities of South Korea's defense systems which failed to deny access to highly classified materials including core U.S.-South Korea war response plans. However, this increasing trend appears to have somewhat abated in recent years[28] as the regime activities, at least on the surface, have focused on achieving a different objective: raising money.

The Financial Gain Attacks

In recent years, there has been increased sanctions pressure on North Korea to deter its nuclear weapons program. Consequently, North Korea has performed numerous attacks against financial institutions in 2017 and 2018, while the cyber espionage attacks have seemingly become less prominent compared to the 2013-2016 period.

- **2017** - In April, YouBit, a South Korean crypto-currency exchange was attacked. The hackers stole 3816.2028 Bitcoin (US ~$5M). In December, the same exchange was attacked again with the loss estimated at around $15.6M. It lost 17% of its assets forcing it to declare bankruptcy.[29] The hacker group called Blunenoroff, a subgroup of Lazarus specializing in financial crime which started operating in 2016, is believed to be responsible for the attacks.[30]

- **2018** - In June, South Korea's crypto-currency exchange institutions were again under attack. Coinrail lost $37M[31] while Bithumb lost $40M as a result.[32] In the aftermath of the attack on Coinrail, the bitcoin suffered a 5% devaluation. These incidents reinforced the fear of investing in an unregulated market.

North Korean cyber-attacks on financial institutions have been observed globally since 2015. For example, the attack on Vietnam's Tien Phong bank, the $81M heist on Bangladesh's Central Bank, the attack on Polish banks, the transfer of $60M from the Far Eastern International Bank in Taiwan, the attack on Turkish banks and finance agencies the latest attacks on Bancomext in Mexico and Chile's Banco de Chile are attributed to North Korea.[33] Remarkably, North Korea is also deemed responsible for the world's biggest cryptocurrency heist, worth $530 million, to the detriment of the Japanese exchange Coincheck.[34] It appears cyber thefts have become an integral part of Pyongyang's strategy as a way of survival.

No Shift in North Korea's Cyber Strategy

Although North Korea's interests in displaying its cyber capabilities have diminished, its clandestine operations have become sophisticated. As a result, the international community, influenced by the growing threat to financial institutions, often overlooked other types of attacks that Pyongyang was possibly still carrying out. There are several reports suggesting that North Korea is very much engaged in information gathering.

- FireEye, a private security firm, published a report claiming to have proved the ongoing espionage activities of hacker groups linked to the North Korean regime. Its report analyzes the activity of the group named APT37; it states that the group targets mainly South Korean firms and healthcare systems by exploiting the vulnerabilities of the Hangul World Processor (HWP). It suggests that the mission of the hacker group would be "covert intelligence gathering in support of North Korea's strategic military, political and economic interest."[35] The group conducted several attacks throughout 2017, such as the "Golden Time" campaign and the "Evil new year" campaign, the specific targets and quantitative damage inflicted are not clear, and the media coverage of those attacks remains poor.

- AlienVault, another private security firm, analyzed the ongoing offensive behaviors of North Korea. Its report states that cyber-attacks such as those occurred between April and May 2018 were executed out by the Lazarus APT Group which exploited the vulnerabilities of ActiveX, a plug-in that runs on Internet Explorer, disabled on most system abroad but still in use by most South Korean organizations.[36] The *modus operandi* of these attacks much resembles the North Korea's cyber espionage campaigns of 2017. There is no clear information available on what was leaked during the attacks. North Korea's cyber operations have become less detectable and less striking than in the past.

- The North Korean regime appears to increasingly internationalize its action in the latest operations. According to the McAfee report of 2014, North Korea is responsible for a new hidden campaign dubbed "Operation Ghost Secret," a global data reconnaissance campaign implanting malware in 17 countries' industries, including the U.S., Thailand, China, and Honk Hong. The Hidden Cobra hacker group was behind the campaign. A McAfee researcher Ryan Sherstobitoff said, "The evolution in complexity of these data-gathering implants reveals an advanced capability by an attacker that continues its development of tools."[37] No case is registered in South Korea even though it is highly unlikely that the group would avoid targeting South Korea in the future.

These latest reports indicate that North Korea has been carrying out diverse target-specific attacks while siphoning off millions of dollars into its account. There has been no discernible shift in North Korea's cyber strategy. With improving sophistication in covert cyber operations, North Korea is undoubtedly eager to keep spying on South Korean military secrets. However, it has refrained from displaying its cyber capabilities as the regime is well aware that the countermeasures have also become more sophisticated. If caught and punished, North Korea will find it increasingly difficult to bear the economic sanctions pressure.

Figure 1: Number of Major North Korean Cyber-Attacks against South Korea by Year

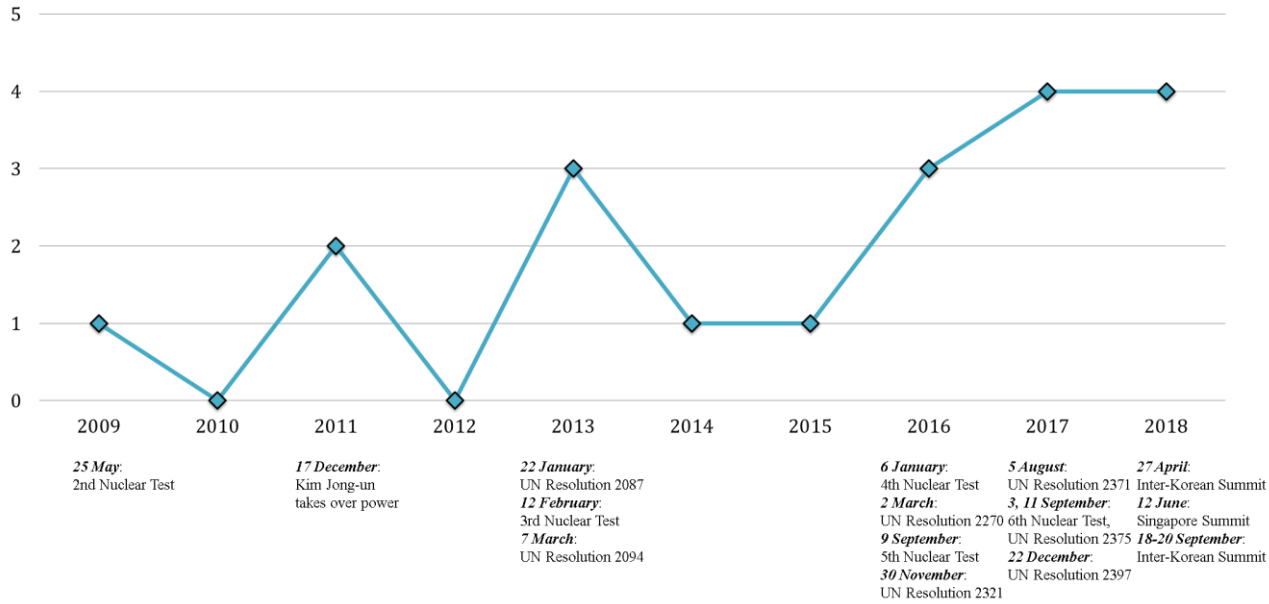

Figure 2: Percentage of Major North Korean Cyber-Attacks against South Korea by Type

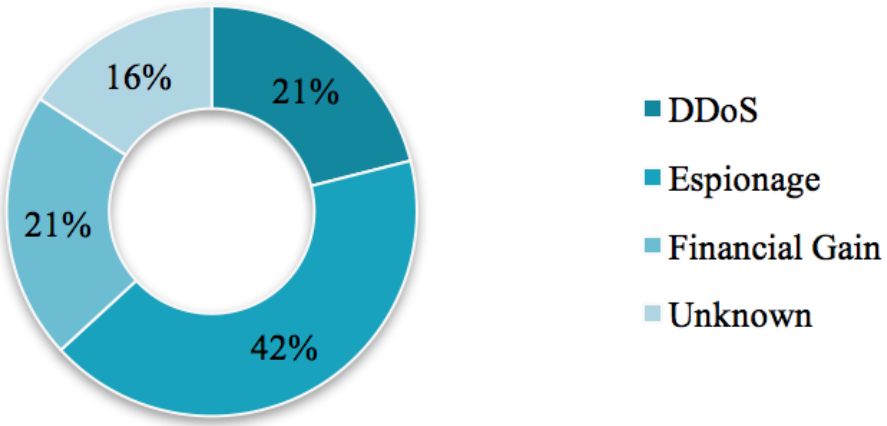

Figure 1 shows an increasing trend in the number of major North Korean cyber-attacks against South Korea over the years. In Figure 2, the percentage of major North Korean cyber-attacks against South Korea by type is shown with Espionage attacks representing the largest proportion.

Conclusions

The North Korean cyber threat is continuously evolving and adapting. Many institutions including government agencies across the world have fallen victims to cyber-attacks. Identifying patterns in past attacks and understanding the reasons for these attacks can help South Korea better prepare for the future. The latest pattern shows that North Korea's strategy is oriented towards siphoning off large amounts of money from various financial institutions. This can be possibly interpreted as a sign that North Korea is feeling the effects of sanctions. It gives all the more reasons to keep up sanction pressure until the denuclearization of North Korea is achieved. The evidence also indicates that there has been no let-up in espionage activities. The Panmunjom Declaration provides powerful incentives for North Korea to increase the number of future espionage attacks on South Korea.[38] Kim Jung-un reportedly said, "Cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."[39] How well the South Korean authorities will be able to respond to these attacks will surely depend on their level of readiness.

- Responses

In recent times, the U.S. and the U.K. have responded to cyber-attacks by explicitly naming the culprits and the organizations behind these attacks. In the U.S., Department of Justice (DOJ) has gone as far as indicting members of foreign cyber espionage units. Hitherto no country has ever brought charges against individuals acting on behalf of foreign intelligence services for malicious cyber-attacks. For instance, DOJ has specifically charged Park Jin Hyok, a North Korean national, for his involvement with multiple destructive cyber-attacks on NHS (UK), Sony Pictures, Bangladesh's Central Bank and others last September.[40] The UK's National Security Cyber Center has attributed GRU, Russia's foreign intelligence service, for cyber-attacks on the Democratic National Committee, the World Anti-Doping Agency, a UK-based TV station and the BadRabbit ransomware.[41] Attributions, indictments, calling out *'bad behavior'* and expressions of solidarity with stricken nation are some of the tools used increasingly to deter future attacks as well as alerting the home nation to be on guard.

South Korea may find further ideas in the work of various regional organizations, such as ASEAN or APEC. Further afield, the work of NATO, of which South Korea is a partner, may offer some useful lessons. NATO has made much progress in the cyber domain since NATO leaders agreed in 2014 that a cyber-attack could trigger an Article 5 response: Where an attack on one ally is treated as an attack on all allies.[42] In 2016, NATO has designated cyberspace as a domain of operations in which it must defend itself along with land, sea and air. All NATO member states made a Cyber Defence Pledge, and have all upgraded their cyber defenses ever since. Another European regional security organization, the Organization for Security Co-operation in Europe (OSCE), has been working on Confidence-Building Measures (CBMs) to reduce the risks of conflict stemming from the use of information and communication technologies.[43] Also, Tallinn Manual (v. 2.0) offers a body of expert views on the applicability of international law, and could be useful in helping officials determine the legal considerations regarding different types of cyber-attacks (e.g. do they constitute an armed attack

under Article 51 of the UN Charter?). All these developments can provide guidance and direction for South Korea's future cyber defense strategy.

- Recommendations

Specifically, South Korea must keep a close watch on espionage activities in order to correctly estimate North Korea's cyber capabilities. It must continuously adapt and build up capabilities to counter rapidly evolving cyber threats not only in the technical domain, but also through devising common responses with international partners. South Korea could also consider other levers of power - attribution; declarations; sanctions; continually calling out these attacks and their unacceptability at appropriate times to reinforce the idea that such cyber-attacks will not be tolerated. The protection of military secrets, war plans and tactics must take priority without question. As there is no such thing as a foolproof system, it is imperative to have a critical system designed to minimize the impacts of cyber infiltration from the outset. Its core functions should continue to operate even after the system has been compromised. Hence, it must be highly resilient (i.e., redundant and robust). For a system that stores important documents, there should be layers of defenses to protect these documents which must be encrypted. A loss of one document is better than ten or a hundred documents. Once the infiltration is identified, a highly capable computer emergency response team (CERT) should be able to assess, contain and remediate the damage so that the system can continue to operate. It has been noted that complex and fragmented systems all reduce South Korea's defense capabilities[44] and its response structure to cyber-attacks still lacks swiftness and efficiency.[45]

The Ministry of National Defense would not have suffered a serious security breach if it had followed the existing guidelines properly. Along with developing good policies, efforts must also go into raising awareness of cyber security and changing user behavior of government employees to ensure policies stick and are implemented properly.[46] As the proverb says, "A small leak will sink a great ship." It is also worthwhile to carry out a thorough evaluation of computer systems in use by South Korean government organizations and agencies overseen by a senior official in the administration, perhaps through creating a single high level official of cabinet rank to drive ownership and accountability for cyber issues. Addressing vulnerable systems must be prioritized according to a standardized risk approach, taking into account the nature, probability and impact of a cyber-attack to each system. They must be prioritized according to their levels of access to sensitive information. Enough resources must be allocated to carry out these tasks and to fix any vulnerabilities identified. Unfortunately, there is a tendency for people to overlook the importance of having an adequate budget for cyber security.

South Korea could benefit from establishing closer collaboration, both on a bilateral and multilateral level, with the countries which have experienced or become the victims of the North Korean cyber-attacks. Intelligence sharing can help all the parties involved to overcome their security problems by addressing each party's system weaknesses. Also, sharing the lessons South Korea has learned from its past with different countries will enhance its position in the international arena as an "issue specific" security provider. South Korea has already been active in promoting regional and international forums

on cyber security.[47] It could participate and help restart the UN Group of Government Experts process since it became stalled in 2017. Whilst South Korea is not a member of the OSCE, it could perhaps take a leadership role regionally in transporting the ideas on OSCE's CBMs to an Asian forum like ASEAN or APEC. Also, the decision-making power and capabilities of existing institutions such as the Cybersecurity Alliance for Mutual Progress (CAMP) should be strengthened. The ROK/U.S. Mutual Security Treaty could provide avenue for exploring closer cooperation on cyber security.

Finally, it is very concerning that over the last few years social media has become the latest battleground as Russia vie for influence in the US and Europe. Its alleged interference in US election and Catalonia's Independence referendum shows, social media channels provide ideal stage for influencing public opinion. South Korean social media is a fertile ground for North Korea to exploit, especially after the Panmunjom Declaration, as a way of chipping away at sanctions, widening the fault lines in the society and driving a wedge between allies. A holistic approach would necessitate a more comprehensive and updated Cyber Security Master Plan including counter-measures against manipulation of social media.

Acknowledgements

We would like to thank Ham Geon Hee and Jason Bartlett for their assistance with graphics and proofreading.

[1] This research was carried out as part of my postgraduate studies at the University of Bologna, Italy.
[2] Adam Segal, *The Hacked World Order: Elements of Cyber Power*, Council on Foreign Relations, February 23, 2016. https://www.cfr.org/blog/hacked-world-order-elements-cyber-power
[3] Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, Catherine A. Theohar, *North Korean Cyber Capabilities: In Brief*, Congressional Research Service, August 3, 2017.
[4] Timothy W. Martin, North Korea, While Professing Peace, Escalated Cyberattacks on South, The Wall Street Journal. May 25, 2018. https://www.wsj.com/articles/north-korea-while-professing-peace-escalated-cyberattacks-on-south-1527239057
[5] Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, Catherine A. Theohary, *North Korean Cyber Capabilities: In Brief*, Congressional Research Service, August 3, 2017.
[6] Due to the closed nature of DPRK society, there is a lack of direct sources on North Korea cyber strategy as well as data.
[7] Choe Sang-Hun writes: "North Korea's state-sponsored hackers are increasingly going after money rather than secrets, according to a report published on Thursday by a South Korean government-backed institute, " *North Korea Tries to Make Hacking a Profit Center*, The New York Times, July 27, 2017. https://www.nytimes.com/2017/07/27/world/asia/north-korea-hacking-cybersecurity.html
[8] *Connect the Dots on State-Sponsored Cyber Incidents*, Council of Foreign Relations. https://www.cfr.org/interactive/cyber-operations#CyberOperations
[9] North Korea's government has denied any involvement in the attacks analyzed in this paper.

[10] *South Korea government websites targeted in cyber attack*, The Guardian, March 4, 2011. https://www.theguardian.com/world/2011/mar/04/south-korea-websites-cyber-attack
[11] *South Korea Hit by Cyber Attacks*, BBC News [online], March 4, 2011. http://www.bbc.com/news/technology-12646052
[12] Kim Rahn, *NK Launched Cyber-Attack on Nonghyup*, The Korea Times, May 3, 2011. http://www.koreatimes.co.kr/www/news/nation/2011/05/117_86369.html
[13] Yoo Eun Lee, *Who was Behind South Korean Cyber-attacks?*, Aljazeera, April 1, 2013. https://www.aljazeera.com/indepth/opinion/2013/03/20133319531732780.html
[14] Jonathan A.P. Marpaung, HoonJae Lee, *Dark Seoul Cyber Attack: Could it be worse?* Proceedings of CISAK 2013 Conference May 12, 2013. http://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Dark_Seoul_Cyberattack.pdf
[15] Ibid.
[16] Choe Sang-Hun, *South Korea Blames North for June Cyberattacks*, The New York Times, July 16, 2013. https://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html
[17] Martyn Williams, *Hackers attack North, South Korean websites, North Korea Tech*, June 25, 2013.
[18] See Also: *Lazarus Arisen, Architecture/ Tools/ Attribution*, Group –IB, 2017, pp.3
[19] Ibid.
[20] Dick K. *Nanto, North Korea: Chronology of Provocations*, 1950 – 2003, Report for Congress, March 18, 2003. http://www.au.af.mil/au/awc/awcgate/crs/rl30004.pdf
[21] Dmitry Tarakanov, *The "Kimsuky" Operation: A North Korean APT?,* SecureList, September 11, 2013. https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/
[22] A keystroke logger or keylogger, is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard. See also: *What is a Keylogger?*, Kaspersky Lab. https://www.kaspersky.com/resource-center/definitions/keylogger
[23] Directory listing is a web server function that displays a list of all the files contained in the directory (also called folders, or drawers) when there is not an index file.
[24] Elizabeth Shim, South Korea considering new law to combat North Korea cyberattacks, UPI, Oct. 23, 2015. https://www.upi.com/Top_News/World-News/2015/10/23/South-Korea-considering-new-law-to-combat-North-Korea-cyberattacks/8411445623690/
[25] Paula Hancocks and K.J. Kwon, *North Korea hacked government officials' smartphones, South Korea says*, CNN, March 8, 2016. https://edition.cnn.com/2016/03/08/asia/south-korea-smartphone-hack/index.html
[26] Kanga Kong, *North Korea Hacks South Korean Warship Blueprints, Report Says*, Bloomberg, October 31, 2017. https://www.bloomberg.com/news/articles/2017-10-31/north-korea-hacks-south-korean-warship-blueprints-report-says
[27] This attack resulted in 235GB of data being stolen. To put this data in perspective, it is equivalent to ~2km of books standing side by side.
[28] It is noted that prior to the third inter-Korean summit in Pyongyang in 2018, there were attempts to steal the summit-related information by North Korean hackers.
[29] *Bitcoin exchange Youbit shuts after second hack attack*, BBC News, December 19, 2017. http://www.bbc.com/news/technology-42409815
[30] For more, please see *Lazarus under the Hood*, Kaspersky Lab, April 3, 2017.
[31] *Bitcoin tumbles as hackers hit South Korean exchange Coinrail*, Reuters, June 11, 2018. https://www.reuters.com/article/us-markets-bitcoin-korea/bitcoin-tumbles-as-hackers-hit-south-korean-exchange-coinrail-idUSKBN1J703I

[32] The perpetrators of the attack remain unspecified in most newspapers; however, BBC reported that South Korea's spy agency had held North Korea responsible for the Bithumb attack. *Bithumb: Hackers 'rob crypto-exchange of $32m*', BBC News, June 20, 2018. https://www.bbc.com/news/technology-44547250
[33] *N. Korean hackers steal hundreds of millions of dollars*, The Chosunilbo, October 4, 2018. http://english.chosun.com/site/data/html_dir/2018/10/04/2018100400891.html
[34] *South Korean intelligence says N. Korean hackers possibly behind Coincheck heist-sources*, Reuters, February 6, 2018. https://www.reuters.com/article/uk-southkorea-northkorea-cryptocurrency/south-korean-intelligence-says-n-korean-hackers-possibly-behind-coincheck-heist-sources-idUSKBN1FP2XX
[35] *APT37 (REAPER) The overlooked North Korean Actor*, FireEye Special Report, February 20, 2018.
[36] Chris Doman and Jaime Blasco, *More Details on an ActiveX Vulnerability Recently Used to Target Users in South Korea*, Alien Vault Blog, June 11, 2018. https://www.alienvault.com/blogs/labs-research/more-details-on-the-activex-vulnerability-recently-used-to-target-users-in-south-korea
[37] Ryan Sherstobitoff and Asheer Malhotra, *Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide*, McAfee, Apr 24, 2018. https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/
[38] In early October, there were attempts of a similar kind using a fake email, supposedly from a member of the National Assembly's Defense Committee. It also emerged that a similar incident took place in early 2018, but this time it appeared to be from the Blue House, South Korea's presidential office. The Dong-A Ilbo, December 12, 2018.
[39] David Sanger, David Kirkpatrick and Nicole Perlroth, The World Once Laughed at North Korean Cyberpower, No More, The New York Times, October 15, 2017.
[40] North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions, Justice News, the U.S. Department of Justice, September 6, 2018.
[41] The new weapon against Russian cyber-attacks: Naming and Shaming, ZDNet, October 4, 2018.
[42] Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, Ecole militaire, Paris. May 15, 2018.
[43] Decision No. 1202. OSCE Confidence-Building Measures to reduce the risks of conflicts stemming from the use of information and communication technologies, OSCE, March 10, 2016.
[44] Boo, Hyeong-wook, *An Assessment of North Korean Cyber Threats*, The Journal of East Asian Affairs, vol. 31, no. 1, 2017, pp. 97–117, JSTOR. www.jstor.org/stable/44321274
[45] Jeong Yoon Yang, So Jeong Kim, and Il Seok Oh (Luke), *Analysis on South Korean Cybersecurity Readiness. Regarding North Korean Cyber Capabilities*. In: Information Security Applications 17th International Workshop, WISA 2016 Jeju Island, Korea, August 25–27, 2016 Revised Selected Papers, Springer International Publishing AG, 2017. pp. 108- 109.
[46] Hackers stole the personal data of 1,000 North Korean defectors settled in South Korea from a PC at a resettlement center. This incident failed to follow the rules potentially endangering the lives of these people. https://www.telegraph.co.uk/technology/2018/12/28/hackers-stole-personal-data-1000-north-korean-defectors/
[47] It was recently reported that South Korea is considering joining the Budapest Convention on Cybercrime. The Convention, the first of its kind to combat computer crime globally, was drawn up by the Council of Europe in 2001. It currently lists 62 states parties and 10 observer states.