2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

The All-Purpose Sword: North Korea's Cyber Operations and Strategies

Ji Young, Kong
ROK Air Force First Lieutenant
Department of Information Security
Korea University, Agency for Defense Development
Seoul, Republic of Korea
jykong27@gmail.com

Kyoung Gon, Kim
Industry-University Cooperation Professor
Department of Information Security
Korea University
Seoul, Republic of Korea
anesra@gmail.com

Jong In, Lim
Professor
Department of Information Security
Korea University
Seoul, Republic of Korea
jilim76@gmail.com

Abstract: According to a 2013 briefing from the South Korean National Assembly by the South Korean National Intelligence Service, North Korean leader Kim Jong-un stated, "Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles." Kim has secretly executed all-purpose cyberattacks to achieve his agenda, regardless of North Korea's diplomatic and economic situation. The "all-purpose sword" has been adapted to the different purposes it has pursued against North Korea's adversaries, such as creating ransomware for financial gain, a cyberweapon to destroy computer systems, and an invisible espionage tool to accumulate sensitive information. This paper is divided into three parts. The first section discusses the will of North Korea to use cyber warfare for different purposes by explaining how its administrative agencies take charge of different fields but carry out cyber operations to achieve their goals. The second section describes and analyzes the interconnectivity in North Korea's suspected cyber operations: specifically, Campaign Kimsuky, Operation KHNP, Operation DarkSeoul, Operation Blockbuster, the Bangladesh Central Bank Heist, and Wannacry. The operations will be categorized by operational goals, showing North Korea's success at achieving its various purposes by these means. In the last section, we suggest a future cyber strategy direction for North Korea based on our analysis of its tactics, techniques and procedures; and how North Korea cooperates with other countries, including countermeasures for countries around the world.

Keywords: *North Korea, North Korean cyber forces, state-sponsored cyber operations, mixing tactics, techniques and procedures, cyber strategies*

1. INTRODUCTION

Kim Jong-un's interest in cyber warfare predated the start of his regime. Kim Jong-il, the former North Korean leader, perceived the advantage of having a networked military after monitoring the 1991 Gulf War, the 1999 Kosovo War, and the 2003 Iraq War (Jun, LaFoy, and Sohn 2015). Subsequently, Kim Jong-il had stressed the importance of building cyber capabilities. In the *Electronic Warfare Reference Guide* published by the Korean People's Army's Military Publishing House in 2005, he stated, "If the Internet is like a gun, cyber-attacks are like atomic bombs"; and "modern war is decided by one's conduct of electronic warfare," thus "cyber units are my detached force and backup power." (Ahn 2011) Moreover, after the Iraq War, he convened a high-level meeting and asserted:

> If warfare was about bullets and oil until now, warfare in the 21st century is about information. War is won and lost by who has greater access to the adversary's military technical information in peacetime, how effectively one can disrupt the adversary's military command and control information, and how effectively one can utilize one's own information. (Kim 2010)

Based on his father's work, Kim Jong-un, the current leader of North Korea, established and extended specific mission-oriented cyber units. Having taken a degree majoring in computer science and the military, he emphasized the importance of cyber warfare. In February 2013, he visited the cyber units of the Reconnaissance General Bureau (RGB), and proclaimed that "With intensive information and communication technology, and the brave RGB with its [cyber] warriors, we can penetrate any sanctions for the construction of a strong and prosperous nation.” (Lee 2013)

North Korea aims to develop its asymmetric military power by enlisting elite soldiers for their cyber capabilities while minimizing Internet dependency in the country. A North Korean defector who had been a high-ranking official testified that the country annually sends 50 to 60 elite soldiers abroad to study computer science, who later work as cyber attackers in the RGB and other cyber units (Han 2016). As a result, there are an estimated 6,800 trained cyberwarfare specialists in the North’s cyber units (ROK Ministry of National Defense 2018). Meanwhile, the North chooses to protectively control the Internet rather than provide open information, since Kim believes, along with China, that open information would harm his regime. Accordingly, only a few people can access and use the Internet; additionally, the North developed its own intranet in 1996, which is separate from the Internet and only accessible within its territory (Lim, Kwon, Jang, and Baek 2013).

Therefore, cyber warfare is an optimal choice for North Korea considering its costs and effects. It ensures continuous effects during peacetime and wartime, with covert and low-cost cyber operations that achieve various missions from the upper leadership of North Korea, without leaving irrefutable physical traces as conventional military forces would.

Although public interest has increased, few studies have been conducted on North Korea’s cyber capabilities and strategies due to information limitations. Lim, Kwon, Jang, and Baek (2013) analyzed the North’s cyber capabilities and proposed 10 cyber strategies, based on technical, political, and international aspects, for South Korea to counteract North Korea. Jun, LaFoy, and Shon (2015) made policy recommendations to the U.S. and the U.S.–ROK alliance after analyzing the approach of North Korea’s cyber operations, based on conventional military strategies, specific institutions within the government, and the technology and industrial base. However, these related works had limitations in considering North Korea’s cyberwarfare as extended capabilities, i.e. taking North Korea’s cooperation with third-party countries to conduct operations into account.

Ha and Maxwell (2018) suggested using case studies to explain North Korea’s capabilities and its avoidance of sustained Cyber-Enabled Economic Warfare Operations because of its primary strategic objective of prolonging the Kim regime’s survival and its desire to remain within the gray zone.[1] However, this suggestion has limited ability in emphasizing the importance of viewing cyber units under North Korea’s military command structure. Accordingly, the authors emphasize the

[1] U.S. Special Operations Command defines the “gray zone” as a realm of competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality. See U.S. Special Operations Command (2015).

significance of the Kim regime's use of cyber warfare, by evaluating North Korea's military command structure, cyber operations, and relations with other countries.

2. ORGANIZATIONS OF CYBER OPERATIONS IN NORTH KOREA

FIGURE 1. NORTH KOREA'S MILITARY COMMAND STRUCTURE (ROK MINISTRY OF NATIONAL DEFENSE 2018; JUN, LAFOY, AND SHON 2015; PARK 2018; MOK 2017B)
Remark: The dark-shaded units are directly relevant to cyber operations; the lighter-shaded units may have the potential to conduct cyber capabilities.

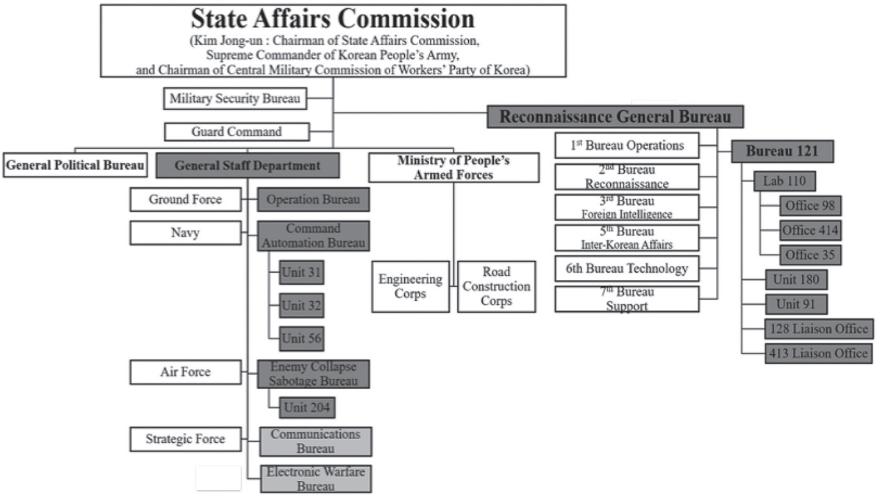


Figure 1 shows North Korea's military command structure based on the Defense White Paper of the ROK, published in December 2018. In addition, it illustrates other recent, open-source media regarding newly formed units that are relevant to cyber operations. Kim Jong-un, who serves as Chairman of the State Affairs Commission (SAC) (국무위원회 위원장), Supreme Commander of the Korean People's Army (KPA) (인민군 최고사령관), and Chairman of the Central Military Commission of the Workers' Party of Korea (WPK) (당 중앙군사위원회 위원장), maintains practical command and control over the North Korean military. As Chairman of the SAC, Kim oversees the affairs of the North Korean state and decides which policies are important to the country. As the Supreme Commander of the KPA, Kim commands the General Political Bureau (총정치국, GPB), General Staff Department (총참모부, GSD) and the Ministry of the People's Armed Forces (인민무력성, MPAF). Specifically, the

GPB oversees party organs within the military and is responsible for issues related to political ideology; while the GSD is responsible for conducting military operations; and the MPAF for administering military diplomacy, military logistics, procurement, and finance. Furthermore, as the Chairman of the Central Military Commission of the WPK, Kim deliberates and decides what measures are necessary for implementing military policy and provides guidance for overall defense affairs at a party level (ROK Ministry of National Defense 2018).

As shown in Figure 1, military units that carry out cyber operations in North Korea's military command structure are largely divided into two groups: the GSD of KPA; and the Reconnaissance General Bureau (정찰총국, RGB). This division illustrates the RGB's high degree of strategic importance. Since it is independent of the GSD and MPAF, this indicates that it acquires tasks and reports directly to the upper leadership of the SAC, Kim Jong-un, in both peacetime and wartime (Bechtol Jr. 2018).

Reconnaissance General Bureau: The RGB was formed in 2009; it is equivalent to the U.S. Directorate of National Intelligence (Madde 2018). The RGB reports directly to the SAC: it used to report directly to the senior leadership of the National Defense Commission, which was replaced by the SAC in the 2016 constitutional revision (Bechtol Jr. 2018). Since the SAC tasks the RGB with North Korea's terrorist, clandestine and illicit activities, and the RGB conducts these tasks independent of North Korea's conventional military (the KPA), previous studies have suggested that North Korea sees cyber capabilities as extending beyond military assets (Ha and Maxwell 2018, 11).

Under the RGB, Bureau 121 is the primary office tasked with disruptive cyber operations, such as infiltrating computer networks, hacking to extract foreign intelligence, and deploying viruses on adversary computer networks (Chung and Lee 2017, 21). According to the Radio Free Asia interview with Kim Heungkyang, the leader of North Korean Intellectuals Solidarity, his report. "The actual state of North Korea's Cyberwarfare Reinforcement and Counterstrategies for South Korea", submitted to the National Assembly Defense Committee of South Korea on September 30, 2016, introduced the newly formed organizations after reorganizing Bureau 121: specifically, Lab 110, Unit 180, Unit 91, 128 Liaison Office, and 413 Liaison Office (Mok 2017b).

Lab 110 is the key cyber unit under the RGB; it applies cyberattack techniques to conduct intelligence operations. The South Korean military discovered that Lab 110 was an expansion and reorganized adaptation of Unit 121 under the RGB, credited with researching computer command systems and electronic jamming in 1998 (Kim 2014). According to Park's presentation at DragonCon 2018, Lab 110 is divided into three offices according to their function. Office 98, located in Pyongyang, primarily collects information on North Korean defectors, organizations that support them, overseas research institutes related to North Korea, and university professors in South Korea. Office 414, located in Pyongyang and Shenyang, China, gathers information on overseas government agencies, public agencies, and private companies. Office 35 is in Pyongyang and concentrates on developing malware, researching and analyzing vulnerabilities, exploits, and hacking tools (Park 2018).

Unit 180 specializes in conducting cyber operations to steal foreign money from outside North Korea. Hackers in Unit 180 generally operate overseas to obscure the link between their operations and North Korea (Ha and Maxwell 2018); the state offers them every support in coming and going abroad to conduct their operations. Unit 91 focuses on cyberattack missions targeting isolated networks, particularly on South Korea's critical national infrastructure such as KHNP and the ROK Ministry of National Defense. Moreover, Unit 91 targets stealing confidential information and technology to develop weapons of mass destruction with a "super striking power," as ordered by Kim Jong-un (Mok 2017b).

The term "Liaison Office" usually denotes an office responsible for "escorting and communicating with any commando or special operations forces sent to infiltrate South Korea" in North Korea. 128 Liaison Office and 414 Liaison Office are likely responsible for maintaining communications with espionage networks in South Korea, including relaying missions and receiving reports rather than directly impacting targets using cyber capabilities. Specifically, 128 Liaison Office works on hacking foreign information intelligence websites and studies cyber strategies, while 414 Liaison Office cultivates cyber experts to conduct cyberwarfare (Jun, Lafoy, and Sohn 2015).

General Staff Department: The GSD is responsible for the operational command and operational planning of the Korean People's Army (Jun, LaFoy, and Sohn 2015). Its primary goal with cyber capabilities is to integrate emerging tools and weapons of cyber capabilities into North Korea's warfighting strategy (Park 2018). The Operations Bureau does not directly perform cyber operations but may serve an important role in making key decisions related to cyber force planning, defining and disseminating cyber strategy, and mission. The Command Automation Bureau is responsible for conducting cyberwarfare operations. Units 31, 32, and 56 are responsible for malware development, military software development, and command and control software development, respectively. The Enemy Collapse Sabotage Bureau is tasked with information and psychological warfare (Jun, LaFoy, and Sohn 2015).

3. CYBER OPERATIONS ATTRIBUTED TO NORTH KOREA

TABLE 1. CATEGORIES OF OPERATIONS BASED ON OBJECTIVES

Objectives	Cyber Operations	Period	Remarks
Information Espionage	Campaign Kimsuky	2009–2018	Variants and affiliations have been found up until 2018
	Operation KHNP	2014.12.15	Causing social chaos in South Korea
Cyber Terrorism[2]	Operation DarkSeoul	2013.3.20	The attackers shared TTPs[3] with malicious activities from 2007
	Operation BlockBuster	2014.11.24	*The Interview* movie that plotted the assassination of Kim Jong-un kindled the attack The FBI attributed this attack to North Korea
Financial Warfare	Bangladesh Central Bank Heist	2016.02.04–05	Stealing bank credentials and sending fraudulent transactions to SWIFT
	WannaCry	2017.05	Demanding a ransom for files taken hostage The FBI attributed this to North Korea

Table 1 shows the notable cyber operations attributed to North Korea, categorized into three objectives: Information Espionage, Cyber Terrorism and Financial Warfare. Although some analysts include psychological warfare to describe the objectives of cyberwarfare, this paper does not define the objectives as the goals of warfare, only as the primary goals of the operations. Accordingly, it does not include cyberattacks which aim for psychological warfare, based on the authors' determination that they did not reach the level of operations. Moreover, the objectives of operations may not be exclusive to each other, so an operation can fall in more than two categories. Therefore, this paper categorizes operations with only one primary goal for each operation.

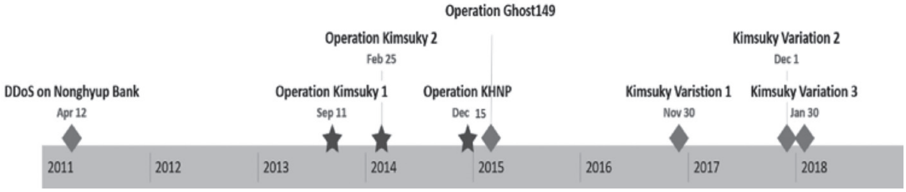
There are several recognizable state-sponsored actors in North Korea, such as: Lazarus, Bluenoroff, Hidden Cobra, Andariel, Bureau 121, APT37, ScarCruft, Reaper, Group123, DarkHotel, etc. These groups have been named by various security analysts to identify them as actors by the malware and tactics they used, which has resulted in multiple naming conventions used for specific actors. To avoid confusion arising from the various naming conventions, this paper has decided to identify the actors as a singular group executing orders from their country.

[2] NATO's definition of cyber terrorism is: "A cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal." Center of Excellence, Defence Against Terror (2008, 119).

[3] TTP, in the context of cyber threat intelligence, is short for Tactics, Techniques, and Procedures, and also sometimes referred to as Tools, Techniques, Procedures. TTPs represent the behavior or *modus operandi* of cyber adversaries.

A. Information Espionage Operations

FIGURE 2. TIMELINE OF OPERATIONS FOR INFORMATION ESPIONAGE

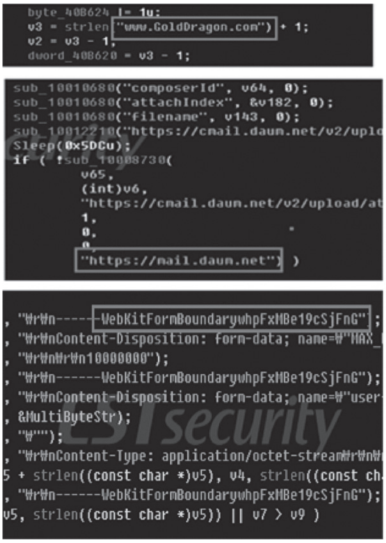


Campaign[4] Kimsuky: The first attack of Campaign Kimsuky started in Sep 11, 2013 when phishing emails that contained malicious files were sent through Belgian mail accounts. All the information collected by the malicious files was sent to two master mail accounts: iop110112@hotmail.com and rsh1213@hotmail.com, which were registered with the names “kimsukyang” and “kim asdfa,” leading to the campaign being dubbed “kimsuky” (Tarakanov 2013). The second attack of Campaign Kimsuky started on Feb 25, 2014 and more attacks were conducted on March 11, 12, 17, and 19 (AhnLab 2014).

Operation KHNP: From Dec 15, 2014, anti-hacktivists attributed to North Korean hackers calling themselves “Who am I = No Nuclear Power” started releasing information about Korea Hydro and Nuclear Power (KHNP) employees and confidential technical documents on nuclear power plants after launching cyberattacks (Security News Special Coverage Team 2014). The South Korean government concluded that Operation KHNP was a hacking incident caused by North Korean hackers with the purpose of creating social unrest in South Korea by targeting the critical national infrastructure of nuclear power plants (Seoul Central District Public Prosecutors’ Office 2015).

Links: There are ongoing espionage investigations into the affiliations of the Kimsuky malware. On Nov. 30, 2016, Dec. 1, 2017, and Jan 30, 2018, a substantial number of e-mails with malicious hwp files attached that contained variants of the Kimsuky malware were sent to specific universities and public organizations in South Korea. Some of the malicious files had an exact copy of the HwpSummaryInformation code in their shellcodes and the same creator account “MOFA,” which stands for Ministry of Foreign Affairs, an acronym strongly associated with South Korea (Alyac 2018). This means that the same attackers used the same metadata for more than a year while conducting these attacks. There is another link indicating that the same group conducted the attacks in February 2015 and on January 30, 2018 by using similar names for its C&C Server and using the same HTTP parameter to communicate with the C&C Server (Gil 2018). Figures 3 and 4 show the similar C&C Server hostnames, “mail.daum.net” and “mail-daum-net.atwebpages.com,” respectively, and the same HTTP parameter “WebKitFormBoundarywhpFxMBe19cSjFnG.”

FIGURE 3. MALWARE IN THE 2015 APT ATTACK (ALYAC 2018)

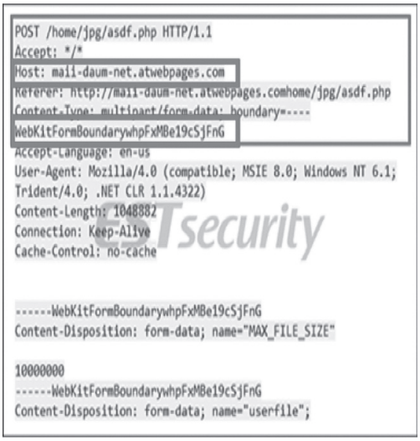


```
   byte_408624 |= 1u;
   v3 = strlen("www.GoldDragon.com") + 1;
   v2 = v3 - 1;
   dword_408620 = v3 - 1;
```

```
 sub_10010680("composerId", v64, 0);
 sub_10010680("attachIndex", &v182, 0);
 sub_10010680("filename", v143, 0);
 sub_10012210("https://cmail.daum.net/v2/uplo
 Sleep(0x5DCu);
 if ( !sub_10008730(
         v65,
         (int)v6,
         "https://cmail.daum.net/v2/upload/at
         1,
         0,
         0,
         "https://mail.daum.net") )
```

```
, "₩r₩n------WebKitFormBoundarywhpFxMBe19cSjFnG");
, "₩r₩nContent-Disposition: form-data; name=₩"MAX_
, "₩r₩n₩r₩n10000000");
, "₩r₩n------WebKitFormBoundarywhpFxMBe19cSjFnG");
, "₩r₩nContent-Disposition: form-data; name=₩"user
, &MultiByteStr);
, "₩"");
, "₩r₩nContent-Type: application/octet-stream₩r₩n₩
5 + strlen((const char *)v5), v4, strlen((const ch
, "₩r₩n------WebKitFormBoundarywhpFxMBe19cSjFnG");
v5, strlen((const char *)v5)) || v7 > v9 )
```

FIGURE 4. MALWARE IN THE 2018 APT ATTACK (GIL 2018)



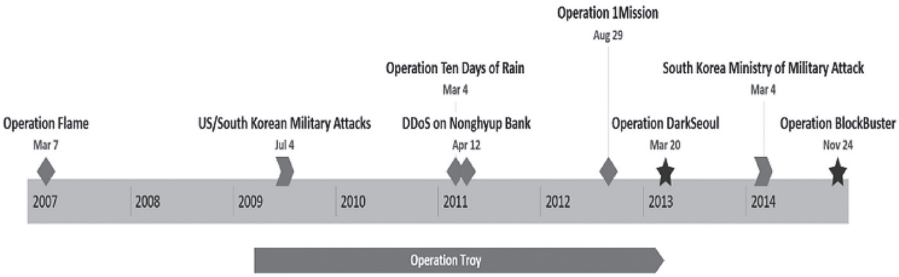
```
POST /home/jpg/asdf.php HTTP/1.1
Accept: */*
Host: mail-daum-net.atwebpages.com
Referer: http://mail-daum-net.atwebpages.comhome/jpg/asdf.php
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarywhpFxMBe19cSjFnG
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1;
Trident/4.0; .NET CLR 1.1.4322)
Content-Length: 1048882
Connection: Keep-Alive
Cache-Control: no-cache


------WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
------WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="userfile";
```

B. Cyber Terrorism Operations

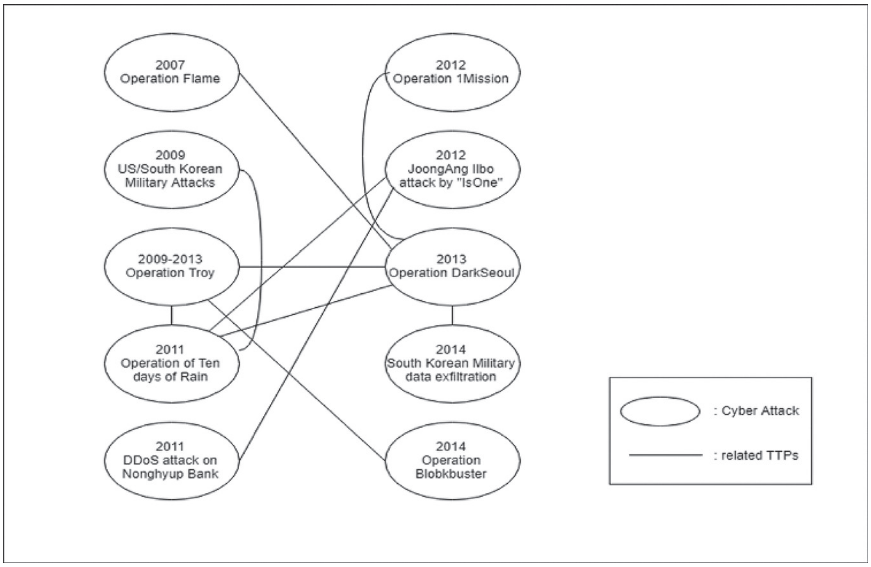
FIGURE 5. TIMELINE OF OPERATIONS FOR SYSTEM DESTRUCTION



Operation DarkSeoul: On March 20, 2013, a cyberattack paralyzed the network services of South Korean media and financial companies. The South Korean government officially announced that the attack was conducted by North Korean hackers for the following three reasons: first, it had discovered the logs that had targeted the victims, which indicated that the attackers had prepared for the operation for a long time; second, well-known IP addresses used by North Korean attackers were found in the South Korean C&C servers; third, the attackers had re-used malware from past operations, specific paths and strings used for creating malware (Kim 2013).

Operation Blockbuster: On November 24, 2014, employees of Sony Pictures Entertainment arrived at work to find their computer screens taken over by a picture of a red skeleton with a message signed "Guardians of Peace." The malware erased data stored on 3,262 of the 6,797 company's personal computers and 837 of 1,555 servers (Elkind 2015). U.S. officials believed that Operation Blockbuster was retribution for the upcoming Sony movie, *The Interview*, a comedy film that involves a plot to assassinate North Korea's leader, Kim (Bing and Lynch 2018). According to the FBI Director, James Comey, due to "mistakes" made by the North Koreans while conducting the operation, the FBI were able to find IP addresses "exclusively used by the North Koreans…several times." (Sanger, Kirkpatrick and Perlroth 2017)

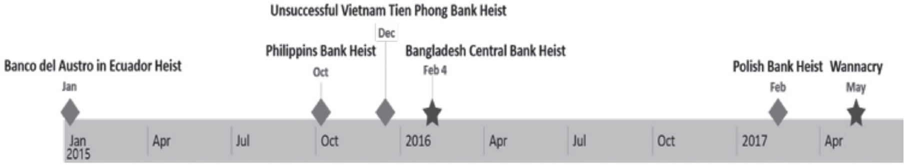
FIGURE 6. THE RELATIONSHIPS BETWEEN CYBERATTACKS IN 2007–2012 BASED ON SHARED TACTICS, TECHNIQUES, AND PROCEDURES (NOVETTA 2015; SYMANTEC SECURITY RESPONSE 2013)


2007 Operation Flame
2009 US/South Korean Military Attacks
2009-2013 Operation Troy
2011 Operation of Ten days of Rain
2011 DDoS attack on Nonghyup Bank
2012 Operation 1Mission
2012 JoongAng Ilbo attack by "IsOne"
2013 Operation DarkSeoul
2014 South Korean Military data exfiltration
2014 Operation Blobkbuster
: Cyber Attack
: related TTPs

Links: Figure 6 lists various security analyses, revealing the relationships between each cyberattack conducted in 2007–2012 based on shared Tactics, Techniques and Procedures (TTPs), which may indicate the attackers' proximity. It is notable that three attacks – Operation Troy, Ten days of Rain, and DarkSeoul – have the most shared TTPs in their malware, and all ten attacks are linked to the others with at least one shared relationship. TTPs cannot define whether attackers in the 10 attacks were from the same group or had code exchanges, but reveal the possibility of an attacking group's development as follows: Operation Flame → Operation 1Mission → Operation of Ten days of Rain → Operation Troy → Operation DarkSeoul.

C. Operations for Financial Warfare

FIGURE 7. TIMELINE OF OPERATIONS FOR FOREIGN EXCHANGE EARNING



Bangladesh Central Bank Heist: In February 2016, a cyberattack hit Bangladesh Central Bank by exploiting weaknesses in its security to infiltrate its network and steal its SWIFT credentials. The attackers used the stolen SWIFT credentials to make several fraudulent transactions – requests to the Federal Reserve Bank of New York to transfer a total of $101m of the Bangladesh bank's money to locations in the Philippines and Sri Lanka. Four requests to transfer $81m to the Philippines succeeded, but one request to transfer $20m to Sri Lanka was denied because the attackers misspelled the word "foundation" as "fandation." (Volkov 2017)

Operation WannaCry: In May 2017, WannaCry ransomware spread throughout the world via Jaku, a tool for targeted tracking and data exfiltration disguised as botnet malware (Ilascu 2018). The ransomware demanded $300 in Bitcoin per victim; however, according to London-based Elliptic Enterprises, an organization tracking illicit Bitcoin activities, very few victims of the WannaCry attack paid up: only $91,000 had been deposited in the three Bitcoin wallet accounts associated with the ransomware as of May 19, 2017 (Talmadge 2017).

Links: A series of bank heists in the timeline show TTPs related to the Bangladesh Central Bank heist. According to Symantec, researchers uncovered shared TTPs among the three bank heists at the Bangladesh Central Bank, the Philippines Bank, and the Vietnam Tien Phong Bank (Pham, Nguyen and Finkle 2016), meaning that different banks were targeted by the same group (Symantec Security Response 2016). The attackers used stolen credentials to send what looked like legitimate transfer requests to the SWIFT network and used malware after the attack to cover up the evidence of fraudulent transfers (Carter 2017).

D. Recent Attacks and Expected Future Attacks

In 2016–2018: Through human intelligence, the authors were able to gather a list of 21 cyberattacks attributed to North Korean hackers in 2016–2018. The attribution could be proved by the access logs of definitive IP addresses of North Korean attackers in Korean C&C Servers. The targets of these attacks were all located in South Korea or were North Korean defectors abroad. The data will be visualized for legibility.

FIGURE 8. CYBERATTACKS OF NORTH KOREA IN 2016–2018 CATEGORIZED BY TARGET

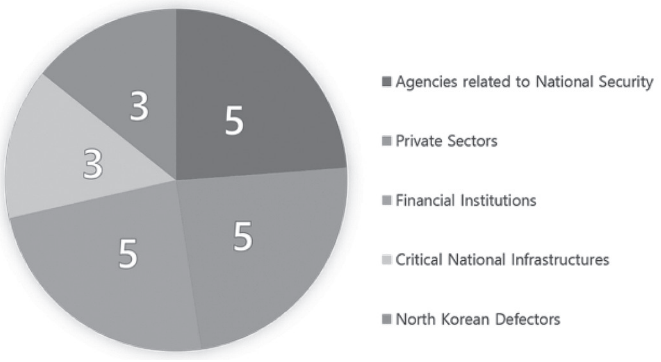
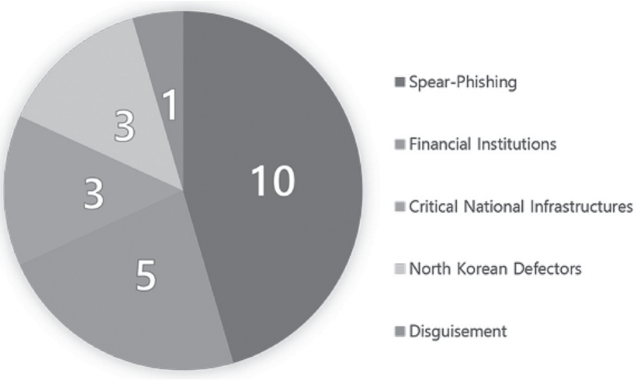


FIGURE 9. CYBERATTACKS OF NORTH KOREA IN 2016–2018 CATEGORIZED BY ATTACK VECTOR



It is noticeable in Figure 8 that a high proportion of targets were related to South Korean national security. The specific agencies related to South Korean national security are the ROK Ministry of National Defense, the National Police Agency, and Defense Industries. Critical National Infrastructure in South Korea includes airports, airplane companies, and telecommunications companies. Figure 9 shows that a spear-phishing attack is the most common attack vector used by North Korea.

Expected Future Attacks: The 2018 Defense White Paper stated that North Korea's military strategy is as follows: "During contingencies, there is a strong possibility that North Korean forces will launch surprise attacks using their asymmetric capabilities mainly to set favorable conditions to terminate the war early." North Korea will likely develop cyber operations in more strategic forms by choosing targets with careful consideration and creativity such as the recent attack on Automated Teller Machines, a blind spot that the US and South Korea have had to address directly (Ha 2018).

4. STRATEGIES

A. Overview: TTPs of North Korean Cyber Forces

Analyzing TTPs helps to highlight credential information in cyber operations and to define attackers' attributes such as attack vectors, scenarios, and identities. The followings are the features of TTPs elicited by North Korea's cyber operations: mainly attacks that targeted South Korea in 2007–2018.

Tactics: The tactics of conventional North Korean forces are analogous to the blitzkrieg military strategy: launching attacks quickly and with massive force, without giving victims time to counter it. However, the tactics of the cyber forces have become stealthy and long-term, since the cyberspace environment requires sufficient time for attackers to understand and invade their targeted information systems. (Jun, LaFoy, and Sohn 2015).

Techniques: The techniques used in North Korean cyber operations to target South Korea are comparatively sophisticated. The most common are one-day exploits and zero-day exploits of Adobe Flash, hwp files, and ActiveX programs (FireEye 2018). However, some analysts criticize the exaggerated media portrayal of these cyberattacks' technical sophistication. Ben Buchanan's report provides a rigorous framework with which to analyze the technical and operational factors of attacks; and highlights other important considerations, such as attackers' tendency to be cost-effective (so that they do not always perform technically sophisticated attacks), the choices that intruders make, tradeoffs between cost and effect, the timeliness of attacks, and barriers to entry for certain types of operation (Buchanan 2017).

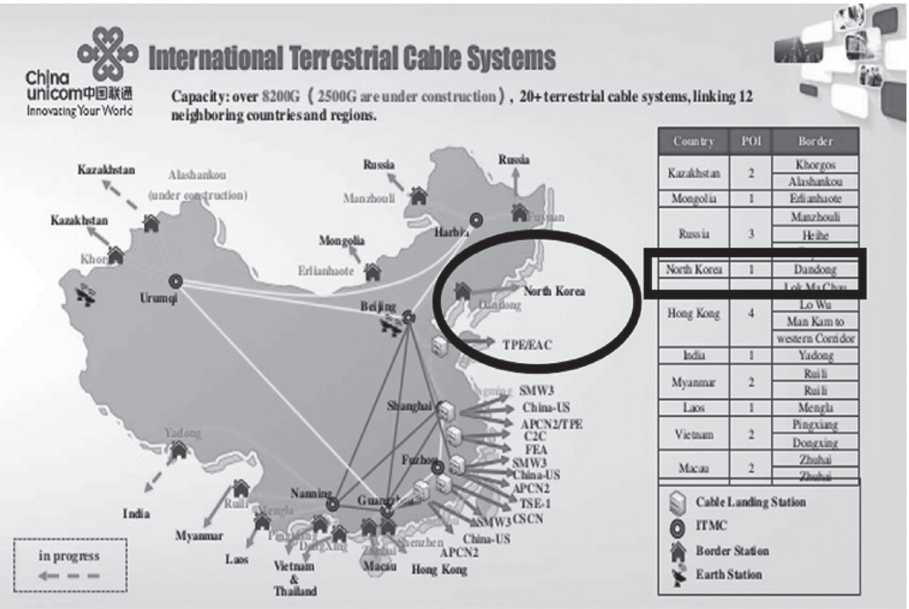
Procedures: North Korea spends a long time reconnoitering targets before attacking through highly profiled means, such as sending spear-phishing emails to infect targets' computers. Meanwhile, attackers hack websites to use them as watering-hole attack vectors or C&C servers. Once attackers have successfully penetrated the internal network of a target system by visiting the target router to the infected website, they initiate an investigation of valuable information. Obtained information is compressed and sent to the C&C server through a secure channel. Finally, the attackers destroy targets or leave bots for additional purposes (Meyers 2018).

B. The Future Military Strategy of North Korean Cyber Forces and Countermeasures

North Korea can mix its TTPs with those of other countries in two ways by sending North Korean cyber forces to third-party countries to conduct cyber operations, with or without the cooperation and consent of the host countries. By sending cyber forces to other countries, North Korea can overcome its limitations, gaining access to a continuous and stable electricity supply and avoiding any need to use North Korea-assigned IP addresses for conducting cyber operations (Sanger, Kirkpatrick and Perlroth 2017).

North Korea with China: North Korea's cyber strategy is said to imitate Chinese military doctrine. The JomHul strategy means pursuing the best result by targeting the weakest part of the enemy's information system to paralyze the whole (Lim, Kwon, Jang, and Baek 2013).

FIGURE 10. THE FIBER-OPTIC CABLE OF CHINA UNICOM LINKS DANDONG IN CHINA TO NORTH KOREA (CHINA UNICOM 2016)



International Terrestrial Cable Systems

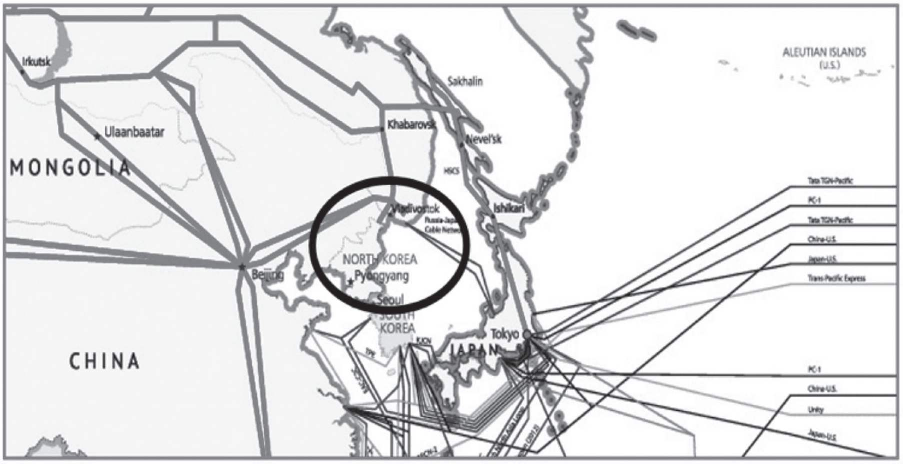
Capacity: over 8200G（2500G are under construction）, 20+ terrestrial cable systems, linking 12 neighboring countries and regions.

Country	POI	Border
Kazakhstan	2	Khorgos
		Alashankou
Mongolia	1	Erlianhaote
Russia	3	Manzhouli
		Heihe
		[illegible]
North Korea	1	Dandong
Hong Kong	4	Lok Ma Chau
		Lo Wu
		Man Kam to
		western Corridor
India	1	Yadong
Myanmar	2	Ruili
		Ruili
Laos	1	Mengla
Vietnam	2	Pingxiang
		Dongxing
Macau	2	Zhuhai
		Zhuhai

It has been consistently reported that North Korean cyber units are active in China. Defectors have verified that North Korea dispatches teams of hackers to carry out offensive cyber operations in Shenyang, China (Horowitz 2017). The U.S. Department of Justice revealed that North Korean cyber operatives such as Park Jin Hyok operate from China (U.S. Department of Justice 2018). Conducting operations under the shadow of China provides North Korean hackers with benefits in terms of attributing attackers; and even when attributed, North Korea can avoid diplomatic issues due to the jurisdiction problem. In fact, the Chinese Embassy in Washington D.C. refused to answer questions regarding whether China had supported North Korean cyber operations (Clayton 2013). This relationship is not explained by a historically trusted partnership; but rather, that the attacks conducted by North Korea do not harm China but instead help to balance power with the U.S. in Asia (Sin 2009).

North Korea with Russia: North Korea decided to expand its Internet connection to Russia after its network was paralyzed twice. The first paralysis of the North Korean network was conducted by the U.S. after Operation Blockbuster. The second network paralysis occurred for nine hours after North Korea launched an ICBM on July 29, 2017, according to BGPM (Mok 2017). As a result, TransTeleCom (TTK), one of Russia's largest telecommunications companies, started to provide the Internet to North Korea on October 1, 2017 (Williams 2017).

FIGURE 11. THE FIBER-OPTIC CABLE OF TTK LINKS VLADIVOSTOK IN RUSSIA TO THE NORTH KOREAN BORDER (WILLIAMS 2017)



The wireless network system failure during the opening ceremony of the 2018 PyeongChang Winter Olympics revealed that Russia tried to cause confusion when tracing cyberattacks by mixing its TTPs with those of North Korea (Ellen 2018; GReAT 2018).

North Korea with Iran: North Korea and Iran have had a technology-sharing treaty focused on the cyber sphere since 2012 (Stevenson 2012). Moreover, there are remarks which show that they have cooperated in sharing their TTPs and experiences on cyber warfare to prepare and conduct cyber operations. Several security analyses have indicated that Operation Shamoon, said to be Iran-backed, which hit Saudi Aramco and other oil company networks in August 2012, shared attack techniques and used the same commercially available EldoS RawDisk driver files as Operation Blockbuster (Kaspersky Lab 2014). In addition, Iran may have shared information about the uncovered Stuxnet with North Korea. According to Reuters, a U.S. intelligence official said there was a Stuxnet variation made for North Korea under the condition of only activating when it encountered Korean-language settings on an infected machine. However, due to North Korea's extremely isolated network, the malware could not successfully access the core machines that ran the North's nuclear weapons program (Noyes 2015).

North Korea with India: A report by Recorded Future concluded with confidence that there was a physical presence of North Korean cyber forces in India, by analyzing what significant cyber activity they had conducted. Their cyber activity showed that North Korean students in at least seven universities around the country might be working with several research institutes and government departments (Insikt Group 2017).

North Korea with other countries: North Korean cyber forces can be dispatched to third-party countries to conduct cyber operations without the consent of their governments. According to Recorded Future, which analyzed data on the Internet usage of North Korean cyber forces between April and July 2017, eight nations were identified in which North Koreans maintained an active physical and virtual presence: India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, Indonesia, and China (Insikt Group 2017). A follow-up report by Recorded Future analyzed data for December 2017–March 2018: and added Thailand and Bangladesh to states where North Koreans were likely living and conducting illicit revenue-generation activities (Moriuchi 2018).

Countermeasures: Overall, the above cases indicate the possibility of North Korea conducting cyber operations in cooperation with other countries to make attribution more difficult. If this is true, it may be a great potential threat to other countries around the world, as it means that a targeted country will need to prepare and counteract the cooperating countries. Moreover, even if the attack's attribution is assumed with strong intelligence, collaborating countries can deny their involvement by denying their cooperation and publicly shirking their responsibility to the other country.

To confront the threats imposed by these possible movements in cyberwarfare, a new collective defense coalition model is suggested. The model starts from countries realizing these growing cyber threats as common threats, then gathering states to develop a collective defense against them, in anticipation of this deterrence power being consolidated. NATO is an example of this, as its members built a defensive coalition against common threats.

5. CONCLUSIONS

North Korea develops military strategies by monitoring other wars. By imitating NATO's utilization of C4I Surveillance and Reconnaissance in the Kosovo War, North Korea prepared for its networked military, allowing it to garner attention worldwide for its cyber capabilities and rise as a big player in cyberspace. Despite its relatively weak infrastructure environment, North Korea realized the importance of cyber warfare within asymmetric capabilities and has gradually developed its cyber power in sequential phases.

Through its analysis of cyber units in North Korea's military command structure, this paper stresses the importance of cyber warfare by making direct connections between North Korea's upper leadership and cyber units. The cyber units are largely divided into the RGB and the GSD; the former reports directly to the upper leadership, while the latter conducts cyber operations within its conventional military capabilities. Then, by arranging cyber operations conducted by actual cyber forces, this paper analyzes various operation objectives. This confirms the North Korean leader's resolve to utilize cyber capabilities and illustrates the relationship between operations presumed to be conducted by North Korea through TTP confirmation.

To avoid being traced as an aggressor by TTPs, this paper suggests that North Korea's future strategic direction will involve mixing TTPs with other countries. Considering its limited infrastructure, it is very likely that TTPs will move to and operate in third-party countries. There are two methods through which this can be fulfilled. One involves conducting operations based on preset coordination through diplomatic, political, and military channels, while the other involves dispatching cyber forces and conducting operations without the target country's acknowledgment. Expected future cyber threats from North Korea will be harder to identify; they will grow more sophisticated by continuing and expanding their efforts with third-party countries. As the attacks are apparently conducted by collaborating nations, the target country will face limitations in its ability to protect itself. This paper therefore proposes a defensive coalition model to respond to the growing common cyber threats imposed by North Korea and those countries it cooperates with.

REFERENCES

Ahn, Yonghyun. 2011. "North Korea's Electonic Warfare Capability." *ChosunIlbo*, March 7, 2011. http://news.chosun.com/site/data/html_dir/2011/03/07/2011030702345.html.

AhnLab. 2014. "APT Attack - New 'Kimsuky' malware emerged." *ASEC Threat Research & Responding Blog*, March 19, 2014. http://asec.ahnlab.com/993.

Alyac. 2018. "Operation Kimsuky's secret activities, Korea customized APT attack is currently in progress." *ESTsecurity Alyac Blog*, Feb 12, 2018. http://blog.alyac.co.kr/1536.

Bechtol Jr., Bruce E. 2018. *North Korean Military Proliferation in The Middle East and Africa*. Kentucky: The University Press of Kentucky.

Buchanan, Ben. 2017. *The Legend of Sophistication in Cyber Operations*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Bing, Christopher and Lynch, Sarah. 2018. "U.S. charges North Korean hacker in Sony, WannaCry cyberattacks." *Reuters*, Sep 6, 2018. https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W.

Carter, William. 2017. "Forces Shaping the Cyber Threat Landscape for Financial Institutions." *SWIFT Institute Working Paper*, No.2016-004 (October).

Center of Excellence Defence Against Terror. 2008. *Responses to Cyber Terrorism (NATO Science for Peace and Security)*, 199. Texas: IOS Press.

China Unicom. 2016. "China Unicom Global Brief Introduction." Published on Sep 21, 2016 at *Slideshare*, Slide 9. https://www.slideshare.net/AbhijitDatey/china-unicom-global-profile.

Chung, Kuyoun and Lee, Kitae. 2017. *Advancement of Science and Technology and North Korea's Asymmetric Threat: Rise of cyberwarfare and unmanned aerial vehicle*. Seoul: Korea Institute for National Unification.

Clayton, Mark. 2013. "In cyber arms race, North Korea emerging as a power, not a pushover." *The Christian Science Monitor*, Oct 19, 2013. https://www.csmonitor.com/World/Security-Watch/2013/1019 /In-cyberarms-race-North-Korea-emerging-as-a-power-not-a-pushover.

Elkind, Peter. 2015. "Part 1: Who was manning the ramparts at Sony Pictures?" *Fortune*, Jun 25, 2015. http://fortune.com/sony-hack-part-1.

Ellen, Nakashima. 2018. "Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say." *The Washington Post*, Feb 24, 2018. https://www.washingtonpost.com/world/ national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.e4c57176 51a3.

FireEye. 2018. "APT37 (Reaper): The overlooked North Korean actor." *FireEye*, Feb 20, 2018. https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html.

Gil, Mingwon. 2018. "Korea Customized APT Attack of Kim Soo-ki Hacking Organization... Still." *Dailysecu*, Feb 13, 2018. https://www.dailysecu.com/?mod=news&act=articleView&idxno=30007.

GReAT. 2018. "OlympicDestroyer is here to trick the industry." *Kaspersky Lab*, March 8, 2018. https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295.

Ha, Mathew. 2018. "North Korea's cyber threats are serious, the network of RGB should be disabled." Interview by No Jungmin. Radio Free Asia, Sep 17, 2018. Audio, 5:47. https://www.rfa.org/korean/ in_focus/news_indepth/ne-jn-11162018162726.html.

Ha, Mathew and Maxwell, David. 2018. *Kim Jong Un's 'All-Purpose Sword' North Korean Cyber-Enabled Economic Warfare*. Washington, DC: FDD Press.

Han, Sangmi. 2016. "North Korea sends 50 to 60 talented students to study abroad to train as cyber agents." *Voice of America*, June 14, 2016. https://www.voakorea.com/a/3375411.html.

Horowitz, Josh. 2017. "Researchers have found an unexpected axis of North Korea's cyber activity: India." *Quartz*, Oct 22, 2017. https://qz.com/1105149/india-is-an-unexpected-axis-of-north-koreas-suspect-cyber-activity.

Ilascu, Ionut. 2018. "A First Look at the North Korean Malware Family Tree." *Bleepingcomputer*, August 9, 2018. https://www.bleepingcomputer.com/news/security/a-first-look-at-the-north-korean-malware-fam ily-tree.

Insikt Group. 2017. "North Korea Cyber Activity." *Recorded Future*, July 25, 2017. https://go.Recordedfutu re.com/hubfs/reports/north-korea-activity.pdf.

Jun, LaFoy, and Sohn. 2015. *North Korea's Cyber Operations: Strategy and responses*. Maryland: Rowman & Littlefield. CSIS Reports.

Kaspersky Lab. 2014. "Sony Sony/Destover: Mystery North Korean actor's destructive and past network activity." *Kaspersky Lab*, Dec 4, 2014. https://securelist.com/destover/67985.

Kim, Heungkwang. 2010. "Responses and Strategies against North Korea's Cyber Information Warfare." *North Korea Intellectuals Solidarity*, July 2, 2010. http://www.nkis.kr/board.php?board=nkisb501&page =1&sort=hit&command=body&no=3.

Kim, Kyungae. 2013. "Detailed explanation of government announcement of 3.20 cyber terrorism case." *Boan News*, April 12, 2013. https://www.boannews.com/media/view.asp?idx=35649.

Kim, Seungju. 2014. "North Korea's cyber-attack, and our response." *Monthly North Korea*, no. 516 (December): 66-71.

Lee, Yongsu. 2013. "Kim Jong-un, 'with brave cyber warriors, we can penetrate any sanctions.'" *ChosunIlbo*, April 8, 2013. http://news.chosun.com/site/data/html_dir/2013/04/08/2013040800165.html.

Lim, Kwon, Jang, and Baek. 2013. "North Korea's Cyber War Capability and South Korea's National Counterstrategy." *The Quarterly Journal of Defense Policy Studies*, 29th Issue 4 Winter 2013(Article 102)

Madde, Michael. 2018. "Kim Yong Chol, A Biography." *38 North*, May 29, 2018. https://www.38north.org/2018/05/mmadden052918.

Meyers, Adam. 2018. "Negotiations with North Korea may have Cyber Consequences." *38 North*, MARCH 13, 2018. https://www.38north.org/2018/03/ameyers031318.

Mok, Yongjae. 2017. "After ICBM provocation, North Korea Internet 9 hours paralysis." *RFA*, Jul 31, 2017. https://www.rfa.org/korean/in_focus/nk_nuclear_talks/internetdown-07312017092147.html.

Mok, Yongjae. 2017b. "6 Cyber Units were built after Kim Jong-un regime." *RFA*, Nov 22, 2017. https:// www.rfa.org/korean/in_focus/news_indepth/ne-jn-11162018162726.html.

Moriuchi, Priscilla. 2018. "North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny." *Recorded Future*, April 25, 2018. https://www.recordedfuture.com/north-korea-internet-behavior.

Novetta. 2015. "Operation Blockbuster: Unraveling the Long Thread of the Sony Attack." *Novetta*, Feb 5, 2015. https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Rep ort.pdf.

Noyes, Katherine. 2015. "The NSA reportedly tried - but failed - in Stuxnet strike against North Korea." *IDC News Service*, Jun 1, 2015. https://www.computerworlduk.com/security/nsa-reportedly-tried-failed-use-stuxnet-variant-against-north-korea-3613758.

Oxford Dictionary. n.d. “Campaign.” Accessed March 26, 2019. https://en.oxforddictionaries.com/definition/campaign.

Park, Moonbeom. 2018. “Let’s learn about enemy through various IoCs of real APT cases.” In *DragonCon 2018*, Dec 8, 2018. Dragon Threat Labs.

Pham, Nguyen and Finkle. 2016. “Vietnam bank says interrupted cyber heist using SWIFT messaging.” *Reuters*, May 15, 2016. https://www.reuters.com/article/us-vietnam-cybercrime/vietnam-bank-says-interrupted-cyber-heist-using-swift-messaging-idUSKCN0Y60EN.

ROK Ministry of National Defense. 2018. “2018 Defense White Paper.” Seoul: ROK Ministry of National Defense.

Sanger, Kirkpatrick and Perlroth. 2017. “The World Once Laughed at North Korean Cyberpower. No More.” *The New York Times*, Oct 15, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

Security News Special Coverage Team. 2014. “KHNP, staff information leaked to technical data.” *BoanNews*, Dec 14, 2014. https://www.boannews.com/media/view.asp?idx=44734.

Seoul Central District Public Prosecutors’ Office. 2015. “Intermediate investigation result of KHNP cyber terrorism case.” *Supreme Prosecutors’ Office*, March 16, 2015. http://www.spo.go.kr/spo/notice/press/press.jsp?mode=view&board_no=2&article_no=593028.

Sin, Steve S. 2009. “Cyber Threat posed by North Korea and China to South Korea and US Forces Korea.” *Defense and Technology*, 364 (2009): 28-33.

Stevenson, Alastair. 2012. “Iran and North Korea sign technology treaty to combat hostile malware.” *V3*, Sep 3, 2012. https://www.v3.co.uk/v3-uk/news/2202493/iran-and-north-korea-sign-technology-treaty-to-combat-hostile-malware.

Symantec Security Response. 2013. “Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War.” *Symantec Official Blog*, Jun 26, 2013. https://www.symantec.com/ connect/blogs/four-years-darkseoul-cyberattacks-against-south-kore a-continue-anniversary-korean-war.

Symantec Security Response. 2016. “SWIFT attackers’ malware linked to more financial attacks.” *Symantec*, May 26, 2016. https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-finan cial-attacks.

Talmadge, Eric. 2017. “Experts question North Korea role in WannaCry cyberattack.” *AP News*, May 20, 2017. https://www.apnews.com/ed3298eaaff84e8ebb091cbbd4bc4ab6.

Tarakanov, Dmitry. 2013. “The ‘Kimsuky’ Operation: A North Korean APT?” *Securelist*, Sep 11, 2013. https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915.

U.S. Department of Justice. 2018. “North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyberattacks and Intrusions.” Press Release, Sep 6, 2018. https://www.justice.gov/usao-cdca/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyberattacks.

U.S. Special Operations Command. 2015. “White Paper: The Gray Zone.” *USSOCOM*, Sep 9, 2015. https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

Volkov, Dmitry. 2017. “Lazarus Arisen: Architecture, Techniques and Attribution.” *Group IB*, May 30, 2017. https://www.group-ib.com/blog/lazarus.

Williams, Martyn. 2017. “Russia Provides New Internet Connection to North Korea.” *38 North*, Oct 1, 2017. https://www.38north.org/2017/10/mwilliams100117.