NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FINDING EFFECTIVE RESPONSES AGAINST CYBER ATTACKS FOR DIVIDED NATIONS

by

Ji Min Park

December 2015

Thesis Advisor: Neil C. Rowe
Second Reader: Wade L. Huntley

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE FINDING EFFECTIVE RESPONSES AGAINST CYBER ATTACKS FOR DIVIDED NATIONS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ji Min Park			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

There can be hostile relations between nations that are divided politically or ideologically, and there are threats in cyberspace as well as physical space. Although every cyber threat, like a physical threat, has countermeasures, this can be hard because of the complexity of cyberspace and the ethics in cyberspace.

This study tries to find effective countermeasures for South Korea in cyberspace against North Korea's continuing cyber attacks in light of the Korean peninsula's situation, a typical example of divided nations in the world. To find good solutions, South and North Korea's cyber capabilities are compared in terms of infrastructure, organization, defensive capabilities, offensive capabilities, and vulnerabilities. Characteristics and features of North Korea's cyber attacks are inferred by analyses of past attacks. Based on these analyses, this study recommends defensive and offensive countermeasures to mitigate these cyber threats and prevent escalation. Each countermeasure is assessed using considerations such as prevention of escalation, efficient use of limited resources, international laws and ethics, and bargaining power in the real world.

14. SUBJECT TERMS cyberwarfare, South Korea, North Korea, cyber attacks			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

FINDING EFFECTIVE RESPONSES AGAINST CYBER ATTACKS FOR DIVIDED NATIONS

Ji Min Park
Captain, Republic of Korea Air Force
B.E., Republic of Korea Air Force Academy, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2015

Approved by: Neil C. Rowe
Thesis Advisor

Wade L. Huntley
Second Reader

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There can be hostile relations between nations that are divided politically or ideologically, and there are threats in cyberspace as well as physical space. Although every cyber threat, like a physical threat, has countermeasures, this can be hard because of the complexity of cyberspace and the ethics in cyberspace.

This study tries to find effective countermeasures for South Korea in cyberspace against North Korea's continuing cyber attacks in light of the Korean peninsula's situation, a typical example of divided nations in the world. To find good solutions, South and North Korea's cyber capabilities are compared in terms of infrastructure, organization, defensive capabilities, offensive capabilities, and vulnerabilities. Characteristics and features of North Korea's cyber attacks are inferred by analyses of past attacks. Based on these analyses, this study recommends defensive and offensive countermeasures to mitigate these cyber threats and prevent escalation. Each countermeasure is assessed using considerations such as prevention of escalation, efficient use of limited resources, international laws and ethics, and bargaining power in the real world.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAA	Anti-Air Artillery
ACC	Area Control Center
ADD	Agency for Defense Development
AFCCS	Air Force Command and Control System
AOC	Air Operation Center
APCERT	Asia Pacific Computer Emergency Response Team
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AS	Autonomous System
ATCIS	Army Tactical Command Information System
BBC	British Broadcasting Corporation
C2	Command and Control
CCRA	Common Criteria Recognition Arrangement
ccTLD	Country Code Top-Level Domain
CEH	Certified Ethical Hacker
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
C-I-A	Confidentiality-Integrity- Availability
CIC	Central Inspection Committee
CNO	Computer Network Operation
COIC	Combat Operation Intelligence Center
CONCERT	Consortium of Computer Emergency Response Team
CPC	Central Party Committee
CRC	Control and Reporting Center
CSTEC	Cyber Security Training and Exercise Center
CSTIA	Central Science and Technology Information Agency
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DOD	Department of Defense
DOJ	Department of Justice

DoS	Denial of Service
DSC	Defense Security Command
ETRI	Electronics and Telecommunications Research Institute
EW	Early Warning
FIRST	Forum of Incident Response and Security Teams
FBI	Federal Bureau of Investigation
GSD	General Staff Department
HP	Hewlett-Packard
HQ	Head Quarter
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
ICS	Industrial Control System
IFF	Identify-Friend-or-Foe
INFOCON	Information Operations Condition
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
ITSCC	Information Technology Security Certification Center
IUE	Institute of Unification Education
JCS	Joint Chiefs of Staff
KCSA	Korea Convergence Security Association
KIDA	Korea Institute of Defense Analyses
KIISC	Korea Institute of Information Security and Cryptology
KISA	Korea Internet and Security Agency
KISC	Korea Internet Security Center
KHNP	Korea Hydro and Nuclear Power Co., Ltd
KISIS	Knowledge Information Security Industry Support Center
KJCCS	Korea Joint Command and Control System
K-NBTC	Korea National Biometric Test Center
KNCCS	Korea Naval Command and Control System
KOPA	Korea Online Privacy Association
KPA	Korean People’s Army

KR	Key Resolve
KrCERT/CC	Korea Computer Emergency Team Coordination Center
LTE	Long Term Evolution
MAC	Media Access Control
MCRC	Master Control and Reporting Center
MEI	Ministry of Electronics Industry
MND	Ministry of National Defense
MOU	Ministry of Unification
MPS	Ministry of People's Security
MPT	Ministry of Posts and Telecommunications
MSIP	Ministry of Science, ICT and Future Planning
MSS	Ministry of State Security
NDC	National Defense Committee
NIS	National Intelligence Service
NISA	National Information Security Agency
NPT	Nuclear Non-Proliferation Treaty
OCO	Offensive Cyber Operations
OS	Operating System
PC	Personal Computer
RFI	Remote File Inclusion
RGB	Reconnaissance General Bureau
ROK	Republic of Korea
ROKA	Republic of Korea Army
ROKAF	Republic of Korea Air Force
ROKS	Republic of Korea Ship
RTDS	Real-Time Track Display System
SAM	Surface to Air Missile
SCADA	Supervisory Control And Data Acquisition
SSAC	Security Stability Advisory Committee
SSD	State Security Department
SQL	Structured Query Language
TROKA	Third Republic of Korea Army

UFD	Unified Front Department
UFL	Ulchi Focus Lens
URL	Uniform Resource Locator
WMD	Weapons of Mass Destruction
WPK	Worker’s Party of Korea

ACKNOWLEDGMENTS

I would like to thank my wife, Mi Yoo, for the unconditional love and support she has shown during my time at the Naval Postgraduate School. I would also like to thank my advisor, Dr. Rowe, as this work would not have been possible without his contributions, helpful feedback, and guidance throughout the thesis learning process. In addition, I would like to thank Dr. Huntley for his insightful comments and assistance with this paper.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Due to advances in computer science and Internet technology, people are enjoying the advantages of a high level of information sharing and effective work. In spite of these advantages, cyber threats that threaten cyber tools and systems are increasing. There are many kinds of cyber threats, including cyber crimes and cyber attacks. Cyber criminals are trying to steal personal information and achieve financial gains by spam and phishing. Cyber attackers are also influencing international relationships, as in the cyber attacks against the Estonian government and financial institutions in 2007, the Russia-Georgia cyberwarfare in 2008, and the Stuxnet attacks against Iranian nuclear facilities in 2010 (Chae, 2013). Recently, there was what appeared to be a state-run cyber attack against Sony Pictures Entertainment related to the film *The Interview* that depicted the assassination of North Korean leadership (Federal Bureau of Investigation [FBI] National Press Office, 2014).

Cyberwarfare is not limited in physical location and time as conventional warfare is, and cyber attacks can be conducted relatively cheaply by anyone because of the proliferation of technologies and information (Schelling, 1966). If a state has continuing hostile relations with another state, the cyber threat can be increased. In the Korean peninsula, the two Koreas divided by ideological issues and a war have this kind of hostile relationship. After the armistice agreement of the Korean War in 1953, North Korea expressed their strong desire of the unification, and they conducted many provocations, such as the Blue House Raid, an unsuccessful attempt by North Korean commandos to assassinate the president of South Korea in 1968, and the Republic of Korea Ship (ROKS) Cheonan sinking and bombardment of Yeonpyeong Island in 2011.

Since the 2000s, because of proliferation of the Internet globally and development of information technology, North Korean provocations are changing. In the past they distributed leaflets and broadcast propaganda to the South as psychological warfare. Now they conduct “psychological operations” on the Internet (Hewlett-Packard [HP] Security

Research, 2014). Cyber attacks against South Korean websites are also increasing. There were more than 70,000 attacks against South Korean government sites from 2008 to 2012 (Chae, 2013). Among these, significant attacks such as a malware infection on government computers in 2004 and Distributed Denial of Service (DDoS) attacks in 2009, were attributed to North Korea. North Korea has attacked not only government organizations but also private companies (HP Security Research, 2014).

The North Korean provocations attempt to express their political will and attempt to create a favorable environment for negotiation. They follow a plan with these provocations. North Korean official media first makes critical statements, then conducts cyber attacks, and then possibly conducts armed provocations. In 2008, when the South Korean administration changed from President Roh to Lee, North Korea intensified both their criticisms and attacks. In 2009, they conducted extensive DDoS attacks on South Korea and the United States. After six months, they did a demonstrative tank maneuver training using names of places in South Korea in January 2011. In the same month, the North Korean National Defense Committee (NDC) announced that they would start a retaliatory war against the Republic of Korea (ROK)-U.S. alliance, and they conducted a field artillery firing exercise toward the Northern Limit Line (NLL) that is the border in the West Sea between South and North Korea. In February 2011, the North Korean State Security Department (SSD) stated that they would take a step against South Korea's subversion attempts and seized South Korea's properties in Mount Kumkang Tourist Region. Finally, they carried out a torpedo attack against the ship ROKS Cheonan (Ahn, 2011).

If South Korea could plan good responses to North Korean cyber attacks, North Korea might stop their provocations before they escalate. Proper defensive and offensive countermeasures to cyber provocations can help reduce threats and prevent needless damages and sacrifices. However, it is important to find effective responses in cyberspace, which has different features than conventional space.

North Korea appears to be trying to build asymmetric forces instead of conventional capabilities because they have financial difficulties (Institute of Unification Education [IUE], 2014). Asymmetric capabilities are those addressing not their own

weaknesses, such as replacement of old aircraft, but the strengthening of offensive war potential toward adversaries' weaknesses by adding nuclear weapons, ballistic missiles, special forces, long-range artillery, and submarines. Since South Korea depends more on cyberspace, North Korean cyber capabilities are asymmetric. As a result, it is important for South Korea and the United States to prepare good responses in cyberspace.

B. GOAL AND PURPOSE

Current South Korean responses to cyber attacks have been limited to economic and diplomatic sanctions with little beyond that (K. Choi, 2011). The goal of this thesis is to find better responses in cyberspace to reduce future cyber attacks. Responses in cyberspace include defensive and offensive countermeasures. Defensive countermeasures include not only barriers to block and negate the adversary's attacks, such as powerful firewall systems, but also resilience that maintains operability of assets under attacks with fast restorations and tolerances. Offensive countermeasures should let the adversary recognize that the potential damage on their side would be much bigger than the benefits of their future cyber attacks. Delivering this message is important for cyber counterattacks because it is very easy to escalate cyberwarfare (Woods, 2015). Ordinary democratic states that follow international laws, such as South Korea and the United States, cannot conduct indiscriminate cyber attacks like North Korea's, but they can find offensive countermeasure that could be acceptable to the international society. We explore that here.

With more than 80% of the population using the Internet, South Korea has the twelfth highest number of Internet users in the world, and the society enjoys a high level of information technology (Ministry of Science, ICT, and Future Planning [MSIP] & Korea Internet and Security Agency [KISA], 2014). Nevertheless, little planning of the proper responses against cyber attacks in cyberspace has been done in South Korea. This thesis investigates effective responses in cyberspace to the uncommon condition of a nation divided by ideological differences.

C. OUTLINE

This thesis has five chapters. Chapter II discusses general definitions related to cyberwarfare and techniques. Chapter III studies the cyber capabilities of the two divided nations in the Korean peninsula that is the background of this thesis. For each the chapter summarizes cyber infrastructures, organizations, defensive and offensive capabilities, and vulnerability analyses. In addition, Chapter III analyzes past cyber attacks that were attributed to North Korea against South Korea. Chapter IV recommends effective responses for South Korea with considerations, limitations, and scenario analyses. Finally, the thesis concludes with a summary and future works in Chapter V.

II. CONCEPTS OF CYBERWARFARE

A. CYBERSPACE, CYBERWARFARE, AND CYBER COERCION

According to Joint Publication 3–12(R) of U.S. Department of Defense (DOD) Division of Cyberspace Operations, cyberspace is one of the five warfare domains, the others being air, land, marine, and space (Joint Chiefs of Staff, 2013). Cyberspace consists of computers and digital devices. Similar to air operations that depend on bases, cyber operations depend on infrastructures of physical domains. In addition, cyberspace consists of multiple overlapped networks which connect globally.

Activities in cyberspace can have big effects with relatively cheap costs due to proliferation and standardization of technologies (H. Yoon, 2012). Furthermore, because cyberspace is a virtual space that is not limited by physical locations and time zones, there are no front lines or boundaries: Any area could be vulnerable to cyber attacks and targeted without any physical limitation. However, cyberwarfare, like nuclear or conventional warfare, can be conducted with layered defenses or offenses (Flemming, 2014), so it is possible to coerce adversaries by cyber actions during the escalation of hostile levels.

B. RELATIONSHIP BETWEEN REAL-WORLD NEGOTIATIONS AND CYBER ACTIVITIES

Cyber responses can prompt an agreement to cease a cyber conflict between two states. Compensation for losses can then be discussed at the bargaining table. For these reasons, we should consider the effects of cyber activities on real-world negotiations.

Pillar suggests how to use military capabilities for negotiations (Pillar, 1983). Many of these considerations can be applied to cyberspace. First, we should use cyberspace operations to change our bargaining stance if we can. Second, we should convince the enemy that they would incur more costs without peace agreements. For cyberwarfare, we should prepare defensive responses to minimize damage to us from the adversary's cyber attacks and show that our offensive capabilities that could incur high damages for the adversary. Third, we should use a level of force that suggests that there

are further counterattacks available to an adversary's continued hostile acts. Finally, during negotiation, we should refrain from further escalation to show the adversary the advantages of stopping their attacks. Another consideration is that, as in past negotiations between South and North Korea (Ko, 2009), the amount of information and intelligence available about the attacks has important effects on the bargaining table. If a country prepares enough information related to its adversary's cyber capabilities, it could gain an advantage.

C. TECHNIQUES OF CYBERWARFARE

Just as there are many kinds of weapon systems and techniques in traditional warfare, there are also many kinds of attack techniques in cyberspace.

Cyber security consists of confidentiality, integrity, and availability (C-I-A). Confidentiality means the ability of a system to ensure that an asset is viewed only by authorized parties. Integrity is the ability of a system to ensure that an asset is modified only by authorized people. Availability is the ability of a system to ensure that an asset can be used by any authorized parties (Pfleeger & Pfleeger, 2012). Cyberwarfare can be considered activities that attack at least one component of the C-I-A triad. For example, a distributed denial-of-service (DDoS) attack creates excessive traffic to exhaust a target system's resources, such as computing power or memory. During this attack, the target system cannot provide normal service, which hurts availability (Patrikakis, Masikos, & Zouraraki, 2004).

1. Types of Frequent Attacks on South Korea

According to analysis by the Korea Internet and Security Agency (KISA), the most frequent cyber attacks reported in South Korea are spreading malicious code from Web pages, defacement of Web pages, DDoS, and phishing (Yoo & Yoo, 2014).

Spreading malicious code from Web pages is an attempt to infect users of the target server. The attacker uses various methods to penetrate the server and implant malicious code, including Remote File Inclusion (RFI) and Structured Query Language (SQL) injection. Regular inspections of vulnerabilities and timely applications of update

patches are important to mitigate this kind of attack. Note that malicious code can exist in links or advertisements instead of content created by the Web page owners or administrators.

Defacement of Web pages changes the content of Web pages for propaganda purposes. Such attacks indicate the intentions of attackers and show off an attacker's capabilities in addition to delivering the propaganda.

A DDoS attack usually generates many packets and much traffic by using botnets. When a service is under DDoS attack, unusual patterns of repeated traffic are often seen. Therefore, analysis of current abnormal packets provides a good start for mitigation.

Phishing is the use of fake sites to steal personal information by enticing users through the impersonation of others, such as patronized businesses, acquaintances, or celebrities. This kind of attack is often used for bank fraud by criminals.

2. Types of Attacks Categorized by Certified Ethical Hackers

A Certified Ethical Hacker (CEH) is a computer-security expert who uses hacking technologies for legitimate purposes. According to the CEH's criteria, a cyber attack on a system can be an Operating System (OS) attack, a misconfiguration attack, an application-level attack, or a shrink-wrap-code attack (EC-Council, 2013). All these methods try to exploit vulnerabilities of systems to gain unauthorized access. Then attackers can exploit specific protocol implementations, attack the built-in authorization system, break the security of the file system, or crack passwords and the encryption mechanism.

For an OS attack, attackers find vulnerabilities in design, installation, and settings of an OS and exploit these vulnerabilities to gain access. A misconfiguration attack attacks a misconfigured system. These misconfigurations can cause illegal accesses to Web servers, application platforms, databases, and networks. System administrators should check configurations and remove unnecessary service and software to reduce these threats.

An application-level attack involves the attacker gaining unauthorized access by exploiting vulnerabilities of running applications and manipulating or stealing data. If applications do not check for errors sufficiently, application-level attacks such as buffer-overflow attacks, cross-site scripting, session hijacking, man-in-the-middle attacks, DoS attacks, and SQL injection attacks are possible. Lastly, a shrink-wrap code attack exploits vulnerabilities of off-the-shelf library and codes.

3. Types of Network Attacks

Today, most computer devices are connected to the Internet or other networks, and cyber attacks are often conducted through networks. Network-based cyber attacks can be categorized as DoS attacks, DDoS attacks, sniffing attacks, spoofing attacks, and session-hijacking attacks (Eom, Jung, Han, & Park, 2009).

DoS and DDoS attacks were mentioned previously; both are attacks against availability. Sniffing attacks get information by collecting traffic in transmission. They can be divided into media access control (MAC) flooding, domain-name service (DNS) flooding, address-resolution protocol (ARP) poisoning, dynamic host configuration protocol (DHCP) attacks, password sniffing, and others (EC-Council, 2013)

Spoofing attacks impersonate unique identifiers used in transmitting data, such as Internet Protocol (IP) or MAC addresses. Spoofing can be helpful in concealing the country of origin of an attack. Session hijacking means that the attackers interpose themselves between two communicating hosts and take control of their sessions.

III. CYBER CAPABILITIES IN THE KOREAN PENINSULA

In the Korean Peninsula, two divided countries since the Korean War confront each other militarily. South and North Korea are continuing in a conflict state, and, according to the statistics, North Korea violated the armistice agreement 221 times and carried out 26 military attacks from 1953 to 2011 (Shin, 2011).

North Korea builds up asymmetric war capabilities instead of conventional forces to overcome an inferiority of military power. They are ignoring international opinion and focusing on weapons of mass destruction such as nuclear weapons, missiles, chemical weapons, and biological weapons. Furthermore, with the lessons from the Gulf War and Iraq War, they have also been increasing their special forces as an asymmetric power since the 1990s. Recently, there are many indications that North Korea is preparing the "fourth generation warfare" by establishing cyberwarfare units and developing cyber-provocation capabilities against South Korea (Institute of Unification Education [IUE], 2014). More than 70,000 cyber attacks have been conducted against South Korean government Websites, and many significant attacks, including the large-scale DDoS attack in 2009, have been attributed to North Korea (Chae, 2013).

In this situation, it is helpful to survey infrastructures, organizations, defensive capabilities, offensive capabilities, and vulnerabilities in detail. Research on infrastructure and organizations can show each country's overall capabilities, and vulnerabilities can be analyzed by defensive and offensive capabilities. Vulnerabilities of the adversary can be considered for targeting procedures and finding proper responses, and our vulnerabilities can influence our defensive postures.

A. NORTH KOREA

As North Korea is one of the most closed countries in the world, information about it is relatively scarce. In addition, because their citizens and media are strongly controlled by the North Korean government, it is very hard to find the precise facts of their situation. Although many of people outside of North Korea use personal devices such as personal computers and smart phones, North Koreans are strictly limited in

obtaining those devices and connecting to the Internet. This also makes it harder to get information about the North Korean people. Moreover, it is not easy to estimate current conditions. Although information from ROK and U.S. government agencies are more reliable, most of them do not provide detailed information because of security concerns. We summarize here what we do know about North Korean cyber infrastructure, organizations, capabilities, and vulnerabilities based on recent research.

1. Infrastructure

Most analysis of North Korea's cyberwarfare focuses on North Korea's cyber strategy and policy proposals, although there are a few analyses of infrastructure in detail. The Cyber Defense Research Center at Korea University conducted a study to analyze North Korea's cyber capabilities from the viewpoints of infrastructure, investments, systems, education and training, research and development, doctrine, strategy, and tactics (Lim, Kwan, Chang, & Baek, 2013). According to this study, the most distinctive feature of North Korea's cyber infrastructure is the separation of the local networks from networks for the Internet. North Korea regards the Internet as a very useful tool, but it also can be a great threat to the North Korean government. In 1996, North Korea constructed the domestic intranets "Kwangmyong (bright)" for citizens, "Bulguengom (red sword)" for the Ministry of People's Security (MPS), "Bangpae (shield)" for the Ministry of State Security (MSS), and "Kuembyol (gold star)" for the military. The unclassified intranet "Kwangmyong" connects 3,700 organizations and its estimated users are 50,000. To connect to the Internet, optical-fiber cables link from Dandong, China, to Sinuiju, North Korea, and they use Chinese IP addresses. Use of the Internet in North Korea is strictly controlled by the North Korean government, and users are estimated to be only hundreds of high-ranked officials. Furthermore, because they have an electrical power shortage, operating hours are limited.

A U.S. research institute, the Korea Economic Institute of America, noted that North Korea's cyberspace is evolving now although it is limited (Mansourov, 2014). For example, it was significant progress when they opened six official Websites to the public. North Korea has installed millions of devices that were imported from China over the

past few years, and local networks are steadily expanding. Their networks are based on Linux, and the “Kwangmyong” intranet is operated through 2.5GB backbone optical-fiber cables. There is reported to be a PC café in which people can use email services and do Web surfing in their intranet. Cellular networks are provided by Koryo Link, a joint venture between the Egyptian company Orascom and the North Korean Ministry of Posts and Telecommunications. The cellular network provides 3G-network cellphone service, and the number of users is estimated at 2.5 million, 10% of the population. General users cannot access the Internet now; however, according to the executive chairman of Google, it is easy to connect to the Internet from the North Korean cellular network (Mansourov, 2014). Some high-ranking officials use a North Korean smartphone “Arirang” which connects to their intranet Websites. North Korea has one additional security layer on the Internet because they connect to the Internet via China.

HP Security Research made a more detailed analysis of North Korea’s cyber infrastructure (HP Security Research, 2014) that confirmed that there are two separate networks. The OS in North Korean networks is “Bulguenbyol (red star)” that was developed based on Linux in 2002. It includes software packages developed by North Korea, including “Naenara (my country),” a Web browser based on Firefox. No limitations and controls are imposed to use this OS, but purchases of computer devices are strictly controlled by the North Korean government. The North Korean government can monitor the usage of devices and networks easily with this OS.

North Korea’s owned IP block is 175.45.176.0/22, and the North Korean Ministry of Posts and Telecommunications is registered as 210.52.109.0/24 in China Unicom. The autonomous system (AS) number of North Korea is AS1312179, and its only peer is China Unicom AS4837. The country code Top-Level Domain is .kp, and they have three name servers, ns1.kptc.kp, ns2.kptc.kp, and ns3.kptc.kp. As for related equipment production, North Korea does some hardware and software development because of the required technologies. However, they have difficulties doing so because of their lack of modern production facilities and reliable electricity. They appear to develop their own software, but hardware is dependent on China because of international sanctions and the problem of production infrastructure. Despite this limited infrastructure, their footprints

in cyberspace are being identified more frequently. Table 1 summarizes North Korea's cyber infrastructure.

Table 1. Summary of Infrastructure

	Characteristics
Internet	Strictly restricted. Connected via China.
Intranet	Separated from the Internet. Domestic use only.
OS	Self-developed OS "Bulguenbyol (red star)" based on Linux. Easy to monitor users.
Software	Developed in North Korea. Based on Linux.
Hardware	Limited production. Depends on imports from China.
Cellular	3G network without Internet access. Smart phones can access the intranet.

2. Organizations

Despite their limitations in software and hardware, North Korea has tried to expand offensive cyberwarfare organizations since the 1980s. The National Defense Commission (NDC) has established several cyberwarfare organizations under the Reconnaissance General Bureau (RGB) and the General Staff Department (GSD; Cho, 2013). The RGB manages Unit 121, which is in charge of hacking, cyberwarfare, cyber espionage, and virus dissemination. Other organizations under RGB are the No. 91 Office

(a hacker unit), the No. 31 and No. 32 Offices (cyber psychological-operations units), the Investigation Office (a hacking organization targeting political, economic, and social organizations), the Technical Reconnaissance Team (a hacking organization targeting military and strategy organizations), and Lab 110. GSD, which commands military forces, has two cyberwarfare organizations. One is the Command Automation Bureau, which controls the No. 21 Office that develops hacking programs, the No. 32 Office that develops military software, and the No. 56 Office that develops command and control software. Another is the Enemy Attack Bureau, which commands the No. 204 Office that is in charge of cyber psychological operations against South Korean military.

There are additional cyberwarfare organizations besides those (Lim et al., 2013). The Unified Front Department (UFD) in the Worker's Party of Korea (WPK) controls an Operations Department that conducts psychological operations aimed at the South Korean people with conventional and cyber means, and the No. 225 Office in the UFD has charge of development and installation of cyber hiding places, issuance of spy directives, and communication by cyberspace. Cyberwarfare units are also in the front corps (K. Yoon, 2011). Each has a battalion-size cyberwarfare unit in charge of cyber defense. Unit 121 conducts operations and trainings in China or other countries where it is easier to access the Internet than in North Korea. The Command Automation Bureau in the GSD controls two brigade-level units, and each unit consists of approximately 600 people. There is an independent cyber command in the Korean People's Army, though it is not on the same level as the Air Force, Navy, Army, or Strategic Rocket Commands (Mansourov, 2014).

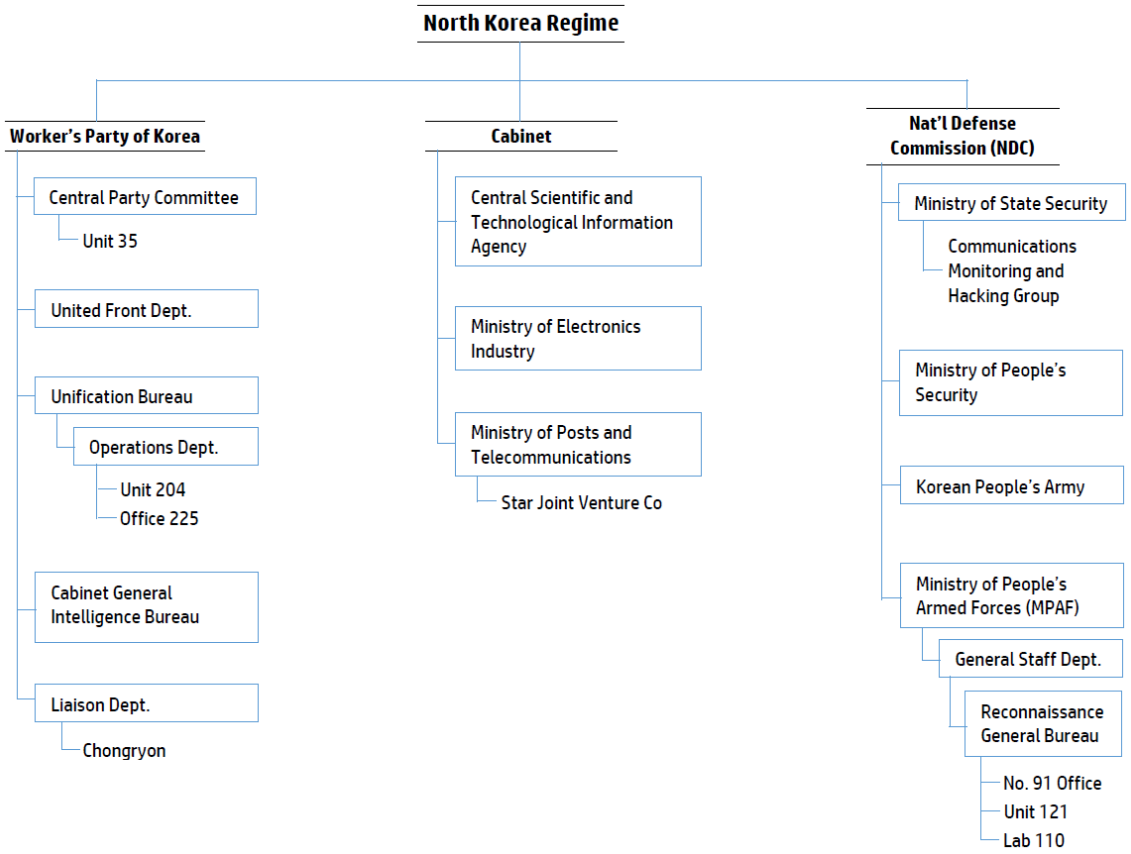
The three larger organizations in North Korea concerned with cyberspace are the NDC, the WPK, and the Cabinet (HP Security Research, 2014). The NDC is the most powerful organization in North Korea, and the first chairman is Kim Jung-un, who is the dictator of North Korea. The NDC is made up of the MSS, the MPS, the Ministry of People's Armed Forces (MPAF), and the KPA. As an intelligence agency, the MSS is in charge of counterintelligence and has a subordinate unit for communications monitoring and hacking. The MPS is in charge of the domestic public peace, so it is not related to cyberwarfare. The MPAF supervises the KPA and the GSD, and the GSD controls the

military operations of the KPA and supervises the RGB. The RGB is in charge of secret operations and conducts those operations with both conventional and cyber means; it controls the No. 91 Office, Unit 121, and Lab 110 as cyber-warfare organizations. The No. 91 Office conducts hacking operations from North Korea, Unit 121 carries out hacking missions from foreign countries such as China, and Lab 110 maintains technical teams.

Another large organization, the WPK, is the dominating political group in North Korea. It consists of the Central Party Committee (CPC), the UFD, the Unification Bureau, the Cabinet General Intelligence Bureau, the Liaison Department, and others. The CPC supervises the Central Party Investigative Group, known as Unit 35, and Unit 35 is in charge of the training and education of cyber warriors. The Operations Department of the Unification Bureau manages cyber psychological operations and espionage and supervises Unit 204 and the No. 225 Office. Unit 204 is in charge of the planning of cyber psychological operations, and the No. 225 Office manages conventional spy activities instead of cyber espionage. The UDF takes charge of conventional propaganda to South Korea. The Liaison Department does not have any cyber-related subordinate organizations. However, it supervises Chongryon, a pro-North Korean organization in Japan, and acquires resources and information through Chongryon.

Finally, the Cabinet is an administrative organization in charge of domestic affairs. It controls the Central Science and Technology Information Agency (CSTIA), the Ministry of Electronics Industry (MEI), the Ministry of Posts and Telecommunications (MPT), and others. The CSTIA is the biggest technology facility in North Korea, and it is in charge of collection and analysis of advanced technologies. The MPT supervises communication industries in North Korea. Figure 1 gives the North Korean cyber and intelligence organizational chart from HP Security Research.

Figure 1. North Korean Cyber and Intelligence Organizational Chart



Source: (HP Security Research, 2014). *Profiling an enigma: The mystery of North Korea's cyber threat landscape* (HP Security Briefing Episode 16). Retrieved from http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf

North Korea's cyberwarfare is conducted by the NDC's and the WPK's subordinate organizations. The Cabinet is far from cyberwarfare. As each study was researched at different times and there are several translational mistakes in studies from the United States, there is some lack of clarity about cyber capabilities. For this reason, it will be helpful to refer to the official organization analysis of North Korean leadership by the South Korean Ministry of Unification (MOU; MOU, 2014).

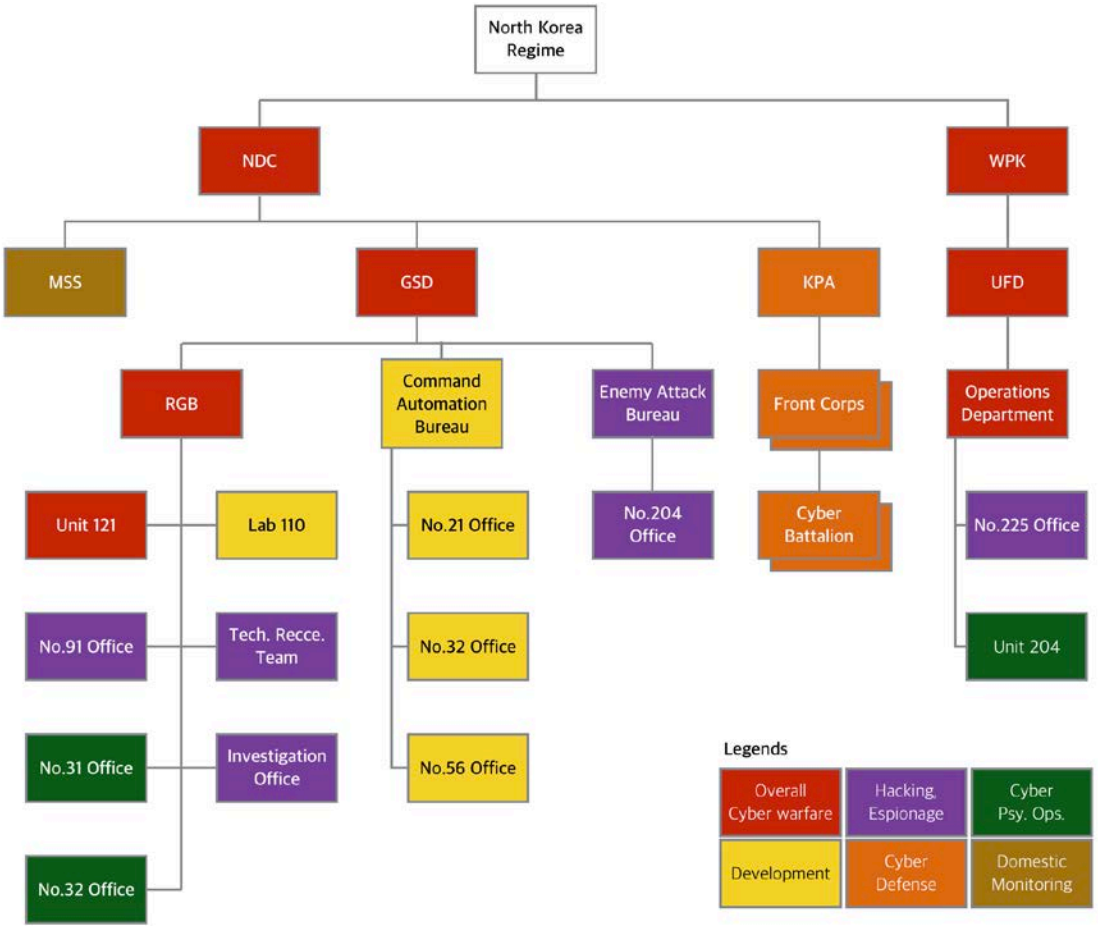
The cyberwarfare organizations in the NDC are considered to be under the control of the GSD. The GSD is described as the subordinate organization of the MPAF, but the MOU claims that the GSD commands military forces at large and oversees military

operations and training, and the MPAF carries out all activities and affairs related to munitions, equipment, construction, military diplomacy, and civil defense, which means they are equal-level organizations (MOU, 2014). There is no cyberwarfare organization under the MPAF. According to the MOU's studies of North Korea's cyber organizations, the RGB is the most important organization, and it is subordinate to the GSD. Many studies said there are a Unit 121, a No. 91 Office, a No. 31 Office, a No. 32 Office, a Lab 110, and others. As cyber footprints, including their cyber attacks, are increasing, these subordinate organizations and their functions are expanding. Although the Command Automation Bureau and Enemy Attack Bureau in the GSD take charge of cyber-related missions, the RGB and its subordinates are more responsible for cyberwarfare. Since the MSS tracks down and handles spies and dissidents within the KPA and prevents espionage, it focuses on domestic cyber monitoring more than overseeing cyber attacks.

In the WPK's case, the UFD can be considered the most relevant organization to cyberwarfare. Although HP Security Research described it as concentrating on conventional means and the Unification Bureau as more responsible for cyber operations, no organization named the Unification Bureau exists in official documents of North Korean organizations. But apparently there is an Operations Department under a Unification Bureau, and the Operations Department is subordinate to the UFD, which could be a translational mistake. It is reasonable to think that the cyberwarfare organization in the WPK is the Operations Department of the WFD. In addition, the Central Party Investigative Group that is in charge of cyber-warrior training and education in the WPK also does not exist in the official analysis, and this can be a translational error of the Central Inspection Committee (CIC; WPK, 2010). According to the WPK Charter, the CIC is a monitoring agency in charge of the eradication of dissidents in the WPK.

As a result, North Korea's cyberwarfare organizations can be best described in Figure 2. This chart is based on the analysis discussed previously.

Figure 2. North Korean Cyber and Intelligence Organizational Chart



3. Defensive Capabilities

Lim and other researchers of Korea University analyzed North Korea's defensive capabilities based on past cyber attacks against North Korea (Lim et al., 2013). All attacks against North Korea were attacks against their external Websites, which are for propaganda, and not against intranets such as Kwangmyeong. Propaganda Websites such as www.Uriminzokkiri.com have been attacked by users of www.dcinside.com, a South Korean community portal site, in 2011 and by Anonymous in 2013, but the damage was temporary denial of services or defacement (H. Jung, 2011). North Korea's outside sites are easy to attack because there are not many users and the servers are relatively small. Outside propaganda sites contain only public content, which means a high level of

defense is not required; (Lim et al., 2013) assumed North Korean intranets are well-defended by network separation and isolation.

Another study analyzed North Korea's self-developed OS, Red Star, as an important feature of their cyber defense (Cho, 2013). Most North Korean computers are using Red Star, and it is not very vulnerable to attack because it is not a common OS in the world compared to Microsoft Windows. However, since this OS is based on open-source Linux software, it is still vulnerable to Linux attacks such as DDoS, backdoors, and packet inspection (M. Lee, 2011). Leakage of information is not very useful from these sites anyway because the North Korean government has separated their military and other important intranet from it (Mansourov, 2014).

4. Offensive Capabilities

North Korea is one of the countries, along with China and Russia, that is using cyberspace most aggressively (Hong, 2011). The Agency for Defense Development in South Korea pointed out that the level of North Korean hackers compares with that of the CIA (Jung, S., 2013). However, there are different assessments (Singer & Freidman, 2014). One interview claims that North Korea's cyber attacks against South Korea are not significant and are exaggerated (Danchev, 2012). Another assessment claims that North Korea's cyber capabilities are ranked second after Russia, with offensive capabilities ranked as sixth and cyber intelligence ranked as seventh (Coleman, 2010) as shown in Table 2.

Table 2. World's Top 10 Cyber Capable Countries in 2009

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

Source: Coleman, K. (2010). The weaponry and strategies of digital conflict. *Proceedings of the 5th International Conference on Information Warfare and Security* (p. 498). Wright-Patterson Air Force Base, OH: Air Force Institute of Technology.

North Korea's offensive cyber operations (OCO) and computer network operations (CNO) capabilities became apparent as early as 2004 when North Korea gained access to 33 of 80 wireless communication networks of the Republic of Korea military (HP Security Research, 2014). North Korea is reported to be developing hacking technologies to paralyze the alliance's network, extort military secrets, and spread computer viruses (Mansourov, 2014). North Korea uses cyberwarfare training simulation software and gathers intelligence widely by using phishing and spyware to target high-ranking officials. Also, the South Korean National Intelligence Service (NIS) has estimated that North Korea has developed offensive cyber capabilities to take over power-supply systems in South Korea (Kshetri, 2014).

5. Vulnerabilities

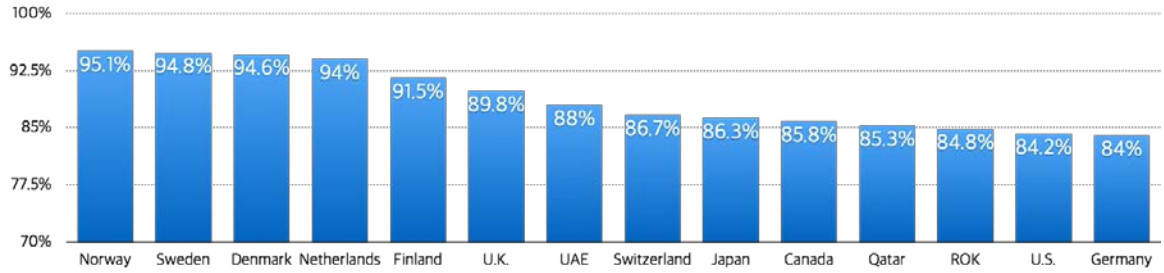
The North Korean infrastructure does not have enough electricity for cyber operations, and the attacks directly from North Korea are easy to attribute because they have few IP addresses (Lim et al., 2013). So North Korea overcomes these limitations by going through China, and usually organized attacks are launched from outside of North Korea. However, many media reports indicate that the relationship between China and North Korea has cooled (Oh, 2015), and China opposed North Korea's nuclear program indirectly (Chae, 2015).

North Korea does have certain disadvantages in cyberspace that can be exploited. Since there are no voluntary hacker groups in North Korea because the North Korean government strongly controls all networks, all cyber attacks from North Korea can be attributed to the North Korean government (HP Security Research, 2014). Because of economic sanctions due to their nuclear program and lack of production infrastructure, North Korea has difficulty in acquiring technologies and devices for developing their cyber capabilities. In addition, devices from China can be imported with vulnerabilities, which means that North Korean networks cannot be completely secured even though their intranets are air-gapped.

B. SOUTH KOREA

According to statistics from the International Telecommunication Union (ITU), South Korea has the 12th highest number of Internet users in the world, which means that the country has a high dependency on the Internet as well as high Internet availability (MSIP & KISA, 2014). This is shown in Figure 3. According to the MSIP, 98% of businesses in South Korea with more than 10 employees are connected to the Internet, and 86.7% of employees are using the Internet for business. In addition, most citizens have smart phones. This wide connectivity has many risks such as cyber crimes and cyber attacks.

Figure 3. Internet Usage by Country



Source: (MSIP & KISA, 2014). *Korea Internet white paper 2014* (GPRN 11-B551505-000008-10). Seoul, Republic of Korea: Myeong-jin C&P, p. 497.

1. Infrastructure

South Korea is connected to the Internet via nine international undersea fiber-optic cables in eight areas, and the cables provide a 27 Tbps connection (MSIP & KISA, 2014). The country operates three communication satellites that aid Internet connections. Individual users can access the Internet via not only a wired connection up to 1 Gbps, but also by 4G LTE connections with smart phones. In 2014, South Korea had approximately 122 million IPv4 addresses, which is the 6th highest rank in the world, and had 1,018 Autonomous System (AS) numbers as the 13th rank. In contrast to that, North Korea has only a few IP blocks and one AS number. South Korea's Country Code Top Level Domain (ccTLD) is .kr, and more than 110 million domains are registered. The national Domain Name Service (DNS) consists of 15 sites, and the average daily query total of it is about 1.6 billion.

South Korea keeps many external networks, and Internet services are provided by a number of Internet Service Providers (ISPs) instead of by the government. Though North Korea operates only one OS, South Korea uses a variety of OSes, including Windows, OS X, and Linux. However, as most government organizations provide Windows-friendly Web pages and applications, the majority of people are using Windows. In the case of software, South Korea uses many applications from various companies, such as Microsoft Office or Adobe Photoshop. However, many South Koreans prefer to use domestic word processors and domestic anti-virus software. Furthermore, due the policy of favoring domestic software manufactures, government

organizations tend to use domestic products. In the case of hardware, many domestic and imported products are being used together, and most foreign devices are imported for technical or price competitiveness. In contrast with North Korea, there are no limitations on imports or production.

Although South Korea also manages intranets, these intranets are operated in a limited way for special purposes by major organizations and military units, and there are no intranets like North Korea's intranet.

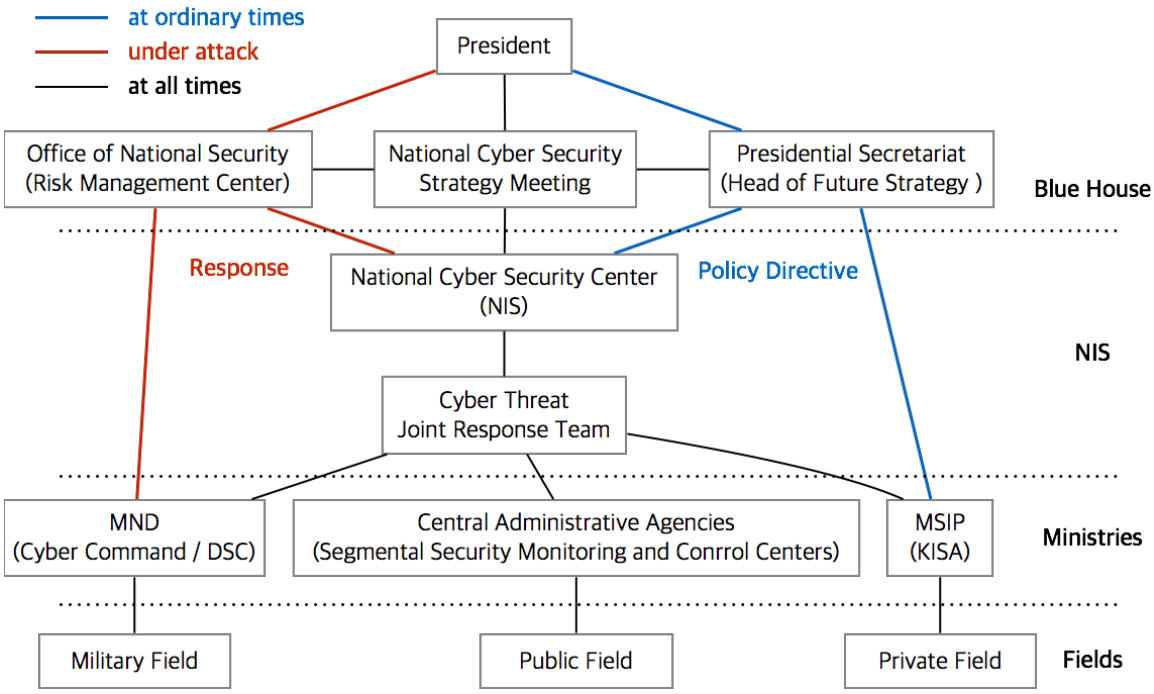
2. Organizations

In contrast with South Korea's advanced Internet environment, organizations for cyberwarfare and cyber security were created relatively late in South Korea. A triggering event for South Korean cyber organization was the extensive DDoS attack from North Korea in 2009 (K. Choi, 2011). Before the attack, the only cyber-related organizations in the military were Computer Emergency Response Teams (CERTs) for each military branch and the Defense Security Command (DSC) and the National Defense Information Warfare Response Center, both of which were focused on defensive operations. After the attack in 2009, a number of weaknesses of the current cyber organizations were identified, and in 2011, South Korea formed a Cyber Command that is in charge of cyberwarfare.

The National Defense Cyber C2 Center in Cyber Command shares information with National Risk Management Center in the executive office of the president of the Republic of Korea (the Blue House) and collects reports from subordinate CERTs (K. Choi, 2012). The establishment of the Korea Computer Emergency Team Coordination Center (KrCERT/CC) in KISA, the National Cyber Security Center in NIS, and the Information Warfare Response Center in MND in 2003 were the first steps towards South Korean cyber organizations (H. Yoon, 2012). The South Korea National Police Agency has formed offices of cyber investigation nationally, and they are in charge of personal information leakage, online illegal pornography, gambling sites, Internet frauds, cyber smears, and digital copyright infringement. Yoon argued that attacks in cyberspace are harder to classify than in the real world because the targets are varied, such as states, the private sectors, and military units, and each cyber organization responds differently to

each category of event, such as cyberwarfare or cyber crime, and this procedure makes coordinated responses difficult. The Blue House, which is the highest national organization in South Korea, acts as an overall manager of cyber security, and the National Intelligence Service (NIS) manages working-level businesses, including coordination of joint-response actions between the private, government, and military sectors (NIS, 2015). These organizations are shown in Figure 4.

Figure 4. South Korea National Cyber Security Organizational Chart



Source: National Intelligence Service (NIS), 2015. National Information Security White Paper 2015. Retrieved from http://isis.kisa.or.kr/ebook/ebook2.html

The Office of National Security in the Blue House does situation reports on cyber crisis and directs responding acts when under attack, and the Head of Future Strategy establishes laws, systems, and policies as a control tower in peace times. The NIS manages the National Cyber Security Center, which has responsibility for the prevention of national and public cyber attacks, cyber investigations, and cyber-threat analyses. The National Cyber Security Center in the NIS operates the Joint Response Team, which

combines forces with various agencies in different fields. The Ministry of National Defense (MND) has the DSC and the Cyber Command for cyber operations, and is in charge of prevention of and response to cyber threats, including defense, fulfillment of cyber operations, and development of technologies related to cyberwarfare. The MSIP has responsibility for cyber security in the private sector, including monitoring abnormal symptoms in domestic cyberspace and malware interdiction. For cyber security in the public sector, each central agency operates segmental security monitoring and control centers. The Korea Communications Commission and Personal Information Protection Commission formulate policies for personal-information protection in cyberspace, the Ministry of Government Administration and Home Affairs manages information security of electronic government, and the Financial Services Commission sets policies for electronic-banking security.

There are several specialized institutions and agencies for cyber security in South Korea, such as the Korea Internet and Society Agency (KISA), the National Security Research Institute (NSR), the Electronics and Telecommunications Research Institute (ETRI), and the Financial Security Institute. KISA has several subordinate organizations. The Korea Internet Security Center (KISC) is in charge of computer-security incident-information sharing. The KISA Academy is an educational facility to train experts. The Knowledge Information Security Industry Support Center (KISIS) supports the development of cyber-security technologies. In addition, there are subordinates such as the Korea National Biometric Test Center (K-NBTC), the Illegal Spam Response Center, and the Phishing Response Center. The NSR manages the Security Monitoring and Control Technical Support Center for domestic-research-institute networks, the Cyber Security Training and Exercise Center (CSTEC), and the Information Technology Security Certification Center (ITSCC). The ITSCC is responsible for security certification based on the criteria of the Common Criteria Recognition Arrangement (CCRA). The ETRI is the research facility for core technologies in the private sector, and it manages the Cyber Security Research Center, which is in charge of research on cyber-security technologies, including digital cryptography and cyber-security system

technologies such as network-security technologies and mobile-security solutions. The Financial Security Institute focuses on security technologies related to electronic finance.

In addition, in South Korea there are several private organizations such as the National Information Security Agency (NISA), the Korea Institute of Information Security and Cryptology (KIISC), the Korea Convergence Security Association (KCSA), and the Korea Online Privacy Association (KOPA). Among these organizations, the National Cyber Security Center under the NIS can be considered the most important for cyber security. In addition, since cyberwarfare is a domain for military operations, the Cyber Command in the MND can conduct cyberwarfare as well as the NIS. The DSC is in charge of defensive tasks in cyberspace because the command focuses more on counter-espionage and conventional security than cyberwarfare.

The CERT Building and Operations Book published by KISA and the Consortium of CERT (CONCERT) provides the guidelines for public and private organizations to establish CERTs, and it suggests how CERTs for small units and organizations in South Korea can be structured (KISA and CONCERT, 2010). According to the book, each CERT should consist of a committee, squads, and a working-level consultative group. The committee makes decisions, and squads are working groups that conduct information protection and vulnerability checks in the enterprise.

3. Defensive Capabilities

According to the National Information Security White Paper (NIS, 2015), South Korea's information security is divided into public information security, infrastructure information security, and private information security.

Public information security is divided broadly into national-information communications network security and electronic-government security. The national-information communications network security is achieved by an information-security-management state inspection by the NIS, which assesses the security level of each organization in regard to operations of CERTs, verification processes of security suitability and cryptographic modules, and so on. Electronic-government security is conducted by central and local e-government cyber-response centers under the Ministry

of Government Administration and Home Affairs, and includes a software-development security system to minimize vulnerabilities of public software. In addition, because the administrative environment is changing from paper to electronic documents, they developed electronic signature authorization systems to enhance security.

Infrastructure information security is related to protection of communications infrastructure including electronic control and management networks for national security, administrative, defense, police, finance, communication, transportation, and energy. The NIS and MSIP carry out security inspections for protection of this infrastructure, and the KISA, NSR, and other institutes support technical issues. Private information security is divided into response and prevention of computer emergencies. For computer emergencies, the MSIP and KISA operate the Computer Emergency Response Center, which is responsible for carrying out the detection of malware, implementing responses against DDoS attacks by establishing cyber shelters and zombie PC treatment systems, and implementing responses against wire frauds. To minimize emergencies, the KrCERT/CC cooperates with the Forum of Incident Response and Security Teams (FIRST), the Asia-Pacific Computer Emergency Response Team (APCERT), and other international organizations, and runs cyber-security professional groups that consist of security experts.

The White Paper and related works do not report defensive capabilities of the defense and intelligence areas because most of this information is classified. Although some military networks and other essential networks are connected to the Internet, they also operate air-gapped intranets with security measures such as cryptographic modules that correspond to security levels. The MND does maintain the public Information Operation Condition (INFOCON) to respond appropriately (Kshetri, 2014).

South Korea could expand their defensive capabilities because they have many more cyber resources than North Korea (Kshetri, 2014). South Korean anti-virus software manufacturers such as AhnLab and HAURI should have enough capabilities to detect and halt cyber attacks given adequate resources.

4. Offensive Capabilities

The cyber-attack capabilities of South Korea are classified. According to recent media reports, the South Korean intelligence agency NIS is exploring hacking software (Kang, 2015). The BBC reported that the South Korea Cyber Command is developing Stuxnet-like cyber weapons (BBC, 2014). According to the report, the offensive capabilities of Cyber Command have increased since 2010. Previously it focused on cyber psychological operations, but is now shifting attention to preparing cyberwarfare. The MND announced the Cyber Command Development Plan, which contains development of Stuxnet-like cyber weapons and enhancement of comprehensive cyberwarfare capabilities (Shin, 2014). Another report said that the Stuxnet-like cyber weapon might attack the adversary's cyber attack source itself (K. Kim, 2014).

South Korea could develop offensive capabilities more than North Korea because of their much greater cyber resources (Kshetri, 2014). Then it does seem foolish for North Korea to cyber-attack South Korea, and this point should be made clear in negotiations. Furthermore, South Korea and the United States have agreed that they will develop cyber weapons together (E. Kim, 2013), which means South Korea's cyber offensive capabilities can be expanded as necessary with U.S. capabilities.

Other kinds of offensive cyber activities can be considered. One of North Korea's external propaganda Websites, uriminzokkiri.com, was hacked by users of dcinside.com, one of the online community services in South Korea, in 2011 (H. Jung, 2011). Although the past attack from Anonymous against North Korea was hard to attribute to any country, the attack in 2011 was obviously from South Korea. South Korea is, however, limited in how it can control and use these voluntary hackers because it follows international laws. Based on all of this, as well as South Korea's cooperative relationship with the United States, South Korea's offensive capabilities should be at least equal to those of North Korea.

5. Vulnerabilities

South Korea's vast cyber resources and dependency on digital culture could also be a disadvantage (Kshetri, 2014) since so many potential targets exist in its extensive

cyberspace (Lim et al., 2013). In addition, it is hard for the South Korean government to control cyberspace because much of the space is in the private sector, in contrast with North Korea. One reason why South Korea does not respond well against North Korea's attacks is that the role division and role sharing between organizations is not always settled (Boo, 2013). South Korea does provide diverse public services in cyberspace via its electronic-government service. A number of services, such as distribution of important documents and issuing of administrative papers, are provided by wired or wireless communication channels. Although they are secured by encryption, digital signature, and other digital security technologies, additional defensive technologies are needed to protect against an advanced attack. Networks in the public sector could especially be a target because they have much personal and sensitive information. These networks can also be attractive if an attacker wants to make political effects because the availability of online public service is associated with the credibility of the country. The past DDoS attacks against the Websites of the Blue House and central government agencies are good examples.

Many enterprises and people are connected to the Internet for their business. Although they do have security measures corresponding to the type of services and the scale of businesses, the measures are often weaker than those of the government. North Korea has attacked the private sectors, including the press, the media, and the finance companies.

Vulnerabilities of the infrastructure sectors are hard to analyze because of the lack of open information. However, a report from the NIS suggests that North Korea has an offensive capability against electric-power facilities. In an attack against the Nonghyup Bank in 2011, North Korea succeeded in attacking a physically isolated intranet, which means that highly secured networks for infrastructure could also be attacked even though they are air-gapped. If critical infrastructure such as power plants and energy facilities are not available because of cyber attacks, the collateral damage could be significant. In 2014, there was an attack on Korea Hydro and Nuclear Power Co., Ltd. (KHNP; Y. Kim, 2015), although it did not affect physical systems.

The military sector is managed by the cyber command. ROK military units operate diverse intranets according to security levels, purposes, and organizations. The intranets are generally isolated networks from the Internet and are divided broadly into resource-management systems and battlefield-management systems (K. Choi, 2012). Resource-management systems are monitored and controlled by the Cyber Command, but the battlefield-management systems are not because the Joint Chiefs of Staff (JCS), Air Force, Navy, and Army operate their own systems, such as Korea Joint Command and Control System (KJCCS), the Air Force Command and Control System (AFCCS), the Korea Navy Command and Control System (KNCCS), and the Army Tactical Command Information System (ATCIS). Since the roles of the Cyber Command are expanding, the South Korean military can be vulnerable during joint operations if monitoring of the battlefield management systems is not integrated. There were many cyber attacks and especially cyber espionage on the ROK armed forces and the MND. For example, the Agency for Defense Development (ADD), which is in charge of the development of military technologies as a subordinate organization of the MND, was hacked by an unknown hacking group in 2014, and hundreds of confidential military documents were leaked (J. Yoon, 2014). While this attack was not attributed to North Korea, it shows a vulnerability in military confidential networks.

Thus, South Korea has vulnerabilities in every sector. These vulnerabilities can give adversaries many chances from which to choose targets. Adversaries could exploit vulnerabilities of the public and military sectors for cyber espionage and could attack private-sector vulnerabilities for cyber psychological operations or propaganda. Moreover, if adversaries want to cause considerable damage, they could exploit the vulnerabilities of infrastructure. If they intend to begin full-scale war, they would try to exploit the vulnerabilities of military networks.

C. CYBER ATTACKS FROM NORTH KOREA AGAINST SOUTH KOREA

This Section reviews North Korea's cyber attacks on South Korea from 2004 to 2015.

1. Overview

North Korea frequently uses cyber attacks as a provocation to achieve the government's political objectives as well as send propaganda and make armed provocations against South Korea. Their targets of provocations are not limited to South Korean government or military, but also include civilian properties since their main purpose is to perturb the South Korean people and undermine public confidence in the South Korean government (IUE, 2014). Targeting civilians is against the international laws of armed conflict, but North Korea does not respect international law. This section identifies the major features of North Korea's cyber attacks by observing previous cyber attacks that were attributed to the North Korean government. The North Korean government threatens South Korea in cyberspace similarly to how it does so with conventional armed forces.

The first cyber attack that was clearly attributed to North Korea was in 2004. There have been changes in targets and techniques with attacks over the last 10 years. North Korea's cyber attacks tend to occur in certain periods related to political, military, and cultural events, in contrast with attacks of cyber criminals. And the type of targets has changed over time from government Websites to the private sector.

2. Details of North Korean Attacks and South Korean Responses

We review North Korea's cyber attacks chronologically.

a. 2004

On June 10, 2004, the South Korea National Assembly, the Coast Guard, KIDA, the Atomic Energy Research Institute, and private institutes were attacked by malware that appeared to be coming from China (H. Kim, 2010). According to statistics, among 301 damaged computers, 222 devices belonged to the government, and 79 computers were for private companies and universities. Based on the analysis, the origin of the attack was China, but the IP addresses were Chinese ones being leased by North Korea. According to Chae's analysis, secret information related to national security was leaked for six months (Chae, 2013). In addition, HP Security Research indicated that North

Korea accessed South Korean military wireless communication networks (HP Security Research, 2014).

South Korea recognized the domestic cyber weaknesses from this incident, so the government established a National Cyber Security Center and related regulations (Chae, 2013). However, the investigation encountered obstacles due to lack of cooperation by the Chinese government. International cooperation is important for cyber-attack investigation and responses.

b. 2005

North Korea penetrated South Korea's military communication channel in 2005 during Ulchi Focus Lens, the annual combined military exercise with the United States (Ventre, 2011). South Korea's Defense Security Command revealed 33 military wireless connections were reached to North Korea (K. Kim, 2005). There is little available information since the target was a military network. Because North Korea treats the combined exercises as preparations for the invasion of North Korea, the attack could have been a protest of the exercise.

c. 2006

According to (HP Security Research, 2014), the U.S. State Department was attacked by unknown entities in cyberspace in June 2006 (HP Security Research, 2014). At that time, the United States and North Korea were carrying on a conversation about North Korea's missile and nuclear weapons. Although the detailed information is not publicly open, the South Korean military reported that North Korea's Unit 121 was implicated in this attack. This attack likely intended to strengthen bargaining power against the United States.

d. 2007

In March 2007, the Third Republic of Korea Army (TROKA) Command and the Center for Chemical Safety Management of National Institute of Environment were attacked in cyberspace (Mansourov, 2014). After the hackers obtained certificate passwords from TROKA to access the center, they stole information related to chemical-

accident response. This information was related to approximately 700 enterprises and organizations associated with chemicals. South Korea spent about seven months identifying this cyber attack, and the potential damage was estimated to be bigger than the identified information leakage since it covered a long period. There was no strong evidence that North Korea was responsible for it, but South Korea's government announced that the malware was from a foreign country, and it could have been from North Korea (S. Lee, 2009).

In addition, (HP Security Research, 2014) claimed that North Korea tested a kind of cyber weapon, a logic bomb, in October 2007. In response, the international community imposed sanctions on the import of related devices and technology to North Korea (Ventre, 2011).

e. 2008

North Korea in 2008 sent malicious emails with Trojan Horses to the South Korean military, and social engineering attempts such as spear phishing were also identified (Ventre, 2011).

f. 2009

A significant cyber attack occurred in July 2009. It was a DDoS attack targeting 21 Websites, including government sites such as the Blue House, MND, NIS, media, and financial institutes. According to (Chae, 2013), North Korean hackers used sophisticated methods, such as automatic deletion of source files and destruction of zombie PC's hard disks to hide evidence and the attacker's identity. The attack exploited over 400 servers in the world to make tracing hard. The total number of bots was approximately 20,000 devices. Among them, 12,000 infected computers were located in South Korea, and others were in foreign countries (Mansourov, 2014).

This attack did not target only South Korea. On July 4, the first phase of the attack occurred against U.S. government Websites. On July 7 and 9, similar attacks occurred in South Korea. Some IP addresses that were used for this attack were the IP addresses of the North Korean Ministry of Posts and Telecommunications that were leased from

Chinese ISP (H. Kim, 2010). Although the command-and-control of this attack was conducted from the United Kingdom, the attack could be attributed to North Korea because the attack codes targeted websites in the Korean language (Carr, 2011). This attack on the availability of targeted systems is definitely different than the previous cyber-espionage or penetration attacks because it had a certain scenario with specific targets, methods, and schedules (Boo, 2013). Apparently, this attack was meant to test the resilience of South Korea and the United States in cyberspace (Ventre, 2011).

Since this DDoS attack hurt the availability of public services, it made a large impact. The South Korean government realized the importance of inter-organization cooperation for early detection and proper response to attacks (Chae, 2013). South Korea thus established a Cyber Command (Kshetri, 2014).

Although the attack against South Korea started July 7, the first attack occurred in the United States on July 4, which is the important U.S. national holiday of Independence Day. In June, a month before the attack, the North Korean government officially announced that they were fully ready for any form of high-tech war. Based on these facts, the attack could be considered a well-prepared attack against the ROK-U.S. alliance (HP Security Research, 2014).

g. 2010

In 2010, several cyber attacks involving information leakage were targeted against South Korean military officers via malware (Ventre, 2011). In July, there was a DDoS attack against the Blue House, the Ministry of Foreign Affairs and Trade, the Korean Exchange Bank, and Naver.com, but the damage was not as great as that of the DDoS attack in 2009 (Mansourov, 2014). Although the attack was not large-scale, it appeared that North Korea was using a cyber attack to deliver their political intentions because this attack occurred in the same period as the previous year with a similar type of method. According to the South Korea National Policy Agency, this DDoS attack was conducted by the same botnets that were used for the massive DDoS attack in 2009, and the signature of malware was also the same (Y. Jung, 2010). In 2010, the South Korean MND established a Cyber-Protection Policy Team (Kshetri, 2014).

h. 2011

On January 3, 2011, a South Korean private website, Free North Korea Radio, was attacked by North Korea. This attack was likely a counterattack because users of the South Korean Internet site DCinside.com had hacked a North Korean external website, uriminzokkiri.com (Mansourov, 2014). Free North Korea Radio is a private organization that mainly consists of North Korean defectors, and it broadcasts news about North Korea such as the North Korean government's human rights violations as well as developments in South Korea. Unusually, this attack did not use proxy servers, but came from North Korea directly, which indicated that they wanted the attack to be attributed.

In March 2011, a more massive DDoS attack than that of 2009 was conducted against the South Korean government and private services. Over 700 servers and 100,000 infected PCs were mobilized for this attack (Chae, 2013). The attack was similar to previous attacks known to be from North Korea (Ahn, 2013). The attack used illegal game sites to spread malware that infected PCs and set up botnets (Mansourov, 2014).

In April 2011, South Korean bank Nonghyeop was hacked and their banking service was paralyzed for several days because much data in their network was damaged (Chae, 2013). The South Korean prosecutor announced that this attack was conducted by North Korea's RGB after seven months of a sophisticated preparatory period (Park, 2011). This was a more developed attack than the previous DDoS attacks since it caused monetary losses in the real world and involved an attempt of an Advanced Persistent Threat (APT; Boo, 2013). McAfee, a U.S. security company, did identify signatures of North Korea in the attack codes (Cisneros, 2015). In addition, (HP Security Research, 2014) reported that North Korea attempted a DDoS attack on transportation infrastructures such as Incheon International Airport.

i. 2012

In June 2012, North Korea attacked the website of Joongang Ilbo, a conservative press company (Mansourov, 2014). The South Korean Cyber Terror Response Team in the National Police Agency reported that the IP addresses of this attack were related to the North Korean Ministry of Posts and Telecommunications (Park, 2013). Before the attack,

the North Korean government did threaten South Korean media that reported North Korea's issues negatively. The North Korea's General Staff Department announced that several media in South Korea insulted the leader of North Korea as Adolf Hitler, and North Korea would attack Chosun Ilbo, Joongang Ilbo, Dong-A Ilbo, the Korea Broadcasting system, the Seoul Broadcasting System, and the Munhwa Broadcasting Corporation, among others, if South Korea did not apologize (Jun, 2012). Databases related to news articles and pictures were destroyed by this attack. Also in 2012, South Korea established a Cyber-Defense School with Korea University, and the school cultivated 30 cyber experts for the military section (Kshetri, 2014).

j. 2013

In March 2013, North Korea attacked PCs, servers, and automated teller machines of six broadcast companies and financial institutes, causing deletion of data and service interruptions (Chae, 2013). This attack was an APT attack similar to the Nonghyeop hacking in 2011, with several months of preparation (Boo, 2013). According to (HP Security Research, 2014), an Internet and communications company in South Korea, LG U+, was also attacked similarly, and there was defacement on the damaged Web page with a message, "Hacked by Whois Team." "Whois" is occasionally used by South Korea's white hat team, RAON_ASRT, but given the targets, it seems more likely that North Korea used this word intentionally to shift the blame.

According to the detailed analysis, this attack was prepared over eight months, and approximately 57,000 PCs and servers were damaged (B. Lee, 2015). The hackers first stole information from internal PCs of targeted facilities to find network vulnerabilities and spread malware to PCs attached to the networks via fake antivirus software. In this process, the IP addresses belonging to North Korea were identified 13 times, and many intermediate pathways used were identical to their past attacks. In addition, about 30 types of malware among the total 76 malware used for this attack were reused from previous North Korean attacks. A new feature was that North Korean hackers exploited vulnerabilities in the groupware of targeted networks, such as electronic-document transfer systems. They also tried to bypass South Korean domestic

antivirus software, using its updated server to spread their malware (HP Security Research, 2014).

The March 13 attack showed that the level of North Korea's cyber threat was higher than the attack in 2009 (B. Lee, 2015). There were significant losses, such as a decrease in markets from the degrading of South Korea's international credibility. According to (B. Lee, 2015) research, the damage estimation of this attack was 805.1 billion won, which was 15 times bigger than the damage of the attack in 2009, 54.4 billion won.

In April 2013, the international hacking group Anonymous attacked North Korea's networks (HP Security Research, 2014). Apparently in response, malicious smartphone applications infected approximately 20,000 devices in South Korea from May to September (Mansourov, 2014). These malicious applications were spread as free mobile games, and they had eavesdropping and video-recording capabilities.

In June 2013, North Korea conducted a large cyber attack against South Korea's government and think tanks such as the MOU, the Sejong Institute, the KIDA, and the Hyundai Merchant Marine (Mansourov, 2014). The DDoS attack was attributed to the DarkSeoul hacking group, which is related to North Korea's Lab 110 (HP Security Research, 2014). This attack was different from the previous attack in March because the malware did not use any timer and destroyed hard drives immediately when the system was infected (B. Lee, 2015). Since this attack spread malware via shared folders of intranets, and administrative passwords were required to access share folders, this attack was a type of APT attack that obtained passwords in advance. Furthermore, in September, Kimsuky malware that targeted South Korea's think tanks was detected (HP Security Research, 2014).

To reinforce cyber-related organization in response to North Korea's continuing cyber threats, the South Korean MND established a Cyber Policy Department, and the NIS announced that the Third Department would focus more on monitoring of cyberspace and telecommunications (Kshetri, 2014). Moreover, the South Korean

government stated that they would double the budget related to cyber security and cultivate 5,000 cyber experts every year.

k. 2014

In 2014 there were no large-scale cyber attacks like in 2013, but North Korea appeared to attack Sony Pictures Entertainment in response to the film *The Interview*, which depicted the assassination of a North Korean leader (HP Security Research, 2014). The FBI attributed this cyber attack to North Korea and made a conclusion that the attack was destructive malware; the data theft included "proprietary information as well as employees' personally identifiable information and confidential communications" (FBI, 2014). Experts have estimated the damages were up to $100 million (Richwine, 2014). The U.S. government issued an executive order on strong sanctions as a response.

In December 2014, Korea Hydro and Nuclear Power Co., Ltd (KHNP) was hacked, and the South Korean Public Prosecutor's Office claimed North Korea as the source based on traces of IP addresses that belonged to North Korea (Y. Kim, 2015). After the hacking group first tampered with retired employees' email accounts, they then stole and posted some of the company's internal information, such as blueprints of nuclear facilities, on social network services (NIS, 2015). The purpose of the attack appeared to be public disruption. In response to the increasing North Korean cyber threat, in 2014 South Korea made greater efforts to prepare organized responses. In April 2015, the South Korean government established the office of Cyber Security Secretary under the Office of National Security and enforced comprehensive countermeasures to strengthen cyber-security postures.

l. 2015

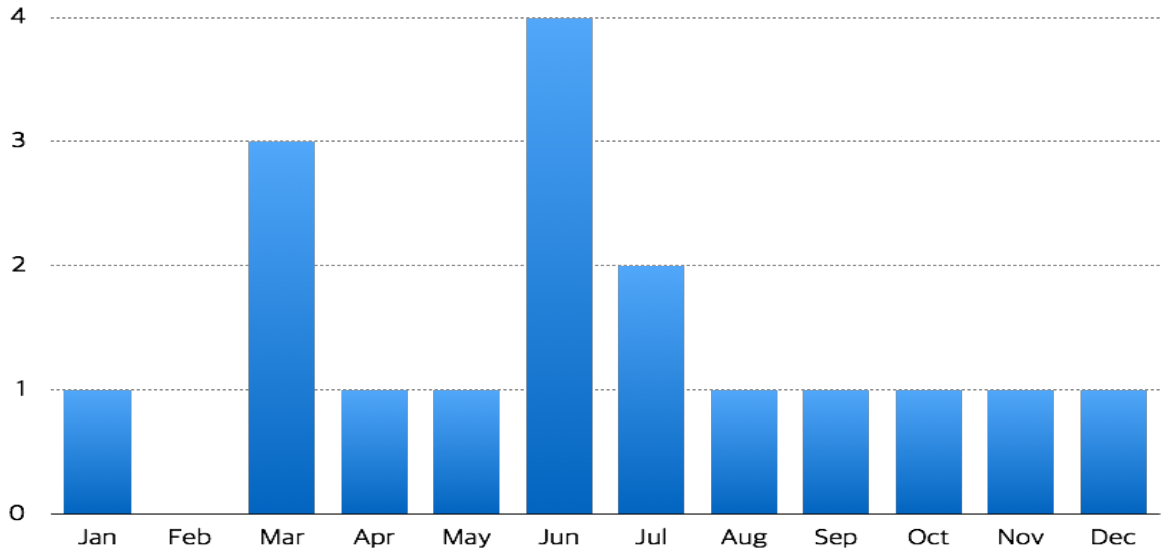
In June 2015, North Korea's external propaganda website uriminzokkiri.com was out of service for three weeks, and the North Korean government claimed that it was caused by U.S. cyber attacks (B. Lee, 2015) but provided no evidence. The reason that the website was nonfunctioning was not revealed.

3. Analysis

HP Security Research (2014) analyzed cyber activities related to North Korea from 2004 to 2014 in regard to malware and hacking. Cisnero (2015) did analysis that suggested that North Korea preferred attacks that had large effects regardless of the international laws of war because they attacked the private sector many times. These analyses suggest that North Korea's cyber attacks have certain patterns in timing and political issues, and future attacks may often be predicted.

The total number of major cyber attacks attributed to North Korea is 17 since 2004. Many attacks occurred in March, April, and July. In March, there is an annual large-scale combined military exercise, Key Resolve (KR), involving the ROK and the United States. The information leakage in 2007, the massive DDoS attack in 2011, and the APT attack on the media and banks in 2013 occurred in March. North Korea has claimed that these combined military activities are preparations for the invasion of North Korea and has conducted large-scale military training in response during the same period. Apparently, the intention of the cyber attacks in March is to protest and disturb the exercises. Figure 5 shows monthly trends.

Figure 5. Monthly Statistics of North Korea's Cyber Attacks from 2004 to 2015



In June and July, there are several anniversaries of the ROK-U.S. alliance, such as the start of the Korean War, June 25, and U.S. Independence Day, July 4. The first massive DDoS attack was started on July 4, 2009, and the APT attack on South Korean media and banks were conducted on June 25, 2013.

Furthermore, since the birthday of Kim Il-Sung, the first leader of North Korea, is April 15, the foundation day of the KPA is April 25, and the foundation day of the WPK is October 10, North Korea typically conducts large-scale armed protests or military training on these dates to show off their power to their people and the world. The logic bomb test in October 2007 and Nonghyeop hacking on April 4, 2011, occurred in conjunction with these historic events.

For these reasons, South Korea should intensify its defensive posture from March to October. But cyber attacks occurred during other periods as reactions to events such as the DDoS attack on Free North Korea Radio in January 2011 and the attack on Sony Pictures Entertainment in November 2011. In addition, when North Korea has used APTs it prepared for several months with penetration of networks and exploitation of vulnerabilities.

Overall, since the massive DDoS attack in 2009, large-scale cyber attacks have occurred every other year. In 2009, the relationship between North Korea and the ROK-U.S. alliance deteriorated because a North Korean soldier shot a South Korean tourist, Wang-Ja Park (K. Lee, 2008). The North Korean government launched a long-range ballistic missile in April 2009 (K. Kim, 2009), and North Korea did a second nuclear weapon test in May 2009 (T. Kim, 2009). In addition, the North Korean government announced that they were fully ready for any form of high-tech war in June 2009 (HP Security Research, 2014). After these events, North Korea attacked the United States and South Korea in July 2009. They also launched seven ballistic missiles on the same day of the cyber attack against the United States (Son, 2009).

North Korean provocations continued. In September 2009, North Korea opened the floodgate of Hwang-Gang Dam without notice, and South Korean civilians were killed (K. Lee, 2009). In November, North Korean naval patrol ships invaded the

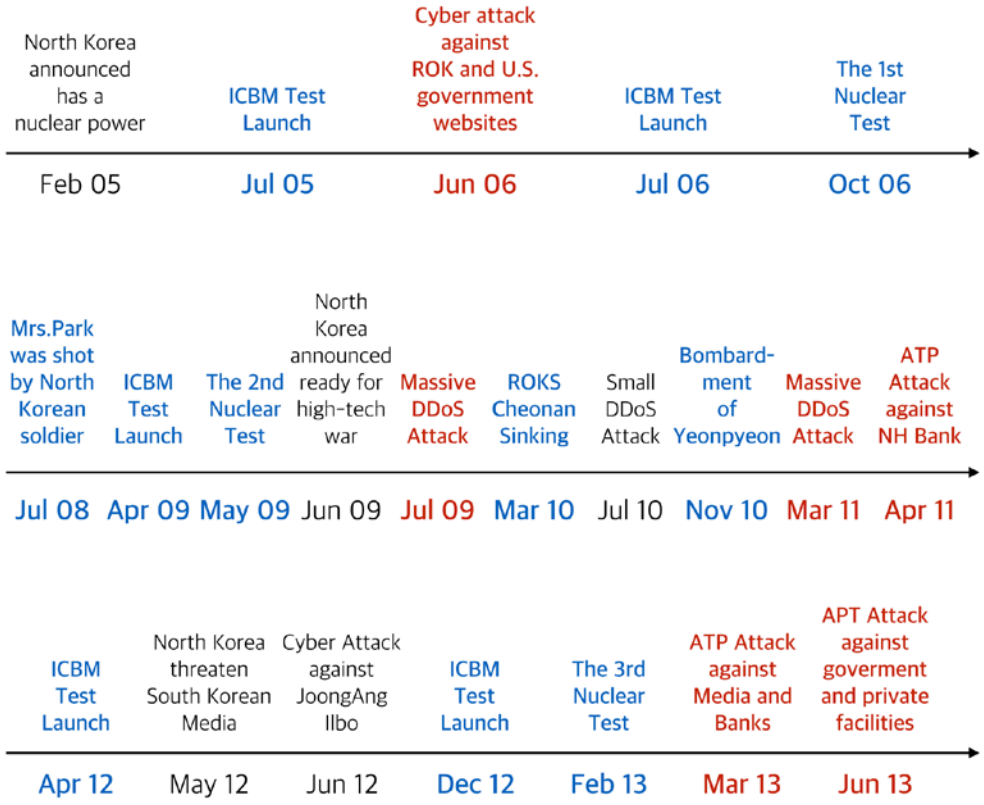
Northern Limit Line, the western sea border between South and North Korea, and South and North Korean naval ships engaged (D. Lee, 2009). In March 2010, North Korea conducted a torpedo attack on ROKS Choenan (M. Jung, 2010). During this state of tension, the North Korean government attacked government and private Websites in cyberspace, and finally they bombarded the South Korean island Yeonpyeongdo in November 2010 (D. Kim, 2010). The largest cyber attacks occurred in March and April 2011.

The chain of events from 2009 to 2011 shows the purpose of North Korea's cyber attacks. They conducted strategic provocations to make themselves look powerful, such as launching missiles or doing nuclear testing. They hope these actions will allow them leverage in the Korean peninsula and will reinforce their bargaining power against the United States, but this has not worked. Yet they continue with these power plays nonetheless. These cases also suggest that North Korea considers their cyber capabilities as strategic assets like missiles and nuclear weapons.

Since the 1990s, the North Korean government has practiced brinkmanship for getting economic support and protecting the regime by creating an atmosphere of conflict with nuclear tests and missile launches (IUE, 2014). In addition, the North Korean government believes that they can solve their urgent problem with nuclear weapons and long-range missiles that can threaten the United States directly in the Korean peninsula theater. The characteristics of these weapon systems are that they can threaten many distant objects. These characteristics are similar to those of cyber attacks since cyber attacks also could threaten many targets indiscriminately without the constraints of physical space.

Figure 6 shows the timelines of cyber attacks and conventional provocations.

Figure 6. Chart of North Korean Provocations



This analysis suggests that if the relationship between the two Koreas worsens or if major real world provocations occur, it will be necessary to strengthen cyber-defense postures even when there are no symptoms related to cyberspace.

By analyzing the changes in their cyber targets, we also can forecast future attack targets. From 2004 to 2008, most attacks were information-gathering from government and research agencies. However, since 2009, the North Korean government has conducted DDoS attacks against the private sector, such as media and financial institutes. In addition, North Korean hackers have increasingly seized internal groupware and anti-virus systems, destroying internal systems instead of external systems. Damages have increased, and more resources and time are required for restoration. In addition, in December 2014, they hacked KHNP, part of the national infrastructure.

So the targets of North Korea's cyber attacks have shifted from intelligence collection to DDoS attacks and then to APT attacks on the private sector related closely

to the public. Following this trend, future targets are likely to be the infrastructure operated by private companies, which has weaker defenses because of the concentration on national cyber security by the establishment of Cyber Command in 2010 and NIS' concentration on cyber security.

IV. FINDING EFFECTIVE RESPONSES

According to the analysis of Chapter III, the North Korean government conducts cyber attacks with strategic goals, much as it does with nuclear weapon tests and long-range missile launches. This shows that the North Korean government aims to achieve political goals by showing off their asymmetric capabilities. In fact, comparing military forces between South and North Korea in 2014, North Korea has 1.5 times more field artilleries, 27 times more rocket launchers, and 7 times more submarines than South Korea, which means that artilleries and submarines are asymmetric forces for them (S. Kim, 2015).

In this chapter, we investigate South Korea's possible countermeasures against North Korea's continuous cyber attacks.

A. THE GOAL STATE

The most important thing before finding proper responses is to define what South Korea's ultimate goal state is. According to a Defense White Paper from the South Korean MND (MND, 2015), South Korea's national defense has three objectives: "protecting the country from external military threats and invasion" (p.37), "supporting peaceful unification" (p.37), and "contributing to regional stability and world peace" (p.37). In terms of the situation in the Korean peninsula, these objectives could be interpreted as protecting South Korea from North Korean threats, deterring war in the Korean peninsula to support peaceful unification, alleviating military tension, and establishing a lasting peace. In cyberspace, the goals would be protecting South Korea's information technology environment, assets, and resources from North Korea; deterring cyber war and alleviating tensions in cyberspace; and establishing a lasting peace in cyberspace. This means that South Korea should prepare good defensive countermeasures to protect cyber assets and develop coercive methods to encourage the North Korean government to stop cyber attacks without escalating a cyber arms race.

B. CONSIDERATIONS

There are several considerations to find and assess countermeasures.

1. Prevention of Escalation

South Korea does not want to trigger a cyber arms race or escalation, although it should prepare defensive and offensive countermeasures. However, South Korea cannot concentrate only on defense in disregard of offense because a strong shield might cause North Korea to develop stronger weapons. Thus, South Korea should demonstrate possible counterattacks. The bargaining power in the real world can be reinforced by cyber coercion (Flemming & Rowe, 2015), and this can be achieved by showing offensive capabilities and will.

Preparing and applying offensive cyber methods to coerce might cause a cyber arms race. Escalation could have serious and unpredictable consequences (Woods, 2015). Escalations could be more likely if the level of countermeasures is too high or targets of the countermeasures are not chosen well (Flemming, 2014). Joint coercion with cyber and conventional military forces might better prevent escalation since effects of conventional military forces are more predictable. As a result, to coerce without escalation, very sensitive procedures to set the level and targets of the counteractions are required.

2. Legality and Ethics

Other considerations are international legality and ethics. The North Korean government tends not to follow international law. It has negated or broken away from international treaties and rules many times. For example, in 1993, North Korea left the Nuclear Nonproliferation Treaty (NPT) to develop nuclear weapons. South Korea generally follows international law and rules. Although North Korean cyber-attack targets are expanding from the military and government to private sectors and infrastructure, South Korea could not attack such targets. According to the Tallinn Manual that provides guidelines for international cyber conflicts, “The civilian population as such, as well as individual civilians, shall not be the object of cyber attack”

(Schmitt, 2013, p. 113), “Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian populations, are prohibited” (Schmitt, 2013, p. 122), and “Attacking, destroying, removing, or rendering useless object indispensable to the survival of the civilian population by means of cyber operation is prohibited” (Schmitt, 2013, p. 225). Even though the Tallinn Manual is not yet part of international law, South Korea cannot ignore it because the government puts great emphasis on international relationships since it has many connections to the rest of the world. If South Korea follows international guidelines, legitimacy of its countermeasures can be secured.

3. Resources and Resiliency

Cyberwarfare requires resources much like conventional warfare. Large expenses are not required to produce a single cyber weapon compared to advanced fighter jets, nuclear aircraft carriers, or precision-guided missiles. Although double the cost is required to make two identical fighter jets, computer viruses can be copied at very little cost. However, although the life cycle of fighter jets from development to retirement is decades, the life cycle in cyberspace is quite short because of the swift pace of development of information technology. Therefore, both cyber defense and offense will be expensive in the long run because both require constant new investments. Investing large amounts to establish a so-called perfect cyber protection system would be inefficient because it could become useless after the development of new attack methods. Similarly, a large investment in cyber weapons is also not efficient because cyber weapons usually cannot be reused as word of their effects spreads and patches of the vulnerabilities become available. Thus, cyberweapon offense and defense must be designed in moderation as just one part of a strategic offense and defense.

4. Bargaining Power

If defensive and offensive countermeasures in cyberspace also have effects in the real world, they could be more efficient. A desirable purpose of much cyber coercion could be to make the adversary return to the negotiating table (Woods, 2015), and bargaining power in the real world could be reinforced by cyber coercion (Flemming & Rowe, 2015). Usually, cessation of hostilities is negotiated between decision makers on

both sides. It is helpful to consider whether a proposed countermeasure will enhance bargaining power. Bargaining power could be strengthened if one side targets objects that the other side thinks are important, and the effect can be increased if the counter attack could be reversible. An example of reversible cyber activities is ransomware that encrypts a victim's data, which means that nobody except for the attacker could decrypt it, followed by asking for a ransom. An example is the CryptoLocker that attacked approximately 234,000 computers from 2013 to 2014 (DOJ Office of Public Affairs, 2014). Between countries, reversible measures could encourage parties to negotiate a solution quickly.

C. DEFENSIVE COUNTERMEASURES

Despite news reports, the defender is not always powerless in cyberspace (Singer & Friedman, 2014). Attackers can choose a type, time, and target of attack, but they must infiltrate all protective layers to make their attack successful. Defenders could defend successfully if at least one of the protections succeeds in blocking the attack at a layer. Here we recommend some innovative defensive ways.

1. Defensive Techniques

Several cyber defensive countermeasures are possible based on the idea of active defense (Harrington, 2014): beaconing, threat counter-intelligence gathering, sinkholing, honeypots, and retaliatory hacking. Retaliatory hacking is more related to offensive countermeasures and is discussed later. Threat counter-intelligence gathering is beyond the scope of the technical means discussed here.

Beaconing transmits the current user information, such as IP addresses, via an Internet connection when the stolen file is opened. This permits tracing of attacks when the attacker downloads information. By more sophisticated programming, beaconing can be upgraded to deletion of files or gaining control of the attacker's computer.

Honeypots are systems designed to attract attackers and record their methods (Harrington, 2014). This can be effective against file stealing, DDoS, malware installation for APT, and other kinds of attacks. Honeypots can collect information such

as penetration or scanning patterns (Fredrick, 2011). Honeypots are already deployed in many organizations for general cyber security purposes.

Sinkholing intercepts malicious traffic from botnet clients by masquerading as one of its command-and-control servers (Harrington, 2014). Because redirecting from suspected domain names or IP addresses is required, support from the domain manager is necessary.

2. Cyber Early-Warning System

A cyber early-warning system provides a wider viewpoint to defense (Robinson, Jones, & Janicke, 2015). Many modern countries have a well-prepared early-warning system for conventional military attacks. A good cyber early-warning system should provide information about the current situation, the attacker, the targets, and the attack methods (Golling & Stelte, 2011). Early warning systems have the disadvantage that they only detect attacks after they are launched. Attribution and reverse-engineering to figure out who implemented a cyber attack and how it was done can take a long time. For example, after the cyber attack on June 25, 2013, approximately three weeks passed until the joint investigation group announced a result (I. Choi, 2013).

Early warning for cyber attacks is closely related to social, economic, political and cultural issues (Sharma, Gandhi, Mahoney, Sousan, & Zhu, 2010). Cyber attacks motivated by political issues usually have five phases: latent tension, cyber reconnaissance, an initiating event, cyber mobilization, and a cyber attack (Carr, 2011). Since the purposes of North Korea's cyber attacks are to reinforce their bargaining power and to achieve their political goals, we should see the five stages from them. That suggests that defense should be collecting a good deal of cyber data when an attack appears to be imminent. However, excessive information collecting can raise privacy and legal issues. In addition, it is not reasonable to collect more than one's analytic capabilities.

One thing that aids early-warning systems is that classification of cyber attack groups and prediction of attacks based on a cyber-defense operations framework is possible in advance (Kim, Park, Lee, & Lim, 2014). A good cyber-defense framework

has six stages. The first stage is detection, in which suspicious traffic or code is detected by intrusion-detection systems (IDSs), intrusion-prevention systems (IPSs), anti-virus software, and firewalls. The second stage extracts attack artifacts, which are analyzed and stored in a database together with any relevant open-source information. In this stage, signatures of the attack and its distinctive parameters are acquired. Signatures and parameters include such things as email sender identification, the sender's IP address, hash values to figure out identical malicious attachment or malware, IP addresses of command-and-control servers, and related Internet addresses (URLs). The third stage tries to classify the attack group by using the parameters of the second phase. The fourth stage analyzes the attack group using digital evidence and timeline plotting, looking for patterns or preferred resources for the attack. The fifth stage makes predictions by monitoring the resources' states. If an attacker tends to use a certain server to command its botnet, early warning can be provided when the server behaves atypically. The final phase is a reaction phase to prevent damage from similar future attacks by fixing vulnerabilities and blocking the attacking sites and protocols.

3. Concept of Integrated Cyber Defense

Another way to describe an integrated cyber defense (Cloud, 2007) is that it can be divided into technology employment, operational command and control, and operational employment. Technology employment consists of a cyber-sensor network similar to an air-surveillance radar, a cyber identify-friend-or-foe (IFF) system, and defensive cyber weapons similar to surface-to-air missiles (SAM). Operational command-and-control implements the operational chain of command-and-control in cyberspace. (Cloud, 2007) recommends a unified chain that removes ambiguity for efficient computer network operations. The operational employment concept consists of posture, maneuver, and recovery. Posture is related to protective measures that maintain survivability and operability of cyber assets by modification of the cyber readiness posture according to the situation. It can use cover, concealment, camouflage, hardening, deception, dispersal, and redundancy. Maneuver is associated with responses during attacks, such as attacking, defending, relocating, augmenting, withdrawing, and delaying.

Finally, recovery means restoring cyber capabilities, including battle damage assessment, containment, repair, and reconstitution.

4. Building a South Korean Integrated Cyber Defense Based on Cyber Early-Warning System

Today in South Korea the chain of command-and-control for cyber defense is controlled by the NIS. The MSIP and KISA are responsible for the private sector, and the MND and the cyber command are in charge of the military sector. After so many cyber attacks from North Korea over ten years, organizations are well-prepared to cooperate by devising methods for detection of threats and for sharing related information quickly. Cooperation with ISPs and sharing related information between associated organizations is also important (Harrington, 2014).

Most of North Korea's recent provocations by military forces occurred on the ground and the sea (Noh, 2015). North Korea has not provoked in the air because their airpower is inferior to that of South Korea and South Korea's air defense system is working well. This is likely is because the Master Control and Reporting Center (MCRC) integrates all radar information and shares it in a short time. This could be a model for the timely detection of cyber threats and sharing of cyber information, which are important parts of a cyber defense posture.

South Korea can detect malicious activities on networks via IPSs, IDSs, firewalls, and beaconing, honeypots, sinkholing, and other techniques, monitor the detected information, and share the information with each organization. The National Policy Agency can operate cyber criminal investigation units for cyber crimes. Since North Korea's cyber attacks have targeted civilians and private sectors as well as government and military organizations, and attacks on infrastructure are also expected in the future, a cyber early-warning system should be unified into one place, and the NIS is an appropriate place because they already have authority for overall cyber issues. However, unique, independent, or air-gapped intranets, such as military intranets for the MND and units, should be locally managed to avoid propagation of unnecessary information. For

example, the cyber command, the cyber-specialized organization under the MND, would be the suitable organization to conduct cyber early warning for military intranets.

Controlling a limited number of aircraft in the air is different from handling the much more numerous items of information related to cyber threats and attacks from scattered information systems. A big-data handling approach is required, which is a key technological issue for integrated cyber defense. Furthermore, cooperation between the cyber early-warning system of the NIS and network infrastructures such as ISPs is necessary, much as the MCRC and the AOC must cooperate with the area-control center (ACC), which controls civilian air traffic. Also, North Korea's cyber attacks tend to occur together with other strategic provocations, so for an integrated cyber early-warning system, overall intelligence analysis is required. Because the NIS is responsible for the national level of intelligence analyses, the NIS should provide this.

Currently, each cyber organization detects and reports to its interagency, and interagencies report to the NIS. This structure could cause delays in sharing threat information since additional processing time for data integration might be required if each organization does not have unified procedures or policies. Furthermore, information consolidation with current-circumstance analysis and other intelligence is limited due to each organization's limited intelligence capability. Thus, an integrated system at the NIS to consolidate information is required. Figures 7 and 8 display South Korea's current and recommended NIS-centric cyber early-warning systems, respectively.

Figure 7. South Korea's Current Cyber Threat Information Reporting System

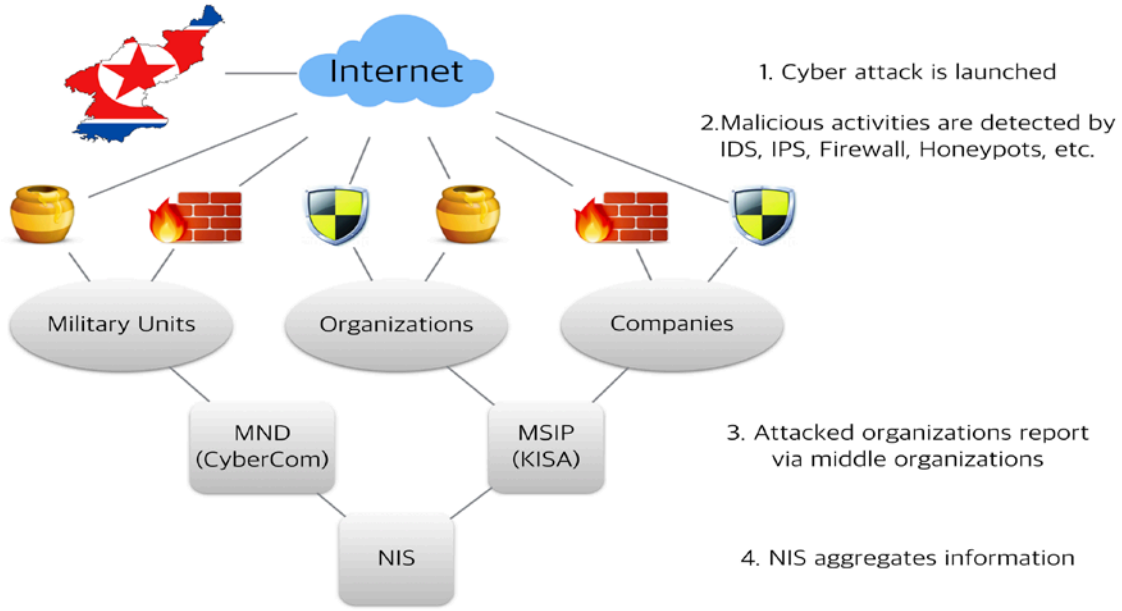
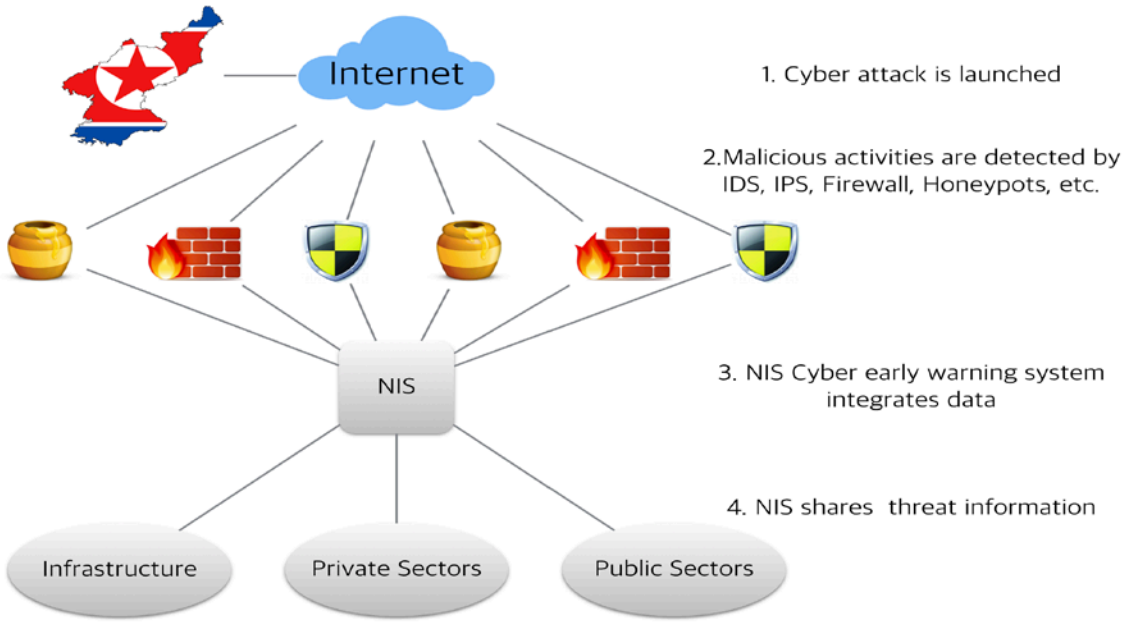


Figure 8. Recommended Cyber Early-Warning System



5. Details of Cyber Early-Warning System

If an integrated cyber early-warning system is established, the system should provide information about the subject of the attack, the target of the attack, and the method of the attack (Golling & Stelte, 2011). For early warning, the information about subject, target, and method could be incorrect, but immediacy is more important than accuracy because it is not for negotiations but for defense.

An early-warning system should share threat information quickly. It should notify everyone of the approaching threat, prepare a defense posture, and reinforce cooperation. In the private sector, executives determine the balance between investment of cyber security and risk that can be afforded. The government cannot provide security devices and software to every individual and company, but close cooperation and intervention with ISPs and other network infrastructure is required because they have very important responsibilities on network availability. Moreover, critical infrastructure could cause enormous damage nationwide if it goes down, so critical assets such as power plants and water-supply plants require additional cooperation and supervision. Joint cyber-defense exercises and training are needed similarly to joint training for local military units, polices, and related organizations together. Furthermore, since North Korea has exploited vulnerabilities of South Korea's domestic anti-virus software to spread malware, cooperation with foreign cyber-security companies is also necessary.

After issuing warnings, several steps can reinforce the defensive posture, such as checking security configurations and doing backups. We could change network configurations at a certain level of threat much like how important military units change communication frequencies to specially assigned ones for an operation. This method can block concealed malware that communicates for activation. As we discussed previously, honeypots attract attackers, collect attack information, and defend real systems. During an attack, the existing honeypots are probably already identified by the attacker, but deploying a new one could be a good way to mitigate the attack. Honeypots can provide a new source of warnings (Cloud, 2007), and cyber-security companies and institutes could then recommend defensive techniques.

Despite upgraded cyber defense postures and preparations, damage could still occur from a cyber attack. Resiliency is important (Singer & Friedman, 2014), as is the recovery stage (Cloud, 2007). Even if services are not available due to DDoS attacks or important documents are spilled by cyber espionage, mitigation of damage and restoration of normal services in a short time is important. In the case of DDoS attacks, services can be restored by identifying and filtering malicious packets and attacking Internet addresses. It will also help to repair the bots in DDoS botnets and block their communications. There are several ways to respond immediately, such as source-address validation, secure configuration of the DNS server, disabling open recursive DNSs, and blocking and filtering (Internet Corporation for Assigned Names and Numbers [ICANN] Security and Stability Advisory Company [SSAC], 2006). If systems are infected by destructive malware or logic bombs that damage storage, backups are critical. With early warning, organizations can set backup periods shorter than normal conditions while enhancing stability of backups by separating backup storage physically from the network to prevent attacks on it as well. In the case of stealing information, planting beacons or watermarks into the information could help mitigate damage. For example, a planted beacon could prohibit opening a file when the file is outside of the organization's network.

6. Assessments

In terms of resources, diversified investment of limited resources in both protection and resiliency is desirable. If investment is focused on blocking attacks, the costs of loss will be high when the blocking fails. If the target is critical infrastructure such as a power plant, and it takes a long time to restore, damage to humans and other irrevocable damage could occur. On the other hand, if investment is focused on resiliency only, services would have outages frequently even though they could be fixed in a short time. An approximate calculation method for damage of downtime due to DDoS attacks (Dubendorfer, Wagner, & Plattner, 2004) says that costs of loss increase with the amount of downtime. A very long downtime from one significant attack could make a big loss, as well as a high level of accumulated downtime from frequent outages.

If warnings can be provided by an early-warning system and related events, it is possible to identify periods that require additional defensive capabilities. With finite resources, utilizing them for production parts such as research and development during ordinary days and switching resources to defense at other times is more effective than using a constant amount of resources at all times.

In collecting more information to provide more accurate warnings, several legal issues can occur concerning how much information should be collected and handled. When information is collected from foreign countries, legal cooperation is required. Privacy problems can occur if excessive information is collected, so it is required to identify and gather essential information only with advance preparation of the associated regulation.

If a victim country provides objective damage assessments and attributions that can be accepted by international society, its bargaining power at a negotiation table could be stronger. Even though there are no military logos as with conventional military forces, attribution in cyber space is possible due to advanced technology like evidence in files and network traffic (Rowe, 2015). Attribution via files is conducted by similarity of code and data, and attribution via traffic is possible with back-tracing and beaconing. Usually, it is hard to hold an entire country responsible for the cyber attack; for example, even if a blackhat in the United States hacks the South Korean government, the government cannot claim U.S. responsibility without detailed evidence that the U.S. government sponsors the hacker. However, in the situation of North Korea, North Korea's Internet connections are so strongly controlled by the North Korean government that there is little possibility that cyber attacks from North Korea are not related to the government.

Other factors can also affect bargaining power from the viewpoint of attackers (Pillar, 1983), but they are not suitable to defensive measures. Information and intelligence capabilities could, however, strengthen bargaining power (Ko & Kim, 2009) because of the importance of objective damage assessments and robust evidence of attribution.

D. OFFENSIVE COUNTERMEASURES

Counteracting an adversary's cyber attacks in cyberspace is similar to the concept of retaliatory hacking mentioned by (Harrington, 2014). He argued that this hacking back from private companies to respond to cyber crimes could make many legal and ethical problems. Both private companies' activities that are regulated by domestic laws and internationally activities that are associated with international laws could face many legal and ethical problems before even discussing effectiveness. In this section, we discuss suitable offensive measures to achieve South Korea's cyber goal states, such as protection of South Korea's information technology (IT) environment, deterrence of cyber war, and establishment of persistent peace in cyberspace. As we discussed, since offensive methods could face more legal and ethical issues than defensive measures, we should approach them more carefully.

Cyber counter attacks are conducted by cyber weapons. Cyber weapons can be defined as weapons related to software to achieve desirable effects and a type of program that is modified to control the adversary's computers and devices (Rowe, 2015). In addition, (Rowe, 2015) mentioned that cyber attacks are attempts to subvert the adversary's computers to give the attacker advantages, and usually sabotage of the opponent's system is the main purpose. In this section, we review existing research related to applicable options to seek for effective offensive countermeasures in terms of prevention of escalation and reinforcement of bargaining power as well as international laws and ethics, and examine options based on considerations.

1. Targets

Targeting is the first consideration to achieve the goal in cyberspace that deters North Korea's cyber threats by offensive responses. North Korea does not have many activities on the Internet, and most domestic data is distributed by intranets. For this reason, possible cyber targets in North Korea could be divided into targets on the Internet and targets on intranets.

North Korea's intranets are physically disconnected from the Internet, and North Korean people can access official media and information provided by the government

through the intranets (HP Security Research, 2014). The military and government organizations operate separate intranets for classified information. There might be more effective targets in the intranets than the Internet, but detailed targeting is difficult because it is hard to connect to the intranets.

Most Internet services of North Korea provide North Korean propaganda to the outside world. Although many cyber attacks from North Korea have originated in third countries, the attacks in 2014 were from the IP addresses that were managed by North Korean Ministry of Post and Telecommunication, so North Korea has used their Internet resources for cyber attacks (Y. Kim, 2014). As a result, cyber targets in the North Korean Internet environment could be divided into propaganda services and cyber attack resources. Although the North Korean entities on the Internet are less effective to attack than entities in the intranets, they are technically easier to access from the outside world.

First of all, if attribution and the origin of the attack are solid, South Korea could consider the resources of the cyber attack in North Korea as possible targets since they could satisfy the principle of proportionality (Rowe, 2010). Second, because the North Korea government maintains their systems by controlling information to the people and by international propaganda to the outside world, the government responds strongly to denigration of their leadership, for example, distribution of negative information of Kim Jong-un (IUE & Ministry of Unification, 2014). In this context, the propaganda services can be good targets on the Internet. Synthetically, counterattacks to North Korea's cyber-offensive capabilities and obstructions of their propaganda activities could be good targets to send South Korea's message successfully. Alternatively, a good attack need not harm North Korea at all, just provide accurate information about the outside world on their intranets, since the North Korean government fears this information so much.

Although the best way to select targets is to choose targets that can make the biggest impacts, it is very difficult to choose targets that we cannot attack technically or targets that are risky to attack. For these reasons, recommendation of targets should be considered with attack methods. The following sections discuss possible attack methods.

2. The Stuxnet Computer Worm

According to media reports in 2014, the South Korean armed forces plan to cooperate with U.S. forces in cyberspace, which includes developing Stuxnet-like cyber weapons (BBC, 2014). Stuxnet, as revealed in 2010, is considered the first cyber weapon, and it has capabilities to attack precisely targeted facilities, such as centrifuges in Iranian nuclear enrichment facilities (Kerr, Rollins, & Theohary, 2010). Although the attack was not attributed to any country, many researchers estimate that there were national-level organizations behind this weapon because sufficient financial support, expertise associated with many technical fields besides computer science, and intelligence capabilities to collect information related to targets are required for development of this kind of weapon. Stuxnet was a computer worm that attacked a Siemens supervisory control and data acquisition (SCADA) system (Kerr et al., 2010). It likely spread to physically isolated networks by a thumb drive. This worm only did physical damage to Iranian nuclear facilities, but also infected SCADA systems in Indonesia, India, Pakistan, Germany, China, and the United States, as well as Iran.

Stuxnet has been criticized because its code still lingers on many other machines after the sabotage of Iranian nuclear programs. Ethical cyber attackers should be responsible to repair damages of cyber attacks (Rowe, 2015). Although the size of the Stuxnet's effects was reduced by anti-virus software after exposure of its existence, it was not perfectly removed.

Nevertheless, the Stuxnet code appears to have been developed by careful and sophisticated processes to achieve its goals, in contrast with cyber attacks from criminal organizations. It caused physical damage only to targeted objects and it successfully spread to physically separated networks. The first characteristic suggests the cyber weapons can be precision-guided, and the second characteristic suggests that it is possible to attack precise targets in North Korean cyberspace even though they have limited Internet connections.

3. Distributed Denial of Service Attacks

DDoS attacks were conducted by North Korea against South Korea's public and private Websites in 2009 and 2011. Most DDoS attacks are based on botnets (Radunovic, 2013). A botnet is a network of zombie PCs that are hijacked and infected to perform tasks by attackers, and are controlled remotely by command-and-control servers. Attackers deplete resources of targeted systems, such as processing power, memory, or bandwidth, with bogus requests and traffic from bots. The estimated costs to form a DDoS botnet that could attack national-level targets are 6,000 euros (Radunovic, 2013). Recently the ROKAF announced that they would purchase long-range air-to-air missiles named Taurus, which have a 500km attack range and cost 2 billion wons each, equal to 2 million dollars (Park, 2015). DDoS botnets are a considerably cheaper option with global attack capabilities.

4. Cyber Attacks for Coercion

Adversaries' weapon systems, such as air-defense systems or cyber units, could also be targets for cyber coercion (Flemming, 2014). Cyber attacks on weapon systems do not attack overall war capabilities, but attack essential parts of systems to either make the systems unreliable or cause adversaries to consider their systems to be unreliable. Most combatants will not risk conflict with infected weapon systems at the risk of their lives. Attacking on opponents' cyber units could undermine cyber offensive capabilities when both sides use cyber capabilities offensively.

Cyber attacks can also be on military supply chain and associated networks, manufacturing processes, and databases (Woods, 2015). An encryption attack of adversaries' software managing supply chains could be effective for cyber coercion. Although tension might escalate if victims respond with counterattacks, their trust of their system's integrity could be decreased. Furthermore, if an attacker possesses reversible capabilities to decrypt encrypted targets, they could hold an advantage at the negotiation table. Another strategy is DDoS attacks to hinder availability of adversaries' communication network for military supply, but they may not be enough to affect victims because their durations are limited. A third strategy is attacks on military manufacturing

processes that embed backdoors or malware in adversaries' key systems to control them. Victims have several options, such as negotiating with coercers, using other weapon systems, or repairing compromised systems, but unavailability of weapon systems for preplanned operations means strategic weaknesses. However, extensive plans and operations are required to embed a cyber weapon during a manufacturing process, and there are risks that tensions will escalate rapidly if this embedding is uncovered by the victim.

We should prepare cyber weapons for a full-scale war to handle every eventuality; we should develop many levels and kinds of cyber weapons just as an air force has many kinds of air munitions according to range, explosive power, and penetration power. However, offensive cyber coercion in response to cyber provocation in ordinary times has the more limited goals of mitigating adversaries' future attacks and preventing escalation. From this point of view, among the suggestions from (Woods, 2015), precise encryption attacks on valuable assets of opponents would be the most effective because damage from the attacks can be reversed in a short time after cessation of hostilities.

5. Recommendations: Possible Cyber Attacks

Collateral damage, difficulties of damage localization of cyber weapons, and direct damage from cyber attacks could be redeemed to a certain degree by reversibility (Rowe, 2010). Damage cannot always be recovered fully in some cases such as time-sensitive operations. Nevertheless, using reversible cyber attacks has advantages for cyberwarfare. If attackers provide recovery or assume responsibility for the damages, criticism of the attack could be reduced. Reversibility could also provide strategic flexibility. According to the international laws of war, counterattacks are justified when conducted by the principle of proportionality. However, results from activities in cyberspace are hard to predict because of the complexity and cascading effects in virtual space. Reversibility could provide a chance to reverse some or all parts of attacks if they were excessive (Rowe, 2010). However, reversibility could be less possible over time due to victims' responses.

Reversibility can be achieved using encryption attacks, obfuscating attacks, withholding-information attacks, or resource-deception attacks (Rowe, 2010). Encryption attacks affect adversaries' availability of data or programs by encrypting it in traffic or in storage. Obfuscating attacks modify data on computer systems to impede them, but do something other than encrypt it. Withholding-information attacks prevent adversaries' data handling by intercepting their traffic with deployment of man-in-the-middle interceptors. Resource-deception attacks cause adversaries inconvenience with bogus error messages about system resources.

Consider how South Korea could deploy a reversible cyber attack against North Korea. Following Chapter 2, North Korea uses their own original operating system based on Linux and applications, and their Internet connections are limited. The fact that North Korea uses only one version of an operating system means that South Korea has a simplified task in finding vulnerabilities. On the other hand, limited connections to the Internet in North Korea mean that South Korea's available targets are limited, and additional approaches are needed to access air-gapped systems. In contrast with the Internet environment, scanning and footprinting are very limited since they require direct connections to North Korea's intranets. Additional efforts from intelligence agencies and conventional espionage activities are required.

North Korea also has a vulnerability in its dependence of cyber resources on foreign countries, especially China. Due to lack of a production infrastructure, North Korea depends on importation of computers and network devices. A cyber weapon could be embedded in Chinese products that would be exported to North Korea (Woods, 2015). But there is little possibility that the Chinese government would approve, and an attempt to install malware in Chinese manufacturers without any conversation with the Chinese government could significantly hurt relations between South Korea and China. So, diplomatic conversations to reduce support from China to North Korea would be a better choice than direct deployment of cyber weapons to Chinese manufacturers.

Another method could construct new separate data-communication channels for deployment of cyber weapons (Peterson, 2013) using a Power Pwn that connects to separate wireless networks and looks like a harmless power cable, products that provide

wireless networks and look like a plug-in air cleaner, or installation of wireless network cards into their network devices or servers. North Koreans near the border between China and North Korea are already using mobile phones illegally since Chinese mobile coverage reaches them (Yeom, 2015). If modified devices are installed into their intranet near this border area where Chinese mobile data network coverage reaches, connection to North Korean intranets could be established via the Internet. Since this attempt requires installing such devices behind the North Korean border, it is more dangerous than pure cyber activities.

The next consideration is attack points. According to the principle of proportionality, after robust attribution of North Korea's cyber provocations, the Internet resources that were used for cyber attacks against South Korea would be the most justified attack points. This is similar to the situation after North Korea's land-mine provocations in 2015 when South Korea started a broadcasting campaign of psychological warfare as a response. Extraordinarily at this time, North Korea asked for conversations with the South Korean government to stop the psychological operations (Cheon & Kim, 2015), the first such response during the last 19 years since the submarine penetration provocation in 1996 (Jang, 2015). The North Korean government is very sensitive about psychological operations against their soldiers and people, and these can be good targets.

Thus, it could be very effective if South Korea could penetrate North Korean internal networks that are used by their people. However, not much is known about the North Korean intranet. If North Korea's few media Internet Websites such as Rodong (http://www.rodong.rep.kp/) have similarities to intranet sites, it could be very helpful to figure out the mechanisms of flow between them. Also, since the North Korean government is afraid that their people could get more outside information about the world, it can be effective to change their sites' contents to include news.

In addition, because joint coercion with conventional forces enhances bargaining power and prevents escalation (Flemming, 2014), South Korea should consider joint coercion or counterattacks with conventional capabilities. In addition, joint operations could include psychological operations (Cheon & Kim, 2015).

6. Assessment

The recommended cyber attacks should not have a high possibility of escalation or creating an arms race. Considering North Korea's limited Internet infrastructure, if South Korea attacks it, the North Korean government should not be able to counterattack quickly with the compromised resources. And attacks on the North Korean government's propaganda services should be less disruptive to the country than North Korea's thoughtless targeting to public and private sectors of South Korea, so the provocation is less. From the strategic point of view, reversibility could be valuable because it could provide capabilities to recover damage in a short time and gives the flexibility to use other forms of coercion if cyber coercion is ineffective. Thus, the risk of escalation is relatively less than those of viruses, worms, or other methods with hard-to-predict results.

Developing offensive countermeasures uses national resources. However, the cost of constructing a classic cyber attack tool like a DDoS botnet is only 6,000 euros, which is considerably less expensive than development and acquisition of conventional weapons (Radunovic, 2013).

Reversible cyber attacks have advantages in negotiation. The adversary may have enough resources and time to recover by itself, but the compromised service is not available during the long repairing process, which means significant losses and damage. With reversible cyber attacks, there is an incentive to negotiate an end to the conflict, because coercers hold key information to recover the compromised services in a short time (Pillar, 1983). It can also be useful to deliver a message that says there will be more powerful attacks if the adversary conducts additional hostile activities.

There are also ethical issues that occur with cyber weapons that need to be considered (Rowe, 2015). One issue is whether justification of cyber attacks is possible. Counterattacks against pure cyber attacks are hard to justify because of the difficulty of attribution in cyberspace. However, in the case of North Korea, offensive cyber capabilities and resources for cyber attacks such as Internet connections and devices are strongly controlled by the North Korean government, which means cyber attacks from North Korea may be relatively easy to attribute to the North Korean government. A

second issue is the problem of product tampering and perfidy (Rowe, 2015). Since cyber attacks involve manipulation of existing software and data without approval, this could violate end-user license agreements for software. However, in North Korea, software is owned by the North Korean government. Also because cyber attacks are more nonlethal than conventional attacks, this tampering could be excused (Strawser & Denning, 2014).

The third issue is the unreliability of cyber weapons (Rowe, 2015) because cyber attacks depend on vulnerabilities that may disappear unpredictably, including connections that could be blocked after launching attacks. However, reversible attacks with self-attribution could reverse collateral damage to noncombatants of multiple ineffective attacks, so possible problems related to this issue could be reduced. A fourth issue is related to repairing damage from cyber attacks since ethical coercers should try to make an effort to repair their damage. This could be more easily achieved by reversible attack with self-attribution than with other types of cyber attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

North Korea has conducted a range of cyber attacks against the ROK-U.S. alliance as provocations over the last 10 years. These cyber provocations are intended to press the United States and ROK as much as nuclear tests, long-range missile launches, and armed provocations at the border do on the strategic level. However, even though South Korea has highly advanced information technologies, its government has not responded well in cyberspace due to difficulty of control, ethical issues, and worries about escalation. This has enabled the North Korean government to utilize offensive cyber capabilities mostly with impunity.

North Korea's cyber attacks were conducted to reinforce their bargaining power obtained by physical provocation, which suggests that South Korea also should respond properly in cyberspace as well as physical space. To find effective countermeasures for South Korea, this study compared each of the two Koreas' cyber capabilities and analyzed previous North Korean cyber attacks. The North Korean government possesses relatively isolated internal networks and strongly controlled Internet connections. South Korea has made organizational improvements of cyber capabilities such as establishment of a cyber command. The North Korean government's cyber attacks are not random, but are related to main political issues and tend to be linked to provocations such as military tests. In cyberspace, the North Korean government has used a wide range of methods, from simple data-stealing techniques to DDoS and sophisticated attack methods by APT. North Korea has increasingly attacked the private sector and has started to threaten critical infrastructure.

This thesis recommends an integrated South Korean cyber defense based on a centralized cyber early-warning system in its network infrastructure. It further recommends coercing the North Korean government into negotiating a settlement with reversible counterattacks on Internet resources under North Korea's control and its external propaganda services. Psychological operations, which can be highly effective against North Korea, can be linked with cyber countermeasures, yielding further positive effects on bargaining power. A good defense plan could enhance South Korea's cyber

posture, boost the alliance between South Korea and the United States, and increase international cooperation in cyberspace.

For future work, detailed technical research is needed to implement these recommended measures. A good strategy could be applicable to not only South Korea but also other countries that are in similar situations with cyber threats. Establishing a cyber early-warning system requires study related to big-data methods because of the enormous data from network traffic. Further research on cyber rules of engagement could also be helpful.

LIST OF REFERENCES

Translations for titles of works notated with "in Korean" have been provided by the author.

Ahn, Y. (2011). Unusual activities of North Korea: Similar to Cheonan sinking. *The Chosun Ilbo*. Retrieved from http://media.daum.net/politics/north/view.html?cateid=1019&newsid=20110307031026751 (in Korean).

Ahn, Y. (2013). Study of development plan for national defense system against cyber attacks. *Review of the Korea Institute of Information Security and Cryptology, 23*(2), 48–54 (in Korean).

BBC. (2014). South Korea to develop Stuxnet-like cyberweapons. Retrieved from http://www.bbc.com/news/technology-26287527

Boo, H. (2013). Issue of cyber security and policy directions: discussions for the establishment of defense Ministry's Cyber Policy. *Journal of National Defense Studies, 56*(2), 97–122 (in Korean).

Carr, J. (2011). *Inside Cyberwarfare* (2nd ed.) Sebatopol, CA: O'Reilly Media.

Carr, J., & Shepherd, L. (2010). *Inside Cyberwarfare*. Sebastopol, CA: O'Reilly Media.

Chae, B. (2015). China opposed North Korea's nuclear program. *JoongAng Daily*. Retrieved from http://article.joins.com/news/article/article.asp?total_id=18108960&cloc=olink|article|default (in Korean).

Chae, J. (2013). Changing security environment and cyber security. *The Journal of Political Science and Communication, 16*(2), 171–193 (in Korean).

Cheon, G., & Kim, D. (2015). South and North Korea's agreement. *Kookmin Ilbo*. Retrieved from http://news.kmib.co.kr/article/view.asp?arcid=0009784865&code=61111611&cp=nv (in Korean).

Cho, S. (2013). North Korea's cyberwarfare capabilities and cyber threat assessment to South Korea: implications for South Korea's cyber security. *North Korean Studies Review, 17*(2), 119–147. (In Korean)

Choi, I. (2013). 6.25 Hacking Was Also Conducted by North Korea. *Yonhap News*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=0006375409 (in Korean).

Choi, K. (2011). Analysis of national defense information protection environment and study of security management model research direction to respond cyberwarfare. *Review of the Korea Institute of Information Security and Cryptology, 21*(6), 7–15 (in Korean).

Choi, K (2012). Study of real condition of national cyber defense against cyber threats. *Review of the Korea Institute of Information Security and Cryptology, 22*(8), 36–40 (in Korean).

Choi, W. (2012). North Korea launched long range missiles five times for 14 years. *Voice of America*. Retrieved from http://www.voakorea.com /content/article/1563146.html (in Korean).

Cisneros, M. (2015). *Cyber-Warfare: Jus Post Bellum*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Cloud, D. W. (2007). *Integrated Cyber Defenses: Towards Cyber Defense Doctrine*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Coleman, K. (2010). The weaponry and strategies of digital conflict. *Proceedings of the 5th International Conference on Information Warfare and Security* (p. 498). Wright-Patterson Air Force Base, OH: Air Force Institute of Technology.

Danchev, D. (2012). Q&A of the week: the current state of the cyberwarfare threat featuring Jeffery Carr. *ZDNet*. Retrieved from http://www.zdnet.com/article/q-ampa-of-the-week-the-current-state-of-the-cyber-warfare-threat-featuring-jeffrey-carr/

Department of Justice (DOJ) Office of Public Affairs. (2014). *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* [Press Release]. Retrieved from http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Dubendorfer, T., Wagner, A., & Plattner, B. (2004). An economic damage model for large-scale Internet attacks. In *13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises* (pp. 223–228). Los Alamitos, CA: IEEE Computer Society.

EC-Council (2013). *Ethical Hacking and Countermeasures* (ver.8). Clifton, Park, NY: Cengage Learning.

Eom, J., Jung, T., Han, Y., & Park, S. (2009). *Cyber Attack and Security Technology*. Seoul, Korea: Hongrung (in Korean).

Federal Bureau of Investigation (FBI) National Press Office. (2014). *Update on Sony Investigation* [Press release]. Retrieved from https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation?utm_campaign=email-Immediate&utm_medium=email&utm_source=national-press-releases&utm_content=386194

Flemming, D. R. (2014). *Offense-In-Depth: An Analysis of Cyber Coercion*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Flemming, D. R., & Rowe, N. C. (2015). Cyber coercion: cyber operations short of cyberwar. *Proceedings of the 10th International Conference on Cyberwarfare and Security ICCWS-2015* (pp. 95–101). Sonning Common, England: Academic Conferences and Publishing International.

Fredrick, E. E. (2011). *Testing a Low-Interaction Honeypot against Live Cyber Attackers*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Golling, M., & Stelte, B. (2011) Requirements for a future EWS - cyber defence in the Internet of the future. *Proceedings of the 3rd International Conference on Cyber Conflict (ICCC*; pp. 1–16). Tallinn, Estonia: CCD-COE.

Green, J. A. (2015). *Cyberwarfare: A Multidisciplinary Analysis*. London, England: Routledge.

Han, S. (2013). North Korea pushed ahead with the third nuclear weapon test. *Voice of America*. Retrieved from http://www.voakorea.com/content/article/1601823.html (In Korean)

Harrington, S. L. (2014). Cyber security active defense: Playing with Fire or Sound Risk Management? *Richmond Journal of Law & Technology*, *20*(4), pp. 1–41

Hewlett-Packard (HP) Security Research. (2014). *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape* (HP Security Briefing Episode 16). Retrieved from http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf

Hong, S. (2011). North Korea's cyber attack methods, advanced and intelligent. *The Unified Korea, 328*, 34–35 (in Korean).

Institute of Unification Education (IUE) & Ministry of Unification. (2014). *Understanding North Korea 2014*. Seoul, Republic of Korea: Nuel-Pum Plus.

Internet Corporation for Assigned Names and Numbers (ICANN) Security and Stability Advisory Company (SSAC). (2006). *SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks*. Retrieved from https://www.icann.org/en/system/files/files/dns-ddos-advisory-31mar06-en.pdf

Jang, H. (2015). MOU said this is the first expression of regret since 1996. *Seoul Traffic Broadcasting*. Retrieved from http://www.tbs.seoul.kr/news/bunya.do?method=daum_html2&typ_800=9&seq_800=10105480 (In Korean)

Joint Chiefs of Staff. (2013). *Cyberspace Operations* (Joint Publication 3–12[R]). Washington, DC: Author.

Jun, B. (2012). North Korea announced they will attack South Korean media. *The Kyunghyang Shinmun.* Retrieved from http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201206042159245&code=910303 (In Korean)

Jung, H. (2011). DC Insider users hacked North Korean website uriminzokkiri.com. *Dong-A Ilbo*. Retrieved from http://news.donga.com/3/all/20110108/33797197/1 (In Korean).

Jung, M. (2010). ROKS Cheonan was sunk by North Korean torpedo. *Tongil News*. Retrieved from http://www.tongilnews.com/news/articleView.html?idxno=90244 (In Korean).

Jung, S. (2013). Level of North Korea's hackers equal to CIA. *Money Today*. Retrieved from http://news.mt.co.kr/mtview.php?no=2013011611435302323 (In Korean)

Jung, Y. (2010). Reccurence of DDoS attack against the Blue House, the ministry of foreign affair, and naver.com. *News Hankuk*. Retrieved from http://www.newshankuk.com/news/content.asp?news_idx=20100708092500n5131 (in Korean).

Kang, S. (2015). NIS opened logs of hacking software. *E Daily*. Retrieved from http://www.edaily.co.kr/news/NewsRead.edy?SCD=JF21&newsid=03286566609435504&DCD=A00602&OutLnkChk=Y (In Korean)

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (R41524). Washington, DC: Congressional Research Service.

Kim, D. (2010). North Korea announced they targeted ROK marine units. *YTN*. Retrieved from http://www.yonhapnews.co.kr/politics/2010/11/26/0505000000AKR20101126105800014.HTML?cd8ec7c0 (In Korean)

Kim, E. (2013). S. Korean military to prepare with U.S. for cyberwarfare scenarios. *Yonhap News*. Retrieved from http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML (In Korean)

Kim, H. (2010). Cyber terror and national security. *Justice, 121*, 319–356 (in Korean).

Kim, H. (2010). North Korea's cyber terror and information warfare capabilities, and cyber security countermeasure proposals. *Boan.com.* Retrieved from http://www.boan.com/news/articleView.html?idxno=1391 (in Korean)

Kim, K. (2005). South Korean military and intelligence agencies worries wireless connection near military demarcation kine. *Yonhap News*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=001&aid=0001119419 (in Korean)

Kim, K. (2009). North Korea confirmed ICBM technology. *The Hankyoreh*. Retrieved from http://www.hani.co.kr/arti/politics/defense/348041.html (in Korean).

Kim, K. (2012). North Korea threatened south korean news media. *The Hankyoreh*. Retrieved from http://www.hani.co.kr/arti/politics/defense/536122.html (in Korean)

Kim, K. (2014). South Korea develops Korean stuxnet. *Yonhap News*. Retrieved from http://www.yonhapnews.co.kr/politics/2014/02/19/0505000000AKR20140219061700043.HTML (in Korean).

Kim, S. (2015). Comparison of South and North Korea's military power according to the 2014 defense white paper. *KONAS Net*. Retrieved from http://konas.net/article/article.asp?idx=39857 (in Korean)

Kim, T. (2009). North Korea announced nuclear test was successful. *YTN*. Retrieved from http://www.ytn.co.kr/_ln/0101_200905251258363886 (in Korean)

Kim, W., Park, C., Lee, S., and Lim, J. (2014) Methods for classification and attack prediction of attack groups based on framework of cyber defense operations. *Journal of Korean Institute of Information Scientists and Engineers (KIISE): Computing Practices and Letters, 20*(6), 317–328 (in Korean).

Kim, Y. (2015). KHNP hacking is attributed to North Korea. *Pressian*. Retrieved from http://www.pressian.com/news/article.html?no=124755 (in Korean).

Ko, J., & Kim, J. (2009). Empirical analysis of negotiation determinants on economic cooperation of South-North Korea. *The Journal of Korea Research Society of Customs, 10*(4), 447–469 (in Korean).

Korea Internet and Security Agency (KISA) and Consortium of Computer Emergency Response Team (CONCERT). (2010). *Computer Emergency Response Team (CERT) Building and Operation Book*. Seoul, Republic of Korea: Ho-jung C&P (in Korean).

Kshetri, N. (2014). Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses. *East Asia, 31*, 183–201.

Lee, B. (2009). North Korea discharged hwangkang dam, six people missing. *SBS*. Retrieved from http://news.sbs.co.kr/news/endPage.do?news_id=N1000640205 (in Korean).

Lee, B. (2015). North Korean website Uriminzokkiri unserviceable. *Yonhap News*. Retrieved from http://www.yonhapnews.co.kr/bulletin/2015/06/24/0200000000AKR20150624144800014.HTML (in Korean).

Lee, D. (2009). The third naval battle. *SBS*. Retrieved from http://www.ytn.co.kr/_ln/0101_200911101859106272 (in Korean).

Lee, H. (2013). *Development Trends of National Defense Cyberwarfare* (Agency for Defense Technical Investigation Paper 2013; 86–99). Seoul, Republic of Korea: Defense Agency for Technology and Quality (in Korean).

Lee, M. (2011). North Korean OS 'Red Star 2.0', very vulnerable against cyber attacks. *Digital Daily*. Retrieved from http://www.ddaily.co.kr/news/article.html?no=84158 (in Korean).

Lim, J., Kwan, Y., Chang, K., & Baek, S. (2013). North Korea's cyber war capability and South Korea's national counterstrategy. *The Quarterly Journal of Defense Study Policy Studies, 29*(4), 9–45 (in Korean).

Lee, K. (2008). Joint Investigation Group, Mr. Park, Wang-ja was shot at 05:15. *Tongil News*. Retrieved from http://www.tongilnews.com/news/articleView.html?idxno=79817 (in Korean).

Lee, S. (2009). National important information was leaked through a hole of the military Internet. *Yonhap News*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=001&aid=0002922925 (in Korean)

Lee, Y., Kwon, H., Lee, J., & Shin, D. (2015). Development of countermeasures against North Korean cyberterrorism through research case studies. *The Korean Journal of Defense Analysis, 27*(1), 71–86 (in Korean).

Mansourov, A. (2014). *North Korea's Cyberwarfare and Challenges for the U.S.-ROK Alliance* (Korea Economic Institute of America Academic Paper Series 2014). Washington, DC: Korea Economic Institute of America, 1–17.

Ministry of National Defense (MND). (2015). *2014 Defense White Paper* (MND 02–748-6237). Seoul, Republic of Korea. Retrieved from http://ebook.dema.mil.kr/home/view.php?host=main&site=20150108_150108 (in Korean)

Ministry of Science, ICT, and Future Planning (MSIP), & Korea Internet and Security Agency (KISA). (2014). *Korea Internet White Paper 2014* (GPRN 11-B551505-000008-10). Seoul, Republic of Korea: Myeong-jin C&P.

Ministry of Unification (MOU). (2014). *Organizational Chart of North Korean Leadership*. Seoul, Republic of Korea. Retrieved from http://nkinfo.unikorea.go.kr/nkp/pblictn/viewPblictn.do

National Intelligence Service (NIS). (2015). *National Information Security White Paper 2015*. Seoul, Republic of Korea. Retrieved from http://isis.kisa.or.kr/ebook/ebook2.html (in Korean)

Noh, H. (2015). U.S. condemns N. Korea's planting of landmines. *Yonhap News*. Retrieved from http://www.yonhapnews.co.kr/bulletin/2015/08/12/0200000000AKR20150812011000071.HTML (in Korean).

Office of the Secretary of Defense. (2013). *Military and Security Developments Involving the Democratic People's Republic of Korea 2012*. Washington, DC: Author.

Oh, Y. (2015). North Korea omitted the news of the Chinese ambassador: reflection of cold relationship between North Korea and China. *Yonhap News Agency*. Retrieved from http://www.yonhapnews.co.kr/bulletin/2015/06/19/0200000000AKR20150619172500014.HTML?input=1195m (in Korean).

Park, B. (2015). ROKAF acquires Taurus missiles. *Segye Ilbo*. Retrieved from http://www.segye.com/content/html/2015/01/05/20150105003958.html (in Korean).

Park, D. (2011). Study of hacking in terms of national cyber security policy. *Review of the Korea Institute of Information Security and Cryptology*, *21*(6), 24–41 (in Korean).

Park, N. (2014). MS 98%, Android 85%, South Korea's OS share rates. *Asia Economics*. Retrieved from http://www.asiae.co.kr/news/view.htm?idxno=2014082810212498335 (in Korean).

Park, Y. (2013). Police announced that hacking on Joongang Ilbo in 2012 was from North Korea. *Yonhap News*. Retrieved from http://www.yonhapnews.co.kr/society/2013/01/16/0701000000AKR20130116090400004.HTML (in Korean).

Patrikakis, C., Masikos, M., & Zouraraki, O (2004). Distributed denial of service attacks. *The Internet Protocol Journal 7*(4), 13–35.

Peterson, D. (2013). Offensive cyber weapons: construction, development, and Employment. *Journal of Strategic Studies, 36*(1), 120–124.

Pfleeger, P. C., & Pfleeger, L. S. (2012). *Analyzing Computer Security: A Threat, Vulnerability, Countermeasure Approach*. Upper Saddle River, NJ: Prentice Hall.

Pillar, P. R. (1983). *Negotiating Peace: War Termination as a Bargaining Process.* Princeton, NJ: Princeton University Press.

Radunovic, V. J. (2013). DDoS – available weapon of mass disruption. *Proceedings of the 2013 21st Telecommunications Forum (TELFOR)*. Piscataway, NJ: IEEE.

Richwine, L. (2014). Cyber attack could cost Sony studio as much as 100 million. *Reuters*. Retrieved from www.reuters.com/article/2014/12/09/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209

Robinson, M., Jones, K., & Janicke, H. (2015). *Cyberwarfare: Issues and Challenges. Computers and Security, 49,* 70–94.

Rowe, N. C. (2010). Towards reversible cyberattacks. *Proceedings of the 9th European Conference on Information Warfare and Security*. Reading, England: Academic Publishing.

Rowe, N. C. (2015). Distinctive ethical challenges of cyberweapons, In N. Tssagourias & R. Buchan (Eds.), *Research Handbook on Cyber Space and International Law* (pp. 307–325), Cheltenham, England: Edward Elgar.

Schelling, T. C. (1966). *Arms and Influence*. New Haven, CT: Yale University Press.

Schelling, T. C. (2008). *Arms and Influence: With a New Preface and Afterword*. New Haven, CT: Yale University Press.

Schmitt, N. M. (2013). *Tallinn Manual on the International Law Applicable to Cyberwarfare*. New York, NY: Cambridge University Press.

Sharma, A., Gandhi, R., Mahoney, W., Sousan, W., & Zhu Q. (2010). Building a social dimensional threat model from current and historic events of cyber attacks. *Proceedings of the 2010 IEEE 2nd International Conference on Social Computing* (SocialCom; pp. 981–986). Los Alamitos, CA: IEEE Computer Society.

Shin, H. (2011). N.K. commits 221 provocations since 1953. *The Korean Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20110105000563

Shin, H. (2014). Cyber command devises a development plan. *Boan.com*. Retrieved from http://www.boan.com/news/articleView.html?idxno=9351 (in Korean).

Singer, P.W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know* (1st ed.). New York, NY: Oxford University Press.

Son, S. (2009). North Korea launched SCUD missiles. *SBS*. Retrieved from http://news.sbs.co.kr/news/endPage.do?news_id=N1000615154 (in Korean).

Strawser, B., & Denning, D. (2014). Moral Cyber Weapons: The Duty to Employ Cyberattacks. In M. Taddeo L. Floridi (Eds.), *The Ethics of Information Warfare* (pp. 85–103). Berlin, Germany: Springer.

Ventre, D. (2011). *Cyberwar and Information Warfare*. Hoboken, NJ: John Wiley and Sons.

Woods, C. M. (2015). *Implementing Cyber Coercion*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Worker's Party of Korea (WPK). (2010). *Worker's Party of Korea Charter*. Pyongyang, Democratic People's Republic of Korea: WPK.

Yeom, Y. (2015). North Korea is at war with cell phones. *Segye Ilbo*. Retrieved from http://www.segye.com/content/html/2015/02/17/20150217002868.html (in Korean)

Yoo, H., & Yoo, D. (2014). Basic matrix to respond to cyber attacks. *Internet and Security Focus, June 2014*, 15–38 (in Korean).

Yoon, H. (2012). *Cyberterrorism: Trends and Responses*. Korean Institute of Criminology (in Korean).

Yoon, J. (2012). *Counterparts Strategy of Korean Army for the Cyber Space Operations*. Master's thesis, Graduate School of Politics and Leadership, Kookmin University, Seoul, Republic of Korea (in Korean).

Yoon, K. (2011). North Korea's cyberwarfare: the capability and threat. *Military Forum, 68*, 64–95 (in Korean).

Yoon, S. (2014). ADD hacked, leakage of military secrets. *Dong-A Ilbo*. Retrieved from http://news.donga.com/3/all/20140410/62408737/1 (in Korean).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California