NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DEFENSE ANALYSIS CAPSTONE

HOW TO IMPROVE THE ROK AND U.S. MILITARY ALLIANCE AGAINST NORTH KOREA'S THREATS TO CYBERSPACE: LESSONS FROM NATO'S DEFENSE COOPERATION

by

Duri Lee

December 2017

Thesis Advisor: Hy Rothstein
Co-Advisor: Dorothy E. Denning

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 2017	**3. REPORT TYPE AND DATES COVERED** Capstone	
4. TITLE AND SUBTITLE HOW TO IMPROVE THE ROK AND U.S. MILITARY ALLIANCE AGAINST NORTH KOREA'S THREATS TO CYBERSPACE: LESSONS FROM NATO'S DEFENSE COOPERATION			**5. FUNDING NUMBERS**
6. AUTHOR(S) Duri Lee			
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 number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

This research explores how South Korea, or the Republic of Korea (ROK), and the U.S. military can cooperate against common cyber threats on the Korean peninsula through open-source data research. The purpose of this research is to suggest recommendations for policy makers on how to exploit North Korea's vulnerabilities and how to mitigate the weaknesses of the ROK and U.S. alliance. Furthermore, it identifies lessons that the ROK and U.S. alliance can glean from NATO's cyber cooperation.

To maintain the balance of power with the ROK, North Korea has focused on the development of asymmetric capabilities. As part of this effort, North Korea's offensive cyber capabilities have targeted South Korea for several years. The ROK's inadequate defense against North Korea's cyber-attacks has caused anxiety for the ROK, which has influenced ROK–U.S. military operations. The study, however, also finds North Korea has four vulnerabilities related to cyberspace. This information can be useful for the ROK and U.S. alliance, which has affirmed its intentions to broaden the cooperation to cyberspace. As cyber cooperation is still an immature cooperation system, it could also benefit from the example of the North Atlantic Treaty Organization's endeavors to achieve cooperation in cyberspace.

14. SUBJECT TERMS North Korea, South Korea, the DPRK, the ROK and U.S. alliance, cyberspace, NATO			**15. NUMBER OF PAGES** 117
			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.

HOW TO IMPROVE THE ROK AND U.S. MILITARY ALLIANCE AGAINST NORTH KOREA'S THREATS TO CYBERSPACE: LESSONS FROM NATO'S DEFENSE COOPERATION

Duri Lee
Captain, the Republic of Korea Army
B.A., Korea Military Academy, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

NAVAL POSTGRADUATE SCHOOL
December 2017

Approved by: Hy Rothstein
Thesis Advisor

Dorothy E. Denning
Co-Advisor

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research explores how South Korea, or the Republic of Korea (ROK), and the U.S. military can cooperate against common cyber threats on the Korean peninsula through open-source data research. The purpose of this research is to suggest recommendations for policy makers on how to exploit North Korea's vulnerabilities and how to mitigate the weaknesses of the ROK and U.S. alliance. Furthermore, it identifies lessons that the ROK and U.S. alliance can glean from NATO's cyber cooperation.

To maintain the balance of power with the ROK, North Korea has focused on the development of asymmetric capabilities. As part of this effort, North Korea's offensive cyber capabilities have targeted South Korea for several years. The ROK's inadequate defense against North Korea's cyber-attacks has caused anxiety for the ROK, which has influenced ROK–U.S. military operations. The study, however, also finds North Korea has four vulnerabilities related to cyberspace. This information can be useful for the ROK and U.S. alliance, which has affirmed its intentions to broaden the cooperation to cyberspace. As cyber cooperation is still an immature cooperation system, it could also benefit from the example of the North Atlantic Treaty Organization's endeavors to achieve cooperation in cyberspace.

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

ACO	Allied Command Operations (of NATO)
ASPI	Australian Strategic Policy Institute
ATC	Allied Transformation Command (of NATO)
CCWG	Cyber Cooperation Working Group (of R – U)
CDMB	Cyber Defense Management Board
CERTs	Computer Emergency Response Teams
CFC	Combined Forces Command (of the ROK and U.S. alliance)
CIS	Communication and Information System
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
DOD	Department of Defense
DDoS	Distributed Denial of Service
DPRK	Democratic People's Republic of Korea
DTICC	Defense Technological and Industrial Cooperation Committee
EASI	East Asia Strategic Initiative
EU	European Union
FMS	Foreign Military Sales
FOC	Full Operational Capability
GPS	Global Positioning System
GSD	General Staff Department (of North Korea)
HQ AIRCOM	Headquarters Allied Air Command
HQ LANDCOM	Headquarters Allied Land Command
HQ MARCOM	Headquarters Allied Maritime Command
IA / CNDSOP	Information Protection / Network Defense Information Exchange Operation Plan
ICT	Information Communications Technology
IP	Internet Protocol
ITU	International Telecommunication Union
IW	Information War
JCS	Joint Chiefs of Staff

JFCBS	Joint Force Commands in Brunssum, the Netherlands
JFCNP	Joint Force Commands in Naples, Italy
JSA	Joint Security Area (on the Korean Peninsula)
KR/FE	Key Resolve / Foal Eagle (on the Korean Peninsula)
KPA	Korean People's Army (of North Korea)
KMAG	Korean Military Advisory Group (of the U.S. military in Korea)
MPAF	Ministry of People's Armed Forces (of North Korea)
NAC	Norther Atlantic Council
NATO	North Atlantic Treaty Organization
NCI Agency	NATO Communication Information Agency
NCIRC	NATO Computer Incident Response
NDC	National Defense Commission
NSA	National Security Agency
NSC8	National Security Council Document No. 8
NPT	Nuclear Proliferation Treaty
OSINT	Open Source intelligence
RGB	Reconnaissance General Bureau (of North Korea)
ROK	Republic of Korea
RRT	Rapid Reaction Team
SAC	State Affairs Commission (of North Korea)
SCM	Security Consultative Meeting (of the ROK and U.S. alliance)
SHAPE	Supreme Headquarters Allied Powers Europe
USFK	U.S. Forces Korea
USSR	Union of Soviet Socialist Republic
UFG	Ulji Freedom Guardian (on the Korean Peninsula)
WPK	Workers' Party of Korea = Korean Worker's Party (of North Korea)
WMD	Weapon of Mass Destruction

ACKNOWLEDGMENTS

I want to thank my family members who always support me, including my father in heaven, and Korea, which gave me a chance to come here. I want to express my love my mother, In-suk; my sister, Yoon-seo; and lovely brother, Jung-woo. I especially am grateful to my dad. who, Whenever I felt stressed, met me you in my dreams to reassure me. His encouragement gave me motivation so that I could study hard. Dad, I really miss you.

The journey in Monterey has been an awesome experience for me. It always will be a pivotal experience in my life. I will not forget what I studied here, nor the friendships I made.

I want to express my gratitude to my advisors, Professors Hy Rothstein and Dorothy E. Denning. I really appreciate your comments. I also appreciate the advice from the Graduate Writing Center Coach Marianne. Lastly, I pray for peace on the Korean peninsula and peace in the world for all who are suffering from war and dictatorship.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

In 2016, the Democratic People's Republic of Korea (DPRK), known as North Korea, hacked the data server belonging to the military of the Republic of Korea (ROK), known as South Korea.[1] The attackers had conducted hacking for several months through the primary server, which connected to every computer in the South Korean military intranet. The effects of the attack were not only the disruption of the system and leakage of clandestine information but also fear and shock for South Korea because it showed that the military network could be a target and suffer critical damage. Although direct threats from nuclear weapons and missiles are currently the main security issues on the Korean Peninsula, the ROK has to remain vigilant at all times against cyber threats.

This research started from the awareness that it is essential to establish effective cyber policy that will enable the ROK military to achieve dominance in cyberspace. The author examines military strategy in cyberspace, keeping abreast of the responsibilities of the government to secure the private sector. The attack in 2016, which directly targeted the military system, underscores the importance of securing the ROK military in cyberspace. Cybersecurity is linked directly to national security in the ROK. Although challenging for the military, as the primary target of adversaries, the military needs to develop its cyber strategy.

B. PRIOR RESEARCH

With the increased dependency on weaponries systems that rely on cyberspace, the importance of securing cyberspace becomes a primary issue on the Korean peninsula. Most of the preceding research about cyber threats to the ROK and the United States on the Korean peninsula focuses on North Korea's cyber threats.

A great deal of research exists on North Korea's cyber capability. In 2015, Scott LaFoy, Jenny Jun, and Ethan Shon explored North Korea's cyber operations, focusing on

[1] "S.Korean Military Says N. Korea behind Last Year's Hacking Attack," *Yeonhap News*, May 2, 2017, http://english.yonhapnews.co.kr/national/2017/05/02/0301000000AEN20170502007600315.html.

its strategy and organization.[2] The report suggests North Korea's cyber strategy is a part of asymmetric methods for achieving national goals. In 2013, Jong-in Lim, Gyu-hyun Jang, and Seung-jo Baek evaluated North Korea's cyber capability in offense and defense, and analyzed several factors for assessing cyber capabilities, including infrastructure, intentions of leadership, weapon systems, cyber warriors, organization, cyber doctrine, strategy and tactics, and foreign affairs.[3] A 2014 report from Hewlett Packard studied factors within North Korea's cyber capabilities from political characteristics to technical developments. [4] Specifically, the report studied North Korea's internal and political environments, capabilities and constraints, past cyber-attacking cases, and foreign affairs related to its cyber threats. To evaluate the cyber capabilities and limitations, the report included open source information about North Korea's infrastructure, intelligence organization, doctrine, cyber doctrine and strategy, and cyber warfare operations. A paper in 2014 by Alexandre Mansourov of the U.S.-Korea Institute at Johns Hopkins University examined North Korea's cyber doctrine, capabilities based on organization analysis, and its vulnerability.[5] A 2017 report from the Congressional Research Service shows North Korea's capabilities have become sophisticated and analyzes that country's intentions for its cyberattacks, focusing on the economic benefits for North Korea.[6]

Because North Korea poses a serious national security threat to the ROK and the United States, most of the research connects to the question of how to develop the counter strategy in the ROK and the United States. Multiple analyses about North Korea's cyber-attacks have centered on an effective counter response at the strategic level

[2]Scott LaFoy, Jenny Jun, and Ethan Sohn, *North Korea's CyberOperations: Strategy and Responses* (Washington, DC: Center for Strategic & International Studies, 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

[3]Yu-jung Kwon, Jong-in Lim, Gyu-hyun Jang, Seung-jo Baek, "North Korea's Cyber War Capability and South Korea's National Counterstrategy," *National Strategy Research* 102 (Winter 2013): 9–45, http://kiss.kstudy.com/journal/thesis_name.asp?key=3203642.

[4]HP Security Research, *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, HP Security Briefing Episode 16 (HP Company, August, 2014).

[5]Alexandre Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*, in Academic Paper Series (Washington, DC: Korea Economic Institute of America, December 2, 2014).

[6]Liana W. Rosen, Emma Chanlett-Avery, John W. Rollins, Catherine A. Theohary, *North Korean Cyber Capabilities: In Brief*, R44912 (Washington, DC: Congressional Research Service, August 3, 2017).

and suggest improved cooperation by the ROK and the United States as a partial solution to counteract cyber threats in the national strategy.[7] In 2015, LaFoy, Jun, and Shon recommended the ROK and U.S. alliance needs to increase resilience and strength toward North Korea's cyber threats.[8] Their report suggested preparing for North Korea's combined cyber and military operations over pure cyber-attacks. Mansourov, furthermore, suggested using the framework of the ROK-U.S. mutual defense treaty for cooperation in cyberspace.[9] As a similar example of expanding the preexisting alliance into cyberspace, the author considers the North Atlantic Treaty Organization (NATO) case.

While it is anticipated that North Korea will threaten the national security of the ROK as well as the ROK and U.S. military on the Korean Peninsula through cyberspace, the research until now is limited in addressing how the combined military will effectively counter these cyber threats.[10] The possible cyber threats of the DPRK toward the ROK and the United States are significant; at the same time, the militaries of the ROK and the United States have in common are high dependency on cyberspace, even in the military operation for securing the Korean Peninsula. Until now, most of North Korea's cyber-attacks have not been combined with kinetic attacks; however, the connection between cyberspace in military operations has become severe. This research can provide possible solutions for securing the new domain within the pre-existing structure of the ROK and U.S. alliance, and enable the alliance to explore effective responses to expected future conditions, such as a decrease in the ROK and U.S. alliance's combat efficiency caused by North Korean cyber operations conducted prior to or during a war.

---

[7]Kwon, Lim, Jang, and Baek, "North Korea's Cyber War Capability and South Korea's National Counterstrategy," 9–45.

[8]LaFoy et al. *North Korea's CyberOperations: Strategy and Responses.*

[9]Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*.

[10]"U.S. Collective Defense Arrangements," U.S. Department of State, accessed October 1, 2017, https://www.state.gov/s/l/treaty/collectivedefense/. The ROK-U.S. mutual defense treaty is "a treaty signed October 1, 1953, whereby each party recognizes that an armed attack in the Pacific area on either of the Parties would be dangerous to its own peace and safety and that each party would act to meet the common danger in accordance with its constitutional processes."

C. METHODOLOGY

This research examines *how the ROK and the U.S. military can cooperate against common cyber threats on the Korean Peninsula* by qualitatively analyzing open source data. In each chapter, the study explores answers to the following four questions, which enables the author to answer the central question.

1. What are the cyber threats on the Korean Peninsula?

2. What is the nature of the existing cooperative agreement between the ROK and the United States?

3. What are the deficiencies in the security agreement between the ROK and the United States relating to cyber threats?

4. How could this agreement be strengthened to better address cyber threats?

In addressing these questions, the thesis examines the steps taken by NATO to address cyber threats against that alliance.[11] NATO has made efforts to improve cyber operational capabilities and international cooperation for cyber defense since 2002.[12] Therefore, this research seeks lessons from NATO. In particular, the 2016 *NATO Cyber Capability: A Strategic and Operational Evaluation*, assessed the current cooperation among NATO countries according to three criteria: operational planning; doctrine and methods; and education, training, and exercises.[13] The study reviewed their efforts to quickly develop a more mature cooperation in cyberspace.

This research reviews various open-source data, including research papers, theses, journal articles, newspapers, government publications, and books related to cyber issues and ROK national security issues. The focused research period starts in 2012 when Kim Jung-Un became the leader of North Korea. [14]

---

[11]Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*.

[12]Jeffrey L. Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution* (Carlisle Barracks, PA: Army War College, 2016), 1.

[13]Ibid.

[14]"Kim Jong Un Fast Facts," CNN Library, September 28, 2017, http://www.cnn.com/2012/12/26/world/asia/kim-jong-un---fast-facts/index.html.

This research has three limitations. First, all of the data comes from open-source intelligence (OSINT), and it is incomplete. Cyber strategy and issues in most countries are either concealed by the government or outdated. OSINT about countries like North Korea also may reflect both misinformation and disinformation. Additionally, the terms and titles of organizations in the report are outdated, because North Korea changed the titles of organizations after the 7th Congress of the Workers' Party of Korea (WPK) in 2016.[15] Lastly, a lack of consensus on terminology between Korean and English also poses challenges.

A study using OSINT in Korean and English, nevertheless, is still valuable. The OSINT of the United States and South Korea provides a great deal of public information on cyber strategy and policy, which helps to understand the two countries. OSINT is also essential in studying North Korea, which is a closed country. Considering the acquisition of information on North Korea is limited, the knowledge gained through open-source data is meaningful. In addition, the cyber issues on the Korean Peninsula are ongoing and impact South Korea and the United States, the main actors in Korean Peninsula security against the DPRK.

D. OVERVIEW OF THE RESEARCH

This research has two broad aspects: the cyber threats on the Korean Peninsula and suggestions on how to strengthen the ROK and U.S. alliance to defend against these *cyber threats*. Chapter II defines the *cyber threats* and asymmetric characteristics of the conflict on the Korean Peninsula as the background for the research. Chapter III studies the cyber threats of the DPRK. It mainly focuses on North Korea's intentions, what makes North Korea a real threat, and finally suggests implications on policy for the ROK and the United States by identifying the vulnerabilities of North Korea. Chapter IV assesses the current stance of the ROK and U.S. alliance to cooperate in cyberspace. It includes understanding the nature of the ROK and U.S. alliance and identifying its

[15]The title of North Korea's organizations was outdated in LaFoy, *North Korea's CyberOperations: Strategy and Responses* in 2015 and in Alexandre Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance" in 2014, because they were changed after the 7th Congress of the WPK in 2016 according to the White Paper of the ROK in December 2016.

deficiencies. Chapter V introduces NATO's process to defend against cyber threats. Finally, by summarizing findings, Chapter VI answers the central question of *how the ROK and U.S. military can cooperate against common cyber threats on the Korean Peninsula*.

II. BACKGROUND OF RESEARCH

A. WHAT ARE CYBER THREATS AND CYBER SECURITY

As the first step, this section explores the background of cyber threats and cyber security.

1. Cyber Threats

The basic terms for this research follow the definitions of the U.S. military, considering its maturity in building the norms and standards of cyberspace. An Australian report on cyber maturity in 2016 rated the United States and South Korea as the leading countries based on the development of governance, business, cybercrime, military, and social structures and assessed that the United States devotes significant effort to cyber issues.[16]

According to the U.S. Joint Publication JP 3-12, *cyberspac*e is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[17] The 2015 Department of Defense (DOD) Cyber Strategy defined *cyber threats* as malicious cyber activities, such as "to steal intellectual property, disrupt an organization's operations for activist purposes, or to conduct disruptive and destructive attacks to achieve military objectives."[18] The definition of the DOD specifies cyber threats based on specific behaviors, intention, and targets.

---

[16]Tobias Feakin et al., *Cyber Maturity in the Asia-Pacific Region 2016* (Austrailia: The Australian Strategic Policy Institute Limited, 2016): 9-11, http://www.spain-australia.org/files/documentos/62_ASPI-Cyber-Maturity-2016.pdf.

[17]Joint Chiefs of Staff, *Cyber Operations*, JP 3-12 (R) (Washington, DC: Joint Chiefs of Staff, 2013), 5, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[18]U.S. Department of Defense, *The DoD Cyber Strategy* (Washington, DC: Department of Defense, 2015), 9, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Cyber threats follow the general notion of threats. First, threats do not exist without the malicious intent of the actor. Even if an unintentional attack happens and causes damage, it is not a threat because it is not coordinated as part of an intentional attack. A temporary vulnerability caused by accident could multiply the real attacker's efficiency and; it might be difficult to control. Second, a threat exists when one who has intention also has the capabilities to attack and inflict damage. If the offender is stronger than the defender, the offender's behavior can be a true threat. On the other hand, if the defender can adequately defend against the attack, the threat has no power.

2. Cyber Security

Cyber security is a complementary concept to cyber threats. While cyber threats focus on adversaries, cyber security focuses on defending potential victims against cyber threats. According to the U.S. DOD definition, cyber security means "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." [19] This research distinguishes between cyber security and cyber threats, and considers the problem of cyber threats.

B. ASYMMETRY

Asymmetry, a term commonly used today, has been practiced in war since ancient times. The battle of Pelusium in 525 BC is one example of the introduction of innovative methods to gain an advantage in war. In the battle, the Persian army broke the Egyptian army by throwing live cats into the middle of the battlefield against the Egyptians who worshipped the animal.[20]

---

[19]U.S. Department of Defense, *Cybersecurity*, DOD Instruction 8500.01 (Washington, DC: Department of Defense, March 14, 2014), 55.

[20]Joshua J. Mark, "The Battle of Pelusium: A Victory Decided by Cats," Ancient History Encyclopedia, last modified June 13, 2017, https://www.ancient.eu/article/43/the-battle-of-pelusium-a-victory-decided-by-cats/.

Asymmetry is an excellent window through which to understand the conflict structure. Steven Metz and Douglas V. Johnson II in 2001 defined strategic asymmetry as "the use of some sort of difference to gain an advantage over an adversary."[21] The origin of strategic asymmetry is founded on the concept of deception in the book the Art of War by Sun Tzu.[22] "Asymmetry in armed conflict," in particular, comes from the varied disproportion of military and economic power.[23] It refers to the disparity in resources and potential power, specifically the gaps of various elements of national power between the strong and the weak.

As a great power, the United States has identified asymmetric capabilities, possibilities, and threats of the enemy to counteract the dominance of the United States.[24] The first use of asymmetry comes from different response methods, and the United States has used "asymmetric engagement" to define the surface-to-air missiles (Army based) to counter an opponent's air superiority.[25] As the threats and environment have changed, the concept of asymmetry has evolved and broadened to include new threats. For example, the National Military Strategy included the threat of Weapons of Mass Destruction (WMD) and information warfare in 1995.[26] Through the Iraq and Afghanistan War,

---

[21]Steven Metz and Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2001): 1, http://ssi.armywarcollege.edu/pdffiles/pub223.pdf.

[22]Edward Luttwak, *Strategy: The Logic of War and Peace*, Revised and Enlarged Edition (Cambridge, MA: The Belknap Press of Harvard University, 2001), quoted in Metz and Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, 1.

[23]Ekaterina Stepanova, *Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects,* SIPRI Research Report No. 23 (New York: Oxford University Press, 2008), 14–15, https://www.sipri.org/sites/default/files/files/RR/SIPRIRR23.pdf.

[24]Kuyoun Chung, "Strategic Asymmetry and North Korea's Asymmetric Threats, " in *Innovation of Science and Technology and North Korea's Asymmetric Threat : Rise of Cyber Warfare and Unmanned Aerial Vehicle*, ed. Kuyoun Chung and Gi-tae Lee (Seoul, Republic of Korea: Korea Institute for National Unification, Innovation of Science and Technology, 2016), 9.

[25]John M. Shalikashvili, *Doctrine for Joint Operations* (Joint Pub 3-0), (Washington, DC: Chairman of the Joint Chiefs of Staff, February 1, 1995), III-10.; quoted in Chung, "Strategic Asymmetry and North Korea's Asymmetric Threats," 10.

26John M. Shalikashvili, *National Military Strategy* (Washington, DC: Chairman of the Joint Chiefs of Staff, February 1995), 19, quoted in Chung, "Strategic Asymetry and North Korea's asymetric threats,"10.

asymmetric threats have included terrorism, guerrilla warfare, cyber-warfare, and Information War (IW)."[27]

Currently, *strategic asymmetry* has become a broadly used expression related to maximizing the vulnerability of the adversary or its superiority to gain the freedom of movement or initiative in relations with other countries in military or national security.[28] This concept can be divided into two different types: *positive asymmet*ry, in which one's dominance can be a threat to others, and *negative asymmetry*, in which the dominance of adversaries can be a threat to oneself.[29] The elements of strategic asymmetry are not limited to traditional military factors—the size of weapon systems and physical forces—but include non-military factors—technologies, social structures, and normative factors—that indirectly affect the conflict situation.

1. Asymmetry of Cyber Threats

Asymmetry is a useful concept to explain *cyber threats* for the following reasons. First, the damage that can be wrought in cyberspace is asymmetric among the countries. The difference in dependency of national infrastructure on the network between nations causes the asymmetric results. In South Korea, all sectors of society are structured on networks, so they are structurally vulnerable to cyber threats from North Korea. North Korea, by contrast, may be relatively free from the effects of cyberattacks as it makes much less use of cyberspace. Second, unlike kinetic warfare, the attacker in cyberspace has tremendous benefits compared to the defender. In kinetic conflicts, to penetrate the well-prepared defender, the attacker needs considerable capability and effort. In cyberspace, however, the attacker can penetrate the system by exploiting a single weakness, while the defender must be prepared to defend against all potential vulnerabilities, some of which may not even be known. Although the perfect defense in conventional warfare is limited as well, with cyberspace the degree of asymmetry has

[27]Stephen Blank, *Rethinking Asymmetric Threats* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2003): 4, https://www.globalsecurity.org/military/library/report/2003/ssi_blank.pdf.

[28]Metz and Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, 5–6.

[29]Blank, *Rethinking Asymmetric Threats*, 1, quoted in Chung, "Strategic Asymmetry and North Korea's Asymmetric Threats."

grown. Lastly, differences in cyber governance give rise to asymmetries. For example, most democratic countries pursue the free flow of information in cyberspace, but some countries like China and Russia control the flow of data and cyberspace for the purpose of domestic stability. These differences between national political systems result in the differences in the possible degree of government security control. Overall, both cyberspace and cyber threats have asymmetric attributes.

2. Asymmetry on the Korean Peninsula

Asymmetry is a helpful concept to understand the complicated relationship between North Korea and the ROK-U.S. alliance on the Korean Peninsula. The threats of North Korea are primarily directed at North East Asia, including the ROK, and are chief among security issues on the Korean Peninsula.[30] The relationship between North Korea and South Korea has been one of conflict since the Korean War, and the asymmetric development of these nations has changed the conflict structure. [31] As a result of the gaps in national growth in economy, military, and political structures, these two countries have taken different directions. [32] North Korea has focused on the strengthening of its asymmetric capabilities, while the ROK and its ally, the United States, have focused on the increase of military forces based on the conventional concepts. The DPRK's provocations using asymmetric methods have increased on the Korean Peninsula and threaten the regional peace in North East Asia as well.

North Korea focuses on *asymmetry* because of the limitation of its symmetric response capability in the face of the power of the ROK and U.S. alliance.[33] The DPRK

[30]*2016 Defense White Paper* (Seoul, Republic of Korea: ROK Ministry of National Defense, 2016), 21, http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_201705180311469090.pdf.

[31]This research uses the nation to indicate North Korea, although there is the domestic dispute over whether it is a nation or not. The ROK constitution demonstrates, "The territory of the Republic of Korea is the Korean Peninsula and its attached islands." Interpretation of the validity of the DPRK based on the constitutional clause is contested because of its lack of legal status as a nation. The ROK judicial precedent declares the DPRK as a rebel organization, but the object of negotiation at the same time. However, the United States recognizes the DPRK as a nation state. Therefore, this research assumes the DPRK is a country to prevent confusion in concepts, because the main idea is inducing meaningful cooperation between the ROK and the United States.

[32]Duk-ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy," *Naval War College Reviews* 65, no. 1 (Winter 2012).

[33]Kim, "The Republic of Korea's Counter-Asymmetric Strategy," 65.

has never stopped communicating its national goal of the unification of the two Koreas and has projected its intentions through constant provocation. Although the provocation of the DPRK toward the ROK has been persistent, it has not escalated to total war since the Korean War (1950–1953). Two significant provocations, the blue house raid in 1968 and the Burma terror incident in 1983 are cases that targeted the president of the ROK.[34] North Korea, however, has since changed to asymmetric methods for provocation. After a series of sea battles—the first Yeonpyeong Sea Battles in 1999, the Second Yeonpyeong Sea Battles in 2002, and the Daechung Sea Battle in 2009—North Korea acknowledged its weakness in symmetric warfare.[35] In 2010, DPRK asymmetric threats became significant security issues for South Korea through two attacks: the sinking of ROKS Cheonan, and the provocation at Yeonpyeong Island.

North Korea developed its military forces to achieve a national goal by developing its asymmetric attack capabilities; on the other hand, the ROK has pursued the consolidation of military powers through technological development and an alliance as part of a national strategy.[36] According to a 2016 ROK white paper, North Korea continues provocations "in the form of developing WMD such as nuclear capabilities and ballistic missiles, expanding its conventional forces, carrying out armed provocations in contact areas, conducting cyber-attacks, and small-sized drone infiltrations."[37] Based on their specialized asymmetric forces, North Korea has relatively superior asymmetric capabilities.

DPRK's asymmetric threats result, in part, from the possession of WMD. North Korea has multiple nuclear and chemical weapons, and South Korea does not have any

[34]LaFoy et al. *North Korea's CyberOperations: Strategy and Responses*, 39–40: the blue house raid in 1968 was the attempted assassination of Park Chung-hee, the president of the ROK. The team of commandos infiltrated across the DMZ but failed in front of the residence of the president at the end of a firefight. The Ministry of the People's Armed Forces Reconnaissance Bureau, a predecessor of the RGB, was linked with the provocation. The attempts to assassinate Chun Doo-hwan, the president of the ROK in 1983 happened when he was visiting the Martyr's Mausoleum in Rangoon, Burma. A bombing intended to kill the president failed, but several officials in the ROK cabinet and the Burmese government were left dead.

[35]Kim, "The Republic of Korea's Counter-Asymmetric Strategy," 55.

[36] Ibid., 59–60.

[37]*2016 Defense White Paper*, 21.

methods to deter such threats other than through its alliance with the United States. Furthermore, North Korea has developed its nuclear arsenal since its withdrawal from the Nuclear Non-proliferation Treaty (NPT) in 2003 and its claim to have miniaturized a nuclear weapon after a test in 2016.[38] After its sixth nuclear weapon test on September 3, 2017, North Korea insisted its hydrogen bomb "could be mounted on an intercontinental missile." In particular, North Korea declared itself a nuclear power in its constitution and solidified nuclear power as permanent policy in the 7th Congress of the WPK, 2016.[39] Chemical weapons are another form of WMD that pose a serious potential threat. As illustrated by the assassination of Kim Jong Nam, Kim Jong-Un's half-brother, by VX nerve agent on February 13, 2017,[40] North Korea's chemical gained global attention. North Korea already has "the capability to effectively employ throughout the Korean Peninsula, significant quantities and varieties of chemical weapons."[41] Considering the noteworthy escalation of North Korea's WMD threats, South Korea does not have a weaponry system to deter North Korea's WMD use. Without the U.S. military forces, to the ROK cannot offset the positive asymmetry of North Korean WMD.

In addition, asymmetry of the internal civilian and military power structure gives an advantage to North Korea.[42] The ROK and the United States are liberal democracies, so public opinion can affect defense policy, which can be seen as a weakness in the policy-making process. The DPRK, however, is a dictatorship.[43] Kim Jung-Il focuses on

[38]"North Korea Nuclear Timeline Fast Facts," CNN Library, September 4, 2017, http://www.cnn.com/2013/10/29/world/asia/north-korea-nuclear-timeline---fast-facts/index.html.

[39]The ROK Unification Education Institute, *2017 North Korea* (Seoul, Republic of Korea, 2016): 116. http://www.unikorea.go.kr/books/understand/understand/ebook/under_NK_2017/assets/contents/download.pdf.

[40]Joshua Berlinger, "Kim Jong Nam: The Plot to Murder North Korea's Exiled Son," *CNN*, September 26, 2017, http://www.cnn.com/2017/07/26/asia/kim-jong-nam-killing/index.html.

[41]Joseph S. Bermudez Jr., "North Korea's Chemical Warfare Capabilities," 38 North, (U.S.-Korea Institute at Johns Hopkins University), October 10, 2013, http://www.38north.org/2013/10/jbermudez101013/.

[42]Gi-tae Lee, "Cyber Threats and the Relationships between South Korea and North Korea," in *Innovation of Science and Technology and North Korea's Asymmetric Threat : Rise of Cyber Warfare and Unmanned Aerial Vehicle*, ed. Kuyoun Chung and Gi-tae Lee (Seoul, Republic of Korea: Korea Institute for National Unification, Innovation of Science and Technology, 2016), 43.

[43]HP Security Research, *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape.*

risk management using the military forces to help maintain order.[44] DPRK's leadership has absolute power, so the military forces are controlled by Kim Jung-un. In other words, North Korea's active internal control can be an asymmetric advantage in policymaking and decision making.

Another aspect of North Korea's asymmetric threats arises from the asymmetry of effects.[45] Comparable strikes from the North or South can have dramatically different effects on their societies. Global Positioning System (GPS) jamming is a typical example. North Korea is relatively unaffected if South Korea conducts a GPS jamming attack, because the DPRK has a relatively low GPS usage rate. On the other hand, the effect of GPS jamming in South Korea would be considerable, because it uses GPS technology in various ways. As another example, the damage of a war that destroyed Seoul would be greater than the loss of any city in North Korea, because Seoul is the center of South Korea's politics, economy, and culture, where over 10,000,000 people from all around world are living. Therefore, even the threat without an actual attack can cause a great deal of chaos.

In conclusion, North Korea's asymmetric threats are apparent on the Korean Peninsula in multiple ways. The asymmetric structure already formed by North Korea and its overall national strategy seem to suggest these asymmetric threats will only increase. Cyber threats, in particular, have been realized under what has been a highly favorable environment, which is discussed in Chapter III.

C. CONCLUSION

Chapter II has explored the asymmetric conflict structure on the Korean Peninsula so that the reader can understand the context of the North Korean cyber threat. Because of the benefits, North Korea has intimidated South Korea in cyberspace. Chapter III studies the common *cyber threats* on the Korean Peninsula. More specifically, it examines North Korea's previous cyber-attacks that have targeted the ROK and the U.S. militaries.

---

[44]The ROK Unification Education, *2017 North Korea*, 115.

[45]Chung, "Strategic Asymetry and North Korea's Asymetric Threats," 18–19.

III. COMMON CYBER THREATS ON THE KOREAN PENINSULA

A. CYBER THREATS BY NORTH KOREA

Cyber-attacks on the Korean Peninsula have been aimed at critical national organizations, social infrastructure, financial institutions, and the military. Many of these attacks have threatened national security. The main actor that conducted these cyber-attacks is suspected to be North Korea.[46] The Distributed Denial of Service (DDoS) attack in 2009[47] and the DDoS attacks in March 2011 targeted the ROK government, the military, an information technology (IT) company, a bank, and other major portal web pages.[48] The ROK's main media and bank servers suffered from attacks in 2013, and Korea Hydro & Nuclear Power and a Seoul Metro control server in 2014. In 2015, a major hospital network system was hacked,[49] and in 2016, hackers stole the operational plans for war against North Korea from the central server of the ROK Ministry of National Defense.[50]

Because of North Korea's significant threats on the Korean Peninsula, this chapter focuses on how South Korea and the United States defend against North Korea's cyber-attacks. Although both offense and defense in cyberspace are necessary, North Korea currently stands in the advantageous position in cyber-attacks.[51] When countries with well-developed networks, including South Korea, built cyberspace, they focused on network construction and connectivity without consideration of security issues. As a

[46]Do-kyeong Ok, "A Policy Study of Cyber-Warfare Capacity," *Journal of Strategic Studies* 23, no. 3 (November 2016): 155–180, http://www.dbpia.co.kr/Article/NODE07047776.

[47]"DDoS Attacks, How to Respond?: 7.7. DDoS Attack Pattern Analysis and Suggestion," Cisco Team Korea, July 16, 2009, https://www.cisco.com/web/KR/learning/events/down/July_DDoS_Webseminar.pdf.

[48]"2013 Major Cyber Attacking Cases and Response," Korea Internet Security Agency, December 4, 2013, http://www.kisa.or.kr/uploadfile/201312/201312041443047984.pdf.

[49]Ok, "A Policy Study of Cyber-Warfare Capacity," 159.

[50]Kwanwoo Jun and Nancy A. Youssef, "North Korea Suspected of Hacking U.S.-South Korean War Plans," *Wall Street Journal*, October 10, 2017, http://www.wsj.com/article/north-korea-suspected-of-hacking-u-s-south-korean-war-plans-1507636641.

[51]Though the overall flow of research focuses on North Korea's cyber-attacks, partially, the sections about North Korea's vulnerability refer to the defense of North Korea in cyber operations.

result, South Korea could be more vulnerable than nations with immature network systems.

The purpose of this chapter is to answer the first research question: *What are the cyber threats on the Korean Peninsula?* Therefore, the chapter first studies North Korea's cyber operations and the reasons why North Korea focuses on cyberspace. With an understanding of North Korea's cyber threats, the chapter examines the impact of North Korea's cyber threats on the ROK and the U.S. militaries. Lastly, North Korea's vulnerabilities are examined to determine avenues for possible exploitation that address the central question: *How can the ROK and the U.S. military cooperate against common cyber threats on the Korean Peninsula*.

B. NORTH KOREAN CYBER OPERATIONS

In this section, the author examines North Korea's threats in cyberspace by analyzing North Korea's intention, its current organization, and its influence on foreign affairs through cyber operations.

1. Intent

North Korea, Iran, China, and Russia are significant cyber threats to international cyberspace.[52] Among these nations, North Korea is the main actor for cyber threats on the Korean Peninsula because of its aggressive intentions to exploit the vulnerabilities of the ROK and the United States in cyberspace. The leadership in North Korea reportedly states the importance of wielding a cyber capability in public. For example, when Kim Jung-un visited the Reconnaissance General Bureau (RGB,정찰총국) in February 2013, he commented that "only powerful cyber warriors in the RGB and powerful information communication technologies can penetrate all sanctions, and building a strong nation is not a problem at all."[53]

[52]Will Edwards, "North Korea as a Cyber Threat," *The Cypher Brief*, July 1, 2016, https://www.thecipherbrief.com/north-korea-as-a-cyber-threat.

[53]Chul Baek, "North Korea 'What is the Truth of Cyber Capabiity?'," *Kyunghyang News*, April 13, 2013, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201304131549251.

North Korea has recognized the importance of information warfare since the 1990s, and it recognized the noteworthiness of IW after the United States successfully used the network in 2003 to defeat Iraq, which "succumb[ed] to psychological warfare aimed at inspiring shock and awe."[54] The current DPRK regime follows the previous leadership, which highlighted the importance of IW; however, Kim Jung-un tends to use the term cyber warfare instead of information warfare. Although the importance of cyber warfare is disputed among military strategists of the DPRK, the consensus is that cyberspace is a principal domain for battle.[55] North Korea's concept of cyber warfare is said to include intelligence warfare, computer network warfare (NW), psychological warfare, military deception, and IW.[56]

Kim Jung-un's science and technology-oriented policy is strongly connected to its strength in cyber operations. North Korea has pursued technological development to enhance the military and economic development, as it announced again in the "Economy and Nuclear Armed Forces centralized policy (Byung-Jin: 병진)" with the 7th Congress of WPK in May 2016.[57] North Korea started to find a solution for its economic collapse in the latest science and technology after the industry as a whole collapsed in the 1990s.[58] Fostering science and technologies is the method to increase efficiency and maximize cost reduction in industrial production. Current interests in high-end technology are the result of North Korea's policy. For instance, North Korea has been interested in developing technology like Artificial Intelligence (AI) and has made efforts to respond to global changes in digital technology convergence.[59] It has also initiated the "New

---

[54]Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*, 4.

[55]Ok-chu Ri, "Cyberspace Appears as New Battlefield," Minju Joson (electronic edition, in Korean), July 19, 2011, Full text of press statement by a spokesperson for the Ministry of the People's Armed Forces under the DPRK National Defense Commission; "Bad Habit of Finding Fault with Others Must Be Relinquished," Pyongyang Korean Central Broadcasting Station (in Korean)," May 10, 2011, quoted in Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*, 4.

[56]Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*, 4.

[57]*2016 Defense White Paper*,, 187; *Byung-jin* means parallel development. In other words, the DPRK will put equal emphasis on the two values for development.

[58]Young-sil Kang, "Science Technology Industry Trends Evaluation of Kim Jung-un Regime," in *KDI Review of the North Korean Economy* 19, no. 2 (February 2017):63.

[59]Kang, "Science Technology Industry Trends Evaluation of Kim Jungun Regime," 63.

Century Industrial Revolution" and has made every effort to create new domestic industries based on the Information Communications Technology (ICT).[60] The ICT industries support future economic sectors that include small-scale manufacturing industries and large-sized mainstream industries focusing on automation.

The development of military industries, including modernization and asymmetric weapons, is noteworthy along with North Korea's science and technology-oriented policy.[61] According to North Korea's national strategy named the Byung-Jin (병진)) and Son-gun (선군), facilities for the production of armaments and munitions have priority for raw materials and production base elements such as electricity. In 2016, North Korea concentrated on nuclear development and the modernization of military factories as well as the development of new weapons systems. Drone development is an example. In December 2016, North Korea reportedly succeeded in developing 'Bang-Hyun 5,' a large-scale attack drone made of titanium and carbon composite materials.[62] In May 2016, Kim Jong-un reportedly announced that "our defense technology is at the top of its class, and in the defense industry sector, we are producing precise, lightweight, unmanned and intelligent advanced weaponry equipment as we want."[63]

North Korea's leadership tends to justify its offensive behavior under the name of self-defense or counter actions toward its enemies' threats. Considering cyberspace, North Korea also has a perception that it will also be the victim of cyber-attacks. It pays attention to the United States' cyber threat to the DPRK, and exaggerates that threat, because North Korea recognizes the superior capability of the United States in cyberspace.[64]In 2013, the DPRK Cabinet newspaper *Minju Chosun* reported that the U.S.

---

[60]Nam-hun Cho, "2016 North Korea Military Industry Trends and Evaluation," *KDI Review of the North Korean Economy* 19, no. 1 (January 2017):79–80.

[61]Cho, "2016 North Korea Military Industry Trends and Evaluation," 80.

[62]"Development of Large-Attacking Drone of North Korea to Attack South Korea," *Yeonhap News*, December 27, 2016, http://www.yonhapnews.co.kr/bulletin/2016/12/26/0200000000AKR20161226165651014.HTML.

[63]"Business Summary Report(사업총화보고)," *Ro-dong Sinmun*, May 8, 2016, quoted in Cho, "2016 North Korea Military Industry Trends and Evaluation," 82.

[64]Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*, 5–6.

presidential policy directive No. 20 "termed the cyber-attacks an indispensable capability to restrain and overthrow the enemy doing harm to U.S. interests in times of peace and war. This means that the U.S. is ready to mount fierce cyber-attacks on anyone going against it at any moment." [65] The WPK's official mouthpiece, *Rodong Sinmum*, asserted that the policy showed that "the United States is attempting to find a pretext for military aggression and intervention in other countries." [66] North Korea's reports show the country could be vulnerable to cyber threats and that it requires defensive capabilities, but considering the current phase of cyberspace development, that view is an overestimation.

North Korea's offensive intention, however, is significant. Kim Jung-un has called cyber war "the All-in-One Sword."[67] Currently, after increasing its cyberattack capability, North Korea views cyberspace as a means to solve the national problems in the economy and technological development. Its organizational structure mirrors North Korea's intention to reinforce offensive capabilities in cyber operations. Reportedly, Kim Jong-un has recently reorganized the Cyber Strategic Command[68] to combine distributed units for cyber-attacks, cyber terrorism, cyber psychological warfare, and GPS jamming.[69] While the exact current cyber organization is still veiled, it would be helpful to understand how it has been organized for comprehension of how North Korea intends to use cyberspace.

2. Organizations

Notably, North Korea is known for unifying its own capabilities for cyber-attacks. Although this research uncovered no official announcement of how the DPRK has

---

[65]Ra Myŏng-sŏng, "Cyber Warfare That Draws International Concerns," *Ro-dong Sinmun* (electronic edition, in Korean), September 29, 2011, quoted in Mansourov, *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance,* 4.

[66]Ibid.

[67]"Kim Jung-un, Cyber War is the All-in-One Sword," *Joong-ang Ilbo*, November 5, 2013, http://news.joins.com/article/13048072.

[68]The author translates the Korean expression (*사이버 전략 사령부*) directly into English (*Cyber Strategic Command*).

[69]Heung-kwang Kim, "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability," Korea Freedom Federation, September 1, 2016, http://www.posuni.com/pds/view.php?idx=2295&page=11&section=%C7%D0%BC%FA%BC%BC%B9%CC%B3%AA.

formed its cyber organizations, it seems to include highly mission-specified agencies with cyber-capabilities: the Reconnaissance General Bureau (RGB: 정찰총국) and the General Staff Department (GSD: 총참모부) of the Korean People's Army (KPA). The mission of the RGB is to conduct clandestine cyber operations during peacetime for force projection, and the main tasks of the GSD are cyber operations for merging cyber operations into conventional military efforts during battle.[70]

The RGB is new and was organized in 2009 to address asymmetric warfare, which is "political warfare, foreign intelligence collection, subversion, kidnapping, special operations, and assassinations."[71] Kim Yong-chol was the first leader of the RGB from 2009 to 2016 and is known as the expert in North Korea's asymmetric operations.[72] The new leader of the RGB, Jang Gil-sung, is also known as an expert in asymmetric warfare.[73]

North Korea's Cyber Organizations and Military Command Structure are depicted in Figure 1.

[70]Feakin et al., *Cyber Maturity in the Asia-Pacific Region 2016*, 59.

[71]LaFoy et al. *North Korea's CyberOperations: Strategy and Responses*, 35–36.

[72]Ibid., 36–37.

[73]"Japanese Media, Gil-sung Jang Took Over as Chief of the North Korea's RGB," *Yeonhap New*, October 13, 2017, http://www.yonhapnews.co.kr/bulletin/2017/10/13/0200000000AKR20171013078600073.HTML.

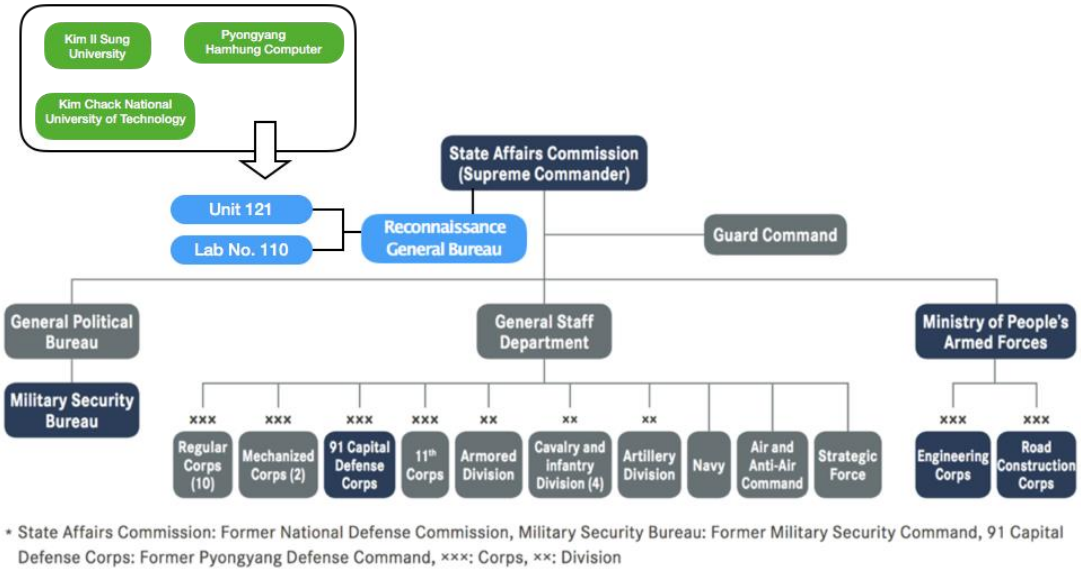

Figure 1. North Korea's Cyber Organizations and Military Command Structure[74]

The RGB, known as a sub-organization of the State Affairs Commission (SAC),[75] is the center of cyber operations in the DPRK. It reorganized units from intelligence and cyber warfare organizations under the WPK and the Ministry of the People's Armed Forces (MPAF).[76] The core unit for cyber-attacks is Unit 121.[77] The officer candidates for Unit 121 are selected from among North Korean teenagers. The candidates receive extensive training. They take a computer class for gifted students and a course at Kim Il Sung University (김일성대학교), Kim Chack National University of Technology (김책공대), Mirim college (미림대학) or Pyongyang Hamhung Computer Technology

[74] *2016 Defense White Paper*, 28; LaFoy, *North Korea's CyberOperations: Strategy and Responses*, 38. The author adds the RGB on the organization structure attained by the ROK white paper, based on the information of *North Korea's CyberOperations: Strategy and Responses.*

[75] North Korea Changes the Name of Organizations in 2016. The National Defense Commission (NDC) in *North Korea's CyberOperations: Strategy and Responses* in 2015 were renamed as States Affairs Commissions (SAC) in 2016.

[76] LaFoy et al. *North Korea's CyberOperations: Strategy and Responses.*

[77] Kim, "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability." The 121 units are called Bureau121 or the Electronic Reconnaissance Bureau's Cyber Warfare Guidance Bureau according to *North Korea's CyberOperations: Strategy and Responses*.

College (평양함흥과학기술대학) before being placed in the unit. Some students go through an additional two-year course of study in software engineering, cryptography, and networking in China or Russia. The members in Unit 121 are known to have considerable skills, such as memorizing thousands of lines of programming code and coding hacking programs in assembler or programming languages. Their skills for cyber-attacks are estimated to be at the level that could damage and physically destroy a network. The missions of Unit 121 are subdivided and tackled by sub-organizations, including the stem analysis team, the attack operation team, the code processing team, the development team, the inspection team, the network analysis team, and the battle planning team.

Lab No. 110 (Computer Technology Research Lab) is the other primary sub-organization of the RGB; its purpose is to increase the efficiency of cyber-attacks executed practiced by Unit 121.[78] The generally acknowledged mission of Lab No.110 is to detect the security flaws of targeted servers, under the direct order of Kim Jung-un. The unit analyzes the technological configuration of the target, diagnoses the behavior patterns of security officers, and develops software for cyber-attacks. Collaboration between Lab No.110 and Unit 121 increases the effectiveness of North Korea's cyber-attacks.

Under Kim Jong-un's regime, North Korea has concentrated its money and human resources on the cyber units.[79] For instance, when Unit 121 created a supercomputer for decryption and encryption efforts by combining imported high-end qualified computers, Kim Jung-un's personal ruling budgets were used to fund it.

While the RGB has conducted most of the known cyber-attacks, the GSD is thought to be in charge of cyber operations for conventional military forces during battle.[80] Recently, the DPRK military structures were changed. According to the

[78]Kim, "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability."

[79]Kim, "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability."

[80]Feakin et al., *Cyber Maturity in the Asia-Pacific Region 2016*, 59.

previously mentioned ROK white paper, the GSD created a new department for Command, Control, Communication, Computer, and Intelligence (C4I) in the military.[81] The GSD reorganized the Command Information Bureau to strengthen its C4I systems. In other words, North Korea focuses on not only the attack capability targeting national critical infrastructure, but also on merging cyber capabilities with battle to enhance the efficiency and defensive capabilities of the command and control systems. North Korea's quantum encryption technology development was also analyzed in its effort to build a remote-control system in Pyeong-yang for launching missiles located at a point more than 150 kilometers away from the capital.[82]

3. Foreign Affairs

This section focuses on North Korea's cooperative relationships related to cyber capabilities, not on its conflict relationships in cyberspace. Although its standing in global society has become weaker, North Korea has maintained diplomatic relationships with several countries like Russia, China, and Iran.[83] Reportedly, those countries have contributed to North Korea's efforts to develop cyber capabilities.

Education and technological cooperation are the primary support mechanisms for North Korea to attain cyber-attack capabilities from these countries. Before it acquired its own internal cyber capability, North Korea relied on help from these countries. Analysts found that Iran shared cyber-attack skills with North Korea. [84] The DPRK's cyber-attacks in March 2013 were linked to Iran's cyber-attacks against Saudi Aramco, the oil company. While recovering from the damage of the Stuxnet attack, Iranian hackers attacked Aramco's 30,000 computers and 10,000 servers in August 2012. The virus had "wiping" functions to demolish data and replace it with pictures of a burning American

[81] *2016 Defense White Paper*, 29.

[82] Martyn Williams, "Catch Me If You Can: North Korea Works to Improve Communications Security," 38 North (U.S.-Korea Institute at Johns Hopkins University), April 12, 2017, http://www.38north.org/2017/04/mwilliams041217/.

[83] *2016 Defense White Paper*, 28.

[84] David D. Kirkpatrick, Nicole Perlroth, and David E. Sanger, "The World Once Laughed at North Korean Cyberpower. No More.," *New York Times*, October 12, 2017, https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

flag. North Korea's cyber-attacks in 2013 during the ROK and U.S. military combined exercises employed a similar attack method—using wiping malware and paralyzing the network—as in the Iranian 2012 Aramco hacking. According to a former British official, Iran has probably taught North Korea cyber-attack methods, rather than North Korea just mimicking Iranian's hacking.[85] Actually, Iran and North Korea are known to have signed a technical exchange agreement, implementing collaborative research and conducting student exchange programs.[86] In addition to Iran's help, Russia and China have also supported North Korea's educational training system. Russia and China provide education in their own institutions and send experts to North Korea for the purpose of helping North Korea develop cyber-attack capabilities.[87] Russia sent 25 professors who graduated from Frunze Military Academy, the military academy in Russia, to support North Korea's cyber experts' training by providing technologies for internet control. Also, the selected North Korean elite hacker officers receive training in Russia and China.[88]

North Korea has also used locations in China to launch its cyber-attacks. A great number of the cyber-attacks against the ROK and the United States mentioned previously originated from inside China.[89] To overcome its limited infrastructure, North Korean hackers have used networks in China and some countries in Southeast Asia with which it has relationships. In particular, Shěnyáng (瀋陽: Sunyang), the east coast of China, is known as the base of North Korea's cyber-attacks.[90] China is one of the countries that control the Internet through the government. It filters information coming into the country or getting posted on sites inside China. North Korea uses facilities inside China

[85]Kirkpatrick, Perlroth, and Sanger, "The World Once Laughed at North Korean Cyberpower. No More."

[86]HP Security Research, *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, HP Security Briefing Episode 16, 42–44.

[87]Kyu-Sik Yoon, "North Korea's Capability for Cyber War and Prospects," in *Military Forum* 68 (ROK: Korea Association of Military Studies, Winter 2011): 76, http://210.101.116.16/kiss6/viewer.asp.

[88]LaFoy et al. *North Korea's CyberOperations: Strategy and Responses.*

[89]Kim, "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability."

[90]In-soo Kim, "North Korea Cyberwar Capability Assessment and Prospect," in *International Journal of Korean Unification Studies* 24, no. 1, (ROK: Korea Institute for National Unification, 2015): 137, http://www.dbpia.co.kr/Journal/PDFViewNew?id=NODE06383222&prevPathCode=.

to launch attacks, but it probably uses them for some legitimate activity as well. According to the ROK Congressman Joo-sun Park, a total of 4,193 cyber-attacks have occurred targeting the ROK Ministry of Unification during the last five years. North Korea is suspected as the attacker, and 43.5 percent of cyber-attacks come from Chinese Internet Protocol (IP) addresses.[91] From 2009 to 2011, the Chinese Internet Protocol (IP) addresses used by North Korea were located in China's three Northeast provinces.[92]

Internet connections are required for conducting most cyber-attacks, and both Russia and China offer North Korea access to the Internet. Though it prohibits most of its citizens from accessing sites outside North Korea, in 2009 North Korea established an Internet connection through the Thai company named Star Joint Venture and has allowed a limited number of people to use it.[93] Though North Korea only has 1,024 IP addresses, it launched cyber-attacks against the ROK from its own network. The listed location information of IP addresses (175.45.178.xx) used in cyber-attacks on March 20, 2013, is Ryugyong-dong Pyeongyang-si Potong-gang District in the DPRK.[94] At the time, the only outside connection was through China, though recent traffic analysis suggests a Russian company is now also providing a connection to North Korea.[95] Figure 2 and Figure 3 show Russia's and China's network maps connected to the border of North Korea.

---

[91]Jin-myeong Kim, "World Is Now Fighting with North Korean Hackers," *Chosun Ilbo*, October 7, 2017, http://news.chosun.com/site/data/html_dir/2017/10/08/2017100800228.html

[92]"From DDoS to Information Espionage and Psyop… Hacking Patterns of North Korea is Changing," Korea Herald Business, June 7, 2016, http://heraldk.com/2016/06/07/%EB%94%94%EB%8F%84%EC%8A%A4%EC%97%90%EC%84%9C-%EC%A0%95%EB%B3%B4-%ED%83%88%EC%B7%A8%E3%86%8D%EC%8B%AC%EB%A6%AC%EC%A0%84%EC%9C%BC%EB%A1%9C%EB%B6%81%ED%95%9C-%ED%95%B4%ED%82%B9-%ED%8C%A8/.

[93]Baek, "North Korea 'What is the Truth of Cyber Capabiity?'"

[94]"The Address of Hacking IP is 'Ryugyong-dong Pyeongyang-si'," *Yeonhap News*, April 11, 2013, http://www.yonhapnews.co.kr/bulletin/2013/04/11/0200000000AKR20130411000900017.HTML.

[95]Martyn Williams, "Russia Provides New Internet Connection to North Korea," 38 North (U.S.-Korea Institute at Johns Hopkins University), October 1, 2017, http://www.38north.org/2017/10/mwilliams100117/.

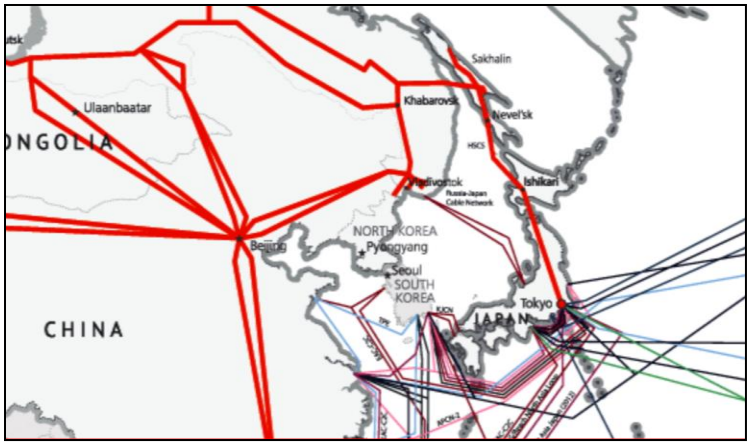

Figure 2. Russia's TTK Network Cable Map on Border of North Korea[96]

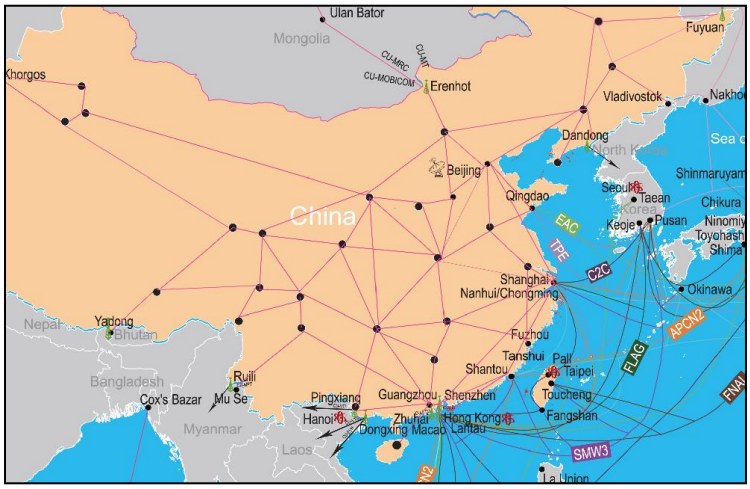

Figure 3. China's Unicom Network Cable Map on the Border of North Korea[97]

Furthermore, Russia and China can support North Korea's Internet connection by assigning IP addresses to North Korea. In addition to its allocated IP addresses (175.45.176.0 – 175.45.179.255), China Unicom assigned its IP addresses (210.52.109.0 – 210.52.109.255) to North Korea. SatGate, the Russian satellite company, assigned its IP

[96]"TTK Network," TTK, accessed October 10, 2017, https://www.ttk.ru/rus/59897/59900/61841/.

[97]"China Unicom Global Network Map," China Unicom, accessed October 10, 2017, http://www.unicomamericas.com/wp-content/uploads/2012/06/unicom-map.jpg.

addresses (77.94.35.0 – 77.94.35.255) to North Korea.[98] Although North Korea was assigned IP addresses by SatGate, that company does not cover North Korea. The Russian company named IntelSat, however, does provide Internet access that covers North Korea. In conclusion, North Korea has a clear intention to use cyberspace and build the organization and cyber-attack capabilities with the support from other countries. But, why did North Korea focus on cyberspace?

C. WHY NORTH KOREA EMPHASIZES CYBERSPACE

North Korea has developed offensive cyberspace to gain economic benefits and acquire technologies. A majority of North Korea's cyber-attacks have focused on the Korean Peninsula, because of asymmetric benefits.

1. Economic Benefits

One reason for North Korea's interest in cyber-attacks is that such attacks can produce lucrative benefits. Reportedly, North Korea stole money and intellectual property from other countries between October 2016 and June 2017.[99] The financial benefits of such attacks can partially compensate for the economic sanctions imposed on North Korea for its nuclear weapons development.[100]

North Korea began to conduct cyber-attacks against South Korea's banking system and companies almost a decade ago. It is suspected of attacking the ROK's banking system in 2009, 2011, and 2013.[101] A cyber-attack in 2009 that employed DDoS operations and disk wiping malware using 115,004 zombie PCs damaged hard disks in 1,446 PCs. Another attack in 2011 used 116,299 zombie PCs and damaged the hard disks in 756 PCs. The major banks in the ROK were included in the damaged web-pages listed for both attacks.[102] In addition, after the April 2011 attacks aimed at the Nong-hyup Bank

[98]"A list of North Korean IP Addresses," Exploit This, January 25, 2015, https://www.exploitthis.com/2015/01/26/a-list-of-north-korean-ip-addresses/.

[99]iDefense, *2017 Cyber Threatscape Report* (Accenture Security, 2017):5.

[100]Rosen et al. *North Korean Cyber Capabilities: In Brief*, 1.

[101]Ibid., 8.

[102]"2013 Major Cyber Attacking Cases and Response."

(The Bank of the National Agricultural Cooperative in the ROK), investigators reported that the attackers had intruded on the internal system and hid the code for several months to execute an attack at the optimal time. Nong-hyup Bank is the primary bank in the ROK and holds $50,000,000,000 from 181 organizations, 70 percent of which is public funds from the ROK government, local governments, educational institutes, and the military. The total assets amount to $487,000,000,000, while the total assets of Samsung, ranked first in domestic businesses, stands at $348,000,000,000, and the Korea Electric Power Corporation, the largest public company in ROK, has $98,000,000,000.[103] The attacks targeting the super bank spread the malicious code using the Patch Management System (PMS) and destroyed 273 of the 587 computers on the bank's network.

North Korea's early cyber-attacks involved simple DDoS attacks and intrusions against ROK and U.S. systems, but its choice of targets has broadened.[104] North Korea has been linked to an attempted cyber heist against the Bangladesh Central Bank in 2016, because the attack methods resembled the cyber-attack against Sony in 2014, according to Richard Ledgett, Deputy Director of the National Security Agency.[105] The attacker tried to send fraudulent messages to request money transfers totaling around one billion dollars from the Bangladesh Central Bank account at the Federal Reserve Bank of New York to the Philippines. The thief reportedly inserted malware into the Society for Worldwide Interbank Financial Telecommunication (SWIFT) terminal used by the Bangladesh Central Bank network, which was inadequately protected from outside attacks.

According to the ROK, in 2016, North Korea attacked a major Internet shopping mall named Inter-park.[106] In May 2016, hackers sent an e-mail containing malicious code to the server manager in the company, and penetrated the server and network. After

[103]Young-ha Kim, "[*Nong-hyup*] Analysis of the *Nong-hyup* Federation of Agricultural Cooperatives NACF Crisis What Should Be Done / Total Assets of 487 Trillion Won," *AM News*, July 22, 2016, http://www.amnews.co.kr/news/articleView.html?idxno=18986.

[104] Kim, "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability."

[105] Rosen et al. *North Korean Cyber Capabilities: In Brief*, 5-6.

[106]"Interpark Customer Information Hijacking, North Korean judgment," *YTN*, July 28, 2016, http://www.ytn.co.kr/_ln/0103_201607281531401705_006.

gaining access to the server of the company, North Korea stole thousands of pieces of information including customers' personal information—phone numbers, resident registration numbers (the ROK social security number), and addresses—and demanded several million dollars by threatening to reveal this information to the public. During the forensic investigation of the attacks, the ROK police found four IP addresses that are often used by one sub-organization of the RGB. In addition to the digital remains, the North Korean style of expression was found in the menacing e-mail demanding money: *Chong-juk (총적)* which means total.[107]

The *WannaCry* ramsomware in 2017 is also linked to North Korea because of its similarity in code to the one used in the cyber-attacks against the Bangladesh Central Bank.[108] The ransomware has struck more than 300,000 users in 150 countries[109] since it was discovered on May 12, 2017. The National Security Agency (NSA) and the United Kingdom put the blame on North Korea, especially the RGB, as the originator of the *WannaCry* ransomware.[110] The parts of the IP addresses found in the remains of the attack were the IP addresses from China known to be used by the RGB. The *WannaCry* malware reused code taken from the NSA and posted online by The Shadow Brokers. [111] The code exploited a vulnerability of unpatched Windows users. Although Microsoft had issued a security patch for the vulnerability two months prior to the attack, many users

[107]Though the ROK and the DPRK use the same alphabet and grammar of Korean, the expressions and the meaning of some terms are different. North Korea intentionally modified the meaning as a part of its effort to make South Korea confused.

[108]Rosen et al. *North Korean Cyber Capabilities: In Brief*, 4–5.

[109] Russell Goldman, "What We Know and Don't Know About the International Cyberattack," *New York Times*, May 12, 2017. Ransomware is a computer program that requires money instead of decryption. Files in the infected computer are encrypted, and the attacker has the key to decrypt it.

[110]Ellen Nakashima, "The NSA Has Linked the WannaCry Computer Worm to North Korea," *Washington Post*, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.6230d7ffdbad.

[111]Bruce Schneier, "Who Are the Shadow Brokers?" *Atlantic*, May 23, 2017, https://www.theatlantic.com/ technology/archive/2017/05/shadow-brokers/527778/.

had not installed the patch. Since the objective of the *WannaCry* was to collect ransom in the form of bitcoins, it is clear that the objective of the attack was to gain money.[112]

The current sanctions on North Korea's economy stemming from its nuclear arsenal will likely drive North Korea to further develop a cyber-attacking capability for financial gain.[113] To North Korea, using cyberspace is one of the optimal ways to gain economic benefits.[114]

2. Acquiring Technology

North Korea focuses on cyber-attacks because such attacks offer an easy way to steal information, including intellectual property for high-end technologies for armaments and for government and military secrets. Although this thesis only covers representative cases of North Korea's cyber threats, multiple reports such as the *2017 Cyber Threatscape Report* have named the DPRK as a significant cyber threat because of its cyber espionage toward other countries.[115] Cyber espionage consists of cyber-attacks conducted to gain information about a government or company illegally by intruding into the computer systems of the targets.[116]

Kim Jong-un recently issued an order to strengthen cyber espionage to extract foreign technology.[117] Reportedly, around the 7th Congress of the WPK, he said high-end science and technologies collected by the DPRK's NSA and the RGB have dramatically improved the science and technologies of North Korea. Kim Jong-un, reportedly, said that illegal extractions from abroad would provide technologies that

---

[112]"Symantec Says 'Highly Likely' North Korea Group behind Ransomware Attacks," *CNBC*, May 23, 2017, https://www.cnbc.com/2017/05/23/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks.html.

[113]Rosen et al. *North Korean Cyber Capabilities: In Brief*, 1.

[114]Sherisse Pham, "North Korea Is Trying to Amass a Bitcoin War Chest," *CNN Tech*, September 12, 2017, http://money.cnn.com/2017/09/12/technology/north-korea-hackers-bitcoin/index.html.

[115]iDefense, *2017 Cyber Threatscape Report* (Accenture Security, 2017), 5.

[116]Global Commission on Internet Governance, Cyber Security in a Volatile World, vol. 5, (Ontario, Canada: Centre for International Governance Innovation and the Royal Institute of International Affairs, July 26, 2017), 97–98, https://www.cigionline.org/publications/cyber-security-volatile-world.

[117]Jie-un Kim, "North Korea, High Technology Hacking Enhencement Directive," *Radio Free Asia*, July 14, 2016, http://www.rfa.org/korean/in_focus/ne-je-07142016101939.html.

North Korea would be unable to develop by themselves, even after ten years. The high-tech information that North Korea is interested in includes military technologies such as WMD and Unmanned Aerial Vehicles (UAV), and energy and construction technologies.

Cyber espionage targeting military technologies is serious. In 2014, North Korea is suspected of having conducted cyber-attacks aimed to attain military technologies from the industries of the ROK.[118] North Korea has penetrated the systems of the major military companies that make F-15K and navy submarine, and stolen the technologies related to missiles and UAVs. In 2014, the media in North Korea announced that it would carry out cyber espionage to steal technologies. Reportedly, North Korea's missile technologies have benefitted from its cyber espionage, including its operations against ROK military companies. It was reported in the ROK media that North Korea hacked the Cold Launch technology of the Navy submarine. [119]

Considering North Korea's intentions, its cyber espionage will likely be extensive, based on its main goals of self-defense and self-renaissance (자력갱생). North Korea faces and admits to its limitations regarding technological development on its own. North Korea has tried to break through its deficiencies by exploiting the vulnerability of cyberspace. In both purposes of cyber-attacks—economic benefits and technological attainment—why does North Korea mainly target the ROK and the United States?

3. Benefits of Targeting South Korea and the United States

North Korea has attempted to penetrate network systems regardless of the nation who owns the targeted networks. The ROK and the combined forces of the ROK and the U.S. military are attractive targets on the Korean Peninsula for reasons that include an asymmetric dependency on cyberspace. Furthermore, the ROK has the best environment for North Korea to test its attack capability.

---

[118]Min-ji Choi, "Have It Prepared Cyber Terrorism ... North Korea Hacked Network of Major Companies," *Digital Daily*, July 13, 2016, http://www.ddaily.co.kr/news/article.html?no=144276.

[119]Hee-wan Jung and Sung-jin Park, "Navy Submarine Missile Cold Lunch Hacked in North Korea," *Kyunghyang News*, September 26, 2017, http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201709260600045&code=910303.

The ROK and the United States are two of the top countries with well-developed network connections used in every aspect of daily life in the private and public sectors. The two countries not only share the same values concerning Internet usage, but are also leading countries in network technology. Both countries, however, have faced the same problems as leaders in technological innovation. While the United States originated the Internet and has created different standards for the Internet, the ROK began systematically introducing policy, related law, and infrastructure for cyberspace under the project named *Cyber Korea 21* in 1999.[120] According to the information index evaluated by the International Telecommunication Union (ITU) in 2016, the ROK has been the premier country for Internet connectivity in the world.[121] Information industries have been the economic growth engines in both countries, and their citizens have received the benefits of technological development such as a convenient life and economic opportunities.

On the other hand, North Korea has a relative advantage in cyber-attacks over its primary adversary, the ROK, and the United States, because the ROK and the United States are both much more dependent on cyberspace. The difference in cyber maturity creates the asymmetry of societal effects from cyber operations. In 2016, Australian Strategic Policy Institute (ASPI) rated the United States and South Korea as the top two nations in cyber maturity in the Asian-Pacific region.[122] The criteria used to rate the countries show high scores for the United States and South Korea but low scores for North Korea, as shown in Table 1. [123] The lack of information about North Korea, though, could affect its low scores. The score for North Korea's maturity on the military use of cyberspace is almost as high as that for the ROK and the United States, but this ranking makes no distinction between the offensive and defensive capabilities of the countries. This assessment, nonetheless, is valuable because it directly shows the asymmetry

[120]"Cyber Korea 21," National Digital Science Library, May 18, 2005, http://www.ndsl.kr/ndsl/search/detail/trend/trendSearchResultDetail.do?cn=DT200501654.

[121]International Telecommunication Union, *Measuring the Information Society Report 2016* (Geneva, Switzerland : ITU, 2016).

[122]Feakin et al., *Cyber Maturity in the Asia-Pacific Region 2016*, 9–11.

[123]Ibid., 14–16.

between two Koreas; the sub-indicators, *Digital economy* and *Social*, indicate the different impact of cyberspace on each regime. This kind of comparison could be common between developed and undeveloped countries, but the cyber-attacks by North Korea can double the effect by inflaming psychological fears when combined with other threats like a nuclear weapon. North Korea's intent to exploit these fears creates a political burden for democratic countries like the ROK and the United States to adapt policies against threats in cyberspace.

Table 1. Cyber Maturity Comparison[124]

Indicator	Sub-indicator	The United States	South Korea	North Korea
Governance	**Organizational structure**	**10**	**8**	**3**
	Legislation / regulation	**8**	**9**	**1**
	International engagement	**9**	**8**	**3**
	CERTs	**8**	**8**	**0**
Cybercrime	**Financial crime**	**10**	**9**	**0**
Military	**Military role in Cyberspace**	**10**	**9**	**8**
Business	**Government–business dialogue**	**9**	**9**	**0**
	Digital economy	**9**	**9**	**1**
Social	**Public awareness**	**10**	**9**	**1**
	Internet connectivity (fixed)	**4**	**5**	**1**
	Internet connectivity (mobile)	**10**	**10**	**1**

Furthermore, North Korea can more easily justify its cyber-attacks on the Korean Peninsula. It would be far more difficult to justify such malicious behavior if it attacked other countries with which it had no prior conflict. At the same time, the two Koreas have been expanding their own military forces based on the preexisting conflict structure between the ROK and U.S. alliance, and North Korea in a kinetic war.

[124]Feakin et al., *Cyber Maturity in the Asia-Pacific Region 2016*, 14–16.

Finally, North Korea is inclined to use South Korea's network as a testing platform for its cyber capabilities. The networks in South Korea are well connected as a result of planned development driven by the ROK government. The disadvantages of new systems are their lack of assurance of system stability. Also, well-developed networks that are successfully attacked can have large social impacts.[125] Once North Korea conducts attacks after finding vulnerabilities, it can evaluate how effective the cyber-attacks were against South Korea. It is easy for North Korea to check its own capabilities and the response of the ROK through the attack analyses found in open-source reports from Congress, security companies, and security research institutes like the Korea Internet Security Agency (KISA). The news media also publicly reports the damages inflicted and the counter measures employed. In sum, North Korea could consider it attractive to target the ROK and the United States compared to targeting other countries. Then, what are the specific effects on the ROK military from North Korea's cyber-attacks?

D. INFLUENCE ON THE MILITARY

North Korea reportedly has targeted the military forces in South Korea since 2004. Some of North Korea's cyber-attacks have succeeded owing to inadequate defenses against them. These offensive cyber-operations effect the ROK and U.S. alliance in military operations.

1. Cyber-attacks Aimed at Military Forces

The cyber-attacks discussed previously support the idea that North Korea will use cyber-attacks at the national strategic level to achieve economic and technological benefits and to optimize psychological effects. But, North Korea's cyber threats against South Korea's military exist not only at the strategic level, such as threats against societal infrastructure, but also at the operational level against military targets. Kim Duk-ki emphasizes the importance of cyber security to the ROK military because the DPRK will maximize its cyber capability by combining it with conventional weaponry in military

[125]Although the software development process has steps to verify before release, a 100 percent secure and perfect program cannot be made at once.

operations.[126] The use of cyber weapons alone would be much less effective than when not coupled with kinetic weapons. It is useful to review what have been North Korea's cyber-attacks on the ROK military and the U.S. Forces Korea (USFK) up to this point. Table 2 summarizes these cyber-attacks.

Table 2. North Korean Cyber-Attacks Targeting Military Related Organizations on the Korean Peninsula

Date	Contents
2004	The ROK Government - 235 PCs hacking and stealing information. (April ~ June):[127] The Maritime Police Agency, National Assembly, Nuclear Energy Research Institute, National Defense Research Institute, National Defense Science Research Institute, Air Force University, and Unification Education Center
2006	"The U.S. Department of State is attacked by entities in the East Asia-Pacific region. The attacks coincide with State Department negotiations with North Korea regarding the regime's nuclear missile tests." (June)[128] A South Korean military official states North Korea's Unit 121 has breached South Korean and U.S. military entities. (July)[129]
2009	DDoS: The ROK – U.S. Combined Forces Command (July)[130]
2010	GPS jamming: base stations (total: 181), airplanes (15), naval ship (1) (August 23~26)
2011	1st DDoS attack:

[126]Kim, "The Republic of Korea's Counter-Asymmetric Strategy."

[127]Sung-pyo Ko, "The North Korean People's Armed Forces Department Has a "CIA-Class" Hacker Organization," *Joongang News*, http://libertyherald.co.kr/article/view.php?&ss%5Bfc%5D=2&bbs_id=libertyherald_news&doc_num=1554.

[128]"State Department Releases Details of Computer System Attacks," Information Week, http://www.informationweek.com/state-department-releases-details-of-computer-system-attacks/d/d-id/1045112?, quoted in HP Security Research, *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*.

[129]"Sisa Magazine 2580, 597, War of Hacking Manuscript," *IMBC*, aired October 29, 2006, http://www.imbc.com/broad/tv/culture/sisa2580/vod/index.html, quoted in HP Security Research, *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*.

[130]"DDoS Attacks, How to Respond?: 7.7. DDoS Attack Pattern Analysis and Suggestion."

Date	Contents
	The ROK Ministry of Defense, the ROK Air Force headquarters, the ROK Army headquarters, the ROK Navy headquarters, the USFK, the ROK Defense Acquisition Program Administration, the ROK joint staff headquarters (March 4) 2nd DDoS attack: The ROK Ministry of Defense, the ROK Air Force headquarters, DAPA, the ROK Army headquarters, the USFK, the ROK joint staff headquarters, the ROK Navy headquarters, tactical fighter wing of the 8th U.S. Army (March 4)
2011	GPS jamming: base stations (145), airplanes (106), vessels (3), ships (7) (March 4~14)
2013	Disclosure of personal information belonging to military of the ROK and the USFK (June 25)[131]
2014	Hacking targeting military industrial companies[132]
2016	Hacking of the ROK Ministry of Defense data server and suspected theft of classified military information[133]

Reportedly, the ROK military announced that North Korea's cyber-attacks against the ROK from April to June 2004 had their epicenter in China. A total of 314 PCs were hacked: 235 PCs of the Maritime Police Agency, the National Assembly, the Nuclear Energy Research Institute, the National Defense Research Institute, the National Defense Science Research Institute, Air Force University, and the Marine and Fisheries Department.[134] In the DDoS attacks in July 2009 and in March 2011, which hit multiple areas of the ROK networks, North Korea also targeted the web servers operated and managed by the military. In 2010 and 2011, North Korea's GPS jamming attacks hit the military. In 2011, North Korea used phishing email that appeared to be sent by alumni of

[131]"6.25 Cyber Terror Analysis," NSHC Security, June 25, 2013, http://www.nshc.net/wp/redalert-report-eng/.

[132]Jung and Park, "Navy Submarine Missile Cold Launch Hacked in North Korea."

[133]Jun and Youssef, "North Korea Suspected of Hacking U.S.-South Korean War Plans."

[134]Ko, "There Is a 'CIA-Class' Hacker Group in North Korea's Ministry of People's Armed Forces -- The World Is Currently at Cyber War."

the Korea Military Academy, from which many generals had graduated, to high ranking Korean officers.[135]

Recent North Korean cyber-attacks against the ROK military seem to be gathering information on the ROK and the U.S. military operations for future attacks. As Sun Tzu said, "One who knows the enemy and knows himself will not be in danger in a hundred battles (知彼知己者, 百戰不殆)." [136] In December 2016, the ROK Ministry of Defense announced that the intranet of the ROK had been hacked.[137] In April 2017, it named North Korea as the attacker in the brief of the investigation on the hacking attacks.[138] Although the brief did not include the exact data set or specify the amount of leaked information, the number of infected PCs was around 3,200 (2,500 PCs for the Internet, 700 PCs for the intranet).[139] The first log of the intranet intrusion was revealed as August 4, but the spread of malicious code was noticed by the ROK military on September 23. The vaccine server, which is connected to nearly 20,000 PCs, was infected first, and the malicious code spread through that server. The evidence pointing to Chinese IP addresses used by North Korea in *Shěnyáng (瀋陽: Sunyang)* was similar to the code used by North Korea and therefore led to the attribution. North Korea had targeted the ROK military network system, especially choosing its sever as the first attack target.

2. Improper Defense against Common Cyber Threats

North Korea has exploited the vulnerability of the military in cyberspace using DDoS attacks, which simply paralyzed the web servers, and by intrusion targeting the intranet server of the military. As the author has argued, North Korea's increasing cyber-attack capabilities have been used to harm the ROK and combined units in cyberspace.

---

[135]"Military Announced North Korean Attack Using Hacking E-mail Alleged the Alumni of Korea Military Academy Happened," *Dong-a Ilbo*, June 20, 2011, http://news.donga.com/3/all/20110602/37736298/1.

[136]It is in the Chapter III of "The Art of War" by Sun Tzu. Originally the chapter is talking about *planning attacks* and this sentence enforces the importance of identifying the enemy in a battle for attackers.

[137]Dae-young Lee, "The ROK Intranet Hacking Summary and Analysis," IT World, December 7, 2016, http://www.itworld.co.kr/news/102451#csidx6451a9f8b72ea3790fca869c3d99d36.

[138]Gi-no Sung, "The ROK Ministry of Defense Announced the Result of Inspection: North Korean Hacking Group Lead," *Boan News*, May 2, 2017, http://www.boannews.com/media/view.asp?idx=54586.

[139]Lee, "The ROK Intranet Hacking Summary and Analysis."

However, their cyber-attacks have succeeded only because their victims are inadequately defended.[140] The ROK and U.S. systems targeted by North Korea lack the capabilities necessary to prevent, detect, mitigate, and respond to cyber-attacks.

Then, whose fault was it? Indeed, no evidence exists that a lack of cooperation in the ROK and U.S. alliance is causing the cyber security issues raised by the North Korean cyber-attacks. Though it has not caused the problem, is it useless for the ROK and the U.S. military to collaborate in cyberspace? Considering the anticipated reciprocal effects of either the ROK or the United States being intruded upon by the North Korea, whose intent is to steal information and weaken combat efficiency, the two countries need to reach consensus on how to cooperate on cyberspace-related activities. The attacks on either country could affect combined operations, as the war plan hack targeting the ROK military affected the operation of the U.S. military. Because cooperation in cyberspace cannot be avoided in this alliance relationship, Chapter IV describes the current ROK and U.S. alliance. Before doing so, however, the author examines the vulnerabilities of North Korea that might be exploited by the alliance, thereby guiding the recommendations in the final chapter of this study.

E. VULNERABILITY IN NORTH KOREA

This section suggests four possible vulnerabilities in North Korea which the ROK and U.S. alliance could exploit.

1. Myth of a Stand-alone Cyberwar to Achieve a Military Purpose

When North Korea's cyber-attacks converge with the use of kinetic weapons, the damage will be much more extensive due to the decrease in the efficiency of the ROK and U.S. military response.[141] Cyber threats cannot be decisive alone.[142] Since North

[140]However, the ROK makes a system whenever the attacks happen, so in the recent North Korean attack on the civilian networks, like ones using ransomware, the damage and shock to both of the countries was minor. Although reportedly South Korea also implemented cyber espionage toward North Korea, this section focuses on defense of the ROK. Cyber activities of South Korea and the United States toward North Korea are referred to in the next section.

[141]Kim, "The Republic of Korea's Counter-Asymmetric Strategy."

[142]Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no.2 (Fall 2013): 41–73, doi: 10.1162/ ISEC_a_00136.

Korea cannot sustain war for a long period, cyber-attack capabilities are needed to downgrade the effectiveness of the ROK and the U.S. military operations.

Continuous cyber-attacks without kinetic attacks could expose North Korea's cyber capabilities without achieving national or military goals. North Korea certainly has developed its attack methods in cyberspace, but its repeated attacks have also revealed its secret organization and cyber capabilities. Specific information gathered by the ROK and the U.S. government is still classified, but a great deal of open-source research exists about North Korea's physical attacking points, methods, and technology. North Korea is gradually losing its biggest advantage of surprise in cyber operations.

2. Limitations of Self-Operation

Many research papers and newspaper articles have noted North Korea's cyber operations from inside China. Although North Korea maintains "self-reliance," it is limited by using its own technology and infrastructure to build cyberspace. Consequently, it is impossible for North Korea to practice cyber operations without assistance from other countries such as China and Russia. North Korea depends on the other countries for its resources—to produce cable, electricity, and network devices—and the methods that support connecting to the network, such as IP address allocation and physical network connection. The lack of cyber technology resources means that North Korea must send its cyber warriors to foreign countries to practice cyber operations. Recalling the first vulnerability—the more North Korea practices cyber-attacks, the more North Korea's capabilities are revealed—we see that not only are their capabilities revealed, but also which countries support their operations. Once these relationships are exposed, it would be difficult for those countries to support the North Korean attacks and ignore the norms of international society. Finally, North Korea's standing in the international community would shrink further**.**

Jong-in Lim analyzed North Korea's cyber limitations from its fundamental weakness: an unstable power supply.[143] Currently North Korea's capability to produce electricity fluctuates: although North Korea has had several decades of building water

[143]Lim, "North Korea Cyber Strategy and National Response Strategy of South Korea," 10–45.

and coal power plants, its power production not only falls behind technical standards in the world, but also has low efficiency, because of cold weather and the lack of coal.[144] While North Korea has technologies transferred from the USSR and the Czech Republic to produce wires, insulators, electronic motors, and transformers, it cannot produce high capacity generators and automated instruments because of insufficient technology to produce semiconductors.[145] Although North Korea manages to prioritize the distribution of electricity, it is unclear if it has enough power production ability to achieve its modernization.

3. Paradox of Modernization

North Korea recently launched the *New Century Industrial Revolution (새 세기 산업혁명)* project for creating new industry.[146] The project includes the IT industry, which ranges from its traditional industries to the construction industry, and financial businesses. It supports process automation and establishes a national standard for technology diffusion. To propel the policy, North Korea invests not only in IT, but also nanotechnology, biotechnology, natural energy, rocket technology, and the nuclear fusion industry. Currently, North Korea's manufacturing technological development is to produce tablet PCs, notebook computers, desktop computers, smart phones, and TVs. It also reports that it has RMC-3000, developed in 2016,[147] and a real-time monitoring system for transportation for subways and trucks.[148] North Korea's future development

[144]Kang, "Science Technology Industry Trends Evaluation of Kim Jung-un Regime."

[145]Hei-jung Kim, "Status and Implications of Korea's Information and Communication Corporation," in *Information Communications Issues*, vol. 13 (Suwon, ROK : KICI, September 2016): 17, http://www.kici.re.kr/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EC%82%B0%EC%97%85%EB%8F%99%ED%96%A5/?mod=document&uid=416.

[146]"Let's Take the Great Kim Jung-il Comrade as the Eternal General Secretary of Our Party and Proceed with the Juche Revolution Shining," *Rodong Sinmun*, April 19, 2012, quoted in Kang, "Science Technology Industry Trend Evaluation of Kim Jung-un Regime."

[147]"Respectable Kim Jung-un Comrade Guides Multiple Industries," *Chosun Jungang*, broadcast September 12, 2016, quoted in Kang, "Science Technology Industry Trends Evaluation of Kim Jung-un Regime."

[148]"The Power of Eternal Victory," *Chosun Jungang*, broadcast February 7, 2017, quoted in Kang, "Science Technology Industry Trends Evaluation of Kim Jung-un Regime," in *KDI Review of the North Korean Economy* 19, no 2 (February 2017)

focuses on the promotion of new technology industries and computerization in production and management.

North Korea's modernization policy for economic development can cause a technological paradox that other nations have already experienced.[149] North Korea's technological development increases its dependency on technologies, thereby diminishing its asymmetric advantage. This development diminishes some advantages for North Korea, which currently does not have any targets to defend against an adversary's attacks. The increase of automation in these industries would increase the scope of damage after attacks. Furthermore, considering its announcement of automation, North Korea could employ cybernetics even in managing WMD and missiles.[150]While North Korea probably develops its WMD around traditional hardwired devices, if it uses any kind of network connectivity or software, its WMD could be the target of cyber-attacks. Therefore, the more focused the DPRK becomes on military modernization, the greater its vulnerability.

In addition to the decrease in asymmetric benefits, North Korea will be compelled to follow global technology standards and to cooperate in technology transfer. While North Korea's cyber espionage allows it to obtain high-end technologies quickly, it is also able to obtain technologies through cooperative ventures with companies in South Korea. In 2001, civilian companies in the ROK, such as KT and Giga link, joined in an ongoing information-communication infrastructure project developed under the Sunshine policies. In 2014, an information-communication construction company also went to North Korea and now supports the topmost facilities, such as remote control and automation control systems, including SCADA.[151] In the end, no matter how North Korea obtains technologies—by stealing, legitimate transfer, or self-development—its technologies are based on international standards.

---

[149] Cho, "2016 North Korea Military Industry Trends and Evaluation."

[150] John Schilling, "How to Hack and Not Hack a Missile," 38 North (U.S.-Korea Institute at Johns Hopkins University), April 21, 2017, http://www.38north.org/2017/04/jschilling042117/.

[151]Hei-jung Kim, "Status and Implications of Korea's Information and Communication Corporation."

4. Internal Information Control

Though North Korea has an Internet connection, it limits access to the Internet. Only a small number of North Koreans and visitors from foreign countries can use the Internet out of North Korea. Also, the government blocks access to some websites. North Korea's control over the Internet is closely related to protecting the current regime. The authorities in North Korea worry about North Koreans being exposed to outside information. In 2015, after ROK soldiers were injured by landmine explosions, South Korea decided to respond strongly by setting up loudspeakers at the demilitarized zone (DMZ) for psychological operations aimed at North Korea.[152] In response, North Korea reluctantly "expressed regret over" the accident in an inter-Korean joint press statement. Another example showing that North Korea's regime is worried about information is its control of mobile communications.[153] Using smart phones, North Koreans started to find information outside their country and find methods to connect privately to the internet. Broadening mobile connectivity might be one of the key vulnerabilities the ROK and U.S. alliance could exploit.[154]

F. CONCLUSION

Chapter III has studied the common cyber threats against the ROK and the United States military on the Korean Peninsula. For the DPRK, cyber-attacks offer the chance to *kill multiple birds with one stone.* North Korea has increased its offensive capabilities and used cyber espionage to steal technological secrets as well as funds from the ROK and the United States. Most of all, its cyber capability impacts the ROK military directly and indirectly. The resulting crisis is caused by inadequate defense against the DPRK, not just by the existence of cyber threats. The ROK-U.S. military alliance needs to pay attention to the increased cyber threats and their impact on military operations. Meanwhile, North Korea also has vulnerabilities and latent weaknesses. The

[152]*2016 Defense White Paper*, 242–247.

[153]Nat Kretchun, "The Regime Strikes Back: A New Era of North Korean Information Controls," 38 North (U.S.-Korea Institute at Johns Hopkins University), June 9, 2017, http://www.38north.org/2017/06/nkretchun060917/.

[154]LaFoy et al. *North Korea's CyberOperations: Strategy and Responses.*

vulnerabilities of the DPRK described in this chapter suggest ways of addressing the central question of how the ROK and the U.S. military can cooperate against common cyber threats on the Korean Peninsula. This is detailed in Chapter VI. Prior to the general conclusion in the last chapter, Chapter IV studies the nature of the ROK and U.S. alliance, and the deficiencies in its structure for addressing cyber threats.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE ROK AND U.S. ALLIANCE IN CYBERSPACE

A. THE NATURE OF THE ROK AND U.S. ALLIANCE

The recent international consensus on the definition of *alliance* is a relationship based on an alliance treaty to provide legal aid to each other under particular conditions (*causus foederis*).[155] Depending on the purpose of the alliance, it is categorized as an offensive, defensive, or offensive and defense alliance. A permanent combination makes a federal state; a temporary union makes the alliance a relationship between two countries. The distinction of the alliance reflecting the security treaty or partnership is a dual duty. It is mainly based on military force, but there is also permission to provide bases, financial and material assistance. Because an alliance includes responding to a common threat using military forces, it required a threat (adversary). Therefore, an alliance inevitably results in a counter-alliance to deal with it, and creates a chain reaction. Theoretically, the chain reaction results in two significant forces, and when they cannot resolve the conflict, war occur. World War I exemplifies this chain reaction.

1. Background: North Korea's Armed Threats

The ROK and the United States established their first military relationship in 1871 and a formal diplomatic relationship in May 1882.[156] Although Cho-sun (Korea's name at that time) expected the United States to provide favorable support through a treaty, the United States signed the Katsura-Taft Agreement in July 1905, which supported Japan's sovereignty on the Korean Peninsula, and the relationship between Cho-sun and the United States ended.

After the defeat of Japan in World War II, the actual cooperative relationship between Korea and the United States began as the U.S. 24th Army corps stayed in Korea

[155]Stephen M. Walt, *The Origins of Alliance* (Ithaca, NY: Cornell University Press, 1990).

[156]"Beginning of the Relationships between Korea and the United States ('49)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50745&titleId=null&siteId=mnd&id=mnd_010701040000.

after September 2, 1945, to disarm the Japanese Army.[157] By November 1945, around 70,000 members of the U.S. military were deployed in South Korea. The U.S. military, however, rapidly dismantled and sought to withdraw troops from areas of lesser importance to the national interests. The United States ranked Korea 15th among the 16 countries regarded as important to security. Based on strategic assessments, the U.S. Army adopted the Island Perimeter Strategy, excluding the Korean Peninsula from its strategic priority. Through policy debates, the U.S. Department of State and military specified the withdrawal plan and issued National Security Council Document No. 8 (NSC8) on April 8, 1948, and a new amendment document (NSC 8/2) on March 22, 1949. As a result, the USFK decided to withdraw at the end of June 1949, and it began withdrawal on September 15, 1948, and completed the withdrawal except for only 495 members of the Korean Military Advisory Group (KMAG) by June 29, 1949. The remaining U.S. military mainly engaged in the execution and supervision of the ROK-U.S. military support, the transfer of weapons, the formation and training of ROK armed forces, and strengthening of military education institutions.

When the Korean War broke out in 1950, the relationship between the ROK and the United States faced a turning point with the participation of the United States.[158] When North Korea launched a surprise attack on the South on June 25, 1950, the United States called for a UN Security Council resolution. The Security Council required North Korea to stop the attack and withdraw by 14:00 on June 25. As the North Korean Army, however, ignored even the second resolution, the UN passed a resolution to support South Korea to repulse the North Korean armed attack and restore international peace and security on June 27, 1950. In accordance with the adoption of a proposal to establish the U.N. Command suggested by Great Britain and France in the UN Security Council on July 7, the UN organized an integrated military command under the U.S. military.

[157] "Beginning of the Relationships between Korea and the United States ('49)." By the U.S. occupation plan of the U.S. Army, the 7th Division replaced Seoul, Gyeonggi, Chungcheong and Gangwon at the beginning of September of that year, the 40th Division replaced Busan and Gyeongsang in September, and the 96th Division in October, and the 6th Division was located in Jeonra areas, respectively.

[158] "The U.S. Intervention in the Korean War and the Official Establishment of the US-ROK Military Relationship ('50 ~ '53)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50746&titleId=null&siteId=mnd&id=mnd_010701040000.

President Truman appointed General MacArthur, the commander of the U.S. Far East, as a commander of the UN forces on July 8, and he established a command in Tokyo on July 24. At the same time, Korean President Rhee sent an official letter to General MacArthur that he had transferred the authority of commanding the ROK military during the war to the UN commander on July 15, 1950. MacArthur accepted the command on August 18. More than 360,000 troops fought in the Korean War, and 35,000 U.S. military were killed.

The Korean War ended on July 27, 1953; subsequently, the ROK and the United States signed a mutual defense treaty on October 1, 1953, to prevent North Korea's provocation. The ROK and U.S. alliance became effective in January 1954.[159] Article three of the treaty stipulates that an armed attack against either country is regarded as jeopardizing the peace and stability of both countries and each should respond to common threats according to the alliance procedures. Article four regulates the presence of the U.S. forces in the ROK. These two parts of the treaty became the legal basis of the current ROK and U.S. military combined defense system.

The relationship of the ROK and the United States has constantly been changing since it began in 1871, but it has primarily maintained a military alliance since the mutual defense treaty was signed in 1953. The coordination for building a new government on the Korean peninsula after WWII resulted in the participation of the U.S. military in the Korean War, and the current state of the ROK and the United States Mutual Defense Treaty.[160] The basic framework for the current relationship between the ROK and the United States has been made in response to the invasion of foreign powers—mainly, to prevent North Korea's armed provocation.

2. Changes and Developments

Since the signing of the Mutual Defense Treaty, the relationship between the ROK and the United States has changed in accordance with circumstances such as

[159] "The U.S. Intervention in the Korean War and the Official Establishment of the US-ROK Military Relationship ('50 ~ '53)."

[160] "The Background of the Mutual Treaty," ROK Ministry of National Defense, accessed October 1, 2017, http://www.mnd.go.kr/mbshome/mbs/mnd/subview.jsp?id=mnd_010701010000.

changing threats from North Korea, the global security situation, and the economic development of both countries. Until the end of the 1960s, the relationship between the ROK and the United States was a relationship of patron-client in the Cold War confrontation structure against the Union of Soviet Socialist Republics (USSR).[161] The United States assisted the economy and military of the ROK, and the ROK provided land and facilities to the USFK. The USFK led the ROK's defense, but internal pressure in the ROK also exists to be independent of the United States. As the ROK dispatched armed forces in the Vietnam War to support the U.S. military, the United States contributed to the ROK military in the form of grant aid, Foreign Military Sales (FMS), support of defense technologies and cooperation projects. Frequent provocations by North Korea made the ROK and the U.S. military ties even stronger. The two countries agreed to open annual defense meetings in 1968, which was renamed as the Security Consultative Meeting (SCM) on February 7, 1971.

During the 1970s, the ROK and U.S. alliance was dynamic.[162] The U.S. failure in Vietnam and the criticism in the United States resulted in a policy of reduced intervention. Accordingly, the United States announce that it would withdraw 20,000 U.S. troops from the Korean Peninsula in July 1969. The international environment, which was marked by communism in Vietnam, however, delayed withdrawal until President, Carter was inaugurated in 1977. Though Carter had advanced his three-phase withdrawal plan, he also cancelled his plan after visiting the ROK in 1979. In the midst of repeated discussions about the U.S. military reduction, the ROK and the U.S. military created the Combined Forces Command (CFC) in 1978. The CFC Commander took control of both

[161]"Patron-Client Alliance ('54 ~ '68)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50747&titleId=null&siteId=mnd&id=mnd_010701040000.

[162]"Seeking the Development of Military Relations Extending to Participation of the ROK ('69 ~ '79)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50748&titleId=null&siteId=mnd&id=mnd_010701040000.

the ROK and the U.S. forces, as specified in "Strategic Direction 1" on October 17, 1978.[163]

The United States did not clarify a further the plan for the withdrawal of the U.S. military from the Korean Peninsula at the summit in February 1981. Under the Reagan administration, military alliances were strengthened to defend against the USSR.[164] Although the strength of the ROK and U.S. alliance greatly increased during the Reagan administration (1981–1989), the United States fiscal deficit intensified while the ROK achieved a rapid economic development. It changed U.S. policy as the United States no larger considered the ROK as a one-way security aid object, and the United States suspended FMS in 1987. Since then, the two countries have determined the defense cost contribution considering the economy of the ROK, the threat level of North Korea, and the political and economic situation in the United States.

With the change of leadership in the United States in 1989, the U.S. Congress again discussed the withdrawal of the U.S. forces.[165] According to the Senate Amendment in 1989, the U.S. DOD issued the Presidential Report, the East Asia Strategic Initiative (EASI), which reviewed the strategy of the U.S. in the Asia-Pacific region. The EASI provided a major opportunity for the development of the ROK and the U.S. military relationship into a 'partnership.' The role of the USFK in the ROK changed from a leading role to a supplementary role in defense on the Korean Peninsula, and the ROK government started to pay more of the defense budget. The ROK military took a series of measures to play a leading role in the defense of the Korean peninsula, like transferring part of the Joint Security Area (JSA) security responsibilities, and normal

---

[163] Ibid. The *command authority* during *the ongoing hostilities* that was entrusted to General MacArthur in 1950 was changed to *Operational Control authority* during the *UN command to burden the responsibilities for defense of the ROK*, in accordance with the [U.S.-ROK Agreement] signed between the ROK and the United States on November 17, 1954.

[164] "Reconnection of the Korea-US Military Alliance ('80 ~ '89)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50749&titleId=null&siteId=mnd&id=mnd_010701040000.

[165] "Reconnection of the Korea-U.S. Military Alliance ('80 ~ '89)." The 13 Senators of the Military Commission, including Democrats and Republicans, initiated it on July 31, 1989. The bill was submitted in the form of an amendment attached to the National Defense Budget Bill for the year of 1990 to 1991, and passed the Senate Plenary Session on August 2.

operational control authority to the ROK Army. Since 1992, the ROK and U.S. government have held joint consultations on the direction of the ROK and U.S. alliance, in preparation for changes in the security situation on the Korean Peninsula, even after unification.

After the withdrawal of 7,000 troops under the EASI in December 1992, however, the United States changed its strategy because of its suspicion of North Korea's nuclear development.[166] Through the East Asia Strategic Report (EASR) in 1995, the debate on the withdrawal of the USFK ended. In the 2000s, reflecting the domestic opinion of both countries, the ROK and the United States agreed on the expansion of the ROK's role on the Korean Peninsula. As a result, they agreed on the early relocation of the USFK base in 2003, and began to transfer part of the USFK missions to the ROK military.[167] In addition, since 2005, discussion has been active about the wartime operational control authority. In February 2007, the ROK and the U.S. defense secretary met and agreed to transfer the war-time operational control authority from the USFK to the ROK military on June 17, 2012.

The Cheonan strike showed that the North Korean threat was considerable. With consensus that the ROK military was not yet mature enough to carry out its own operations, the two countries met at the G20 summit on June 26, 2010, and agreed to postpone transferring the authority until December 1^{t}, 2015. In 2014, the transfer of operational control authority was again postponed from 2015 to after 2020, but both of the countries reaffirmed their willingness to implement the plan in 49th SCM.[168]

---

[166]"Seeking a New 'Security Partnership' and the End of the Cold War ('90 ~ '99)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&siteId=mnd&boardId=O_50735&page=1&boardSeq=O_50750&search=&column=&categoryId=&categoryDepth=&id=mnd_010701040000&parent=.

[167]"Future-Oriented Development of the ROK-US Alliance (Since '00)," ROK Ministry of National Defense, August 5, 2013, http://www.mnd.go.kr/user/boardList.action?command=view&siteId=mnd&boardId=O_50735&page=1&boardSeq=O_50751&search=&column=&categoryId=&categoryDepth=&id=mnd_010701040000&parent=.

[168]"Full Text of ROK-U.S. Security Consultative Meeting Joint Communiqué," *Yeonhap News*, October 28, 2017, http://english.yonhapnews.co.kr/northkorea/2017/10/28/0401000000AEN20171028003000315.html

The ROK and U.S. alliance, established to respond to the common armed threat of North Korea, has evolved dramatically over the past 70 years, with rapid changes in both countries. In accordance with the external situation, such as the Cold War, the internal situation, such as national development, the changes in regime, and the changes in North Korea's threats, the ROK and U.S. alliance has progressed from a defense led by the United States to a defense cooperation between the two countries for stability on the Korean Peninsula. In conclusion, the ROK and U.S. alliance has been flexible, based on the common perception that the cooperation of both countries is beneficial to respond to common threats.

3. Limitations of the Alliance

While the changeable nature of the ROK and U.S. alliance can be seen as positive, this flexibility can be seen as a challenge because it causes controversy about its effectiveness. Some critics say South Korea should build nuclear weapons to counter the threat from North Korea, but the alliance is designed with the U.S. providing the nuclear security guarantee for the ROK.[169]

Another limitation of the bilateral alliance is that the partnership has complicated relationships with countries neighboring the Korean Peninsula such as China and Japan. The serious conflict around the Terminal High Altitude Defense (THAAD) allocation on the Korean Peninsula illustrates the difficulty in deciding and coordinating the interests of each country. Though the ROK and the United States agree on THAAD allocation in the ROK with the increase of North Korea's nuclear weapon threats, THAAD's presence results in China's suspicion and pushback, and generates economic conflict between the ROK and China.[170]

---

[169]Byung-chul Lee, "Preventing a Nuclear South Korea," 38 North (U.S.-Korea Institute at Johns Hopkins University), September 16, 2017, http://www.38north.org/2016/09/bclee091516/.

[170]Hyung-Jung Kim, "China and South Korea Pledge to Ease Tensions Over U.S. Missile Defense System," *TIME*, October 31, 2017, http://time.com/5003532/south-korea-china-thaad-missile-defense/. "Many analysts say China appeared to use its THAAD opposition to bolster its regional clout but that such a stance could push South Korea closer to the United States and Japan for a potential anti-Beijing trilateral alliance."

Despite the limitations of the current ROK and U.S. alliance, it maintains security on the Korean Peninsula. Henceforth, it is imperative to mitigate the vulnerability coming from the limitations of the alliance by understanding and protecting cyberspace. As the ROK and U.S. alliance is based on military cooperation, the military should understand the nature of limitations of the alliance and what to do. Therefore, the next section studies the deficiencies of the ROK and the U.S. military alliance in cyberspace.

B. MILITARY DEFICIENCIES OF THE ROK AND U.S. ALLIANCE IN CYBER OPERATIONS

Based on cyber threats, the ROK and U.S. agreed to cooperate in cyberspace. The alliance, however, has deficiencies in its current structures.

1. Intention of the ROK and U.S. Alliance in Cyberspace

The ROK and U.S. alliance has conferred on not only the roles of the alliance, but also the domains of cooperation required to handle the North Korea's threats. The ROK and the U.S. military have affirmed annually the common the necessity to cooperate in cyberspace since the 43rd SCM in 2011.[171] The ROK and U.S. alliance alluded to "the need to strengthen cooperation with respect to protection of, and access to, the space and cyberspace domains, and to promote the resilience of critical infrastructure, including the security of information and space systems."[172] Since then, the 47th SCM in 2015 has removed "with respect to protection of and access to," from the previous announcement.[173] Also, it has changed "resilience of critical infrastructure, including the security of information and space systems" to "the security of critical infrastructure, including information and space systems." The 49th SCM in 2017 shares the idea that

[171]"Joint Communiqué, the 43rd U.S.-ROK Security Consultative Meeting," ROK Ministry of Foreign Affairs, October 28, 2011, https://mofa.go.kr/webmodule/htsboard/template/read/korboardread.jsp?typeID=24&boardid=11695&seqno=4060&c=TITLE&t=SCM&pagenum=1&tableName=TYPE_KORBOARD&pc=&dc=&wc=&lu=&vu=&iu=&du=.

[172]"Joint Communiqué, the 43rd U.S.-ROK Security Consultative Meeting."

[173]"Full Text of 47th ROK-U.S. Joint Communiqué," USFK, November 1, 2015, http://www.usfk.mil/Media/News/Article/626859/full-text-of-47th-rok-us-joint-communique/.

"cyber capacity [is] a core security issue and decided to expand bilateral defense cooperation in cyber-related areas."[174]

Underneath the common perception of bilateral cooperation in cyberspace, the 43rd SCM in 2011 guided the bilateral cooperation as a "whole-of-government" approach.[175] The 44th SCM in 2012 stated the necessity of "increased cooperation between defense agencies,"[176] and the 49th SCM in 2017 underlines the "elevation of the U.S. Cyber Command."[177]

The domain for cooperation in cyber operations also has been extended to technological development and interoperability. The 48th SCM announced the Defense Technological and Industrial Cooperation Committee (DTICC), which led to the technological cooperation against future North Korean threats.[178] The 49th SCM in 2017 highlighted the successful cooperation "in robotics and autonomous technologies cooperation" based on DTICC, and announced the ROK and the United States would deepen and expand cooperation in it.[179]

Both countries agree on the necessity of extending the defense of cyberspace under the bilateral alliance structure to cover the common cyber threats by North Korea. The statement of the SCM is the basic and official communication channels between the ROK and the U.S. DOD. As a result of the annual SCM, the ROK and U.S. DOD operate the Cyber Policy Working Group (CCWG) and the DTICC as a new organization.

---

[174]"Full Text of ROK-U.S. Security Consultative Meeting Joint Communiqué."

[175]"Joint Communiqué, the 43rd U.S.-ROK Security Consultative Meeting."

[176] "Joint Communiqué, the 44th U.S.-ROK Security Consultative Meeting," ROK Ministry of Foreign Affairs, October 24, 2012, https://mofa.go.kr/webmodule/htsboard/template/read/korboardread.jsp?typeID=24&boardid=11695&seqno=6387&c=TITLE&t=SCM&pagenum=1&tableName=TYPE_KORBOARD&pc=&dc=&wc=&lu=&vu=&iu=&du=.

[177]"Full Text of ROK-U.S. Security Consultative Meeting Joint Communiqué."

[178]"Joint Communiqué of the 48th U.S.-ROK Security Consultative Meeting," U.S. DOD, October 20, 2016, https://www.defense.gov/Portals/1/Documents/pubs/USROKSecurityJointCommunique2016.pdf.

[179]"Full Text of ROK-U.S. Security Consultative Meeting Joint Communiqué."

2. Organizations for Cooperation

The CCWG has met twice per a year since 2014.[180] The 47th SCM in 2015 avowed its role in enhancing military cyberspace collaboration.[181] It is the primary organization for collaboration on "information sharing, cyber policy, strategy, doctrine, personnel, and exercises to improve our collective readiness against cyber threats,"[182] and it will continue to synchronize the combined efforts in cyberspace.[183]

The ROK Ministry of Defense and the U.S DOD held the first CCWG at the ROK Ministry of National Defense on February 7th in 2013.[184] The ROK and the U.S. conducted a Table Top Exercise (TTX) that identified vulnerabilities related to the cyber-crisis response based on the scenario of cyber-attacks, and developed a cooperation plan. Far ahead of the third ROK and U.S. CCWG, the ROK Joint Chiefs of Staff (JCS) and the USFK conducted TTXs twice in July and October of that year, and participated in a cyber-attack exercise on the Nuclear Power Plant, Combined and Joint Command Control System and discussed practical procedures for cooperation.[185] The ROK and U.S. alliance discussed how to cooperate during a cyber crisis.

In addition to the CCWG, the ROK and U.S. DOD signed the Information Protection / Network Defense Information Exchange Operation Plan (IA / CNDSOP) for effective information sharing in 2015.[186] Both parties also organized the DTICC for technology cooperation. SCM states the purpose of technical cooperation is interoperability for future operations.

---

[180] *2016 Defense White Paper*, 67.

[181] "Full Text of 47th ROK-U.S. Joint Communiqué."

[182] "Joint Communiqué of the 48th U.S.-ROK Security Consultative Meeting," U.S. DOD, October 20, 2016, https://www.defense.gov/Portals/1/Documents/pubs/USROKSecurityJointCommunique2016.pdf.

[183] Ibid.

[184] "The 1st Korea-U.S. Cyber Policy Working Group (CCWG)", ROK Ministry of Defense, February 7, 2013, http://www.gov.kr/portal/ntnadmNews/61089?srchOrder=&srchOrgCd=ALL&srchNewsAstCd=ALL&srchStDtFmt=2009.01.01&srchEdDtFmt=2017.10.28&srchTxt=%EC%82%AC%EC%9D%B4%EB%B2%84&initSrch=false&pageIndex=120&hideurl=N.

[185] "The 3rd Korea-U.S. Cyber Policy Working Group (CCWG)", ROK Ministry of Defense, October 29, 2015, http://www.korea.kr/briefing/pressReleaseView.do?newsId=156082384.

[186] *2016 Defense White Paper*, 67.

3. Deficiencies of Current Cooperation in Cyberspace

Although the ROK and U.S. alliance has expressed its intention to cooperate in cyberspace, this cooperation is still at the beginning of development, and specific practices for cooperation have not been revealed. Basically, the general limitations of the ROK and U.S alliance also apply to the cyber domain. First, the flexibility and changeable nature of the alliance makes the actors in the alliance hesitate to decide on the cooperation level. The role of cyber operations of the armed forces will be to increase combat efficiency using the network, to ensure cyberspace, interoperability, to secure the network and to target adversaries. Similar to other security issues, the cyber domain is also connected by complex relationships with many other countries. Moreover, it is inefficient for the United States to embark on separate efforts for cyberspace in each of the different alliances in which it participates.

In addition to the limitations of alliances, the current cooperation in cyberspace is insufficient for the ROK and the U.S. Specific contents of the cooperation are still classified, but the organizational structure for cooperation and consensus on the terminologies exist. Yet, no common strategic response exists, though the United States officially stated a deterrence objective for cyberspace.[187]

C. CONCLUSION

Chapter IV studied the nature of the ROK and U.S. alliance through the history of military cooperation between the two nations. The alliance has been devoted to the security of the Korean Peninsula, but the ROK and U.S. alliance has sometimes showed limitations, such as in complex regional relationships with third countries like China. It is clear, however, that peace on the Korean Peninsula is centered on the ROK and U.S. alliance, which has evolved based on changes in the domestic and international environments. As the alliance has coordinated its responsibilities, roles, and missions in other areas, the ROK and the United States acknowledge the inevitability of cooperation in cyberspace. Unlike their well-developed means of coordinating traditional military

[187]Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: The White House, May 2011, 14.

capabilities, the two countries' teamwork related to cyberspace is still immature and has deficiencies. How could they develop a system for cooperation? Chapter V offers guidance from NATO's accomplishments that can lead to a more mature cooperation for defense in cyberspace.

V. LESSONS FROM NATO

A. COMPARISON OF NATO TO THE ROK - U.S. ALLIANCE

NATO, like the ROK and U.S. alliance, has displayed its intention to cooperate in responding to new threats in cyberspace. The two different alliances both have a common partner in the United States, and both alliances share common values based on similarities in the political systems of the member states. Indeed, the ROK was the cause of establishing armed forces within NATO's defense alliance system. After the Soviet blockade of Germany in 1948, NATO was established out of the necessity for the collective security. After the outbreak of the Korean War in 1950, however, it recognized the need for a substantial military organization to secure Europe in the Cold War. The command center formed by the UN Security Council during the Korean War became the NATO military command after the ceasefire. Since organizing the armed forces, the chief of the NATO command has always been a U.S. four-star general.

The difference between the two alliances is that NATO is a collective security system of 29 countries, but the ROK and U.S. alliance is a bilateral alliance.[188] While only 12 nations participated in NATO at its beginning in 1949, the membership continuously increased, and most recently, Montenegro joined in 2017. The ROK and the U.S. bilateral mutual alliance is a closed relationship, while NATO's membership has been changing since that alliance's inception.

Both alliances depend on the trust and the willingness of the allies. One significant difference between the ROK and U.S. alliance and NATO seems to be the regulation of automatic intervention written in Article Five.[189] It states that members consider an attack on one member of the alliance as an attack on the whole, and they will respond collectively. For instance, when the United States went to war in Afghanistan in response to the 9/11 terrorist attacks, NATO issued a statement on September 12th that

[188]"What is NATO? Pick a Topic and Discover NATO," NATO OTAN, accessed in October 1, 2017, https://www.NATO.int/NATO-welcome/index.html.

[189]"The North Atlantic Treaty," NATO OTAN, April 4, 1949, https://www.nato.int/cps/ic/natohq/official_texts_17120.htm.

triggered article five.[190] It, however, took more than three weeks for NATO to finish the agreement on the specific eight methods of the collective response, finalizing that on October 4th.[191] Indeed, NATO also has article eleven, which requires an administrative procedure for automatic intervention. Every alliance of the United States includes the same article as NATO's article eleven, including the ROK and U.S. Mutual Defense Treaty and the U.S. and Japan treaty.[192]

NATO has addressed international cooperation for cyber defense since 2002, and it has a mature cooperative system compared to the ROK and U.S. alliance.[193] The ROK and the United States affirmed the common intention to extend the current cooperation structure to cyberspace (see the Appendix). Of course, NATO started ten years earlier than the ROK and U.S. alliance. As the predecessor of cyberspace cooperative operations, what did NATO do to improve efficiency and harmonize the existing cooperation? The next section finds some lessons from NATO to guide the direction of the ROK and the U.S. military alliance in cyberspace.

B. MILITARY CYBER OPERATIONS

NATO aims to secure the territory of its allies and supports missions out of the NATO areas, if necessary. Its collaboration in cyberspace has developed under its current military framework. This section analyzes NATO's cyber capabilities in organizations, research planning, doctrine and methods, and education, training, and exercises. Finally, it identifies which points are immature from the assessment in the *NATO Cyber Capability: A Strategic and Operational Evaluation*.[194]

---

[190]"Statement by the North Atlantic Council," NATO Press Releases, September 15, 2001, https://www.NATO.int/docu/pr/2001/p01-124e.htm.

[191]"Collective Defense – Article 5: Invocation of Article 5," NATO OTAN, March 22, 2017, https://www.nato.int/cps/ic/natohq/topics_110496.htm.

[192]"The North Atlantic Treaty."

[193]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 1.

[194]Ibid.

1. Organization for Military Operations

NATO's cyber operation developmental structure follows the same flow of the existing cooperation structure and organization at the tactical levels.[195] Allied Command Operations (ACO) has the responsibility to plan and execute alliance operations from the strategic to the tactical level, as directed by the policy of the North Atlantic Council (NAC) and the authority provided by NATO Headquarters. The ACO has the Supreme Headquarters Allied Powers Europe (SHAPE) for strategic level planning, and the Joint Force Commands in Brunssum, the Netherlands (JFCBS), and in Naples, Italy (JFCNP) for the operational level. For the tactical level, three commands exist: "Headquarters Allied Land Command (HQ LANDCOM) in Izmir, Turkey; Headquarters Allied Maritime Command (HQ MARCOM) in Northwood, UK; and Headquarters Allied Air Command (HQ AIRCOM) in Ramstein, Germany."[196] The Communication and Information System (CIS) Group, which has signal battalions in Germany, Poland, and Italy, supports combined operations.[197]

In the effort to apply cyber operations to the military structures, in July 2012 NATO created the NATO Communication Information Agency (NCI Agency) which provides tactical-level situational awareness.[198] The missions of the NCI Agency are to support the missions of the ACO, so it "connect[s] and defend[s] Alliance networks, and helps the interoperability in communications and information sharing." [199] The NCI Agency operates the NATO Computer Incident Response Center (NCIRC) to support the

[195]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 10.

[196]"Allied Command Operations," NATO OTAN, November 11, 2014, https://www.nato.int/cps/ua/natohq/topics_52091.htm.

[197]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 11.

[198]"NATO Communications and Information Agency: Connecting forces," NATO Communications and Information (NCI) Agency, accessed September 1, 2017, https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx.

[199]NCI Agency, "NATO Communications and Information Agency: Connecting Forces."

technical parts for cyber defense, which have evolved since NATO started to plan at the 2002 Prague Summit.[200]

NATO's approach to the cyber operational domain is designed to achieve Full Operational Capability (FOC).[201] Therefore, NATO operates a Rapid Reaction Team (RRT)[202] and staff-run Coordination Center.[203] The RRT supports the member nations to improve skills and to manage procedures, but the lack of resources of the RRT requires collaborations with industry and the Computer Emergency Response Teams (CERTs).[204]The RRT contains six experts and additional mission-specific professionals to achieve a 24-hour response capability. The missions of the staff-run Coordination Center are to coordinate NATO's cyber defense, to provide support to the Cyber Defense Management Board (CDMB) and to associate with external organizations like the European Union (EU).[205]

At the bottom of operational planning, NATO defines its defense operational domain as the area of the Critical Infrastructure Protection (CIP). It considers the cyber-attacks "against the infrastructures which can affect the military operations" in its operational planning process.[206] It has listed the Critical Information Infrastructure Protection (CIIP),[207] but the response to general threats against the CIP still depends on

---

[200]Jason Healey and Klara Tothova Jordan, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow, Issue Brief,* Brent Scowcroft Center on International Security (Washington, DC: The Atlantic Council, September 2014), 2, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*,11.

[201]George I. Seffers, "NATO Set to Strengthen Cyber- security," *SIGNAL Magazine* 28, no. 8 (August 2011), quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 12.

[202]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 12.

[203]Ibid., 13.

[204]"NATO Rapid Reaction Team to Fight Cyber Attack," NATO OTAN, March 13, 2012, https://www.nato.int/cps/en/natolive/news_85161.htm.

[205]Canton, *NATO Cyberspace Capability: a Strategic and Operational Evolution*, 13.

[206]H. Todd Waller, "Cyberspace Implications for NATO Operations and the Joint Warfare Centre," *The Three Swords, The Magazine of the Joint Warfare Centre*, No. 20 (Summer/Autumn 2011), 2, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 13.

[207]Bart Smedts, *NATO's Critical Infrastructure Protection and Cyber Defence,* Focus Paper 19, (Brussels, Belgium: Center for Security and Defence Studies, The Royal High Institute for Defence, July 2010), 13–18, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 13.

situational decisions. The conference in December 2012 about NATO's position in the CIP contained NATO's need to possess response capabilities for threats against the CIP.[208]

If NATO armed forces consider the CIP as the defensive target, it is important to define the CIP and rank it in terms of all property of the allies and "private business."[209] Nonetheless, whether NATO will allocate cyber mission teams to protect CIP is unclear under NATO's current cyber operation structures consisting of "staffs of the J2 (Intelligence), J3 (Operations), J5 (Plans and Policy), J6 (Consultation, Control and Communications), and J7 (Cooperation and Regional Security Division)". [210] The common method for allocating resources the missions is to establish a coordination group such as the "Cyber Defence Cell and Cyber Defence Working Group."[211]

2. Cooperation for Planning

NATO took a step to enhance cooperation in the planning process. As the NATO Defense Planning Process (NDPP) integrated cyber defense in April 2012,[212] NATO started projects, known as Smart Defense, to achieve cost-efficient resource planning for cyber defense. In April 2015, the first Smart Defense conference was held by the Portuguese Ministry of Defense, and three projects were introduced.[213] First, Belgium led the project to build the Malware Information Sharing Platform (MISP).[214] The aim of

---

[208]"The World in 2020 – Can NATO Protect Us? The Challenges to Critical Infrastructure," Conference Report, NATO Emerging Security Challenges Division, December 10, 2012, 34, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 13.

[209]Ibid.

[210]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*,14.

[211]Peter Hutson, "Cyber Defence in Operations," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, 36, quoted in Canton, *NATO Cyberspace Capability: a Strategic and Operational Evolution*,14.

[212]"North Atlantic Treaty Organization Cyber Security,", quoted in Canton, *NATO Cyberspace Capability: a Strategic and Operational Evolution*, 15

[213]"Smart Defence," NATO official website, last updated September 1, 2015, *nato.int/cps/en/natohq/topics_84268.htm*.

[214]"Sharing Malware Information to Defeat Cyber Attacks," NATO OTAN, November 29, 2013, NATO.int/cps/en/NATOhq/news_105485.htm. Belgium led an initiative to facilitate information sharing of the technical characteristics of malware within a trusted community without having to share details of an attack.

this project is to support the NCIRC Technical Center, so all NATO allies can use it.[215] The second project is the Multinational Cyber Defen[s]e Capability Development (MN CD2) which aims to "cooperate on the development of: improved means of sharing technical information; shared awareness of threats and attacks; and advanced cyber [defense] sensors"[216] It includes four initial work packages: "Technical Information Sharing,[217] Cyber Defense Situational Awareness (CDSA),"[218] "Distributed Multi-sensor Collection and Correlation Infrastructure (DMCCI)," [219] and Cyber Information and Incident Coordination System (CIICS) Enhancements. It includes two new work packages, "the CIICS Support Work Package and a Cyber Security Assessment Team (CSAT) capability."[220] The third project is Multinational Cyber Defense Education and Training (MN CD E&T), which researches the methods "to develop courses for cyber education programs, battle lab support for training, and cyber range support for exercises to enhance professional development and certification of cyber defense personnel." [221] NATO's initiative for cyber defense concentrates on the enhancement of interconnectivity and interoperability among nations. The mission is to achieve the goal

---

[215]*Malware Information Sharing Platform, Factsheet* (Brussels, Belgium: NCI Agency), quoted in Canton, *NATO Cyberspace Capability: a Strategic and Operational Evolution*, 15.

[216]"NATO Nations Launch Multinational Cyber Defence (MN CD2) Project," MN CD2— Cyber Defence Capability Development, March 14, 2013, https:// mncd2.ncia.NATO.int/news/Pages/MN-CD2-MOU-Signed.aspx. The Netherlands led the team of Canada, Denmark, the Netherlands, Norway, and Romania.

[217]"WP1: Technical Information Sharing," MN CD2 - Cyber Defence Capability Development, official website, June 11, 2015, https://mncd2.ncia.NATO.int/ourwork/Pages/WP1-Technical-Information-Sharing.aspx.

[218]"WP2: Cyber Defence Situational Awareness," MN CD2 - Cyber Defence Capability Development official website, May 1, 2015, https://mncd2.ncia.NATO.int/ourwork/Pages/WP2-Cyber-Defence-Situational-Awareness.aspx.

[219]"WP3: Distributed Multi-sensor Collection and Correlation Infrastructure," MN CD2—Cyber Defence Capability, official website, June 11, 2015, https://mncd2.ncia.NATO.int/ourwork/Pages/WP3-DMCCI.aspx.

[220]"MN CD2 Nations Agree to Two New Work Packages," MN CD2 – Cyber Defence Capability Development, official website, August 10, 2013, https://mncd2.ncia.NATO.int/news/Pages/MN-CD2-Board-Meeting-08.aspx.

221"Multinational Cyber Defence Education & Training: PoW and State of Play," Overview Brief (Lisbon, Portugal: NATO Emerging Security Challenges Division Science for Peace and Security (SPS) Programme Information, October 20, 2014), quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*,16. Portugal led 11 NATO countries as well as the EU; currently, the United States is not among the group.

of "a coherent set of deployable, interoperable and sustainable forces equipped, trained, exercised and commanded to operate together and with partners in any environment."[222]

3. Doctrines and Methods

NATO Cyberspace Capability: A Strategic and Operational Evolution estimates the current NATO doctrine still need further development to consider cyberspace.[223] The following paragraphs introduce the related organizations and structures, and then the existing doctrine.

NATO has two main strategic commands: the Allied Transformation Command (ATC), which "concentrates on transformation initiatives for NATO military structure, forces, capabilities, and doctrine," and the ACO, which "focuses on current operations."[224] The ATC, particularly, has close relationships with cyber operations, and has organizations in Europe: the Joint Warfare Centre in Stravanger, Norway; the Joint Force Training Centre in Bydgoszcz, Poland; and the Joint Analysis and Lessons Learned Centre in Monsanto, Portugal. The activities of the Centres of Excellence (COE) in NATO are coordinated with ATC. [225]

NATO has three COEs for cyber-related actions: The Cooperative Cyber Defence Centre of Excellence (CCD COE),[226] and the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) and the Centre of Excellence for Defence Against Terrorism (COE-DAT). In October 2008, the CCD COE in Tallinn, Estonia, was founded to: "enhance cooperative cyber [defense] capabilities of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative cyber [defense]."[227] Since then, the CCD COE has contributed to the development of NATO's cyber defense

---

[222]"Connected Forces Initiative," NATO OTAN, June 22, 2016, https://www.NATO.int/cps/ic/NATOhq/topics_98527.htm.

[223]Canton, "NATO Cyberspace Capability: A Strategic and Operational Evolution," 18.

[224]Ibid., 17.

[225]Ibid.

[226]"About our Missions and Visions," NATO Cooperative Cyber Defence Centre of Excellence, accessed October 28, 2017, https://ccdcoe.org/about-us.html.

[227]Ibid.

in multiple ways such as holding conferences and workshops, and supporting educational and research programs. Its dedication to NATO is enormous, involving research about cyberspace, supporting courses from the strategic level to the technical level, and holding annual exercises. The CJOS COE in Virginia leads the research about cyber security issues on maritime operations.[228] The COE-DAT in Ankara, Turkey researches cyber security, topics such as "Terrorist Use of Cyberspace"[229] and "Critical Infrastructure Protection against Terrorist Attacks."[230]

The current NATO doctrine is immature because of its failure to harmonize cyber concepts consistently based on public sources: specifically, the NATO Allied Joint Doctrine Documents.[231] For example, AJP-01 published in December 2010 includes cyber operations and the significance of its impact to the NATO system,[232] while the other documents of AJP, such as AJP-3, 5, and 6 published several months later, do not contain the concept and use inconsistent terms.[233] Furthermore, in comparison to U.S. Joint Publication 3-12(R), October 2014, NATO does not have a similar cyber doctrine. Although the AJP-3.10 published in November 2009 includes the contents of activities related to cyber operations, it uses old terms such as computer network operations (CNO) and computer network defense (CND).[234]

---

[228]*NATO Accredited Centres of Excellence 2015* (Norfolk, VA: Allied Command Transformation, 2015), 15, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 18.

[229]*Terrorist Use of Cyberspace Course Report* (Ankara, Turkey: Centre of Excellence Defence Against Terrorism, May 2014), www.coedat.nato.int/publication/course_reports/11-Terrorist_Use_of_Cyberspace.pdf, 3, quoted in Canton, *NATO Cyberspace Capability: a Strategic and Operational Evolution*,18.

[230] *Critical Infrastructure Protection against Terrorist Attacks* (Ankara, Turkey: Centre of Excellence Defence Against Terrorism, November 2014), www.coedat.nato.int/publication/course_reports/12-CIP.pdf, 16, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*,18.

[231]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 18.

[232]Allied Joint Publication (AJP)-01(D), *Allied Joint Doctrine* (Brussels, Belgium: NATO Standardization Office, December 2010), nso.NATO.int/nso/zpublic/ap/ajp-01(d).pdf., quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*,18.

[233]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 18–19.

[234]Hutson, "Cyber Defence in Operations."

Currently, the NATO Joint Warfare Centre is driving the foundational work for cyber doctrine like identifying process and methods.[235] The cyber doctrine of NATO is now advancing in a way that reflects the diverse results of exercises, "such as Cyber Prioritized Asset List (CPAL), Cyber Risk Assessment Matrix (CRAM), and Warning Advice and Reporting Points (WARP)."[236] The efforts to develop the operational level application of cyberspace also exist, like the Multinational Capability Development Campaign (MCDC) from 2013 to 2014.[237] Cyber Implications for Combined Operational Access (CICOA), one of seven sub-projects of the MCDC, includes efforts to establish a taxonomy. [238]

In addition, to merge cyberspace into the preexisting system, NATO has collaborated with industry to construct a secure future cyberspace. In September 2014 NATO launched the Industry Cyber Partnership (NICP) in Belgium, where "1,500 industry leaders and NATO policy makers" participated, to enrich the relationships of NATO with commercial cyberspace. [239] The cooperation with the private sector is for reinforcement of defense capabilities of NATO's networks. [240] The Cyber Security Incubator Pilot Project and the partnership between NCI Agency and Microsoft exist as an example.[241]

4. Education, Training, and Exercises

NATO has multiple education and training programs to improve the capabilities of its people to cooperatively defend cyberspace. The NATO Defense College in Rome

---

[235]Ibid., 39.

[236]Ibid., 37.

[237]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution,* 21.

[238]Multinational Capability Development Campaign, *MCDC 2013-2014 Catalog of Products*, All Partners Access Network, 2, available from *https://wss.apan.org/s/MEpub/default.aspx.*

[239]"NATO Launches Industry Cyber Partnership," NATO News official website, September 17, 2014, *https://www.nato.int/cps/en/natohq/news_113121.htm*.

[240]Ibid.

[241]"NCI Agency and Microsoft Sign Cyber Cooperation Agreement," NATO Industry Cyber Partnership official website, September 14, 2015, https://www.ncia.nato.int/NewsRoom/Pages/150914-NCIAgency-Microsoft-GSP.aspx. As part of the company's Government Security Program (GSP) to "evaluate and protect existing systems and maintain more secure infrastructure."

serves as the center for studying strategic level cyber-related issues and their geopolitical implications.[242] The NATO School in Germany runs six courses on operational level cooperation, such as cyber and information operations for staff officers of NATO and network security for employees.[243] The NATO Joint Warfare Centre provides the joint and operational-level headquarters training courses on awareness and appreciation of cyberspace activities and their implications for NATO operations.[244] The NATO Communications and Information Systems School (NCISS) offers "five resident courses for CIS operators and staff personnel." The Cyber Range of the Estonian [Defense] Forces is used to test personnel skills. This testing system makes a firm foundation for NATO's cyber capabilities.[245]

NATO has also implemented exercises focused on cyber operations.[246] Locked Shield is one annual exercise supported by the CCD COE in Tallinn, Estonia. Since its introduction in 2010, the exercise has developed notably, with 400 participants from 16 in 2015.[247] It starting with a scenario involving an attack against critical infrastructure from a virtual country.[248] Another exercise, Cyber Coalition, is NATO's largest annual cyber defense exercise since 2008. In 2014, more than 600 cyber-related personnel in NATO, partner nations, and observers participated in Cyber Coalition. It provides a means of "exercising strategic and operational-level information sharing, senior-level

---

[242]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 22.

[243]NATO School Oberammergau-Academics," official website, www.NATOschool.NATO.int/Academics.; currently provides six resident courses related to cyber and information operations at the operational level to support NATO staff officers and network security personnel.

[244]H. Todd Waller, "Cyberspace Implications for NATO Operations and the Joint Warfare Centre," The Three Swords: The Magazine of the Joint Warfare Centre, No. 20, Summer/Autumn 2011, 24, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 23.

[245]"Courses-Course Descriptions," NATO Communications and Information Systems School, accessed September 10, 2017, www.nciss.NATO.int/courses_description.php.

[246]Rizwan Ali, "On Cyber Defence," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 26, May 2014, pp. 32-34, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 23.

[247]Liis Kangsepp, "In NATO Cyber Wargame, Berlya Fends off Arch Enemy Crimsonia," *Wall Street Journal*, April 24, 2015, blogs.wsj.com/digits/2015/04/24/in-NATO-cyber- wargame-berlya-fends-off-arch-enemy-crimsonia/tab/print/.

[248]Ibid.

decision making, and multi-disciplined coordination in the cyber realm."[249] The Estonian National [Defense] College supports the staff to control the exercise.[250]

NATO also integrates exercises to defend cyberspace into its preexisting exercises.[251] NATO's Joint Warfare Center added cyber defense activities to their Steadfast Juncture 2011 exercise as a means for NATO's battle staff to understand the influences of cyber-attacks.[252] Cyber targets for the exercise were "NATO command and control (e.g., computer networks); NATO operations (e.g., airports, seaports, petroleum, electricity); and NATO mission stability (e.g., energy, medical, financial, transportation, communication) in consideration of real world cyber-attacks." Defensive actions for cyberspace were also included in Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (CWIX) in 2014.[253] The exercises aim to increase interoperability among NATO forces, and to capture the anticipated issues for future operations and budget requirements.[254]

C. ACHIEVEMENTS AND UNRESOLVED ISSUES

NATO's efforts to address better defense operations have led to significant achievements. On the other hand, it still has issues to resolve.

---

[249]Rick McCartney, "Exercise Cyber Coalition 2014," NCI Agency, November 26, 2014, ncia.NATO.int/NewsRoom/Pages/141126-cyber-coalition.aspx.

[250]Ibid.

[251]Ali, "On Cyber Defence," 33-34, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 22.

[252]H. Todd Waller, "The Joint Warfare Centre Launches Cyber Defence Training with STEADFAST JUNCTURE 2011," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 21, Autumn/Winter 2011, 46, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 24.

[253]"NATO Allies Testing Operational Capabilities during the 2014 CWIX," NATO Joint Force Training Centre website, accessed in September 1, 2017, http://www.act.nato.int/nato-allies-testing-operational-capabilities-during-the-2014-cwix.

[254]James A. Lewis, *The Role of Offensive Cyber Operations in NATO's Collective Defense*, Tallinn Paper No. 8 (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/ TP_08_2015_0.pdf, 2, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 25.

1. Achievements of NATO's Efforts

NATO's efforts since 2002 have achieved significant results in extending NATO's framework to cyber defense.

a. Establishment of Education, Training, and Exercise Programs

NATO has developed programs for education, training, and exercises for every level—from the strategic to the tactical levels.[255] For tactical-level cooperation, it has exercise programs for interoperability, including the exercise named by "Stoney Run" between Bravo Company, the 44th Expeditionary Signal Battalion, and the 250th Gurkha Signal Battalion. The exercise programs of NATO try to mitigate deficiencies resulting from cultural differences such as language. [256] The experiences from the Afghanistan War became the background to improve "the Steadfast Cobalt 15 exercise in Poland." NATO also has education programs for its senior leaders. For instance, in 2014, it held the program on Cyber Security Studies in the Georgy C. Marshall Center for experts in worldwide cyber security issues. Participants from 47 nations discussed how to develop or "influence cyber legislation, policies or how to practice cyber security in their countries.[257] In addition, NATO has a system to share its awareness and training program to secure cyberspace.[258]

b. Coordination of Multiple Stakeholders

NATO has successfully coordinated with various stakeholders including industry, partner countries, and international organizations such as the EU in much its cyber-

---

[255]Ibid., 32–33.

[256]Natalie Vanatta, Robert Singley, and James Torrence, "From 'Mixed Signals' European Command brings together Allies," *Army Communicator* 40, no. 1 (Spring 2015): 32–37, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 38. For example, cooperative efforts exist between the USAREUR 102nd Signal Battalion and the 282nd Bundeswehr Command Support Battalion.

[257]Christine June, "EUCOM J6 Discusses Cyber Sovereignty at Inaugural Marshall Center Course," U.S. European Command public website, December 18, 2014, http://www.eucom.mil/media-library/article/30932/eucom-j6-discusses-cyber-sovereignty-at-inaugural-marshall-center-course.

[258]"Think About It…Vigilance Begins with You," U.S. Army Europe public website, accessed September 30, 2015, www.eur.army.mil/ vigilance/, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 38.

related actions. The USEUCOM Cyber Endeavor program goes beyond simple military cooperation by including academia and business.[259] It is a "paramount cyber security collaboration, familiarization, and engagement program" initiated in 2009.[260] Participants have consisted of "the military, academia and companies such as Microsoft, Hewlett Packard, Cisco and Verizon." In 2014, three NATO countries held conferences: "the Czech Republic, focused on configuration management; Bulgaria, focused on vulnerability management; and Romania, focused on boundary defense."[261]

c. Establishment of a Legal Standard

NATO's efforts are noteworthy in applying the legal system to cyber activities. The *Tallinn Manual* is the result of these efforts.[262] The United States, as a member of NATO, actively participated in this effort. In developing the *Tallinn Manual*, Professor Michael Schmitt of the Naval War College served as director of The International Group of Experts. U.S. Cyber Command participated as an observer, while the Naval Postgraduate School and the U.S. Military Academy contributed as reviewers.[263] In addition to this contribution to the *Tallin Manual*, professional and scholarly publications, including the U.S. Naval War College International Law Studies journal[264] and the Air Force Law Review,[265] have discussed the legal concerns of cyberspace. The Cyber

[259]Shaun Cavanaugh, "Cyber Endeavor 2012 – Building Cyber Defense Capacity in Our Partner Nations," U.S. European Command public website blog, February 24, 2012, eucom.mil/media-library/blog%20post/23155/cyber-endeavor-2012-building-cyber-defense-capacity-in-our-partner-nations, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 39–40.

[260] Ibid.

[261]Trina Zwicker, "Cyber Endeavor Capstone 2014 to Expand on Partnerships between Public, Private Sectors," U.S. European Command public website blog, April 17, 2014, https://securityassistance.org/content/cyber-endeavor-capstone-2014-expand-partnerships-between-public-private-sectors.

[262]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 29.

[263]Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence* (Cambridge, UK: Cambridge University Press, 2013), https://ccdcoe.org/tallinn-manual.html, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 40.

[264]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 40.

[265]A dedicated cyber law edition of the *Air Force Law Review*, Vol. 64, 2009, quoted in Canton, *NATO Cyberspace Capability: A strategic and Operational Evolution*, 40.

Defense Review of the Army Cyber Institute addresses the cyber issues of "law, ethics, and policy as well as strategy, operations, tactics, and history."[266]

2. Unresolved Issues

While NATO has established a system to collectively defend cyberspace, it still faces several issues that need to be resolved.

a. Immaturity and Inconsistency of the Doctrine

The procedure for developing NATO's doctrine has been unclear and unhurried.[267] In 2010, the Lisbon Summit announced its integration of cyberspace in the doctrine, but the treatment of cyberspace operations and information operations are still inconsistent in NATO's doctrine. The U.S. military could be a guide for the establishment of NATO's doctrine. The U.S. DOD built a model distinguishing "cyberspace operations in JP 3-12 from information operations in JP 3-13."[268] The U.S. Army published the new Field Manual (FM) 3-12 titled *Cyberspace Operations* in an effort to be consistent with Joint Doctrine. FM 3-12 replaces FM 3-38, "*Cyber Electromagnetic Activities*."[269] As an effort to promote the partnership to share the achievement of the United States with NATO, "Major General Stephen, Commanding General of the Army Cyber COE, and Major General Heinrich-Wilhelm Steiner, Commander of the German Bundeswehr Communication and Information Systems Command," signed a partnership agreement in March 2015.[270]

---

[266]*The Cyber Defense Review* is currently limited to an online-only offering available from *cyberdefensereview.org*, accessed October 23, 2015, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*,41

[267]Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 34.

[268]Ibid., 34.

[269]*United States Army Cyber Center of Excellence Strategic Plan* (Fort Gordon, GA: U.S. Army Cyber Center of Excellence, September 2015), 10, available from cybercoe.army.mil/images/ CyberCoE%20Documents/strategic_plan_2015_revision4_9_14_2015. pdf, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 34.

[270]William B. King, "US Army Cyber Center of Excellence Commander Talks Cyber with German Signal Soldiers," online news article, Wiesbaden, Germany: 5th Signal Command Public Affairs, April 1, 2015, available from www.army.mil/article/145607/.

b. Difficulty with Whole-of-Government Approaches

NATO faces a challenging future to coordinate and integrate a *whole-of-government approach*. Issues such as CIP, both at a national level and in NATO, pose complex challenges, because national sovereignty is important to all member countries. NATO members, however, share the idea that the whole region benefits when "prudent measures and harmonized actions work on the benefit of international security and stability."[271] USAREUR hosted the 2015 Cyber summit in Wiesbaden, Germany, to discuss the importance of cooperation for CIP to assure its interoperability.[272] NATO's difficulty in building cooperation in the whole of government approach is clear. Still, NATO needs to continue deliberating on how to implement such an approach.

c. Issues of Limited Resources and Operational Priority

NATO faces limited resources to cover an expanding domain of cyberspace. The conduct of cyber operations gave NATO an additional mission, but not its most important one. In the 2015 Wales summit, Dr. John Deni insisted that limited resources and increasing tasks were constraints currently facing NATO.[273] They defined six areas, including cyber and energy, as new missions that had overextended NATO.[274] Indeed, the former Supreme Allied Commander Europe (SACEUR) states the priority of cyber operations reflects the significance of those threats. In 2013, former SACEUR commander Admiral James Stavridis ranked cyberspace fourth of six transnational threats in his testimony to Congress.[275] In 2014, the former SACEUR commander General

---

[271]"The Department of Defense Cyber Strategy," 27, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 37.

[272]William B. King, "US, Allied Cyber Defenders Discuss Interoperability at Cyber Summit 2015," online news article, Wiesbaden, Germany: 5th Signal Command Public Affairs, July 29, 2015, https://www.army.mil/article/152994/US.

[273]John R. Deni, *Fulfilling NATO's Missions: The Need for New Structures and Instruments*, Policy Brief, Transatlantic Security and Future of NATO Series (Paris, France: The George Marshall Fund of the United States-Paris, May 2015), 1.

[274]Ibid.

[275]"Testimony of: Admiral James Stavridis, United States Navy, Commander, United States European Command before the 113th Congress, 2013" (Washington, DC: Government Printing Office, March 13, 2013), 7, armed-services.senate.gov/imo/media/doc/Stavridis%2003-19-13.pdf.

Philip Breedlove, in his article, mentioned cyber threats as the most significant threats.[276] While resource allocation for cyber operations is still limited, NATO must continue to reassess its priorities. The U.S. forces have studied resourcing issues for cyberspace. Its efforts could be helpful for NATO.[277]

D. CONCLUSION

Chapter V has reviewed what NATO has developed and what issues NATO faces for further cooperation in cyberspace. NATO is the collective security organization with armed forces consisting of personnel from 29 countries, which have endeavored to extend the alliance's collaboration into cyberspace. NATO's efforts since 2002 have made meaningful achievements, such as the successful establishment of education, training, and exercise programs; coordination of military, governments, academia, and industries; and establishing a legal guide for cyber activities. On the other hand, it still has weaknesses, such as inconsistent doctrine, the unclear usage of cyber operations for deterrence, an undefined method for implementing a whole-of-government approach, and an inadequate strategy to harmonize resource allocations with the other missions. Nevertheless, NATO's accomplishments could guide the ROK and U.S. alliance. Henceforth, Chapter VI summarizes this research about the ROK and U.S. alliance in the cyber domain and explores potential answers to the research question through the lessons learned from NATO.

[276]Philip M. Breedlove, "The New NATO," *The Three Swords: The Magazine of the Joint Warfare Centre*, No. 27, November 2014, 16–19, quoted in Canton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, 41.

[277]Ibid., 40–41.

VI. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION OF THE RESEARCH

This research has examined how the ROK and U.S. military can cooperate against common cyber threats on the Korean Peninsula. Specifically, this effort has considered an approach the alliance can use to address military-focused cyber threats from North Korea. To suggest policy recommendations, the author has answered four questions: what are the cyber threats on the Korean peninsula; What is the nature of the existing cooperative agreement between the ROK and the United States; What are the deficiencies in the security agreements between the ROK and the United States relating to cyber threats; and How could this agreement be strengthened to better address cyber threats?

As the research has shown, the capabilities and effects of warfare between North Korea and South Korea are asymmetric. North Korea has endeavored to develop asymmetric power, notably with WMD, to overcome its weakness in economic power, human resources, and conventional military power. Yet, cyber operations are one of the best asymmetric methods to exploit the vulnerability of the ROK's cybernetic environment. Hence, North Korea has developed its cyber capabilities. Under its strong leadership, North Korea has organized its system for cyber-attacks. To do so, it received help from foreign countries for educational support, technological transfer, and network connection. Since the ROK became a target of cyber-attacks, the ROK government has identified North Korea as the culprit behind most of its most damaging cyber-attacks, such as the DDoS attacks in 2009, 2011, and 2013, and the targeted hacking of ROK banking and government networks.

Recently, North Korea has more actively practiced offensive behaviors in cyberspace to gain economic benefits and acquire technologies. At the same time, it has continued to attack the ROK and the U.S. military on the Korean Peninsula. North Korea has often targeted individual military persons in ways such as sending a fake message connected to malicious code or link. It has also targeted the military network. In the 2009 and 2011 DDoS incidents, North Korea attacked the Internet homepage web server

operated by the ROK military and the USFK. In 2016, it intruded into the intranet of the ROK Ministry of Defense, and reportedly, North Korea is suspected of stealing war plans. North Korea could succeed in its attacks because it has an attack capability and the ROK and the US military inadequately defend against these threats. Nevertheless, as the research finds in Chapter III, North Korea also has vulnerabilities that can be exploited by the ROK and the United States.

The ROK and U.S. alliance has centered on keeping peace on the Korean Peninsula. Since cooperation started in 1953 to thwart North Korea's armed attacks, the alliance relationship between the two nations has changed. The stable security supported by the U.S. military resulted in economic growth for the ROK. Since then, the relationship of patron and client has become a mutual partnership and increased South Korea's accountability for security. In addition to the growth of the two countries, the ROK and U.S. alliance has adapted to the changing threats of North Korea, such as its growing nuclear arsenal and missile launchings, and cyber-attacks.

With the change in threat analysis, the ROK and U.S. alliance has changed its domains and methods for cooperation. Notably, it officially highlighted cyberspace in the 43rd SCM in Seoul. Since then, the SCM has reaffirmed its intentions to collaborate for the defense of cyberspace. As a result, in 2011 the two nations formed a consultative organization, the CCWG, and signed the IA/CNDSOP in 2015. The ROK and U.S. alliance, however, is still immature and needs to develop to defend against North Korea's cyber-attacks successfully.

With the goal of enhancing the ROK and U.S. alliance for cyberspace, this research studied NATO's cooperation for cyber defense. NATO been developing its cyber capabilities since 2002, and it could be an excellent reference for the ROK and U.S. alliance. NATO is a collective security organization consisting of 29 countries and has automatic intervention regulations. Multiple member nations of NATO lead diverse cyber research activities, and NATO members have developed structure and doctrine for cyber operations over the past 15 years. NATO's cooperation in cyberspace has focused mainly on cyber defenses. As a defense alliance like NATO, the ROK and U.S. alliance could refer to NATO's achievements in their transnational cooperation in cyberspace.

NATO has made significant achievements in their establishing education, training, and exercise programs. Additionally, it successfully coordinated myriad core actors such as businesses, academics, and governments to cooperatively create an environment for assuring cyber operations. NATO's efforts to integrate cyberspace into the preexisting legal structure is also noteworthy. While it can boast significant achievements, NATO still has some hurdles to clear. Its doctrine presents some inconsistencies and challenges in dealing with cyber issues. In particular, it must continuously discuss how to coordinate the conflicts of interest among multiple nations, and it must determine how to prioritize and allocate resources to cyber operations in light of the overall mission of NATO. Thus, NATO's achievements, and the challenges it still faces, can guide the ROK and U.S. military for cooperation against common cyber threats on the Korean Peninsula.

B. RECOMMENDATIONS TO THE ROK AND U.S. ALLIANCE

The remainder of this thesis concludes the research by suggesting several recommendations. They include how to overcome the weaknesses of the ROK and U.S alliance in cyberspace and how to exploit North Korea's vulnerabilities. NATO's lessons suggest possible solutions and issues to consider.

1. Mitigation of the ROK and U.S. Alliance's Vulnerabilities

The first recommendation is to resolve the weaknesses of the ROK and the United States discussed in Chapters III and IV. As described earlier, the ROK and the U.S. military inadequately defend against North Korea's cyber-attacks. Similar to the conventional battlefields, avoiding the adversary's willingness to attack is nearly impossible in cyberspace. Essential points, however, are to have the ability to deny North Korea success in cyberspace through appropriate security defenses and to minimize the damage from attacks through rapid detection and response to attacks. The main cyber threat on the Korean Peninsula has so far been North Korean attacks against the South Korean network Nonetheless, both the ROK and U.S., separately and through the alliance, must address the problem, because cyber-attacks can impact the military capabilities of the ROK and U.S. alliance. Apart from its necessity, the current ROK and U.S. alliance for cyberspace has limits. As referred to in Chapter IV, although the security issues on

the Korean Peninsula cannot be separated from the alliance system, each country needs to improve its individual capabilities for self-defense. Three questions are generated from this research about how to mitigate the vulnerabilities while broadening the current cooperation. If the ROK network is the primary target of the attack, is it necessary to increase the connectivity of devices between the two nations? When the alliance suffers cyber-attacks without incurring direct damage, how should it respond? Could the bilateral cooperation be a panacea? The achievements of NATO partially suggest solutions. Additional research is required to consider the implications of recommendations on the ROK and U.S. alliance.

a. Cooperation in Accordance with Autonomy

The ROK and the U.S. alliance should take cautious approaches to link cyberspace to military operations for the following reasons. First, limiting the interoperability of a system in cyberspace could be advantageous to prevent extended damage, considering the current concentrated attacks on the ROK military. Second, the ongoing cooperation between the ROK and the U.S. military already depends on combined units, organizations and humans, not directly on each other's networks. The increased trend of cybernetics in each country, however, raises the question of whether in the long term it is possible to limit the interoperability by connecting systems that are not on the Internet between two nations. NATO has attempted to develop a platform to connect different countries. This example could suggest practical solutions.

b. Strategic Response of the ROK and U.S. Alliance

The next issue is how to respond when one of the counterparts receives a cyber-attack. In the hacking of the ROK Ministry of Defense, the targets were only in ROK's cyberspace, but the attack affecteed all of the alliance's military capabilities. The United States declares the boundary of cyber deterrence to include its alliances. No strategic level response has been reported after North Korea's cyber-attacks on the ROK cyberspace until now, but the two countries need to have a clear consensus on counter-reactions and implications. It should not be in the form of unilateral support from the United States to the ROK, but through mutual cooperation.

c. Reinforcement of Regional Cooperation

In complex international relationships, mere bilateral cooperation should not be a panacea. Then, how can the ROK and the U.S. alliance broaden itself to include multinational collaboration? NATO's efforts to apply cyberspace to a preexisting system could be an excellent guide for to how to lead the transnational partnership. NATO's efforts to legally establish this cooperation are significant in the international community, particularly in democratic countries. The *Tallin Manual*, which was produced by the CCD COE, could be an excellent guide for the ROK and the U.S. military to establish a legal standard for a cooperative response. The ROK and U.S. alliance can extend the collaboration of two nations based on the current consensus regionally around Asia. The ROK and the United States have participated in multinational consultations on cyber policy. The ROK has taken efforts to share the values and definitions of the norms by hosting forums such as Seoul Global Conference on Cyberspace. The active collaboration to standardize values, definitions and norms is important in organizations such as the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) and the Asia-Pacific Economic Cooperation (APEC) can contribute to shared values. In addition, considering the current threat North Korea has imposed on the world, the accumulated threats analysis and response capabilities of the ROK and the U.S. alliance could contribute to international security.

2. Assess of North Korea's Vulnerabilities

The second recommendation is to assess North Korea's vulnerabilities to the alliance's advantage. Although North Korea has an advantage now, the research finds four weaknesses in North Korea's position. First, North Korea cannot achieve its ultimate national and military goals through cyberspace alone. Continuous cyber-attacks without kinetic operations have only revealed their cyber capabilities. Second, North Korea is dependent on other countries for cyber operations because of the DPRK's lack of infrastructure, such as electricity and networks, while it highlights its self-development and self-renaissance. Third, North Korea faces the paradox of modernization. Currently, it boasts about how it has developed a system that includes automation, which makes it a

potential target for the same attacks it has launched against the ROK. Lastly, uncontrollable information is its vulnerability. North Korea wants to control information such as the spread of news from beyond its borders and it limits information sharing among North Koreans internally to promote and protect its dictatorship. The following recommendations address how to use these weaknesses. NATO's efforts partially suggest solutions. Furthermore, for implications on the ROK and U.S. alliance, additional study considering complex security situations is necessary.

a. Sharing Information about North Korea's Cyber Threat

The ROK-US Alliance should build a system that effectively shares information about North Korea's cyber-attacks. North Korea's continuous cyber-attacks without kinetic operations have exposed its proficiencies. NATO's malware information sharing platform could be a guide for organizations of the ROK and the United States to share information. North Korea's attack capability is connected to its government regardless of the intended targets, but the ROK and the United States assign different organizations according to objectives and attacks. Although it is difficult to share the information thoroughly, it could be helpful to build systems to share the information for potential use.

b. Deterrence at National Levels

The ROK and the United States could exploit North Korea's infrastructure limitations. Economic sanctions could be one method. Extending the sanction period for coal, oil, or devices for solar energy could decrease the DPRK's ability to operate its systems. Sanctions on North Korean workers outside of North Korea could decrease their hidden employment to lessen the hackers' ability to practice abroad using concealed identities. Also, if necessary, the international community should address North Korea's use of networks provided by China and Russia

c. Consideration of Offensive Capabilities

As North Korea's modernization proceeds, its asymmetric benefits should decrease. As nations following the rule of law, the ROK and the United States need to discuss, as NATO did, the possibility of using offensive cyber capabilities. If it is

constrained from using offensive capabilities because the ROK and U.S. alliance is defensive, the ROK and U.S. alliance should still consider offensive methods for defensive purposes. Offensive cyber operations could not only be used to defend against North Korean cyber-attacks, but also as an asymmetric method against North Korea's attempts to develop nuclear weapons and missiles.

d. Reflecting on the Failure of the Sunshine Policy

One of the possible methods to exploit North Korea's vulnerabilities would be to undermine North Korea's control over its domestic information. Information could be secretly spread outside North Korea's control, for example through USBs and network development for information sharing. Although media and telecommunication have resulted in the disruption of dictatorships and have promoted democratization, the successful exploitation of this vulnerability is only possible with decisive and consistent measures. For example, the Sunshine policy suggests the possible side effects of supplying material and infrastructure to North Korea. The Gae-sung industrial complex and tour at Mt. Kum-gang started as a collaboration between the two Koreas for the future, but it ended with North Korea being able to use the facility for any purpose whatsoever without limitations after South Korea withdrawal. The supports from the international community for North Korea should be realistically assess the nature and history of the North Korean regime before any technology transfer.

3. Additional Lessons from NATO

Finally, this section discusses NATO's lessons, learned that could advance cyber cooperation between the ROK and the United States. The structure of the ROK and U.S. alliance is constantly changing, and training and exchange programs need to be part of this change. NATO's lessons suggest how and what the ROK and the United States need to consider for an effective partnership in cyberspace.

a. Establishment of Education, Training, and Exercise Programs

First, NATO's initiative in developing education programs is noteworthy and should be duplicated in the ROK and U.S. military alliance. As NATO has developed

education, training, and exercise programs covering a range from the strategic level to the tactical level, the ROK and U.S. alliance needs to establish similar programs. The annual combined exercises, such as Key Resolve / Foal Eagle(KR/FE) and Ulji Freedom Guardian (UFG), could provide an excellent venue to practice cooperation in cyberspace. NATO's efforts to mitigate vulnerabilities caused by cultural differences among member nations are considered in exercises at the tactical level. The ROK and U.S. combined divisions, established in 2015 as the first combined units in the world, could be the guide on how to cooperate in a combined organizational structure.[278] Using an open repository to share content on topics such as situational awareness is an excellent method to share knowledge. Additionally, sending students to U.S. schools to increase mutual understanding is key for future combined cooperation in cyberspace.

b. Avoidance of Inconsistent Doctrine

To avoid the problems of establishing inconsistent doctrine, the ROK and U.S. must understand why NATO struggled with this issue. Jeffrey L. Caton analyzes the issues related to offensive cyber operation that make the process for doctrine sluggish and inconsistent. As NATO has a basic framework of defensive actions, the ROK and U.S. alliance established itself for defense. NATO indeed already considers offensive cyberspace operations (OCO) in publicly available sources; similarly, the ROK and the United States need to agree on when and how to use offensive capabilities. Considering North Korea's offensive trend declared ROK –U.S. OCO could be a meaningful deterrent.

On the other hand, the stated willingness to use offensive cyber capabilities against North Korea could increase tensions. The ROK and U.S. alliance could take an active-defensive approach, similar to NATO, to avoid this potential problem. Furthermore, the alliance could consider the prior research of Clorida Trujillo on the seven deterrence options, which do not require OCO, for adaptable active-defensive operation.

---

[278]"Reinforce the Deterrence to the North Korea," *Yeonhap News*, June 3, 2015, http://www.yonhapnews.co.kr/bulletin/2015/06/03/0200000000AKR20150603049300043.HTML. It operated as the staff in peace time, but the U.S. 2nd Division and the ROK Mechanized Infantry Brigade are additionally organized.

Building a well-organized system using well-defined U.S. doctrine is one solution. The United States has already put effort into developing consistent doctrine for cyberspace. It is advantageous that the ROK and the United States do not waste time going through the doctrine development process if U.S. doctrine is adequate for alliance use.

c. Coordination of Multiple Stakeholders

As NATO has successfully coordinated multiple with actors such as industry, international organizations (e.g., the EU), academia, and the military, the ROK and the United States also need similar interactions to promote assurance of cyberspace for successful military operations. The alliance's current cyber issues are not separate from those of industry. Industry produces hardware and software products for the military. Academia actively interacts with industry and the military through research on high-end security technologies and scenario development based on threat analysis.

d. Issues of Limited Resources and Operational Priority

The ROK and U.S. alliance faces the same matters of resource allocation for cyber operations as NATO. Currently, the priority issues on the Korean Peninsula center on North Korea's nuclear arsenal. Resource allocation and structural cooperation issues for nuclear weapons seems like a perfect opportunity to make sure plans for conventional and cyber military operations are in harmony and carefully coordinated. The DRPK is definitely planning and practicing cyber-attacks; the alliance should have a response strategy ready. In addition, the ROK and U.S. alliance must learn from NATO's achievements and challenges to merge the cyber mission into the overall defense of the Korean Peninsula with limited resources.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. TEXT OF SCM ABOUT CYBER COOPERATION

Year	Location	Contents
2011	43rd SCM (Seoul, the ROK)	"The Minister and the Secretary affirmed the need to strengthen cooperation with respect to protection of, and access to, the space and cyberspace domains, and to promote the resilience of critical infrastructure, including the security of information and space systems. The Minister and the Secretary committed themselves to discuss new ways for the ROK and the United States to confront the challenges posed by increasing threats in cyberspace and welcomed the establishment of a bilateral strategic policy dialogue on cyber-security issues. They also acknowledged that effective bilateral cooperation on cyber-security would require a "whole-of-government" approach and coordination with the private sector."[279]
2012	44th SCM (Washington DC, the United States)	"The Secretary and the Minister reaffirmed the need to strengthen cooperation with respect to protection of, and access to, the space and cyberspace domains, and to promote the resilience of critical infrastructure, including the security of information and space systems. The Secretary and the Minister, noting the increasing need for space cooperation, welcomed the signing of the Terms of Reference (TOR) for bilateral military space cooperation, which includes the creation of a regular consultative body. Based on the TOR, they undertook to consult on issues of mutual interest such as space policy, strategy, training events, and personnel exchange. They welcomed the launch of the U.S.-ROK Cyber Policy Consultations as a "whole-of-government" approach, and also acknowledged that effective bilateral cooperation on cyber-security would require increased cooperation between defense agencies and coordination with the private sector."[280]

[279] "Joint Communiqué, the 43rd U.S.-ROK Security Consultative Meeting."

[280] "Joint Communiqué, the 44th U.S.-ROK Security Consultative Meeting."

Year	Location	Contents
2013	45th SCM (Seoul, the ROK)	"The Minister and the Secretary reaffirmed the need to strengthen cooperation with respect to the protection of, and access to, the space and cyberspace domains, and to promote the resilience of critical infrastructure, including the security of information and space systems. Since the signing of the Terms of Reference (TOR) for bilateral military space cooperation at the previous SCM, the ROK and the United States have consulted on issues of mutual interest, including enhanced combined exercises and more active information sharing, and are working to continue cooperation on issues such as improving space situational awareness. Taking note of the second ROK-U.S. Cyber Policy Consultations held in Washington DC in July 2013, the Minister and the Secretary welcomed the signing of the TOR for the Cyber Cooperation Working Group on September 5, 2013, in Washington DC. The Cyber Cooperation Working Group endeavors to strengthen cooperation in information sharing, cyber policy, strategy, doctrine, personnel, and exercise to improve our collective readiness against cyber threats".[281]
2014	46th SCM (Washington DC, the United States)	"The Secretary and the Minister reaffirmed the need to strengthen cooperation with respect to the protection of, and access to, the space and cyberspace domains, and to promote the resilience of critical infrastructure, including the security of information and space systems. The U.S. and the ROK have consulted on issues of mutual interest, including enhanced combined exercises and more active information sharing, and decided to jointly respond to the increasing threat of space debris by concluding the 'Memorandum of Understanding Between the Department of Defense of the United States of America and the Ministry of National Defense of the Republic of Korea Concerning Sharing Space Situational Awareness Services and Information' this year. The Cyber Cooperation Working Group endeavors to strengthen cooperation in information sharing, cyber policy, strategy, doctrine, personnel, and exercise to improve our collective readiness against cyber threats."[282]

[281]Joint Communiqué, The 45th ROK-U.S. Security Consultative Meeting, October 2, 2013, Seoul, https://www.defense.gov/Portals/1/Documents/pubs/Joint%20Communique_%2045th%20ROK-U.S.%20Security%20Consultative%20Meeting.pdf

[282] Joint Communiqué, The 46th ROK-U.S. Security Consultative Meeting, October 23, 2014, Washington D.C. https://www.defense.gov/Portals/1/Documents/pubs/46th_SCM_Joint_Communique.pdf.

Year	Location	Contents
2015	47th SCM (Seoul, the ROK)	"The Minister and the Secretary reaffirmed the need to strengthen cooperation regarding the space and cyberspace domains, and to promote the security of critical infrastructure, including information and space systems. The Minister and the Secretary reaffirmed the importance of strengthening mission assurance for space capabilities. To that end they emphasized cooperation in Space Situational Awareness exercises, including related table top exercises, and space operator training. The Minister and the Secretary affirmed the efforts of the U.S.-ROK Cyber Cooperation Working Group to enhance military cyberspace collaboration and decided that the two militaries would take steps to further cooperate on cyberspace and enhance the alliance's capacity to address challenges in cyberspace. The efforts are to include Alliance joint cyber training, exercises, and enhancing cyber military education."[283]
2016	48th SCM (Washington DC, the United States)	"The Secretary and the Minister reaffirmed the need to strengthen cooperation in the space and cyberspace domains, and to promote the security of critical infrastructure, including information and space systems. The secretary and the minister reaffirmed the importance of strengthening mission assurance for space capabilities and enhancing cooperation in Space Situational Awareness and the Space Cooperation table-top exercise (TTX). The secretary and the minister affirmed the importance of greater cooperation in cyberspace to improve the Alliance's capacity to address challenges in this domain. They noted the significance of the U.S.-ROK Cyber Cooperation Working Group (CCWG) and its efforts to create a U.S.-ROK Cyber Task Force to study how the United States and the Republic of Korea can better synchronize and enhance our combined cooperation in cyberspace within the alliance construct. They decided that both countries would continue to receive updates on the progress of this study through regular bilateral engagements and continue to explore new opportunities to strengthen our ability to respond to cyber threats. The Secretary and the Minister also committed to advance U.S.-ROK cooperation in science and technology under the auspices of the Defense Technological and Industrial Cooperation Committee (DTICC) to identify new and innovative means of countering the North Korean threat, including collaboration in robotics and autonomous technologies."[284]

[283]"Full text of 47th ROK-U.S. Joint Communique."

[284] "Joint Communiqué of the 48th U.S.-ROK Security Consultative Meeting.".

Year	Location	Contents
2017	49th SCM (Seoul, the ROK)	"The Minister and the Secretary reaffirmed the need to strengthen cooperation in the space and cyberspace domains, and to promote the security of critical infrastructure of information and space systems. The Minister and the Secretary lauded the inaugural Space Cooperation table-top exercise (TTX) in Washington, DC, in September 2017, and pledged to expand bilateral space coordination in response to security threats in the space domain, to enhance mission assurance for space capabilities, and to strengthen cooperation in Space Situational Awareness. The Minister and the Secretary discussed the increase in cyber threats and the elevation of U.S. Cyber Command to a unified combatant command. They recognized cyber capacity as a core security issue and decided to expand bilateral defense cooperation in cyber-related areas. Through regular bilateral engagements and the ROK-U.S. Cyber Cooperation Working Group (CCWG), both sides plan to continue to explore new opportunities to enhance cooperation. The Minister and the Secretary praised advances in ROK-U.S. science and technology cooperation since the last SCM, highlighting successes in robotics and autonomous technologies cooperation, and establishing task objectives and schedules at the Defense Technological and Industrial Cooperation Committee (DTICC). The Minister and the Secretary assessed that such defense science and technological cooperation contributes greatly to defense capabilities and the interoperability of the Alliance, and resolved to seek measures to deepen and expand cooperation."[285]

[285]"Full text of ROK-U.S. Security Consultative Meeting Joint Communique," *Yeonhap News*, October 28, 2017, http://english.yonhapnews.co.kr/northkorea/2017/10/28/0401000000AEN20171028003000315.html

LIST OF REFERENCES

Ahn, Jung-sik. “North, Military Executive Smartphone Hacking.” *SBS News*, March 8, 2016. http://news.sbs.co.kr/news/endPage.do?news_id=N1003456392.

Berlinger, Joshua. “Kim Jong Nam: The Plot to Murder North Korea's Exiled Son.” *CNN*, September 26, 2017. http://www.cnn.com/2017/07/26/asia/kim-jong-nam-killing/index.html.

Bermudez Jr., Joseph S. *North Korea's Chemical Warfare Capabilities*. 38 North, U.S.-Korea Institute at Johns Hopkins University, October 10, 2013. http://www.38north.org/2013/10/jbermudez101013/.

Blank, Stephen. *Rethinking Asymmetric Threats*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2003. https://www.globalsecurity.org/military/library/report/2003/ssi_blank.pdf.

Canton, Jeffrey L. *NATO Cyberspace Capability: A Strategic and Operational Evolution*. Carlisle, PA: U.S. Army War College, 2016.

China Unicom. “China Unicom Global Network Map.” Accessed October 10, 2017. http://www.unicomamericas.com/wp-content/uploads/2012/06/unicom-map.jpg.

Cho, Nam-hun. “2016 North Korea Military Industry Trends and Evaluation.” *KDI Review of the North Korean Economy* 19, no.1 (January 2017):79–80.

Chul, Baek. “North Korea ‘What Is the Truth of Cyber Capabiity?’” *Kyunghyang News*, April 13, 2013. http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201304131549251.

Chung, Kuyoun. ““Strategic Asymetry and North Korea's Asymmetric Threats.” In *Innovation of Science and Technology and North Korea׳s Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicles*, edited by Kuyoun Chung and Gi-tae Lee. Seoul, Republic of Korea: Korea Institute for National Unification, Innovation of Science and Technology, 2016.

Cisco Team Korea. “DDoS Attacks, How to Respond?: 7.7. DDoS Attack Pattern Analysis and Suggestion.” July 16, 2009. https://www.cisco.com/web/KR/learning/events/down/July_DDoS_Webseminar.pdf.

CNBC. “Symantec Says 'Highly Likely' North Korea Group behind Ransomware Attacks.” May 23, 2017. https://www.cnbc.com/2017/05/23/symantec-says-highly-likely-north-korea-group-behind-ransomware-attacks.html.

CNN Library. “Kim Jong Un Fast Facts.” September 28, 2017. http://www.cnn.com/2012/12/26/world/asia/kim-jong-un---fast-facts/index.html

———. “North Korea Nuclear Timeline Fast Facts.” September 4, 2017. http://www.cnn.com/2013/10/29/world/asia/north-korea-nuclear-timeline---fast-facts/index.html.

Deni, John R. *Fulfilling NATO’s Missions: The Need for New Structures and Instruments*. Policy Brief, Transatlantic Security and Future of NATO Series. Paris, France: The George Marshall Fund of the United States-Paris, May 2015.

Dong-a Ilbo. “Military Announced North Korean Attack Using Hacking e-mail Alleged the Alumni of Korea Military Academy Happened.” June 20, 2011. http://news.donga.com/3/all/20110602/37736298/1.

Edwards, Will. “North Korea as a Cyber Threat.” The Cypher Brief, July 1, 2016. https://www.thecipherbrief.com/north-korea-as-a-cyber-threat.

Exploit This. “A List of North Korean IP Addresses.” January 25, 2015. https://www.exploitthis.com/2015/01/26/a-list-of-north-korean-ip-addresses/.

Feakin,Tobias, Jessica Woodall, Liam Nevill, Zoe Hawkins. *Cyber Maturity in the Asia-Pacific Region 2016*. Austrailia: The Australian Strategic Policy Institute Limited, 2016. http://www.spain-australia.org/files/documentos/62_ASPI-Cyber-Maturity-2016.pdf.

Gartzke, Erik. “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security* 38, no. 2 (Fall 2013): 41–73. doi: 10.1162/ ISEC_a_00136.

Global Commission on Internet Governance. *Cyber Security in a Volatile World*, vol. 5. Ontario, Canada: Centre for International Governance Innovation and the Royal Institute of International Affairs, July 26, 2017. https://www.cigionline.org/publications/cyber-security-volatile-world.

Goldman, Russell. “What We Know and Don’t Know About the International Cyberattack.” *New York Times*, May 12, 2017.

HP Security Research. *Profiling an enigma: The mystery of North Korea’s Cyber Threat Landscape*. HP Security Briefing Episode 16. HP Company. August, 2014.

iDefense. *Cyber Threatscape Report.* Accenture Security, 2017.

International Telecommunication Union. *Measuring the Information Society Report 2016*, Geneva, Switzerland: ITU, 2016.

Joong-ang Ilbo. "Kim Jung-un, Cyber War is the All-in-One Sword." November 5, 2013. http://news.joins.com/article/13048072.

Jun, Kwan-woo, and Nancy A. Youssef. "North Korea Suspected of Hacking U.S.-South Korean War Plans." *Wall Street Journal*, October 10, 2017. http://www.wsj.com/article/north-korea-suspected-of-hacking-u-s-south-korean-war-plans-1507636641.

Kang, Young-sil. "Science Technology Industry Trends Evaluation of Kim Jung-un Regime." *KDI Review of the North Korean Economy* 19, no. 2 (February 2017).

Kangsepp, Liis. "In NATO Cyber Wargame, Berlya Fends Off Arch Enemy Crimsonia." *Wall Street Journal*, April 24, 2015. blogs.wsj.com/digits/2015/04/24/in-NATO-cyber- wargame-berlya-fends-off-arch-enemy-crimsonia/tab/print/.

Kim, Duk-ki. "The Republic of Korea's Counter-Asymmetric. Strategy." *Naval War College Review* 65, no. 1 (Winter 2012): 55–74.

Kim, Hei-jung. "Status and Implications of Korea's Information and Communication Cooperation." *Information Communications Issues* vol. 13 (Suwon, ROK: KICI, September 2016).

Kim, Heung-kwang. "Kim Jung-un, Organizing Cyber Strategic Command and Efforts to Maximize Cyber Capability." Korea Freedom Federation. September 1, 2016. http://www.posuni.com/pds/view.php?idx=2295&page=11&section=%C7%D0%BC%FA%BC%BC%B9%CC%B3%AA.

Kim, Hyung-Jung. "China and South Korea Pledge to Ease Tensions over U.S. Missile Defense System." *TIME,* October 31, 2017. http://time.com/5003532/south-korea-china-thaad-missile-defense/.

Kim, In-soo. "North Korea Cyberwar Capability Assessment and Prospect." *International Journal of Korean Unification Studie*s 24, no. 1, (ROK: Korea Institute for National Unification, 2015). http://www.dbpia.co.kr/Journal/PDFViewNew?id=NODE06383222&prevPathCode=.

Kim, Ji-eun. "North Korea, High Technology Hacking Enhencement Directive." *Radio Free Asia*, July 14, 2016. http://www.rfa.org/korean/in_focus/ne-je-07142016101939.html.

Kim, Jin-myeong. "World Is Now Fighting with North Korean Hackers." *Chosun Ilbo*, October 7, 2017. http://news.chosun.com/site/data/html_dir/2017/10/08/2017100800228.html.

King, William B. “US Army Cyber Center of Excellence Commander Talks Cyber with German Signal Soldiers.” Wiesbaden, Germany: 5th Signal Command Public Affairs, April 1, 2015. www.army.mil/article/145607/.

———. “US, Allied Cyber Defenders Discuss Interoperability at Cyber Summit 2015.” Wiesbaden, Germany: 5th Signal Command Public Affairs. July 29, 2015. https://www.army.mil/article/152994/US.

Kirkpatrick, David D., Nicole Perlroth, and David E. Sanger. “The World Once Laughed at North Korean Cyberpower. No More.” *New York Times*, October 12, 2017. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

Ko, Sung-pyo. “The North Korean People's Armed Forces Department Has a 'CIA-Class' Hacker Organization.” *Joongang News*, http://libertyherald.co.kr/article/view.php?&ss%5Bfc%5D=2&bbs_id=libertyherald_news&doc_num=1554.

Korea Herald Business. “From DDoS to Information Espionage and Psyop… Hacking Patterns of North Korea is Changing.” June 7, 2016.

Korea Internet Security Agency. “2013 Major Cyber Attacking Cases and Response.” December 4, 2013. http://www.kisa.or.kr/uploadfile/201312/201312041443047984.pdf.

Korea University Research Management System. “Research for Cyber Threat Scenario and Response.” ROK Chief of Command, 2014. URL?????

Kretchun, Nat. “The Regime Strikes Back: A New Era of North Korean Information Controls.” 38 North, U.S.-Korea Institute at Johns Hopkins University. June 9, 2017. http://www.38north.org/2017/06/nkretchun060917/.

Kwon, Yu-jung, Jong-in Lim, Gyu-hyun Jang, Seung-jo Baek. “North Korea’s Cyber War Capability and South Korea’s National Counterstrategy.” *National Strategy Research* 102 (Winter 2013): 10–45. http://kiss.kstudy.com/journal/thesis_name.asp?key=3203642.

LaFoy, Scott, Jenny Jun, Ethan Sohn. *North Korea’s CyberOperations: Strategy and Responses*.Washington, DC: Center for Strategic & International Studies, 2015. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf.

Lee, Byung-chul. “Preventing a Nuclear South Korea.” 38 North, U.S.-Korea Institute at Johns Hopkins University. September 16, 2017. http://www.38north.org/2016/09/bclee091516/.

Lee, Dae-young. “The ROK Intranet Hacking Summary and Analysis.” IT World. December 7, 2016. http://www.itworld.co.kr/news/102451#csidx6451a9f8b72ea3790fca869c3d99d36.

Lee, Gi-tae. “Cyber Threats and the Relationships between South Korea and North Korea.” In *Innovation of Science and Technology and North Korea's Asymmetric Threat: Rise of Cyber Warfare and Unmanned Aerial Vehicles*, edited by Kuyoun Chung and Gi-tae Lee. Seoul, Republic of Korea: Korea Institute for National Unification, Innovation of Science and Technology, 2016.

Mansourov, Alexandre. *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*. Academic Paper Series. Washington, DC: Korea Economic Institute of America, December 2, 2014.

Mark, Joshua J. “The Battle of Pelusium: A Victory Decided by Cats.” Ancient History Encyclopedia, June 13, 2017. https://www.ancient.eu/article/43/the-battle-of-pelusium-a-victory-decided-by-cats/.

McCartney, Rick. “Exercise Cyber Coalition 2014.” NCI Agency. November 26, 2014. ncia.NATO.int/NewsRoom/Pages/141126-cyber-coalition.aspx.

Metz, Steven, and Douglas V. Johnson II. *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2001. http://ssi.armywarcollege.edu/pdffiles/pub223.pdf.

Min-ji, Choi. “Have It Prepared Cyber Terrorism ... North Korea Hacked Network of Major Companies.” *Digital Daily*, July 13, 2016. http://www.ddaily.co.kr/news/article.html?no=144276.

MN CD2 – Cyber Defence Capability Development. “MN CD2 Nations Agree to Two New Work Packages.” August 10, 2013. https://mncd2.ncia.NATO.int/news/Pages/MN-CD2-Board-Meeting-08.aspx.

———. “NATO Nations Launch Multinational Cyber Defence (MN CD2) Project.” March 14, 2013. https:// mncd2.ncia.NATO.int/news/Pages/MN-CD2-MOU-Signed.aspx.

———. “WP1: Technical Information Sharing.” June 11, 2015. https://mncd2.ncia.NATO.int/ourwork/Pages/WP1-Technical-Information-Sharing.aspx.

———. “WP2: Cyber Defence Situational Awareness.” May 1, 2015. https://mncd2.ncia.NATO.int/ourwork/Pages/WP2-Cyber-Defence-Situational-Awareness.aspx.

———. “WP3: Distributed Multi-sensor Collection and Correlation Infrastructure.” June 11, 2015. https://mncd2.ncia.NATO.int/ourwork/Pages/WP3-DMCCI.aspx.

Multinational Capability Development Campaign. MCDC 2013-2014 Catalog of Products. Accessed in September 10, 2017. https://wss.apan.org/s/MEpub/default.aspx.

Nakashima, Ellen. “The NSA Has Linked the Wannacry Computer Worm to North Korea.” *Washington Post*, June 14, 2017. https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.6230d7ffdbad.

National Digital Science Library. “CYBER KOREA 21.” May 18, 2005. http://www.ndsl.kr/ndsl/search/detail/trend/trendSearchResultDetail.do?cn=DT200501654.

NATO. “Smart Defence.” September 1, 2015. nato.int/cps/en/natohq/topics_84268.htm.

NATO Communications and Information (NCI) Agency. “NATO Communications and Information Agency: Connecting Forces.” Accessed September 1, 2017. https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx.

NATO Communications and Information Systems School. “Courses-Course Descriptions.” Accessed in September 10, 2017. www.nciss.N3, ATO.int/courses_description.php.

NATO Cooperative Cyber Defence Centre of Excellence. “About our Missions and Visions.” Accessed October 28, 2017. https://ccdcoe.org/about-us.html.

NATO Industry Cyber Partnership. “NCI Agency and Microsoft Sign Cyber Cooperation Agreement.” September 14, 2015. https://www.ncia.nato.int/NewsRoom/Pages/150914-NCIAgency-Microsoft-GSP.aspx.

NATO Joint Force Training Centre. “NATO Allies Testing Operational Capabilities during the 2014 CWIX.” Accessed in September 1, 2017. http://www.act.nato.int/nato-allies-testing-operational-capabilities-during-the-2014-cwix.

NATO News. “NATO Launches Industry Cyber Partnership.” September 17, 2014. https://www.nato.int/cps/en/natohq/news_113121.htm.

NATO OTAN. “Allied Command Operations.” November 11, 2014. https://www.nato.int/cps/ua/natohq/topics_52091.htm.

———. “Collective Defense – Article 5: Invocation of Article 5.” March 22, 2017. https://www.nato.int/cps/ic/natohq/topics_110496.htm.

———. “Connected Forces Initiative.” June 22, 2016. https://www.NATO.int/cps/ic/NATOhq/topics_98527.htm.

———. “NATO Rapid Reaction Team to Fight Cyber Attack.” March 13, 2012. https://www.nato.int/cps/en/natolive/news_85161.htm.

———. “The North Atlantic Treaty.” April 4, 1949. https://www.nato.int/cps/ic/natohq/official_texts_17120.htm.

———. “Sharing Malware Information to Defeat Cyber Attacks.” November 29, 2013. nato.int/cps/en/NATOhq/news_105485.htm.

———. “What is NATO? Pick a Topic and Discover NATO.” Accessed in October 1, 2017. https://www.NATO.int/NATO-welcome/index.html.

.

NATO Press Releases. “Statement by the North Atlantic Council,” September 15, 2001. https://www.NATO.int/docu/pr/2001/p01-124e.htm.

NATO School Oberammergau-Academics,” official website. www.NATOschool.NATO.int/Academics.

NSHC Security. “6.25 Cyber Terror Analysis.” June 25, 2013. http://www.nshc.net/wp/redalert-report-eng/.

Ok, Do-kyeong. “A Policy Study of Cyber-Warfare Capacity.” *Journal of Strategic Studies* 23, no. 3 (November 2016): 155–180. http://www.dbpia.co.kr/Article/NODE07047776.

Park, Sung-jin, and Hee-wan Jung. “Navy Submarine Missile Cold Launch Hacked in North Korea.” *Kyunghyang News*, September 26, 2017. http://news.khan.co.kr/kh_news/khan_art_view.html?artid=201709260600045&code=910303.

Pham, Sherisse. “North Korea Is Trying to Amass a Bitcoin War Chest.” *CNN Tech*, September 12, 2017. http://money.cnn.com/2017/09/12/technology/north-korea-hackers-bitcoin/index.html.

ROK Ministry of Foreign Affairs. “Joint Communiqué, the 43rd U.S.-ROK Security Consultative Meeting.” October 28, 2011. https://mofa.go.kr/webmodule/htsboard/template/read/korboardread.jsp?typeID=24&boardid=11695&seqno=4060&c=TITLE&t=SCM&pagenum=1&tableName=TYPE_KORBOARD&pc=&dc=&wc=&lu=&vu=&iu=&du=.

———. “Joint Communiqué, the 44th U.S.-ROK Security Consultative Meeting.” October 24, 2012. https://mofa.go.kr/webmodule/htsboard/template/read/korboardread.jsp?typeID=24&boardid=11695&seqno=6387&c=TITLE&t=SCM&pagenum=1&tableName=TYPE_KORBOARD&pc=&dc=&wc=&lu=&vu=&iu=&du=.

ROK Ministry of Defense. “The 1st Korea-U.S. Cyber Policy Working Group (CCWG).” February 7, 2013. http://www.gov.kr/portal/ntnadmNews/61089?srchOrder=&srchOrgCd=ALL&srchNewsAstCd=ALL&srchStDtFmt=2009.01.01&srchEdDtFmt=2017.10.28&srchTxt=%EC%82%AC%EC%9D%B4%EB%B2%84&initSrch=false&pageIndex=120&hideurl=N.

———. *2016 Defense White Paper*. ROK Ministry of National Defense, 2016. http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_20170518031469090.pdf.

———. “The 3rd Korea-U.S. Cyber Policy Working Group (CCWG).” October 29, 2015. http://www.korea.kr/briefing/pressReleaseView.do?newsId=156082384.

———. “The Background of Mutual Treaty.” Accessed October 1, 2017. http://www.mnd.go.kr/mbshome/mbs/mnd/subview.jsp?id=mnd_010701010000.

———. “Beginning of the Relationship between Korea and the United States ('49).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50745&titleId=null&siteId=mnd&id=mnd_010701040000.

———. “Future-oriented Development of the ROK-US Alliance (since '00).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&siteId=mnd&boardId=O_50735&page=1&boardSeq=O_50751&search=&column=&categoryId=&categoryDepth=&id=mnd_010701040000&parent=.

———. “Patron-Client Alliance ('54 ~ '68).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50747&titleId=null&siteId=mnd&id=mnd_010701040000.

———. “Reconnection of the Korea-U.S. Military Alliance ('80 ~ '89).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50749&titleId=null&siteId=mnd&id=mnd_010701040000.

———. “Seeking the Development of Military Relations Extending to Participation of the ROK('69 ~ '79).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50748&titleId=null&siteId=mnd&id=mnd_010701040000.

———. “Seeking a New “Security Partnership” and the End of the Cold War ('90 ~ '99).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&siteId=mnd&boardId=O_50735&page=1&boardSeq=O_50750&search=&column=&categoryId=&categoryDepth=&id=mnd_010701040000&parent=.

———. “The U.S. Intervention in the Korean War and the Official Establishment of the U.S.-ROK Military Relationship ('50 ~ '53).” August 5, 2013. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_50735&boardSeq=O_50746&titleId=null&siteId=mnd&id=mnd_010701040000.

ROK Unification Education. *2017 North Korea*. Seoul, Republic of Korea, 2016. http://www.unikorea.go.kr/books/understand/understand/ebook/under_NK_2017/assets/contents/download.pdf.

Rosen, Liana W., Emma Chanlett-Avery, John W. Rollins, Catherine A. Theohary. *North Korean Cyber Capabilities: In Brief.* Washington, DC: Congressional Research Service, R44912. August 3, 2017.

Schilling, John. “How to Hack and Not Hack a Missile.” 38 North, U.S.-Korea Institute at Johns Hopkins University. April 21, 2017. http://www.38north.org/2017/04/jschilling042117/.

Schneier, Bruce. “Who Are the Shadow Brokers?” *Atlantic*, May 23, 2017. https://www.theatlantic.com/ technology/archive/2017/05/shadow-brokers/527778/.

Stavridis, James (ADM). “Testimony of Admiral James Stavridis, United States Navy, Commander, United States European Command before the 113th Congress, 2013.” Washington, DC: Government Printing Office, March 13, 2013, 7. armed-services.senate.gov/imo/media/doc/Stavridis%2003-19-13.pdf.

Stepanova, Ekaterina. *Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects*. SIPRI Research Report no. 23. Oxford: Oxford University Press, 2008. https://www.sipri.org/sites/default/files/files/RR/SIPRIRR23.pdf.

Sung, Gi-no. “The ROK Ministry of Defense Announced the Result of Inspection: North Korean Hacking Group Lead.” *Boan News*, May 2, 2017. http://www.boannews.com/media/view.asp?idx=54586.

TTK. “TTK Network.” Accessed October 10, 2017, https://www.ttk.ru/rus/59897/59900/61841/.

U.S. Department of Defense. *Cybersecurity. DOD Instruction 8500.01*. Washington, DC: Department of Defense, March 14, 2014.

———. Joint Communiqué: The 45th ROK-U.S. Security Consultative Meeting. October 2, 2013, Seoul. https://www.defense.gov/Portals/1/Documents/pubs/Joint%20Communique_%2045th%20ROK-U.S.%20Security%20Consultative%20Meeting.pdf.

———. Joint Communiqué: The 46th ROK-U.S. Security Consultative Meeting. October 23, 2014, Washington D.C. https://www.defense.gov/Portals/1/Documents/pubs/46th_SCM_Joint_Communique.pdf.

———. “Joint Communiqué of the 48th U.S.-ROK Security Consultative Meeting.” October 20, 2016. https://www.defense.gov/Portals/1/Documents/pubs/USROKSecurityJointCommunique2016.pdf.

———. The DOD Cyber Strategy. Washington, DC: Department of Defense, 2015. https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.U.S. Department of State. “U.S. Collective Defense Arrangements.” Accessed October 1, 2017. https://www.state.gov/s/l/treaty/collectivedefense/.

USFK.”Full text of 47th ROK-U.S. Joint Communique.” November 1, 2015. http://www.usfk.mil/Media/News/Article/626859/full-text-of-47th-rok-us-joint-communique/.

U.S. Joint Chiefs of Staff. *Cyber Operations.* JP 3-12 (R). Washington, DC: Joint Chiefs of Staff, 2013, 5. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Walt, Stephen M. *The Origins of Alliance*. Ithaca, NY: Cornell University Press, 1990.

Williams, Martyn. “Catch Me If You Can: North Korea Works to Improve Communications Security.” 38 North, U.S.-Korea Institute at Johns Hopkins University. April 12, 2017. http://www.38north.org/2017/04/mwilliams041217/.

———. “Russia Provides New Internet Connection to North Korea.” 38 North, U.S.-Korea Institute at Johns Hopkins University. October 1, 2017. http://www.38north.org/2017/10/mwilliams100117/.

Yeonhap News. "The Address of Hacking IP is 'Ryugyong-dong Pyeongyang-si.'" April 11, 2013. http://www.yonhapnews.co.kr/bulletin/2013/04/11/0200000000AKR20130411000900017.HTML.

———. "Development of Large-Attacking Drone of North Korea to Attack South Korea." December 27, 2016. http://www.yonhapnews.co.kr/bulletin/2016/12/26/0200000000AKR20161226165651014.HTML.

——. "Full Text of ROK-U.S. Security Consultative Meeting Joint Communique." October 28, 2017. http://english.yonhapnews.co.kr/northkorea/2017/10/28/0401000000AEN20171028003000315.html.

———. "Japanese Media, Jang Gil-sung Took over as Chief of the North Korean RGB." October 13, 2017. http://www.yonhapnews.co.kr/bulletin/2017/10/13/0200000000AKR20171013078600073.HTML.

———. "Reinforce the Deterrence to the North Korea." June 3, 2015. http://www.yonhapnews.co.kr/bulletin/2015/06/03/0200000000AKR20150603049300043.HTML.

———. "S. Korean Military Says N. Korea Behind Last Year's Hacking Attack." May 2, 2017. http://english.yonhapnews.co.kr/national/2017/05/02/0301000000AEN20170502007600315.html.

Yoon, Kyu-Sik. "North Korea's Capability for Cyber War and Prospects." *Military Forum* 68 (ROK: Korea Association of Military Studies, Winter 2011). http://210.101.116.16/kiss6/viewer.asp.

YTN. "Interpark Customer Information Hijacking, North Korean Judgment." July 28, 2016. http://www.ytn.co.kr/_ln/0103_201607281531401705_006.

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