North Korea's Cyber Proxy Warfare: Origins, Strategy, and Regional Security Dynamics

Donghui Park

A dissertation

submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

University of Washington

2019

Reading Committee:

Sara Curran, Chair

Jessica L. Beyer

Donald Hellmann

Program Authorized to Offer Degree:

The Henry M. Jackson School of International Studies

University of Washington

Abstract

North Korea's Cyber Proxy Warfare: Origins, Strategy, and Regional Security Dynamics

Donghui Park

Chair of the Supervisory Committee:
Professor Sara Curran
The Henry M. Jackson School of International Studies

North Korea has been viewed as the world's most reclusive, repressive, and isolated country for the last 70 years. However, contrary to its undeveloped image, since the late 2000s, several governments, mainly the U.S. and South Korea, as well as global private cybersecurity companies, have attributed some of the massive and complicated cyberattacks to the North Korean regime. Even, since 2014, the U.S. Intelligence Community's annual report, *Worldwide Threat Assessment of the U.S. Intelligence Community*, has stated that North Korea is one of the four primary nation-state actors in cyberspace who threaten the national security of the United States and its allies, along with Russia, China, and Iran. This paradox prompts the central question of this dissertation: why and how did North Korea become a world-class cyber-threat

actor? This dissertation is composed of three independent, but thematically-linked empirical studies, replying to the central question.

The first study (chapter 2) seeks to bridge the gap between North Korea's undeveloped image and cyber reality. It contends that contrary to its image as a backward country, North Korea has sufficient IT infrastructure and human capital to conduct hostile cyberoperations against the outside world in order to attain its national goals. The second study (chapter 3) is an empirical analysis of North Korea's cyber strategy. It argues that North Korea's cyber-proxy-warfare strategy enables its cyber-warriors to accomplish aggressive cyber-missions while North Korean hackers keep a distance from their state sponsor, North Korea. The last study (Chapter 4) seeks to understand the influence of North Korea's cyber uncertainty on regional and world security dynamics. It illustrates that through the North Korea case, the impact of cyber buildup can be seen as the same as that of conventional military buildup.

When combined, these three studies provide insight into the central question of this dissertation about why and how North Korea became a world-class cyber-threat actor. The Kim dictator family has understood the importance and impact of developing cybercapacity for their survival in security and military areas. North Korea has started to conduct massive and complicated cyberoperations through a proxy-warfare strategy which enables the state to deny its responsibility for those operations. Sufficient IT human capital from state-led intensive education systems is at the core of North Korea's aggressive cyberoperations; this, in turn, threatens the national security of other countries and changes regional security dynamics.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Many people played critical roles, both big and small, in helping make this work possible. First and foremost, I would like to thank Sara Curran, my chair, for her invaluable guidance and support of my research endeavors. I am also grateful to my mentor Jessica Beyer for her many years of advice and support, and her meticulous comments on multiple drafts of my dissertation. I would also like to thank the rest of my dissertation committee, Donald Hellmann and James Caporaso, and Director of the Center for Korea Studies Clark Sorensen.

I would also like to give thanks to the countless colleagues and friends who encouraged and inspired me to finish this dissertation. I would like to acknowledge the following entities within the University of Washington for their financial and resource support: The Henry M. Jackson School of International Studies (JSIS) and the Ph.D. program; the Center for Korea Studies; the Center for Studies in Demography and Ecology; and the JSIS Cybersecurity Initiative. In particular, I am indebted to my country, the Republic of Korea, and its Army for supporting me.

Finally, and most importantly, I owe much to my family, particularly my father Kangchun Park, mother Yeonghae Kim, father-in-law Doowon Rha, mother-in-law Philhee Lee, brother Dongha Park, and sister-in-law Eunyoup Rha and her husband Daehoon Han. I also send endless love and gratitude to my wife Eunsae and sons June and Jayden for putting up with this for five years of our lives.

DEDICATION

This work is dedicated to our Almighty God,

my wife, Eunsae, and two sons, June and Jayden

Chapter 1. INTRODUCTION

1.1 PUZZLE, SUMMARY OF FINDINGS, AND ARGUMENT

North Korea has been viewed as the world's most reclusive, repressive, and isolated country for the last 70 years. Some experts on North Korea have called the state a "hermit kingdom" (Hassig & Oh, 2009; Kihl, 1984; Warf, 2015). Given this underdeveloped image of North Korea, it is understandable that North Korea's cybercapacity is perceived as all but non-existent. Indeed, in daily practical terms, ordinary North Korean citizens are not allowed to access the internet. Since 2014, however, the U.S. Intelligence Community's annual report, *Worldwide Threat Assessment of the U.S. Intelligence Community*, has stated that North Korea is one of the four primary nation-state actors in cyberspace who threaten the national security of the United States and its allies, along with Russia, China, and Iran (Clapper, 2014, 2015, 2016; Coats, 2017, 2018, 2019). This paradox prompts the central question of this dissertation: why and how did North Korea become a world-class cyber-threat actor?

This dissertation breaks the primary question into three sub-questions. These three sub-questions correspond to three independent, but thematically-linked empirical studies. The first question is: Why and how does North Korea have sufficient aggressive cybercapacity to conduct massive and complicated cyberoperations, such as the 2014 Sony hack? The second question is: How has Pyongyang accomplished its hostile cybermissions without being traced and punished by victim countries and the international community? The last question is: How much does North Korea's uncertain cyber buildup impact regional and world security dynamics? These questions arise from doubt about the source of some major cyberattacks—such as the 2009

DDoS attack and 2017 WannaCry ransomware attack—to the North Korea regime across the world.

Regarding the first question, there is debate about whether North Korea has sufficient cybercapability to carry out cyberoperations that increases its national interests around the globe. It is hard to link the image of North Korea as underdeveloped and isolated with the open information age. According to the *2019 Index of Economic Freedom* by the Heritage Foundation, North Korea's overall economic score is ranked last among all 180 countries the Foundation reviewed. In addition, according to U.N. estimates, 40% of North Korea's population—or more than 10 million people—need international humanitarian assistance, and approximately 20% of children suffer from malnutrition (Hyonhee, 2018). Since the collapse of industry during the 'North Korean famine' (1994–1998), the North Korean regime has continuously initiated economic reconstruction plans, but the country has failed to see an economic resurgence. Therefore, North Korea still relies on labor-intensive businesses, along with an abundant, low-cost labor force (Lim & Hong, 2017). Furthermore, North Korea and its people suffer from chronic energy and electricity shortages (Yi, Sin, & Heo, 2011).

In addition to North Korea's general underdevelopment, North Korean society is disconnected from the outside world. Even in the information age, Pyongyang does not allow its citizens any access to cyberspace. It is understandable that the dictatorship is worried about the internet's negative impact on the regime and society more generally. In this regard, some cybersecurity experts have raised doubts about attributing massive cyberattacks to North Korea, arguing North Korea's internet, computer, and energy infrastructure could not carry out unprecedented cyberattacks (Monsegur, 2014; RiskBased Security, 2014).

The first study (Chapter 2) seeks to bridge the gap between North Korea's undeveloped image and cyber reality. It contends that contrary to its image as a backward country, North Korea has sufficient IT infrastructure and human capital to conduct hostile cyberoperations against the outside world in order to attain its national goals. The Kim dictator family of North Korea—Kim Il Sung, Kim Jong Il, and Kim Jong Un—has officially emphasized the importance of information technology for the country's survival. They have continuously improved their IT infrastructure. The family has also established state-led intensive education systems for gifted computer students to increase its cybercapacity. The empirical evidence about North Korea's IT reality supports the first argument of this dissertation which is the reply to the first question: Why and how does North Korea have sufficient aggressive cybercapacity to carry out massive and complicated cyberoperations?

The second question is how the North Korean regime has accomplished its hostile cyberoperations without being traced and punished by victim countries and the international community. In other words, it is how Pyongyang keeps a distance from malicious activities that its cyber warriors conduct in cyberspace. Since the late 2000s, several governments, mainly the United States and South Korea, as well as global private cybersecurity companies, have attributed some of the massive and complicated cyberattacks to North Korea. However, it is difficult to accept this attribution of some invisible cyberoperations. In addition, North Korea has denied its responsibility for these covert operations in cyberspace. It is different, however, from the case of North Korea's nuclear threats. Several countries and international entities have imposed sanctions against North Korea which has clearly carried out nuclear and missile tests.

Governments, their cybersecurity agents, and even global private cybersecurity companies have difficulty persuading the public to accept their attributions of some massive, but intangible

cyberoperations to North Korea. Governments and their cybersecurity entities are reluctant to open all scientific evidence to the public due to the possibility that North Korean cyber-warriors could change their ways, methods, or patterns of cyberoperations to avoid being traced based on this evidence from government entities. Therefore, some people do not believe the attributions. For example, some news journals and IT experts say that targeted governments accused North Korea of massive hacking incidents on their critical national infrastructure and websites, when, in fact, they had failed to trace real cyberattackers (Citizens' Coalition for Democratic Media 2009; Sung-Hwan Kim, 2015; Jung-Hun Lee, 2011). These journalists and experts added that cybercriminals could also carry out those cyberattacks with fake IP addresses (CCDM, 2009; Sung-Hwan Kim, 2015; Jung-Hun Lee, 2011). More specifically, the Chinese government hesitates to blame North Korea for some massive cyberattacks arguably caused by North Korean hackers because evidence about the cyberattacks is inconclusive and does not directly tie the North to the attack (Mozur & Perlez, 2018). In this regard, North Korea has denied responsibility for those cyberattacks while simultaneously stating the attacks might be the righteous work of its supporters and sympathizers (Associated Press, 2014).

In response to the second question, the second study (Chapter 3) contends that North Korea's cyber-proxy-warfare strategy enables its cyber-warriors to accomplish aggressive cyber-missions while North Korean hackers keep a distance from their state sponsor, North Korea. Proxy warfare is traditionally viewed as the indirect involvement of sponsors (mainly state actors) in a military operation by employing third parties (states or non-state actors) as proxies wishing to achieve sponsors' strategic goals (Mumford, 2013, p. 1). A proxy warfare strategy is revitalized in cyberspace by the characteristics of the artificial space (anarchical nature, anonymity, and absence of boundaries) and using information technologies (fake IP addresses,

proxy servers, hop points, and VPNs). Pyongyang's cyber proxy warfare plays a crucial role in keeping a distance from arguably North Korea-related cyberoperations. Thus, Chapter 3 argues that as the sponsor North Korea actively enjoys proxy warfare by using its cyberwarriors as proxies for achieving national goals in cyberspace while not being traced and punished.

The last issue is that policymakers and the public across the globe have largely overlooked the impact of North Korea's cybercapability buildup when compared to North Korea's other conventional arms buildup, including developing nuclear weapons and inter-continental ballistic missiles. North Korea uses cyberattacks to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges in order to evade nuclear-program-related international financial sanctions (Lederer, 2019). Despite this fact, recent inter-Korean and U.S.-North Korean summits have only focused on North Korea's nuclear weapons, without discussion of Pyongyang's cyberoperations. This trend shows that policymakers comparatively minimize the impact of North Korea's cyber development on individual state security, as well as on prospects for world peace.

Stories about North Korea-associated cyberoperations has become a topic of interest for journalists, scholars, and technical report writers. Their work has played a key role in alerting the public about individual North Korea's cyberoperations. Sometimes, they provide a more in-depth analysis of North Korea's cybermissions as part of Pyongyang's short-term strategy for financial benefit. However, these reports do not illustrate *how much* North Korea's unknown cyber buildup impacts regional and world security dynamics.

The last study (Chapter 4) seeks to understand the influence of North Korea's cyber uncertainty on regional and world security dynamics. Pyongyang's focus on the development of cybercapability increases uncertainty and fear on the Korean Peninsula, resulting in the cyber

military buildup of other countries, primarily the United States and South Korea. Moreover, this cyber uncertainty and fear have been transferred to the entire Northeast Asia region, where the Western (the United States, South Korea, and Japan) and Eastern (China, Russia, and North Korea) blocs of the Cold War face each other. Thus, this chapter argues that through the North Korea case, the impact of cyber buildup can be seen as the same as that of conventional military buildup.

When combined, these three studies provide insight into the central question of this dissertation about why and how North Korea became a world-class cyber-threat actor. The Kim dictator family has understood the importance and impact of developing cybercapacity for their survival in security and military areas. North Korea has started to conduct massive and complicated cyberoperations through a proxy-warfare strategy which enables the state to deny its responsibility for those operations. Sufficient IT human capital from state-led intensive education systems is at the core of North Korea's aggressive cyberoperations; this, in turn, threatens the national security of other countries and changes regional security dynamics.

1.2 THE LITERATURE REVIEW

There is a growing literature on the topic of national security in cyberspace. Beginning in the 1990s, some scholars warned of cyberattack threats to national security (Arquilla & Ronfeldt, 1993; Bumiller & Shanker, 2012; Clarke & Knake, 2010; Wirtz, 2017). These scholars contributed to raising public, governmental, and academic awareness about the significance of cybersecurity to security studies. However, they were labeled fearmongers because their work lacked sufficient empirical evidence for their arguments (Sharp, 2017, pp. 1–2).

Empirical data on state-led cyberoperations were accumulated after Russia's cyberattacks on Estonia in 2007. Since then, many scholars have focused on technical aspects of cybersecurity

and cyberwarfare (Applegate, 2011; Qin, Zhou, Reid, Lai, & Chen, 2007; Weedon, 2015). Their studies provide practical guidance for cybersecurity experts, including state cyberwarriors, based on empirical evidence. Other scholars have addressed issues of military doctrine (Colarik & Janczewski, 2012; Monaghan, 2015); national cyberpolicy and strategy (Ciolan, 2014; Czosseck, Ottis, & Taliharm, 2013; Joubert, 2012; Libicki, 2009); and domestic and international law (DeLuca, 2013; Gervais, 2012; Goldsmith, 2015; Schmitt & Vihul, 2014; Stinissen, 2015). These studies are useful for political leaders, policymakers, and other elite groups who are interested in cybersecurity-related issues.

Although relatively few scholars have explored the relationship between classic national security and cybersecurity, a few have presented available empirical evidence more systematically to support their arguments (Buchanan, 2016; Junio, 2013; Rid & Buchanan, 2015; Sharp, 2017; Valeriano & Maness, 2014). This dissertation joins these scholars by examining why and how North Korea became one of the world-class cyber-threat actors through three connected stories: the source of North Korea's cybercapacity, North Korea's cyber strategy, and the impact of North Korea's cyberoperations on regional security dynamics.

The literature on North Korea-associated cyberoperations has grown almost as quickly as the increase in North Korea's cyber threats to the globe. Instead of revisiting this extensive literature, it is sufficient to say that four themes emerge from security experts, policy experts, and computer scientists' research on North Korea's cyber threats. First, some academic articles and books use alleged North Korea-related hacking incidents as single case studies of cybersecurity to support general ideas on cybersecurity and national security (Carr, 2012; Clarke, 2009; Clarke & Knake, 2010; Liff, 2012). Second, some security scholars use North Korea's cyberattack incidents to make generalizable claims about international relations theories (Buchanan, 2016;

Libicki, 2012; Maurer, 2018; Sharp, 2017). Third, several academic articles focus only on North Korean hacking issues in order to identify implications for national cybersecurity policy (Yun-Young Kim, 2016; Lim, Kwan, Change, & Back, 2013; Shin, 2016; Shin & Lee, 2013; Boo, 2017). Fourth, computer scientists in private cybersecurity companies such as Symantec, McAfee, Kaspersky Lab, FireEye, and BAE Systems Applied Intelligence have published technical reports on North Korea-related cyberoperations. Their reports are relatively unbiased and reliable. These reports also provide more scientific evidence to the global public about North Korea-led cyberoperations.

However, aforementioned studies do not seek to illustrate a comprehensive idea of why and how North Korea, a world-class cyber-threat actor, started to conduct malicious cyberactivities. Therefore, this dissertation explores the central question with empirical data linking the cases of North Korea's operations to existing international and security theories: (1) the internet dilemma; (2) the proxy warfare literature; and (3) the security dilemma. These three theories will be detailed in section 1.4.

1.3 Methodology & Data Collection

This dissertation presents a qualitative document analysis of North Korea's cybercapability buildup and cyber strategy to answer the central and sub-questions. Qualitative document analysis remains one of the most common components of social science research methods (Wesley, 2010). Social science studies, however, are increasingly dominated by discussions of quantitative content analysis, interviews, focus groups, experimentation, and field studies. Qualitative document analysis is often left behind in these discussions because it is methodologically misunderstood due to issues of quality and credibility. Thus, this research uses

techniques, such as data source triangulation, for enhancing the quality of document analysis on North Korea's cyberoperations (Patton, 1999).

The evidence analyzed is mainly derived from a triangulation of data: (1) governments (including North Korea) and international organizations' reports, press releases, speeches, documents, and funding priorities; (2) global private cybersecurity companies' technical reports and press releases; (3) reliable news media and some selected articles from North Korean propaganda media; and (4) ten interviews with cybersecurity experts in public and private areas[1] regarding North Korea's malicious activities in cyberspace. The research traces the development of North Korea's cybercapability over four decades (1980s – 2010s) in Chapter 2 and the pattern and outcome of North Korea's aggressive cyber strategy over two decades (2000s -2010s) in Chapters 3 and 4.

Governments and international organizations' official reports, press releases, speeches, documents are the primary data source for this dissertation. Government sources are drawn from traditional security and cybersecurity agencies in South Korea and the United States. This first category also includes congressional and national assembly documents, which serve as checks on the aforementioned executive agencies. Using documents and reports from opposing government organizations is one of the key ways to keep neutrality and independence from the position of specific governments. This dissertation also uses a few, but important data from North Korea, such as North Korean leaders' propaganda books, official propaganda and commercial websites of the state. These data provide an indirect examination of the state and its cyberspace policies and strategy. Moreover, websites, reports, and documents of international organizations provide important information about North Korea's cybercapability. For example, North Korea received

[1] This dissertation project was approved by the University of Washington's Human Subjects Division on June 7, 2017.

a block of 1,024 IP addresses and ‘kp’ domain names from a nonprofit international organization, ICANN (Internet Corporation for Assigned Names and Numbers) around 2007 (APNIC, n.d.).

The second major data source—global private cybersecurity companies—provides insight into the technical-skill levels and patterns of North Korea’s cyberoperations. For example, while an official state report on diverse aspects of North Korea’s cybercapability and strategy is drawn from several government departments, including intelligence groups, these data are biased toward national interests. However, private cybersecurity experts and analysts are not required to consider their own country’s interests when they trace the origin of North Korea-related malicious activities in the virtual world. In other words, their technical reports on North Korea’s cyberoperations usually do not reflect the political interests of a particular state. Thus, these technical reports play a critical role in cross-checking the accuracy of governments’ data.

The third source of data—articles from reliable news media outlets from around the globe—are valuable in gathering facts about North Korea’s cybercapability and strategy, as well as reactions of other governments to North Korea’s aggressive cyberoperations. This data source is valuable for two further reasons. First, governments and officials sometimes announce their positions on cybersecurity issues through news media and interviews with journalists without publishing official reports. Second, North Korean propaganda media is an essential—if indirect—way to understand North Korea’s policies or opinion on global issues and the reality of North Korea’s IT. For example, North Korean leaders introduce their policy directives through New Year’s addresses every year. Some North Korean news articles also cover the daily life of ordinary citizens in the context of information technologies.

As a final note, a few interviews with cybersecurity experts in public and private fields were conducted in the U.S. and South Korea. However, the dissertation does not cite data from those interviews; these data are only used validate the authenticity of three other sources through a cross-verification process because these interviewees were reluctant to have their names revealed to the public.

1.4 THEORETICAL OVERVIEW

This qualitative research seeks to connect existing international and security theories with cybersecurity issues in the language of security studies. There are three main theories from established international and security studies: (1) the internet dilemma; (2) the proxy warfare literature with the principal-agent theory; and (3) the security dilemma. These theories are applied to cybersecurity issues originating from North Korea's cybercapacity buildup to answer the central research questions of this dissertation. The research results provide empirical evidence to bridge the gap between these theories and new national security issues arising in cyberspace.

First, information technologies, primarily the internet, enable people across the globe to increase and enhance the exchange of information about themselves and their countries. This information age has presented serious difficulties for authoritarian regimes. Some scholars, such as Kyungmin Ko, Heejin Lee, Seungkwon Jang, and Evgeny Morozov, call this problem the "internet dilemma" (Ko, Lee, & Jang, 2009, p. 281) or the "dictator's dilemma" (Morozov, 2011). While the internet is regarded as a desirable way to improve the national economy, it is viewed as a potential vehicle to threaten authoritarian countries through the sharing of information, including politically sensitive issues, from the outside world to their countries,

thereby creating political awareness and providing platforms for organizing activities (Boas, 2000, p. 57).

Thus, although there is little evidence that the internet has been a vehicle to turn authoritarian regimes into democracies (Ko et al., 2009, p. 281), most authoritarian countries are reluctant to allow their citizens to access the internet. This is especially true for social media sites, which are often subject to online censorship (Kerr, 2014, p. 5). First, the internet dilemma theory illustrates why Pyongyang does not allow North Koreans internet access (Kerr, 2014, p. 5). However, these restrictions do not necessarily mean that North Korea does not have an IT infrastructure. On the basis of empirical evidence, Chapter 2 contends that despite the internet dilemma, North Korea has sufficient IT infrastructure and human capital to conduct aggressive cyberoperations. The internet dilemma theory is ultimately useful in explaining how an authoritarian country develops computational capability, while also managing the dangers presented by the internet.

The second is the proxy warfare literature (the principal-agent theory). Proxy relationships between states actors and state or non-state actors are pervasive throughout history. Specifically, as the principal states have hired third-party as the proxy to help achieve their strategic goals for a long time (Maurer, 2018, p. 29). The proxy relationship is mainly driven by reasons of maximizing interest, while at the same time minimizing risk. In other words, the principal states have hired non-state actors as proxies to avoid engaging in direct, costly, and bloody warfare, while they seek to further their own national interests through conflicts (Mumford, 2013, p. 11).

Cyberspace brings the proxy relationship into the information age. In this context, it can be called *cyber proxy warfare*. The boundaryless, anarchist nature of cyberspace plays critical roles in state-led cyber proxy warfare. Some IT tools, such as using fake IP addresses, proxy servers,

hop points, and VPNs, enable state actors to use a covert proxy warfare strategy for its cyberoperations. Thus, Chapter 3 argues that the North Korean government carries out malicious cybermissions by employing its own cyberwarriors as third-party, non-state actors in order to distance itself from these missions. In other words, proxy relationships can be understood as North Korea's cyberwarfare strategy.

The security dilemma is the last theoretical reply to the central question of this dissertation. It refers to a situation in which one country takes diverse actions to increase its security, thus inadvertently decreasing the security of other countries with what appear to be offensive acts (Buchanan & Williams, 2018). Moreover, these competing countries are likely to be trapped in a vicious cycle of escalating tension. The other countries, which feel fear and uncertainty about the unknown security steps of the country, also take defensive actions, such as enhancing arms buildup and alliances, in order to increase their national security. For example, the security dilemma between European powers triggered World War I in the early 20th century (George, 1933).

Using empirical evidence, Chapter 4 argues that the security dilemma still applies to cyberspace. It is called as the *cybersecurity dilemma*. Neighboring countries fear North Korea's unknown and uncertain activities in the virtual world. The uncertainty about North Korea's increased cybercapacity leads opponent countries to increase their cyber military buildup and alliances between countries in Northeast Asia. Moreover, North Korea's creation of the cybersecurity dilemma on the peninsula has been transferred to the entire Northeast region. The three theoretical issues – the internet dilemma, cyber proxy warfare, and the cybersecurity dilemma – will be detailed in each chapter.

1.5 CHAPTER OUTLINE

The remainder of the dissertation proceeds as follows. Chapter 2, "Origins of North Korea's Cybercapacity Capacity," seeks to understand why North Korea decided to develop cybercapability among several science and technology areas. It also shows what kind of IT infrastructure North Korea has and how North Korea grooms many IT experts who can be viewed as cyberwarriors of the state. Chapter 3, "North Korea's Cyber Proxy Warfare Strategy," illustrates how North Korea's cyberoperations work. The state uses a classic proxy warfare strategy in cyberspace. Pyongyang conducts malicious cyberactivities by employing its many IT experts as cyber proxies. The cyber proxy warfare strategy plays a critical role in North Korea's cyberoperations by enabling the state to benefit and keep a distance from the operations simultaneously.

Chapter 4, "North Korea's Cyber Uncertainty and Regional Security Dynamics," uses the security dilemma and empirical data to describe how North Korea's cybercapability development has a considerable impact on regional security dynamics. This chapter argues that the impact of North Korea's cyber buildup on regional security dynamics is the same as North Korea's conventional arms buildup. The concluding chapter, Chapter 5, summarizes the dissertation, explains why and how North Korea became one of the world-class cyber-threat actors, offers policy implications, and provides suggestions for future research.

Chapter 2. ORIGINS OF NORTH KOREA'S CYBERCAPACITY

2.1 INTRODUCTION

Since the late 2000s, massive cyberattacks on the United States and South Korea's critical infrastructures have been attributed to North Korea, including attacks on military networks, nuclear plants, and electric companies.[2] These attacks were recognized to be in the political interests of North Korea.[3] Moreover, recent Pyongyang-associated cyberoperations, such as the 2016 Bangladesh Bank cyber heist, and the 2017 WannaCry ransomware, arguably focused on short-term financial benefits of the North Korean regime because of the international economic sanctions against the North, following its consecutive nuclear tests (Perlroth & Corkery, 2016; The White House, 2017a). As cyber threats have increased and diversified, especially after the 2014 Sony hack, the U.S. government has placed North Korea's cyber threat among its top security concerns, along with cyber threats of Russia, China, and Iran (U.S. DoD, 2015; Coats, 2018). Moreover, victim states identification of North Korea as the perpetrator of these attacks has been supported by comparatively unbiased, reliable technical reports of global cybersecurity companies, such as Symantec, McAfee, Kaspersky Lab, FireEye, and BAE Systems Applied Intelligence.[4]

---

[2] Critical websites of the United States and South Korea suffered from massive DDoS attacks in July 2009. The two states accused North Korea of the cyberattacks, which are arguably viewed as the start of North Korea's organized, massive cyberoperations against the outside world.

[3] North Korea's cyberattacks have operated against specific targets, such as North Korean defectors and government and military websites of the South and the United States under clear political goals to benefit the North Korean government. Some of scholars argued that the massive North Korean cyberattacks happened when North Korea tested its nuclear weapons and intercontinental ballistic missiles.

[4] The following are reliable technical reports or blogs on North Korea-associated cyberattacks from private global cybersecurity companies: (1) Symantec: "Collaborative Operation Blockbuster Aims to Send Lazarus back to the Dead" (2016); "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War" (2013); "Symantec Intelligence Report (June, 2013)"; "SWIFT Attackers' Malware Linked to More Financial

Despite the aforementioned reality, North Korea's high-level cyber threat may appear to be a paradox to many people across the globe. Traditionally, North Korea has been understood as the world's most reclusive, repressive, and isolated country. Some experts on North Korea have called the state a hermit kingdom (Hassig & Oh, 2009; Kihl, 1984; Warf, 2015). Based on this image of North Korea, it is understandable that North Korea's cybercapacity is perceived as all but non-existent. One *New York Times* headline ran, "The Internet Black Hole that is North Korea" (Zeller, 2006). It appears that even after the invention of the internet, North Korean people still live in their hermit kingdom in a kind of premodern anomaly, separate from the global market economy and cyberspace. There are no data from North Korea in the *ICT Development Index*[5] (2009–2017), which ranks among over 150 countries' cyber capacity details.

In theory, the North Korean government seems to be faced with a new challenge from the internet: increased interconnectedness, globalization, and the flow of information between countries. While some Asian countries, such as South Korea and Singapore, have embraced information and communication technology as a driving force in their economies and societies,

---

Attacks" (2016); "Attackers Target Dozens of Global Banks with New Malware" (2017); "WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group" (2017); (2) McAfee: "Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea" (2011); "Dissecting Operation Troy" (2013); (3) Kaspersky Lab: "The 'Kimsuky' Operation" (2013); "Lazarus under the Hood" (2017); "Who Is behind of Sony Pictures Hack and Other Dangerous Cyberattacks" (2016); (4) FireEye: "Why Is North Korea So Interested in Bitcoin?" (2017); "APT37 (Reaper): The Overlooked North Korean Actor" (2018); "North Korean Actors Spear Phish U.S. Electric Companies" (2017); (5.) Others: ASeC (AhnLab Security emergency Response Center); "ASEC Report Vol.51" (2014); Alyac, "Covet Activities of Operation Kimsuky" (2018); Infosecurity, "Kimsuky - an Active North Korean Campaign Targeting South Korea" (2013); Novetta, "North Korea, Cyberattacks and 'Lazarus'" (2017); Intezer, "BLOCKBUSTED: Lazarus, Blockbuster, and North Korea" (2017); BAE Systems Applied Intelligence, "Taiwan Heist" (2017); Novetta, "Operations Blockbuster: Unraveling the Long Thread of the Sony Attack" (2016).

[5] IN 2009, the United Nations International Telecommunication Union (ITU) has released an annual statistic report about the ICT Development Index (IDI) to assess comprehensive ICT capacity of every country in the world based on 11 ICT indicators, grouped in three clusters, such as access, use, and skills. The IDI aims to provide a standard tool to measure the digital divide and compare ICT performance within and across countries to help underdeveloped or developing countries. For more information about IDI, see the following link: http://www.itu.int/net4/ITU-D/idi/2017/#idi2017rank-tab

North Korea remains largely disconnected from global circuits of capital and information (Warf, 2015, p. 110). In this regard, some scholars see this as an illustration of a "dictator's dilemma" or an "internet dilemma" (Boas, 2000; Kerr, 2014; Ko et al., 2009; Morozov, 2011, p. 93). This dilemma rests on the assumption that "a new technology, notably the internet, can be a driving force toward the democratization of authoritarian regimes" (Ko et al., 2009, p. 279). As Boas (2000) notes:

> Authoritarian leaders in the information age are confronted with an unmistakable dilemma. On the one hand, the Internet and associated information and communication technologies offer enormous economic potential for developing countries, and the increasingly interconnected global economy thrives on openness of information. On the other hand, the information revolution poses new challenges for regimes that rely on centralized political control. (p. 57)

This negative relationship between authoritarian regimes and developing ICTs (Information and Communication Technologies) appears valid in the case of North Korea, which has continually emphasized self-reliance for survival purposes. Although ordinary people in China and Russia are allowed online access, these two large authoritarian states operate strong online censorship and surveillance programs, such as the Chinese Great Firewall, to avoid challenges to their regimes (Karatzogianni, 2015, p. 46; Mina, 2014, p. 360; Pallin, 2017; Raud, 2016, p. 18). North Korea is a more closed society than China and Russia as it is the only state which does not allow public access to online information. (Ko et al., 2009, p. 280).

Nevertheless, empirical evidence on North Korea's ICT development indicates that North Korea is very different from its old image as the hermit kingdom, as well as the negative theoretical perspective of the dictator's dilemma. Developing technologies, mainly ICTs, has

always been a focus of North Korea's leadership. The Kim family of dictators, Kim Il Sung, Kim Jong Il, and Kim Jong Un, all have emphasized the importance of science and technology for the country's survival in their official speeches and texts (Kim Jong Il, 1992; Kim Jong Un, 2018). More concretely, the state has operated technology-focused intensive education programs for this purpose. It has been manifested in the development of ICT infrastructure. However, it has not been well developed due to North Korea's closed political, economic, and societal structures that are diametrically opposed to internet freedom. This means that while North Korea has limited ICTs and infrastructure, it has many skilled ICT professionals from its intensive education and science and technology policy; these professionals have become the fuel for the state's cybersecurity strategy.

This chapter answers the following question: Why and how does North Korea have sufficient aggressive cybercapacity to conduct massive and complicated cyberoperations while the state does not allow its citizens internet access? The primary aim of this chapter is to reduce the gap between North Korea's negative image and the reality regarding its ICT infrastructure. Some computer experts have approached the scope of North Korea's cyberoperations on the premise that a nation-state without a native computer infrastructure cannot launch an unprecedented cyberattack (RiskBased Security, 2014). For instance, in his interview with CBS News, former Anonymous hacker Hector Monsegur[6] (2014) raised doubts about the attack attribution, arguing that North Korea's inadequate internet infrastructure could not handle the transfer of more than one hundred terabytes of data. Despite this claim, North Korea's development of ICTs began at least as early as the 1980s when Kim Il Sung visited his Communist allies, primarily the Soviet Union.

---

[6] *Former Anonymous hacker doubts North Korea behind Sony attack*. (2014). Retrieved from https://www.youtube.com/watch?v=vWiFtS5F3jc

On the basis of empirical data, this chapter contends that while North Korea has limited ICTs and infrastructure, it has sufficient ICT infrastructure and cyber human capital to conduct massive cyberoperations in its interests against the outside world. The Kim dictator family of North Korea—Kim Il Sung, Kim Jong Il, and Kim Jong Un—have given official emphasis to the importance of information technology for the country's survival. They have continuously improved the state's IT infrastructure. The family also established state-led intensive education systems for gifted computer students in order to increase North Korea's cybercapacity. Moreover, this chapter on the development of North Korea's ICT infrastructure provides an indirect way to assess the origin of North Korea's aggressive cybercapability against the outside world. No one has previously explored evidence that would show the extent of North Korea's offensive cybercapability.

This chapter offers a comprehensive overview of the state's ICT emphasis, infrastructure, and education systems as a means to understand the degree to which the world's digital revolution has penetrated one of the most isolated countries on earth. Although the level of North Korea's ICT infrastructure falls a little bit far behind those of other leading ICT countries, including North Korea's main cyberoperations' targets, such as the United States and South Korea, this chapter demonstrates that North Korea's ICT infrastructure and cyber human capital can enable the state to hack critical national infrastructures and financial entities of others, if it chooses. The story begins with North Korean dictators' emphasis on the importance of developing ICT sector in their official statements and policies. Second, it provides a short history of developing ICT infrastructure by focusing on three components: mobile network service; internet and intranet; and ICT industries. Third, it highlights a hidden driving force behind North Korea's ICT sector, despite its isolation and limited resources: a state-led intensive education

system. The conclusion revisits the main argument that North Korea's ICT reality is far from the stereotypical image of North Korea and revisits the theoretically negative relationship between authoritarian regimes and ICTs.

At the outset to this chapter, it is important to note two critical limitations. First, due to the regime's need to survive, it is difficult to gather accurate, unbiased primary sources as well as information about North Korea's ICT infrastructure in order to measure its cyber-capability in the area of security studies. North Korea is entirely disconnected from the international community. Its official, closed structure does not allow the outside world to access national security-related data that would threaten regime survival. In this regard, North Korea's mass media appears to be the only way to investigate the state. However, state-controlled media outlets speak only in the interest of the regime due to strong censorship programs. Therefore, North Korean news articles and opinions about national security are usually unreliable as they provide only partial or fragmented information that cannot prevent a holistic understanding of national security. Thus, the study focuses on security studies as well as other academic fields, such as science policy and history, education, and computer science to overcome the aforementioned limitations. Several primary sources from the other fields are critical in understanding the degree of North Korea's ICT development. These include North Korea's official statements and documents on ICTs, computer textbooks, websites, and newspapers about other fields.

A second limitation is that secondary sources are typically biased toward against North Korea in favor of countries hostile to North Korea, mainly the United States and South Korea. These sources often portray North Korea in negative terms that parallel the foreign policy positions of their countries. With this caveat in mind, this project assembles available

information from a wide variety of government, academic, and media sources by cross-checking to ensure accuracy. This is accomplished by comparing state-led statements or reports on North Korea's ICTs with academic articles or technical reports from the private sectors, including global cybersecurity companies. On the one hand, while a state's official statement or report may focus on diverse aspects of North Korea's ICTs (based on its national resources from several government departments, including intelligence groups), these sources have a bias toward North Korean national interests. On the other hand, while the private sector has limited sources about North Korea's ICTs, it usually does not speak for the political interests of a particular state. Thus, using diverse sources with cross-checking is vital to strengthen the central argument of this study: while North Korea has limited ICTs and infrastructure, it has many skilled ICT professionals from its intensive education and science and technology policy that has made possible its hostile and aggressive cyber-strategy.

2.2 North Korea and Its Emphasis on ICTs

North Korea has been called as the hermit kingdom for a long time (Hassig & Oh, 2009; Kihl, 1984; Warf, 2015). While this image has stimulated international curiosity about this autocratic state, it has also led people to misunderstand North Korea. For example, Ho-Je Kang (2007), history scholar on North Korea's science and technology, pointed out that South Korean college students in his class think that North Korea has no science and technology capacity at all, even though they have witnessed North Korea's tests of nuclear weapons and long-range missiles (p. 5). However, ever since the establishment of the North Korean state, it has pursued advancement in science and technology to achieve its ultimate goal: regime survival, not economic prosperity. As a result, while North Korea has limited ICTs and ICT infrastructure, it

has many skilled ICT professionals from its intensive science and technology education programs who have become the foundation for its aggressive cybersecurity strategy.

The Kim dictator family—Kim Il Sung, Kim Jong Il, and Kim Jong Un—have officially emphasized the importance of science and technology for the country's survival under its unique ideology, *Juche* (Kim Jong Il, 1992). Juche (주체 in Korean), translated as "self-reliance," is the official state ideology of North Korea, described by the government as Kim Il Sung's "original, brilliant and revolutionary contribution to national and international thought" (French, 2007, p. 30). Its postulates include: (1) that "man is the master of his destiny," (2) that the North Korean masses are to act as the "masters of the revolution and construction," and (3) that by becoming self-reliant and strong a nation can achieve true socialism (Kim Jong Il, 1982, p. 12). Based on the Juche ideology, three articles, 27, 28, and 50, of the Constitution of the DPRK (the Democratic People's Republic of Korea)[7] (1998) say that science and technology are essential for the nation's socialist economic activities. This is why three generations of dictators have been committed to strengthening information and communication technologies (ICTs).

North Korea started to develop ICTs in the mid-1980s, following a new global trend in socialist economies. When Kim Il Sung, founder of North Korea, visited the Soviet Union and Eastern Europe (Poland, East Germany, Hungary, and Romania) in 1984, the Soviet Union had made computer technology and information science a high priority for their national economies (Wellman, 1989, pp. 7–12). More specifically, the U.S.S.R. used a new computer education

[7] "The technical revolution is vital to the development of the socialist economy" in Article 27; "The State shall accelerate the technical revolution in the rural areas in order to eliminate differences between urban and rural areas, and class distinctions between the working class and the peasantry, industrialize and modernize agriculture, strengthen the guidance and assistance to rural areas by enhancing the role of the county" in Article 28; and "The State shall establish Juche in scientific research, introduce advanced science and technology in every possible way, open up new areas of science and technology and raise the country's science and technology to the world level" in Article 50.

campaign in an attempt to reduce its computer science gap with the West. Soviet officials referred to the program as a "second literacy" of major importance to the acceleration of their economy by comparing to the campaign to develop literacy in Russia after the Revolution of 1917 (Wellman, 1989, p. 125). The campaign led the U.S.S.R.'s Politburo to make a plan to install one million micro-computers in the country's 60,000 secondary schools by 1990 (Holden, 1986, p. 109). In his tour of the European Communist states, Kim Il Sung witnessed the new concern of the Soviet Union and its emphasis on computer technology and education (Chan-Mo Park, 1994). Once Kim returned home, North Korea established special secondary schools across the nation for its advanced science students in 1984 (Cho, 2004, pp. 57–60). These secondary schools are now viewed as the central source of North Korea's cybercapacity as well as offensive cyberoperations.[8]

Kim Jong Il,[9] the second dictator from 1994–2011, also emphasized science and technology as central to building a strong and prosperous socialist state since the end of 1998. According to joint 1999 and 2000 New Year's common editorials by the three major North Korean daily newspapers,[10] despite Kim's claims of advocating the "Military First Policy," Kim actually selected three main pillars to ensure his national goal of survival: Juche ideology, military power, and science and technology. Moreover, in 1998, *Rodong Sinmun* argued in the official newspaper of the Central Committee of the Workers' Party of [North] Korea (WPK) that North Korea would become one of the top nations in science technology based on its robust technology

[8] For more detail about North Korea's special secondary schools, see section 2.4.2.
[9] Kim Jong Il had several official titles, such as Supreme Commander of the Korean People's Army (KPA) (1991–2011), Chairman of the National Defense Commission (NDC) (1993–2011), and General Secretary of the Workers' Party of Korea (WPK) (1997–2011).
[10] Those newspapers are *Rodong Sinmun* (로동신문 in Korean), which is translated as the Workers' Party Newspaper, under the control of the party), *Joson Inmingun* (조선인민군 in Korean), which is translated as the Korean People's Army Newspaper, under the control of the army, and *Chongnyon Jonwi* (청년전위 in Korean), which is translated as the "Newspaper for Young Workers" under the control of the Workers' Party of [North] Korea's youth league.

capability to achieve a self-reliant national economy (Rodong Sinmun & Rodongja Sinmun,[11] 1998). Accordingly, Kim Jong II designated 1999 as the Year of Science and Technology and visited the Academy of Sciences of the DPRK to highlight his point (Choon-Geun Lee, 2005, pp. 53–54). More interestingly, Kim Jong Il placed far more emphasis on developing information science and technology than other science fields. In a speech, he said that "while the 20th century is the age of the machine industry, the 21st century is the age of the information and communication industry" ("While the 20th century," 2001). Developing ICTs and building ICT infrastructure were at the core of his new ideas of "New Thinking Theory" (신사고론 in Korean) and the "Theory of One Leaping for All" (단번도약론 in Korean),[12] designed to promote economic recovery during his presidency (Jong-Woon Lee, 2002, p. 58).

Kim Jong Un, the third and current dictator (2011–), has also focused on developing a robust ICT sector. It is not a secret that he is one of the world's most famous Apple users. Videos of Kim Jong Un with his Apple products, such as iPhone, Macbook, and iMac have been aired by North Korea's official news channel, *the Korean Central News Agency* (KCNA) (Chacos, 2016). Kim was exposed to Western ideas, culture, and technology, when he attended the Liebefeld Steinhölzli state school in Köniz near Bern, Switzerland, from 1998 until 2000 (Pak, 2018). The young dictator has also been interested in ICTs as a new way to overcome North Korea's economic hardships (Kim Jong Un, 2018). In the 2015 New Year's Address, Kim adopted the "Practical Education Revolution" as the core strategy for his long-term plan to build a strong science and technology state (Kim Jong Un, 2015). A report of ROK Unification IT

[11] *Rodongja Sinmun* (로동자신문 in Korean), which is translated as "Workers Newspaper," is the organ of the Central Committee of the KWP in North Korea.

[12] North Korea wanted to build IT industry without normal industrialization process from light industry to heavy industry to high-tech industry. Kim Jong Il's regime called it "Theory of One Leaping for All" (Yoo & Ko, 2004, p. 14).

Forum (2015, pp. 82–83) found that Kim Jong Un's 2015 New Year's Address had two emphases on ICTs: (1) science education will foster human capital for ICT infrastructure and (2) secondary and college education systems will be reformed to intensify ICT-based capacity. In other words, Kim Jong Un's regime tries to build a long-term, asymmetric education system that finds talented computer students and trains them for North Korea's future strategic ICT sector, while it simultaneously ignores increasing overall ICT capacity for ordinary citizens (ROK Unification IT Forum, 2015, pp. 80–81).

To highlight his policy focus on ICTs, Kim Jong Un toured the May 11 Factory[13] to supervise the development of the first smartphone of the state, named Arirang (아리랑 in Korean), on August 10, 2013 (ROK Ministry of Unification, n.d.-a; YTN News, 2013). Even though some Western experts on North Korea noted that the first-generation smartphone was only assembled with parts imported from China, North Korea claimed Arirang was designed and produced by the DPRK (Yonho Kim, 2014b; Williams, 2013). Despite the controversy, there is no doubt that many smartphone users in North Korea use Koryolink, a joint venture mobile telecommunications provider between Egyptian Orascom Telecom Media and Technology Holding (OTMT) and the state-owned Korea Post and Telecommunications Corporation (KPTC) (Haeyoung Kim, 2014, p. 100).

More interestingly, building ICT infrastructure has a similar priority to developing nuclear weapons technologies that are the well-known ultimate survival tools. Despite its severe economic hardship after the 1990s while its Communist ally states were collapsing, North Korean dictators continued to focus on developing nuclear weapons and long-term ballistic missiles. They believed that independent development of nuclear weapons was critical to regime

[13] The May 11 Factory is known as a production base for North Korea's electronic devices.

survival. As a result, the rest of the world is now threatened by North Korean nuclear weapons. Nuclear weapons now work well as North Korea's ultimate bargaining chip. At the same time, under the aforementioned support of North Korean dictators, ICT sector expansion also steadily kept pace with that of nuclear weapon development. The process of ICT infrastructure development will be detailed in the following sections.

Other than nuclear weapons and ICTs, North Korea's other areas of science and technology development have been clearly in retreat. According to their aforementioned public comments and statements, North Korea's three dictators—from founder Kim Il Sung to Kim Jong Un—have officially focused on advancement in science and technology for economic development. However, the results have not been promising during and after the North's famine that left more a million people dead (Noland, Robinson, & Wang, 2001). After its terrible economic crisis in the 1990s, when Kim Il Sung and Kim Jong Il continued building nuclear weapons, North Korea's industrial structure remained underdeveloped. Consequently, the country was economically closer to a typical early stage developing country focusing on primary industry, which is very far from the one of a developed country having healthy secondary industries. Analysis by the Bank of [South] Korea found that the percentage of light and heavy industries based on science and technology in North Korea's GDP had declined from 24.6% in 1992 to 17.7% in 2000.[14] The decreased portion was replaced by the service industry. Unlike their official policy, North Korea had not invested adequate money in secondary industries which are important for its national economy as well as the quality of life for ordinary North Koreans. As a result, according to the CIA's World Factbook, North Korea's 2015 GDP (purchasing power parity, ppp) was $40 billion, ranked as 118th, and its per capita income (ppp) of $1,700 was

[14] For more information about North Korea's GDP, see the following link: https://www.bok.or.kr/portal/main/contents.do?menuNo=200091

ranked 214th in the world.[15] Despite this astonishingly poor economic situation, the DPRK was a nuclear power with significant ICT capacity.

In the early 1990s, North Korea suffered shockwaves due to the collapse of the Communist bloc. Following the collapse of these states, North Korea experienced a severe economic crisis. This situation led the state to expand nuclear weapon development to maintain its isolated authoritarian regime, although the nuclear program led the international community to imposing very strong international economic sanctions against North Korea. Despite its financial difficulties, North Korea allocated its limited resources toward ICT infrastructure. North Korean dictators recognized that building the ICT sector was another strategic way—along with having nuclear weapons—to protect their regime.

However, there is no doubt that despite North Korea's intensive, state-controlled policies, including educational system reformation, the development of the ICT sector has stalled. This is because the closed characteristics of its communication system are the opposite of the internet's concept of freedom of information. This has created a paradoxical situation in which North Korea has limited ICTs and ICT infrastructure. That is why it has many skilled ICT professionals from its intensive education program in science and technology. This gap between abundant, highly educated, and skilled ICTs professionals on the one hand, and underdeveloped ICT sector on the other is increasing. There are also growing international concerns about the focus of North Korea on cyberoperations against the outside world.

[15] For more information about the CIA's World Factbook on North Korea, see the following link: https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html

2.3 DEVELOPMENT OF ICT INFRASTRUCTURE

No one has offered definitive evidence that demonstrates North Korea's offensive cybercapability North Korea. Therefore, tracing the development of North Korea's ICT infrastructure is an indirect strategy to examine the origin of North Korea's aggressive cybercapability against the outside world. This indirect method shows that although North Korea's ICT capability remains below global market levels, it can be understood as a fundamental ground of North Korea's offensive cybercapability. North Korea has sufficient technologies and infrastructure to connect its mobile and internet networks with the outside under international standards. Although its software and hardware industries are somewhat underdeveloped, they are adequate enough to foster ICT human capital. Therefore, the ICT development verifies that North Korea has sufficient conditions to enable itself to operate cyberattacks for achieving national interests, contrary to its hermit, isolated information age image. The following section consists of three sub-sections: mobile network service; internet and intranet; and the ICT industry.

2.3.1 *Mobile Network Service*

North Korea's policies have a goal of preventing its citizens from connecting to other societies (Bong-Sik Kim, 2017, p. 2). The state does not allow North Koreans to be exposed to ideas about the free market economy and democracy that would harm its authoritarian regime. Despite that, the state has wire communication cables to connect one point to another within North Korea. Moreover, since the 2000s, the state has made an effort to build domestic mobile networks under their contracts with global IT companies. This means that North Korea has steadily built its own internal mobile network that fosters the ICT industry as well as professionals' development; these professionals, in turn, become the human power of North

Korea's cyber-army. Furthermore, the construction of wire and wireless communication environment can be viewed as the foundation of ICT infrastructure.

In addition, even though North Korea allows its mobile network users only to access domestic intranet service—not global internet—it theoretically has constructed a gateway to global cyberspace. According to StatCounter's (2018a) Global Stats, mobile devices accounted for 52% of worldwide internet usage, compared to 44.1% and 3.89% via desktop and tablet PCs, respectively.[16] North Korea's wireless communication technologies and devices have even been developed with the support of foreign countries and companies who follow international standards. This means that the North Korean regime could, in theory, enable its mobile network users to access global internet service. Furthermore, in this process of building a mobile network environment, North Korean ICT professionals have been exposed to foreign technologies.

The state-owned Korea Post and Telecommunications Co. (KPTC)[17] has played a key role in the control of building and operating mobile services under North Korea's Ministry of Post and Telecommunications. Similar to other countries, fixed-telephone service is an efficient technology for the public area in North Korea. Yet, the service has not been common for ordinary North Korean people for a long time. According to ITU (International Telecommunication Union) statistical data, there were around 500,000 fixed-telephone subscriptions in 2000 (ITU, n.d.). This means that given that there were only 2.18 subscriptions per 100 people (the North Korean population was 22.93 million in 2000). Moreover, Table 2.1 says that fixed-telephone subscriptions slowly increased to 1,180,000 in 2007, which means that

[16] StatCounter Global Stats also said that worldwide internet usage by mobile devices (51.3), including smartphone (46.53 %) and tablet (4.73 %), surpassed desktop (48.7%) for the first time in October 2016.

[17] KPTC is in charge of North Korea's postal service, telephone system, and media, such as television and print press. It is also related to North Korea's internet and intranet services. According to the APNIC Whois Database, KPTC is also known as the registered user of 256 China Unicom's IP addresses ranging from 210.52.109.0 to 210.52.109.255. Thus, some cyberoperations that used KPTC-associated IP-addresses have been attributed to KPTC.

there were 4.48 subscriptions per 100 people. In the early 2000s, telephone installation charges were very expensive—around $800—especially when compared to its per capita income, around $1,000 (CIA World Factbook, n.d.). Since then, the installation charges have decreased steadily. In 2015, North Koreans could install fixed-telephones at home for around $50 (Bong-Sik Kim, 2017, p. 7). After installation, they pay a couple of dollars per year for phone bills (Bong-Sik Kim, 2017, p. 7).

Table 2.1. Fixed-Telephone Subscriptions (Local and International Calls)

	2000	2001	2002	2003	2004	2005	2006	2007 - 2016
Subscriptions, total	500,000	860,000	916,000	980,000	1,000,000	1,000,000	1,000,000	1,180,000
Population,[18] total (million)	22.93	23.1	23.3	23.5	23.7	23.9	24.1	24.2 (2007)
Per 100 Inhabitants	2.18	3.72	3.93	4.17	4.22	4.18	4.15	4.88

Source: ITU, Country ICT data (Until 2016), Accessed on April 2, 2018; World Bank Data, Accessed on May 22, 2018.

Despite the decrease in installation fees, Table 2.1 shows that the number of fixed-telephone subscriptions has not changed since 2008. North Korea has provided very low-quality fixed-phone service. It is known that while those living in small cities had manual telephone exchanges, only those living in Pyongyang and some big cities had automatic telephone exchanges, known as model S1240 types, made by a Chinese company, Shanghai Bel, in the 2000s (Ju-Jin Kim, 2004, p. 46). Even model S1240 types were outdated. South Korea used similar models that were replaced by new automatic telephone exchangers several years ago.[19] These facts mean that quality and speed of fixed-telecommunication service are still very low in

[18] The World Bank Data on Democratic People's Republic of Korea assessed on May 24, 2018. https://data.worldbank.org/country/korea-dem-peoples-rep?view=chart

[19] A South Korean telecommunication company, KT, used to use model S2140. However, it was replaced by new models several years ago.

North Korea. Thus, even though installation charges and monthly phone bills decreased, fixed-phone service still could not attract North Korean citizens enough to request landline services.

In contrast to landline usage, mobile-cellular telephone service has proven popular among North Korean citizens. Bong-Sik Kim (2017, p. 10) claimed that the rise of mobile-cellular telephones might have influenced the fixed-telephone subscriptions stagnation phenomenon. The year the stagnation began, 2008, was also the year when the North Korea government restarted its mobile service with a new 3G standard for its citizens after a four-year ban on 2G cellular phone use. According to Table 2.2, the number of mobile-cellular telephone subscriptions increased rapidly in 2008, compared to that of fixed-phone subscriptions.

Table 2.2. 3G Mobile-cellular Telephone Subscriptions

	2008	2009	2010	2011	2012	2013	2014	2015	2016
Subscriptions, total	1,694	69,261	431,919	1,000,000	1,700,000	2,420,000	2,800,000	3,240,000	3,606,000
Population,[20] total (million)	24.34	24.46	24.59	24.72	24.85	24.99	25.12	25.24	25.37
Per 100 Inhabitants	0.007	0.28	1.76	4.05	6.84	9.68	11.15	12.84	14.21

Source: ITU, Country ICT data (Until 2016), Accessed on April 2, 2018; The World Bank Data, Accessed on May 22, 2018.

Beginning in the late 1990s, North Korea started to build a mobile network environment with the cooperation of global IT companies. In 1998, a joint venture between Northeast Asia Telephone and Telecommunications (NEAT&T), Loxley Pacific[21] (70% equity), and KPTC

[20] The World Bank, Data on Democratic People's Republic of Korea assessed on May 24, 2018. https://data.worldbank.org/country/korea-dem-peoples-rep?view=chart

[21] Loxley Pacific Company Limited provides telecommunications system integration and solutions for government and private companies, such as telecom operators and internet providers in Thailand. It was awarded monopoly rights to install land-line telephone, paging, and intranet services in the North Korean free trade area of Rajin-Sŏnbong for 27 years beginning in 1995 (Banks, 2005, p. 90; "Company Overview of Loxley Pacific Company Limited," n.d.; Mansourov, 2011).

(30% equity) produced the DPRK's first mobile phone network (Hong-Reoul Lee, 2008, p. 138). Since November 2002, NEAT&T provided 2G GSM service to 1,200 mobile communications lines, 1,500 radio pager lines, and 80 pay phones in Pyongyang and the Rajin-Sonbong Economic Special Zone, under a 30-year license (Mansourov, 2011, p. 11). The joint venture established approximately 50 mobile base stations, coverage to several major cities, including Nampo and Kaesong, provincial capitals, and major freeway and highway roads between Pyongyang and Hyangsan; Pyongyang and Kaesong; and Wonsan and Hamhung (Yonho Kim, 2014a, p. 11). The estimated total number of mobile subscribers increased approximately from 3,000–5,000 per 23.3 million people in November 2002 to 30,000–40,000 per 23.7 million in May 2004 (Hong-Reoul Lee, 2008, p. 139; Mansourov, 2011, p. 18).

In the early 2000s, mobile phones could be purchased in a cellphone store in the Pyongyang International Communication Center Building. Around twenty models were available, all of which were imported from foreign countries, including the United States (Bong-Sik Kim, 2017, p. 18). During this same time period, Korea Workers' Party, the military, and business elite groups were the only ones who could afford to use mobile services because of the high price of admission, monthly payments, and the cost of mobile phones. However, following a massive explosion at Yongchon Station in North Pyongan Province that allegedly targeted Kim Jong Il inside his train in April 2004, the North Korean regime suddenly banned the use of cell phones. It was suspected the explosion was triggered by a remote-controlled wireless handset, probably from a mobile phone (Lankov, 2009, p. 58). Thus, around 30,000–40,000 mobile devices were confiscated, except for those of very few of the top North Korean elite and foreigners (Bong-Sik Kim, 2017, p. 19; Hong-Reoul Lee, 2008, p. 139).

In December 2008, after a four-year ban on 2G cellular phone use, North Korea announced the resumption of 3G mobile service through a new joint venture, Koryolink; this venture was between the Egyptian telecommunication firm Orascom (75% share) and KPTC (25% share) (Kim & Han, 2008; Yoon & Ko, 2011, p. 9). According to Table 2.3, Orascom started to invest money in North Korea under a 2007 agreement with the government for 3G mobile business. On October 27, 2008, the state and Orascom made an agreement with Nokia about providing extra mobile services, such as music and video streaming for its potential North Korean customers. This means that despite the issue of limited access, Orascom managed to arrange 3G intranet data service for North Korean subscribers.

Table 2.3. Timeline of Orascom's Business in North Korea

Date	Contents
Jan. 19, 2007	North Korea - Orascom made an agreement for mobile business in the country
Jul. 16, 2007	Orascom Construction Industries, the Egyptian cement producer and construction group, announced a $115m investment in a cement plant in North Korea (Griggs & Fidler, 2007)
Sep. 3, 2007	The 22nd Meeting of NEAT&T's board of directors was held
Jan. 31, 2008	Orascom Telecom was awarded a 25-year concession for mobile business
Feb. 2008	Orascom Construction Industries was sold off to the French cement giant Lafarge
May 2008	Orascom Telecom announced it succeeds its mobile call test.
Oct. 27, 2008	Orascom Telecom made an agreement with Nokia for mobile extra services, such as music and video streaming
Dec. 4, 2008	Orascom Telecom announced its services will be started on Dec. 15, 2008
Dec. 15, 2008	Orascom Telecom started its mobile services in the state

Source: NK Tech's Newsletter 182: North Korea's 3G Mobile Telecommunication Company, 'Koryolink,' Started Its Service, on December 19, 2008.

According to the *Choson Sinbo*,[22] as of April 6, 2009, anyone who needs mobile phone service is allowed to purchase mobile devices and use the 3G services in North Korea (NK Tech, 2009a). Installation fees of 50 euros, 110 to 240 euros for mobile devices, and mobile call charges / monthly payments[23] still were expensive when compared to the average North Korean per capita income of $1,800 U.S. dollars in 2008 and 2009 (CIA World Factbook, n.d.). Despite this, Table 2.2 shows that the number of Koryolink subscriptions increased rapidly from 1,694 per 24.34 million in late 2008 to 2,000,000 per 24.99 million in May 2013 (Yonho Kim, 2013; Orascom Telecom, Media & Technology, 2013). On April 19, 2010, the *Choson Sinbo* reported that the increased demand for mobile services reached the capacity limit of Koryolink's 126,000 mobile lines (Sang-Young Lee, 2010). In June 2010, Koryolink's subscription services were halted due to shortages in infrastructure (Bong-Sik Kim, 2017, p. 22).

In addition to these services, the North Korean government itself established a state-owned second mobile telecommunications company, Kangsong Network (강성네트 in Korean), which means "Strong Network." This development occurred in the second half of 2011, immediately before the expiration of Orascom's franchise in 2012. North Korea's second network company is under the direct control of the Korea Workers' Party (Bong-Sik Kim, 2017, p. 22). It has also increased its subscriptions with cheaper monthly payments and call charges, as compared to Koryolink. Moreover, a third state-led mobile telecommunications company, Byul (별 in

[22] The *Choson Sinbo* is a pro-North Korean newspaper by the General Association of Korean Residents in Japan, published in two language, Korean and Japanese. The North Korean regime has used the newspaper for its propaganda purpose internationally.

[23] According to Monthly Report on North Korea from ROK Ministry of Unification (April 2009, p. 14), there were at least three types of prepaid phone cards (plans) based on talk time. A, B, and C cards were around $ 0.8, $1.7, and $ 2.5. Even, B and C cards provided 125 and 400 free calling minutes; Contrary to that, NK Tech said that one-minute talk was $ 1. (NK Tech, 2009b)

Korean), [24] which means "Stars," was launched to serve only North Korean natives in 2015 (Seo, 2016, p. 20). Bong-Sik Kim (2017, p. 22) found that these two state-owned companies were founded due for two reasons: to reverse the shortage of foreign currencies and to stop leaks of sensitive information. The first reason involved reducing the outflow of foreign currencies (mainly dollars) to a global company, Orasom (75% share) because North Korea suffers from international economic sanctions. Kangsong Network subscribers can pay North Korean won, contrary to Koryolink, which forces its subscribers to use foreign currencies to purchase extra talk-enabled phone cards (Seo, 2016, p. 19). The second reason is that the North Korea government established its state-owned mobile companies to avoid sharing its sensitive domestic information with the foreign company, which would harm its regime.

According to *Country ICT Data (until 2016)*, North Korean mobile-cellular telephone subscriptions numbered 3,606,000 in 2016 (ITU, n.d.). This translates to 14.21 subscriptions per 100 inhabitants during that year. Although some North Korea experts say the number is exaggerated, others argue that given North Korea's societal and economic situation (which includes black markets[25]), the number is probably correct (Yonho Kim, 2014a, p. 13). The spread of black markets in North Korea contributes to increasing the number of new middle class and rich who can afford to buy mobile phones and to subscribe 3G mobile services (Lankov, 2013, pp. 82–93). In a meeting with South Korean National Assembly lawmakers held on November 5, 2018, the Minister of Unification of South Korea, Cho Myoung-Gyon, who had recently visited

[24] The company, Byul, was an Internet service provider for foreigners residing in Pyongyang before. (Seo, 2016, p. 20)

[25] Officially, the free market system is not allowed in North Korea. Kim family's hereditary dictatorship has kept tight control of a Soviet-style command economy. However, the underground market, called as black market, has become the new normal in isolated North Korea. Ordinary North Koreans sells and buy everything from electronic gadgets and cosmetics, to food and household goods there. For more information on the black market, see Pearson, J. (2015, October 29) and North Korea's Black Market Becoming the New Normal. *Reuters*. Retrieved from https://www.reuters.com/article/us-northkorea-change-insight/north-koreas-black-market-becoming-the-new-normal-idUSKCN0SN00320151029

North Korea several times, testified that there were 6 million mobile-cellular telephone subscribers in North Korea, even though the price of a mobile phone ranged from $100 to $200 U.S. dollars (Yeon-Jeong Kim, 2018). However, he also added that North Korean citizens cannot access the internet with their 3G (or less) mobile devices (Yeon-Jeong Kim, 2018).

Adding even more complexity to this picture, it is clear that some North Korean people use Chinese mobile phones and services illegally near the border with China (Lankov, 2013, p. 97). It is useful for those who have businesses with Chinese and relatives in China. Moreover, it is not a secret that some of them use the Chinese mobile service to contact North Korean defectors living in China, as well as South Koreans (Kang, Ling, & Chib, 2017, p. 2).

In this regard, there are at least three interesting points with respect to mobile infrastructure being a fundamental part of North Korea's offensive cybercapability. First, North Korea's mobile network infrastructure technically enables its subscriptions to access the internet. However, the state does not allow its subscriptions to use the internet literally. In August 1990, the DPRK reached an agreement with the United Nations Development Programme (UNDP) to receive assistance to install nationwide fiber optic cable networks between Pyongyang and other major cities (Ko, Jang, & Lee, 2008, p. 244). It completed the fiber optic cable networks installation by 2002 with the help of UNDP and the investment of Loxley (Yonho Kim, 2014a, pp. 25–6). This fiber optic cable construction has accelerated mobile business, helped the state's internet project designated only for covert national missions, and improved the quality of intranet service for North Koreans in general.

Second, even though North Korea does not have the capability to develop its own mobile network environments—including 3G or higher—it has many skilled professionals who operate and maintain its networks and mobile services. As Yonho Kim argues, "The DPRK relies heavily

on Huawei Technologies, the largest networking and telecommunications equipment supplier in China, for procuring its mobile telecommunications equipment" (2014a, p. 27). North Korean technicians were trained by Orascom, and then were sent to North Korea's local provinces (Fahrion, 2011). North Korea also adopted the Global System for Mobile Communications (GSM) system in 2002 for national 2G mobile telecommunications service and the 3G Wideband Code Division Multiple Access (W-CDMA) standard, which offered higher data transmission rates and greater network security (Yonho Kim, 2014a, p. 25; Noland, 2009, pp. 62–74; Mansourov, 2011, p. 10). These technologies strengthen ICTs and cyberoperations among these professionals who could become potential state-sponsored hackers.

Third, North Korea's mobile service subscriptions are allowed to access cyberspace that is literally limited. On the one hand, North Koreans can use North Korea's national intranet with their mobile data plans. Koryolink began to provide free Short Message Service (SMS) in the second quarter of 2009 and video calling service in 2010 (OTMT, 2012, p. 93; Seo, 2016, p. 19). It also offered Multimedia Messaging Service (MMS) to its subscribers in January 2011; Koryolink also provided optional voicemail, Wireless Application Protocol (WAP), and High-Speed Packet Access (HSPA) (OTMT, 2012, p. 93). Kangsong Network also has a similar capacity and service offerings (Seo, 2016).

On the other hand, foreign visitors to North Korea, such as tourists and correspondents, have been able to access some internet services, such as Twitter, Instagram, Skype, and Facebook (Dewey, 2013) via mobile phones since 2013. For example, on January 19, 2016, a foreign correspondent, Jean H. Lee, used to upload photos and comments to her social networking services by her phone about events that happened in North Korea (Jean H. Lee, 2016). This means that despite its low service and speed quality, North Korea has a normal mobile network

infrastructure that can access the internet. Yet ordinary North Korean mobile subscribers are not allowed to use internet-based services at all.

2.3.2 *Internet and Intranet*

North Korean citizens are not allowed to access the internet; allowing them access would threaten North Korea's authoritarian regime. However, they are exposed to a similar virtual world via its well-monitored national intranet. The intranet service is not perfect, but it is sufficient enough to support ICT professionals who are potential cyberwarriors. Moreover, unlike its hermit kingdom image, the North Korean regime has its own and borrowed IP addresses that enable it to participate in diverse activities of the virtual world. North Korea can also use these IP addresses for its online propaganda activities as well as hostile cyberoperations which advance its national interests. The development of North Korea's internet and intranet illustrates the state is not entirely isolated from the virtual world.

The internet enables ordinary citizens to increase and enhance the exchange of information about themselves and their countries. This fact alone can to threaten authoritarian countries. Some scholars, such as Kyungmin Ko, Heejin Lee, Seungkwon Jang, and Evgeny Morozov, call this the "internet dilemma: (Ko et al., 2009, p. 281) or the "dictator's dilemma" (Morozov, 2011). While the internet is regarded as a desirable way to improve the national economy, it is understood as a potential means to threaten authoritarian regimes by transferring political sensitive information from the outside world to citizens, thereby arousing political awareness and providing platforms for organizing movements (Boas, 2000, p. 57). Thus, although there is little evidence that the internet has been a real driver to turn authoritarian regimes into a democracy (Ko et al., 2009, p. 281), most authoritarian countries are reluctant to allow their citizens to access the internet, especially social media sites, without any barriers, such as online censorship

(Kerr, 2014, p. 5). Even, most North Korean citizens have never used the internet for their personal and business purposes under the world's most restrictive policy on internet access (Kerr, 2014, p. 5). However, the restrictive way of North Korea does not necessarily mean that the alleged hermit Kingdom itself does not have internet infrastructure at all.

Contrary to its internet issue, North Korea has created interconnections in North Korean society through nationwide intranet service, Kwangmyong, (광명 in Korean), which means "bright light." This state-controlled intranet service was built in November 2002, based on the aforementioned fiber optic cable network for telecommunications constructed in the 1990s (Bruce, 2012, p. 2; Chen, Ko, & Lee, 2010, p. 651; Lee & Hwang, 2004, p. 79). Thus, North Koreans can access the intranet via computers and mobile devices inside the country. North Korea is technically equipped to provide internet service for its people. Global IT companies, such as Loxley and Orascom, have helped North Korea build its IT infrastructure for internet service. North Korea's traditional allies, China and Russia, have provided internet connections for the closed state. Nevertheless, North Korea has maintained its strict, closed internet policy. Therefore, ordinary North Koreans are not allowed internet access even though the country has the capacity to do so.

Beginning in the 1980s, North Korea developed its IT infrastructure by focusing on research and education in computer science areas. These research and education projects have been led by mainline ministries, the National Academy of Sciences, and its several newly established research institutes: the Information & Communications Institute, the Institute of Computer Science, the Institute of Information Communication, and the Electronics Institute (Mansourov, 2011, pp. 20, 41). In addition, leading national universities, including Kim Il Sung University; Kim Chaek University of Technology; Pyongyang University of Science; and Pyongyang and

Hamhung Colleges of Computer Technology have played a key role in developing the IT sector (ROK Unification IT Forum, 2015, p. 56). In the 1980s, the project to build infrastructure relied heavily on foreign experts, primarily from Japan and the former Soviet Union (Mansourov, 2011, p. 20).

In the first half of the 1990s, North Korea built private LANs (Local Area Networks)[26] between the National Academy of Sciences, the KWP's main building, Kim Il Sung University, Kim Chaek University of Technology, and the Korea Computer Center (KCC) (Bong-Sik Kim, 2017, p. 29). Those LANs were the first stage in achieving national-level exclusive computer connections, also known as an "intranet." The LANs exchanged information via dial-up connections using telephone circuits (point-to-point protocol) (Mansourov, 2011, p. 21). Thus, these LANs enabled some local governments to share information with central departments in Pyongyang.

Since the latter half of the 1990s, these LANs have been replaced by fiber optic cables which connect cities. In 1996, the Central Information Agency for Science and Technology (CIAST) of the National Academy of Science was designated as the nation's internet Service Provider (ISP). CIAST built the Kwangmyong Intranet, connecting all levels of government institutions (from provincial to national government institutions) with industrial factories; banks; transportation units; agricultural cooperatives; institutions of art and culture; Science & Technology (S&T) and educational institutions; trading companies; and a handful of foreign joint investment ventures (Hachigian, 2002, p. 45). By November 2004, CIAST hosted internal websites, provided access to email, electronic news, a search engine, an electronic library, real-

[26] A local area network interconnects computers within a limited area, such as laboratory, university, office or government building, school, or institute, via the two most common technologies, ethernet and Wi-Fi. It is the opposite of a wide area network (WAN), which extends over a large geographical distance or place.

time dialogue in chat rooms, an electronic market, advertising space, a number of user-created websites, and an entertainment center that streamed movies at over 100 megabit per second (Denning, 2007, p. 202).

The North Korean government has made a continual effort to upgrade its intranet service. For instance, its old cables were replaced in 2006 by more advanced cables from a Chinese company, Changfei Optical Fibre and Optical Cable Company, located in Wuhan, Hubei, China (The Economist Intelligence Unit, 2006, p. 17; Mansourov, 2011, p. 29). In October 2010, the intranet ran on the new fiber optic cable with a backbone capacity of 2.5 gigabytes per second[27] (Sangjoo Park, 2008, p. 70). As a result, most central government offices are connected via the intranet network, which is being extended to regional and local offices (Ko et al., 2009, p. 284). Officials now use email to communicate with one another. However, the intranet is closely monitored by the government. While foreigners have easy access to internet service, they are denied access to the North Korean intranet.[28]

Parallel to these internal developments, North Korea emerged on the international online stage with the creation of the official website for Korean Central News Agency (KCNA) (www.kcna.co.jp) in January 1997 (ROK Ministry of Unification, 2004, p. 17). Since then, several North Korean websites have been opened for two purposes: spreading political propaganda and maintaining commercial interests based in other countries, mainly Japan and China (Ko et al., 2009, pp. 294–95). These North Korean-led websites located abroad were not supposed to connect with its domestic network due to security concerns. First, North Korea

[27] The optical networks, mostly in the internet's backbone, supported speeds of 100 gigabits per second (Gbps) in 2013. In 1990, the the state of the art was around 2.5 Gbps. Thus, North Korea's intranet speed was not fast.
[28] Scott Williams, a foreign lecturer in the computer science department at Pyongyang University of Science and Technology said that he was unable to access Kwangmyong due to state rules. Personal Interview on March 6, 2017.

focused on opening political propaganda websites, including KCNA, *Choson Sinbo* (www.korea-np.co.jp / Created in February 1997 / Japan), People's Korea (www.korea-np.co.jp/pk / Unknown/ Japan), *Pyongyang Times* (www.times.dprkorea.com / July 2000 / Japan), and Uriminzokkiri (www.uriminzokkiri.com / April 2003 / China). According to Table 2.4, however, the focus shifted to commercial websites, such as DPRKorea Infobank (www.dprkorea.com / October 1999 / China), Sili Bank (www.silibank.com / October 2001 China), D.P.R.Korea National Tourism Administration (www.dprknta.com / January 2002 Japan), and Naenara (www.kcckp.net / May 2004 / Germany). This signaled that the authoritarian regime realized the internet was beneficial to the North Korean economy. More interestingly, this pattern shift seems to be a precursor to the government's recent change in focus for cyberoperations from pure political threats to financial-based hacking. The shift, in turn, would contribute to the government's ultimate political interest: regime survival. More details about North Korea's cyberoperations will be discussed in Chapter 3.

Table 2.4. A Brief History of North Korea's Intranet and Internet

Date	Major Events
Jan. 1997	Chosun Tongsin (www.kcna.co.jp): The first official website of North Korean News Agency, Korean Central News for political propaganda *Server: Japan (Yun-Young Kim, 2016, 242)
Oct. 10, 1999	DPRKorea Infobank (www.dprkorea.com): The first official website for commercial *Server: China
May 31, 2001	State-controlled intranet, *Kwangmyong,* was tested in some locations *Around 100 organizations
Oct. 8, 2001	silibank.com started to provide its international email communications service *Server: China
Nov. 2002	The intranet *Kwangmyong* started its service nationally
Jan. 7, 2003	DPRK reached a contract for commercial internet via Korea Computer Center Europe (KCCE) *1 million Euro
July 13, 2003	A website with 'kp' domain name was opened in the intranet
Sept. 19, 2003	DPRK announced its plan to link its own network with international internet networks after having firewall
Oct. 1, 2003	The construction of fiber optic cables was finished in small local cities
Feb. 16, 2004	Private international wireless communications network via satellites was installed between KCCE and Korea Computer Center (KCC), providing internet email and website search services
2006	DPRK began to upgrade its optical fiber cable network with more advanced Changfei cables. (Mansourov, 2011; Kim, Yonho, 2014, 29)
Sept. 11, 2007	A country-code Top Level Domain (ccTLD) 'kp' has been assigned to North Korea by ICANN: KCC was authorized to control internet domains it has
Since 2010	China Unicom has provided internet connection for DPRK (Taylor, 2017)
Oct. 10, 2010	KCNA's website (http://175.45.179.68) with 'kp' country domain was directly connected to the internet via its domestic server
Late June, 2011	There are around 13 websites having 'kp'
Since 2011	'kp' domain assigned to Star Joint Venture Company (Williams, 2011): a block of 1,024 internet addresses, reserved for many years for North Korea but never touched, has been registered to the company (Williams, 2010).
Sept. 8, 2017	Russian telecommunications company TransTeleCom became a new internet provider to DPRK (Madory, 2017)

Source: ROK Ministry of Unification, 2004, pp. 15-18; Ko et al., 2009, p. 294; Ko, 2014, p. 79; Bong-Sik Kim, 2017, pp. 29-30.

Meanwhile, three main routes enable North Korea to access the internet. First, accessing the internet via the satellite service of German private companies has been available to North Korea. Several providers from Germany have offered coverage, but it is unclear when the state started to

receive satellite internet service and who is allowed to use the service internally to North Korea. TS2 Space, a satellite telecommunications service provider, has stated that it provides eight different local satellite internet services for North Korea via satellite and Very Small Aperture Terminal (VSAT) and dial-up access.[29] The second route via China Unicom has been available since 2010 (Wagstaff, Auchard, & Kiselyova, 2017). According to Asia-Pacific Network Information Centre (APNIC), the Unicom gave KPTC 256 IP addresses ranging from 210.52.109.0–210.52.109.255.[30] Third, despite the international community's sanctions against North Korea, Russian telecommunications company TransTeleCom (TTK) began to provide an internet connection to the DPRK on September 8, 2017 (Madory, 2017; Williams, 2017). This new, additional provider means that North Korea's access to the internet has become more stable and flexible, thereby increasing its cyberoperations capability.

According to Whois registration data, North Korea uses several IP ranges. When 'kp' was assigned to North Korea in 2007 (IANA, n.d.), North Korea also received four Class C IP ranges,[31] 175.45.176.0–175.45.179.255 (4 x 256 = 1,024 IP addresses in total), from the Internet Corporation for Assigned Names and Numbers (ICANN) (APNIC, n.d.). This block of 1,024 IPs, never touched, was suddenly registered in 2010 to Star Joint Venture, a company with links to the government in Pyongyang (Williams, 2010). North Korea uses these IP addresses via China Unicom who provides 256 IP addresses to North Korea. Then, North Korea moved its KCNA's

[29] TS2 Space is a Poland-based company. For more information about TS2 Space, see the company website, https://ts2.space/en/satellite-internet-form/NORTH-KOREA

[30] APNIC (the Asia-Pacific Network Information Centre) is the Regional Internet address Registry (RIR) for the Asia-Pacific region (Asia-Pacific Network Information Centre, n.d.-a).

[31] IPv4 addresses are 32 bits long (four bytes). An example of an IPv4 address is 216.58.216.164, which is the front page of Google.com. IPv4 IP addresses consist of five Classes: Class A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the Class. Class A, B, and C IP addresses can be used for host addresses. The other two Classes, C and D, are used for other purposes, multicast and experimental purposes. Class C IP addresses range from 192.0.0.0 to 223.255.255.255. The default subnet mask for Class C is 255.255.255.x. There are 254 (2^8-2) host addresses, 2,097,152 (2^{21}) network addresses, and 536,870,912 (2^{29}) total addresses in Class C.

website from ‘jp’ to ‘kp’ domain (http://175.45.179.68) on October 10, 2010, the 65th anniversary of the Korean Workers' Party (KWP). According to Table 2.4., its approximately thirteen websites began to use ‘kp’ by late June 2011.

Table 2.5. IP Addresses Associated with North Korea

IP Network	Number of IP	Real Country	Note
175.45.176.0 - 175.45.179.255	1,024	North Korea	Allocated for Star Joint Venture Co., Ltd. in Pyongyang[32]
210.52.109.0 - 210.52.109.255	256	China	Authorized User: KPTC / Borrowed from China Unicom
5.62.56.160 - 5.62.56.163	4	U.K.	“PoP North Korea” – used by VPN service HMA
5.62.61.64 - 5.62.61.67	4	U.K.	PoP North Korea, Manpo
45.42.151.0 - 45.42.151.255	256	N/A	Manpo ISP NETWORK (OppoBox LLC ROYA hosting)
46.36.203.81 - 46.36.203.85	5	U.S.A.	IAPS Security Services, L.L.C.
88.151.117.0 - 88.151.117.255	256	Russia	LLC “Golden Internet”
172.97.82.128 - 172.97.82.255	128	U.S.A.	“North Korea Cloud” – used by VPN service HMA
185.56.163.144 - 185.56.163.159	16	Estonia	EasyNS-KP VPN service VPNFacile
77.94.35.0 - 77.94.35.24	25	Lithuania	Provided by a Russian satellite company, which currently resolves to SatGate in Lebanon (Insikt Group, 2018, p. 3)
Total Number of IP	1,974	–	–

Source: Asia-Pacific Network Information Centre (wq.apnic.net), Accessed April 26, 2018; Trend Micro Forward-Looking Threat Research Team, 2017.

Moreover, there are additional IP addresses associated with North Korea, beyond its own and those provided by China IP. As detailed in Table 2.5, these IP ranges include: 5.62.56.160–5.62.56.163 (4), 5.62.61.64–5.62.61.67 (4), 45.42.151.0–45.42.151.255 (256), 46.36.203.81–

[32] Its address and other information are Ryugyong-dong, Potong-gang District, +850-2-3812321, postmaster@star-co.net.kp.

46.36.203.85 (5), 88.151.117.0–88.151.117.255 (256), 172.97.82.128–172.97.82.255 (128), 185.56.163.144–185.56.163.159 (16), and 77.94.35.0–77.94.35.24 (25). These blocks of IP addresses are geographically affiliated with the United States, the United Kingdom, Russia, Estonia, and Lithuania. Thus, North Korea has at least 1,974 IP addresses in total. The number of North Korea and its affiliated IP addresses is not as large as those of other countries, notably South Korea and the United States.[33] The wide range of IP addresses, however, is meaningful because it demonstrates that North Korea is not isolated and has the potential to become a member of the global internet community. Above all, it substantiates some technical reports which attributed some aggressive cyberoperations to North Korea based on IP addresses belonging to the state (FireEye, 2018, p. 12).

North Korea's internet and intranet environments prove that it has an adequate base to conduct hostile cyberoperations against the outside world. North Korea is reluctant to allow its citizens to access the internet. Therefore, North Korea has constructed and operated a closed virtual space, Kwangmyong Intranet for its citizens. Though limited in scope and scale, the Intranet is a minimum condition to provide online environments for citizens, especially young people who could become potential cyberwarriors for the state. Like young people outside North Korea, North Korean young generation can also be exposed to a limited, but adequate virtual world that would motivate them to learn computer skills. At the same time, the North Korean regime's intranet can provide a basic foundation for the growth of future hackers.

Meanwhile, although its ordinary citizens have been not allowed to use the internet, North Korea has used the internet to promote its national goals for the last two decades. In the early 2000s, it used foreign servers to promote propaganda and open business websites. Since the late

[33] South Korea has a total of 112,140,992 IP addresses. The United States has a total of 1,598,831,868 IP addresses.

2000s, it has used its own affiliated IP addresses for propaganda and business purposes. Some of North Korea's IP addresses have been suspected of involvement with hostile cyberoperations. Therefore, the development of North Korea's internet and intranet can be understood as a critical sign that the state is not entirely isolated from the virtual world.

2.3.3 *ICT Industry*

Developing a computer-related hardware industry is a key component of building a state ICT environment. Developing software programs is also viewed as a critical part to operate all ICT infrastructure and devices harmoniously. Like other countries, North Korea has focused on developing its own hardware and software industries for the aforementioned reasons under its unique ideology, Juche. As a result, although its ICT industry has not matured, it provides a fundamental base for achieving the state's goals, such as producing and operating ICT devices. North Korea's hardware and software industries can also be a useful tool for conducting propaganda activities and hostile cyberoperations.

North Korea has a long history of developing hardware for the advancement in information technologies. Beginning in 1950, North Korea started to develop IT hardware products, such as semiconductors and computers, after the invention of electronic calculators, as detailed in Table 2.6. North Korea developed its first analogue computer, "Jeon Jin-5500," in the late 1960 (Chan-Mo Park, 1999, p. 150). Korean Chinese scientists who came to North Korea due to the Chinese Cultural Revolution helped to build the first analogue computer (ROK Unification IT Forum, 2015, pp. 35–36). Then, in 1979, Kim Il Sung University built the second-generation computer,[34] known as "Yong Nam San 1" (Chan-Mo Park, 1999, p. 150). Significant progress was made

[34] First generation computers used "vacuum tubes' (1940–1956), second generation used "transistors" (1956–1963), and third generation used "integrated circuits" (1964–1971). (Ullah, 2012)

after an 8-bit PC prototype, "Bong Wha 4-1," was created in 1982 (Chan-Mo Park, 1999, pp. 150–1). During the same period, North Korean scientists started to study semiconductor for making 16-bit and above computers. In 1987, an IC pilot plant was constructed at the Electronics Research Institute of the Academy of Sciences with the help of the UNDP. Since then, the state has manufactured 16-bit, 32-bit, 486 DX level, and more advanced computers on its own.

Table 2.6. A Brief History of North Korea's IT Hardware & Software

Date	Major Events about North Korea's Hardware & Software
After 1950s	DPRK had tried to invent electronic calculators
1969	The first Analogue computer, "Jeon Jin-5500 (전진-5500 in Korean)," was developed
1979	The second generation computer, "Yong Nam San 1 (용남산 1 호 in Korean)," was developed
1982	The first 8-bit PC prototype, "Bong Wha 4-1 (봉화 4-1 in Korean)" was built
1990s	DPRK has started to change its IT focus from hardware to software *Pyongyang Information Center (PIC) and Korea Computer Center (KCC) as the biggest software developing organization were established around 1990
1996	First Word Processing Program, Dangun[35] (단군 in Korean), was developed (Bang Eun-joo, 2018)
1997	Samil Information Center in KCC developed a go[36] computer program (바둑 baduk in Korean), named as 'Silver Star' (Efron, 1999). Its series won several international computer go cups until 2009 (Lee B., 2016).
2000s	Computer gifted and talented schools, such as 'Guemseong Number One secondary school (금성 제 1 고등중학교 in Korean)' were established
Late 2000s	It has begun to develop its own O/S programs *Linux has been taught since the early 2000s *In 2006, a Linux based O/S, 'Red Star (붉은별 in Korean),' was released. Red Star Ver.1.0 (2008), Red Star Ver.2.0 (2009), Red Star Ver.3.0 (2012), and Red Star Ver.4.0 (2017).
2010s	Tablet PCs have come out *In 2012, 'Arirang (아리랑 in Korean)', 'Samjiyon (삼지연 in Korean)', and 'Morning (아침 in Korean)' were made by Factory 511, KCC, and Morning Panda Computer (아침 판다 컴퓨터) *Two more models, '룡흥' and '울림' were released in 2013 and 2014

Source: Chan-Mo Park, 1999, pp. 148–162; The Weekly North Korea, Vol. 686 of ROK Ministry of Unification, 2004.

[35] The first word-processing program's name originated from the birth myth of Korea. In the myth, Dangun was the founder of the first Korean nation.

[36] Go is an ancient abstract strategy board game, which was invented in China more than 2,500 years ago. Two players aim to surround more territory than opponent. See the American Go Association http://www.usgo.org/what-go

In the 1990s, there were two important changes in the ICT industry. First, the DPRK's serious economic hardship led to policy changes regarding ICT hardware development. It reduced its investment in developing its own computers. Instead, the state began to pursue making computers in cooperation with foreign companies. Based on this policy change, the North Korean government established a joint venture in 2001, named "Morning Panda Computer" (아침 판다 컴퓨터 in Korean), between its Ministry of Electronics Industry and China's Panda Electronics Group in order to supply computers to the state at a continuous and stable rate. Even though the joint venture heavily relied on imported Chinese computer components, such as Pentium and more advanced components, Morning Panda Computer has enjoyed its position as one of the main computer and tablet PC producers in North Korea. Therefore, unlike North Korea's claim that it can produce its own computers and tablet PCs, it has only the limited capability to assemble those with imported key parts from the outside world, primarily from China.

Second, North Korea changed its developmental focus on hardware to software in the 1990s (Kim & Lee, 2014, p. 5). It appears North Korea recognized that developing a software industry was cheaper than building a hardware one. In other words, the state chose software among diverse elements of the ICT industry because it does not require ample financial resources; software development requires human capital to develop computer programs. Moreover, the state's view was that software would be more important than hardware in the future. A study by the ROK Unification IT Forum (2015, p. 38) found that "North Korea wants to use software as a way to increase its productivity in the area of economy and industry." It also found that "software is understood as one of the products, which should be circulated in every field of the

society, as well as one of the export goods for trading with other countries" (ROK Unification IT Forum, 2015, p. 38).

With its new focus on software policy, North Korea has sought to increase ICT human capital with organized education programs, to strengthen its control mechanism on software development institutions, and to grow its public interests on the importance of software programs (ROK Unification IT Forum, 2015, p. 38). Two centers established around 1990, the Korean Computer Center (KCC) and the Pyongyang Information Center (PIC), have also played a key role in developing the software industry, alongside the National Academy of Science, Kim Il Sung University, Kim Chaek University of Technology, and Pyongyang Computer University.

This policy shift has led to advancements in North Korea's software industry. Beginning in the late 1990s, the state's software industry received public attention with its Asian-style chess programs. Samil Information Center in KCC developed a Go computer game named "Silver Star" (Efron, 1999). Until 2009, the Silver Star series won international computer Go Game World Cups several times.

Since the mid-2000s, North Korea has started to release its own computer operating system (OS) that is designed for operating personal computers as well as servers according to the directive of Kim Jong Il in 2002 (Korea Development Institute, 2001, 65). Before that time, computers in North Korea had used Red Hat Linux[37] and Windows operating systems. In May 2018, Statcounter's chart said that North Korea's computers, tablet PCs, and mobile devices primarily use Western operating systems (98.8%), including Windows (77.54%), Android (16.51%), iOS (2.41%), OS X (2.16%), Linux (1.25%), and a small number of "unknown"

[37] Contrary to Windows or MacOS, Linux is a family of free and open-source software operating systems (O/Ss) based on UNIX. Red Hat Linux is one of Linux O/Ss. Red Hat Linux was created in 1994.

(0.12%) (StatCounter, 2018b).[38] Despite uncertainty about these statistical results, it is clear that North Korea started to develop its Linux-based OS, "Red Star," in 2006 to avoid using Western countries' operating systems, especially those operating systems from the United States. This development occurred for two reasons. First, OSs from foreign countries are sometimes not compatible with some North Korean software programs (Jong Sun Kim & Choon-Geun Lee, 2014, p. 6). For example, Windows OS does not provide some functions, such as North Korean-style Korean language fonts.[39] Furthermore, the North Korean regime has computer security concerns about Western OSs systems being able to conduct surveillance on the regime and North Korean society. According to a Korea Internet and Security Agency (KISA) report (Kang, 2018, p. 45), some computer experts believe Red Star OS is used for critical computers or servers which must be secured.

Since 2006, the North Korean government has released several commercialized versions of the Red Star operating System: Red Star 1.0 in 2008, Red Star 2.0 in 2009, and Red Star 3.0 in 2012. As of late 2017, Red Star 4.0 was being tested. One of North Korea's propaganda websites, SoGwarng (서광 in Korean), uploaded a video clip about the 28th National Exhibition of IT Successes 2017, which verifies that North Korea has begun to build servers via Red Star 4.0 (Kang, 2018, p. 45). It is known that the website of Air Koryo, North Korea's state-owned national flag carrier airline, is hosted on a Red Star 4.0-based server located in Pyongyang.

Several applications, including a web browser, text editor, anti-virus programs, and games have been embedded in Red Star OS. A modified Mozilla Firefox browser, called Naenara

---

[38] Statcounter says that Windows accounted for 95.64% of desktop operating system market share in May 2018, in North Korea. OS X, Linux, and unknown only covered 2.67%, 1.54%, and 0.15%.

[39] The two Koreas use same language, Korean. They can communicate each other in general. However, the Korean language has changed between the two Koreas due to their long separation since the Korean War in 1950. Western software programs, including O/Ss, such as Windows and MacO/S, provide only Korean Language based on South Korea's standard for their users.

(내나라 in Korean), which means “My Country,” enables users to browse the Naenara portal on Kwangmyong Intranet. The browser comes with two search engines. Red Star OS runs Wine, a piece of Software that allows Windows programs to be run on Linux. Moreover, Red Star 3.0 supports both IPv4 and IPv6 addresses. Computer scientists believe that Red Star 1.0 and 2.0 resemble Windows XP (Williams, 2014). They also say that Red Star 3.0 appears most reminiscent of MacOS (Sparkes, 2014). These findings demonstrate that North Korean people could use Windows and Mac Applications, and then access the internet via their Linux-based OS, Red Star, if the North Korean government would allow them to do so.

North Korea also specializes in some following fields in the software industry: language processing, cryptographic, recognition, and animation technologies (Sun-Ae Kim, 2007). These fields have emerged due to North Korea’s unique historical and political context. It is possible that many Russian- and Chinese-language experts in North Korea have contributed to the advancement in computer language processing. Developing cryptographic technology may be associated with core technologies imported from the Soviet Union and East Germany during the Cold War. It is also likely the state has spent its efforts on computer animation in order to advance its propaganda strategy. In this context, it has also tried to develop computer educational game programs. Notable programs in these sub-fields include Woorimal OS; Korean language input and output support systems; Korean language grammar correction programs; translation programs; fingerprint scanning programs; facial recognition software; medical check-up programs; dictionary programs for several languages; Go game programs; banking programs; and factory automation programs. Surprisingly, these programs not only target domestic audiences, but international audiences as well (including South Korea); the programs are

compatible with Red Star OS, other Linux OSs, Microsoft Windows OS, and MacOS (ROK Unification IT Forum, 2015, pp. 38–9).

More recently, North Korea has turned its attention to developing tablet PCs, along with the aforementioned software programs for every ICT device. In 2012, its first three tablets were released: Samjiyon by KCC; Morning by joint venture Morning Panda Computer; and Arirang by Pyongyang Technology General Company (평양기술총회사 in Korean). These are all Android-based tablet computers. Each has different Android versions, features, and functions. These tablets can access networks like the intranet only via external USB cables because they do not have Wi-Fi access. In 2013, Arirang was replaced by Woolim (울림 in Korean), which means Echo. The replacement marked the first time a North Korean tablet had a Wi-Fi feature. Since then, new, lighter versions of Samjiyon and other tablet PCs have been released with additional applications and features. However, despite North Korea's efforts, these tablet PCs are relatively low in quality. They are not compatible with many other software programs. Moreover, they are assembled only with imported components from other countries, mainly China (Kim & Lee, 2014, p. 19).

In sum, unlike its closed image, North Korea has put effort into developing its ICT industry. Although its sluggish ICT infrastructure development is due to the fact it is a closed state, it does have its own domestic intranet infrastructure. Moreover, North Korea has better software technology than hardware infrastructure. The underdevelopment of the hardware industry was due largely to financial constraints. Therefore, the state has focused more on the software industry, along with developing ICT human capital that will be discussed in the following section. Meanwhile, North Korea's ICT industry can be viewed as a sufficient tool to achieve its

national purposes, producing and operating basic ICT devices with which it conducts propaganda activities and hostile cyberoperations.

2.4 Development of Human Capital

Although North Korea's ICT infrastructure is comparatively advanced beyond some other countries, the state has moved slowly into the information age. Since the mid-1980s, its state-led education system to cultivate ICT human capital has played a vital role in the advancement of the ICT sector. Since Kim Il Sung visited the Soviet Union and its satellite states in 1984, gifted schools have been established to focus on nurturing talented students in science. Beginning in the 2000s, its gifted secondary schools offered special classes only for talented ICT students. After these students graduate, they are sent to computer science departments at top North Korean universities. It would be unfair to categorize everyone in the educational system, however, as hackers who have targeted networks around the world. Nevertheless, they can be viewed as a potential future indirect or direct resources for promoting national interests through North Korea's cyberoperations.

2.4.1 *Emphasis on the Elite Education System for Human Capital*

North Korean defectors and the South Korean National Intelligence Service (NIS), have claimed that North Korea emphasizes the importance of cyberwarfare. One defector, Kim Heung-Kwang, said that Kim Jong Il began to prepare for cyberwarfare after witnessing the Gulf War (Aug 2, 1990–Feb 28, 1991), which was recognized as the first large-scale war that relied significantly on computer and communications technologies, including electronic devices (Jun, LaFoy, & Sohn, 2015, p. 31). After graduating from Kim Chaek University of Technology, Heung-Kwang joined the computer science department at two universities (Sangwon Yoon,

2011).[40] Although his claim about North Korea's cybercapability and its origins were cited by several academic as well as news articles,[41] it is difficult to prove whether it is true. However, in a secret meeting with lawmakers of South Korean National Assembly's Intelligence Committee, a NIS chief testified that Kim Jong Un reportedly declared that "Cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly" (Sanger, Kirkpatrick, & Perlroth, 2017). If this is true, it reveals motivations behind North Korea's current cyberoperations. It is also impossible, however, to verify the source of NIS's claim.

Even though it is difficult to ascertain the North Korean elite's perception of cyberwarfare directly, the origin of the state's cybercapability can be traced to the emphasis on education programs to nurture talented computer students. Kim Jong II stressed that gifted computer students should be identified and trained at a young age. In 1997, Kim Jong Il said that "do not hesitate to ask for anything for developing computer technology" (Kim Jong Il, 2000, p. 296). In January 2001, he stated that "the late twenties are already too late to be a computer programmer. Smart teenagers should be trained as computer scientists in secondary schools" in a meeting with leaders from the Central Committee of the Workers' Party of Korea ("Foster many specialized people," 2003). Thus, in line with Kim Jong Il's wishes, an education doctrine for gifted computer students was enacted in December 2000 ("Foster many specialized people," 2003). Sang-Jung Byun (2011), an expert on North Korea's science and technology policy, said that

[40] While a short North Korean propaganda documentary declined Kim Heung-kwang's arguments and knowledge about North Korea's cyber capability, it verified at least his real identity as a member of computer science departments in two universities, North Korea (*Ugly person Kim Heung-Kwang in an academic scholar's skin*, 2016).

[41] His claims have been cited by major global new outlets, such as the *New York Times*, Reuters, NBC, the *Independent*, AlJazeera, and so forth (Harrison, 2017; Hodge, 2017; Lee & Kwek, 2015; Park & Pearson, 2017; Sanger, Kirkpatrick, & Perlroth, 2017; Wilford, 2017; Sangwon Yoon, 2011). Then, several cybersecurity experts cited his claims too (Jun, LaFoy, & Sohn, 2015, p. 31; Pinkston, 2016; K. S. Yoon, 2011;.).

Kim Jong Il pointed out that one historical cause of socialist state collapse was their failure to adapt to global changes from the information and communications revolution (pp. 175, 183).

The North Korean elite agreed with Kim Jong Il's plans. Su-Rak Lee, Chief of the Center for Educational Information in North Korea, claimed that North Korea's social progress will be determined by the development of human capital in the information age (Su-Rak Lee, 2003, pp. 39–41). According to Su-Rak, North Korea tried to increase its number of experts in information and technology to 100,000 in the short future (Su-Rak Lee, 2003, pp. 39–41). In this regard, North Korea has preferred gifted and talented education to public education in order to achieve its goal of having sufficient ICT human capital (Yoo & Ko, 2004, pp. 19). It can be considered as a way to contribute to not only North Korea's national economy, but also its cyberoperations, whether the state intended to prepare for cyberwarfare or not via state-led gifted and talented education system.

2.4.2 *The Number One Secondary School System and Cyber Human Capital*

In a Moscow Television Service interview on March 22, 1984, roughly the same period as Kim Il Sung's visit to the country, Vice President of the U.S.S.R. Academy of Sciences, Yevgeniy P. Velikhov,[42] stated that "We [the Soviet Union] are currently in transition, where a real revolution is occurring in the sphere of information science and computer technology" (Wellman, 1989, pp. 7–8). Velikhov also recognized that computer science and information technology, which won its place in science, was gradually winning its place in the national economy (Wellman, 1989, p. 8). However, the U.S.S.R. was far behind its Cold War enemy, the United States: "By one Soviet estimate, America's electronic marvels will make roughly 50

[42] Yevgeniy P. Velikhov founded the Department of Informatics, Computer Technology, and Automation in 1983.

billion more computer calculations per day than Soviet machines in 1990—a technological gap that is expected to widen dramatically by the turn of the century" (Wellman, 1989, p. 8). Therefore, the Soviet Union tried to boost its computer industry via the transition to a computer-literate society in order to reduce the ICT gap with the West (Wellman, 1989, pp. 125–126). Youth-education programs were understood as the key to this transition project.

North Korea was not far behind the Soviet bloc in this new transition movement to a computer-literate society in the 1980s. Its computer technology reformation began with the field of electronic engineering; the field was viewed as centrally important technology before the rise in popularity of personal computers. Electronic engineering departments' curriculum in all North Korean universities was updated due to the transition movement in 1983 (Song, 2005, p. 5). In 1984, some colleges of electronic computers were founded in major cities, including Pyongyang and Hamheung (Chan-Mo Park, 1994, p. 22). Shortly thereafter, in 1986, a computer center was established at Kim Il Sung University (Song, 2005, p. 5). More interestingly, after Kim Il Sung witnessed the importance of ICT in his visit to the Soviet Union and other Eastern Europe countries, North Korea began to establish gifted schools for talented science students in 1984. Since the 2000s, these "Number One secondary schools" have been the primary institution to nurture ICT human capital, along with computer science departments at top universities, such as Kim Il Sung University, Kim Chaek University of Technology, the Command Automation University, and others in Pyongyang, Hamheung, or Huichon. Furthermore, some of the ICT human capital could be categorized as employees of cyber units in public as well as 'technically' private areas for North Korea associated cyberoperations.

North Korea has directed its limited resources to Number One secondary schools to cultivate human capital skilled in science, including computer technicians. Its school system consists of

two levels. The four-year elementary-level primary school is called a “people’s school.” The six-year secondary school is a combined middle and high school. The second level also includes the Number One secondary school designed primarily to foster gifted and talented science students. Few of these schools focus on foreign languages, arts, or music. In an April 1984 address to leaders and officials working the education field, Kim Jong Il said that “the Pyongyang Number One Secondary School should be well developed for gifted students, and then the system will be generalized across the state in order to improve the average quality of all secondary schools” (Kim Jong Il, 1998, pp. 77–78).

Following the establishment of the first Number One secondary school, the Pyongyang Number One Secondary School in September 1984, twelve Number One Secondary Schools opened in 1985 in some provinces and major cities under the direct control of the central government (Cho, 2004, 58-9; Hyo-Sook Shin, 2015, pp. 17–18). Since then, approximately 200 of these schools were opened by 1999 (Song, 2005, p. 11). The schools accounted for 4.13% of 4,840 secondary schools in 2000 (You-Yeon Kim, 2014, p. 19). While a small town or city usually has only one of these, Pyongyang has several. It is known that the Pyongyang Number One Secondary School has 1,000 students, while 400–600 students have been registered in other local Number One schools. In 2008, however, the number of the gifted schools dropped to around ten from approximately two hundred for two reasons. The first reason is to increase the quality of the gifted school (You-Yeon Kim, 2014, pp. 38–43). The second is to reduce the gap between gifted and ordinary schools (Chae, 2013). Despite the decrease, the ten schools have been still employed as centers for top young and gifted computer students.

Principals of primary schools select students on an academic basis for admission to Number One Secondary Schools. There is a hierarchy of gifted schools, starting at the bottom with small

towns, then to major cities, provinces, and finally to the capital of the DPRK. In other words, top students who win science, math, or other important competitions go to the gifted schools located in the capital, Pyongyang, at the top of the educational pyramid. Students in the gifted schools use special science and foreign language textbooks written by teachers who have graduated from top universities, such as Kim Il Sung University and Kim Chaek University of Technology. Kim Jong Il created sets of goals for students in gifted schools. For example, they should be trained to make several types of radios by themselves and to read foreign language books with ease ("North Korea's Gifted School, 'the Number One Secondary School,'" 2001). He also emphasized the final goal which was for these students to be eligible to be admitted to top universities after graduation. The capability of these students can be verified with some success stories. Some gifted students from the gifted school system, especially Pyongyang Number One School, have been awarded prizes in many domestic as well as International Mathematical Olympiad competitions (Sung-Jin Kim, 2009; Chae, 2013).[43]

Above all, Number One Schools have played a key role since the 1980s in training talented computer students who will eventually work in the ICT sector. In the late 1980s, gifted schools began to teach six-year computer-related courses as a part of the regular curriculum for everyone, while ordinary secondary schools had to wait until 1998 to have two-hour computer courses per a week for students in the 4th grade or above (You-Yeon Kim, 2017, p. 38). In the late 1990s, North Korea launched its intensive computer education program for selected students from across the country. After attending a national competition for computer programming in February 1998, Kim Jong Il ordered the establishment of a human capital IT training system for

[43] Team North Korea ranked top ten seven times at International Mathematical Olympiad since 2007. For more information, see the official website of the International Mathematical Olympiad. https://www.imo-official.org/country_team_r.aspx?code=PRK

improving the software industry (KDI, 2001, p. 65). Since then, in line with his emphasis on software advancement, a special computer major began at Pyongyang's Guemseong Number One and Two schools in 2001, schools originally designed for gifted arts and music students (Cho, 2004, p. 64). Only 100 students are admitted by each school's computer major every year (Chung, 2006, p. 70). Thus, being allowed to enter the special computer major classes was understood as an honor for the student, their family, and even for their town. For example, in 2001, when two students who studied in a local Number One Secondary School were admitted to the special computer major at Guemseong Number One School, their local county was honored and bought school supplies and daily necessities for the students ("Bless Young Heroes in the Information Age,"[44] 2001).

North Korea's dictators and elite groups have focused heavily on computer training programs and courses for gifted teenagers in Number One secondary schools, especially Guemseong Number One and Two. Although North Korea suffered from serious economic difficulties in 2001, 1,300 personal computers were sent to Guemseong Number One and Two schools (Nam, 2002, p. 90). According to Kyung-Joon Song's research (2005, pp. 8–9), Pyongyang Number One School had around 100 computers, while Number One Schools in Hamheung, known as the second city in the field of science, had less than 20. This means that other local Number One Schools had less than ten computers. In addition, gifted students in Guemseong Number One and Two Schools were allowed to access Kwangmyong Intranet frequently via their school computers in order to share data with teachers and to search for information related to their studies ("Young Heroes for the Information Age Are Growing," 2001; Nam, 2002, p. 76). Finally, Kim Jong Il sent extra gifts, including new school buses and

[44] The *Kyowon Sinmun* (교원신문 in Korean) of North Korea can be translated as the "*Teachers' Newspaper*" in English.

equipment, to the two schools to demonstrate his attention to the computer majors at Guemseong Number One and Two Schools ("Dear Leader Kim Jong Il Sent Gifts," 2001; "Dear Leader Kim Jong Il Provided," 2002).

The level of computer education at a Number One secondary school is higher than the standard expectations of computer education around the world. In general, gifted computer students are supposed to write computer algorithms and to create programs. At a July 2003 visit to Youngwoong Ganggye Jangjasan Number One Secondary School, Kim Jong Il stated that "they should be trained to create computer programs, rather than to type texts only" ("Fly Higher," 2003). Moreover, the special computer major in Guemseong Number One and Two Schools are designed to foster computer geeks. According to a 2001 interview with Lee Chang-Yeon, vice principal of Guemseong Number One School, "special computer major classes for gifted students in his school was established to cultivate computer addicts who will astonish the world by creating their creative programs via only coding programs and computers" ("We Aim to Train World Best Students," 2001). Even Kim Jong Il's directive said that in order to focus on computer courses, gifted students are only required to take a minimum of regular coursework, including major courses, DPRK's revolution history, mathematics, and foreign languages; they are exempt from other less important courses, such as basic science (Kim Jong Il, 2013, p. 356).

Table 2.7. Courses of Special Computer Major in Guemseong Number One & Two Schools

Subjects	Level	Hours (Yearly)	Sub-total
Computer Circuit and Peripherals	1	80	560
C and C++ Languages	1	280	
Windows Operating Systems	1	200	
Computer Math	2	120	680
Data Structures and Algorithms	2	200	
Visual dBase and Access	2	180	
Linux Programming	2	180	
Artificial Intelligence (AI) Language: lisp & prolog	3	120	420
Natural Language Process and AI	3	160	
Computer Communications and Networks	3	140	
Total	1,660 hours		

Source: Song, 2005, p. 14.

Table 2.7 shows well how the North Korean regime trained its teenager computer programmers with the state-led intensive education programs in the 2000s. Those core computer courses can be categorized into three goals (levels) by grade (Song, 2005, pp. 14–15). First, gifted students in the two schools were taught basic courses to increase their understanding of computer fundamentals during their first and second years at school. Second, third- and fourth-year students were required to take advanced courses in computer application programs. For the third level, fifth- and sixth-year students were called to reduce the gap between theory and practice. It is known that senior students and teachers tried to develop their own computer programs together based on the curriculum (“Support the Training Program for Computer Gifted

Students," 2008).[45] Then, many of the well-educated teenagers in the special computer major in the two Guemseong Gift Schools will continue to study advanced computer courses in computer science departments, top universities. As computer science develops, those courses could be replaced by new ones. Regardless of technological advancements, however, the schools still maintain similar processes to achieve the same goals.

North Korea still focuses on computer education courses for its young. For the last ten years, it has been difficult to access details about North Korea's computer education programs and textbooks for foreign scholars due to the rapid deterioration in relations between North Korea and other countries, following the North Korea's nuclear program development. According to its new 2012 curriculum for ordinary students, however, computer-related courses are viewed as important. North Korea increased the number of its mandatory education years from eleven to twelve, which consists of one-year kindergarten, five-year elementary school, and six-year secondary school, because it increased elementary school years from four to five. At the same time, it divided six-year secondary school into three-year basic and three-year advanced middle schools in 2012.[46] Despite the change, the state maintains its emphasis on computer education. Specifically, fourth- and fifth-grade students in elementary school have one-week computer classes every year. Middle school students have two weeks of information technology classes per year. First-year students in advanced middle schools are required to take information technology courses for two hours a week. Sophomore and junior students have information technology

[45] In March 4, 2004, the *Kyowon Sinmun* changed its name to the *Kyoyuk Sinmun* (교육신문 in Korean) that can be translated as the Education Newspaper.

[46] For more information, see North Korea: Education Systems at the Information Portal on North Korea of ROK Ministry of Unification (n.d.-b). http://nkinfo.unikorea.go.kr/nkp/overview/nkOverview.do?sumryMenuId=CL400

classes for one hour a week.[47] Furthermore, North Korea still operates a few but high-quality Number One secondary schools with special computer majors.

2.4.3 *North Korea's Higher Education Institutions for ICT Human Capital*

North Korea's higher education institutions, especially universities, have played a key role in providing advanced computer training programs for young ICT experts who come from Number One secondary schools across the country. In line with establishing Number One secondary schools in the mid-1980s, the North Korean government began to create independent departments, schools, and colleges of computer science in universities in the 1960s and 1970s on the basis of existing electronic engineering and mathematics schools, where students could enroll in basic computer-based courses, such as Computational Mathematics, Fortran Programs, Electronic Computers, and Computer Programs (Chan-Mo Park, 1999, p. 155; Song, 2005, p. 15). For instance, Colleges of Electronic Computers were established in major cities around 1985 (Chan-Mo Park, 1994, p. 22). Since then, the North Korean regime established a series of important higher educational institutions, such as Pyongyang Program School in 1985, [Computer] Information Centers in Kim Il Sung University and Kim Chaek University of Technology in 1997, two Computer Universities in Pyongyang and Hamheung in 1999,[48] and Colleges of Computer Science in the top universities in the 2000s (J.-A. Cho, 2004, p. 64). In other words, North Korea's technology-based colleges have played significant roles in training ICT human capital.

---

[47] For more information, see North Korea: Education Systems at the Information Portal on North Korea of ROK Ministry of Unification (n.d.-b). http://nkinfo.unikorea.go.kr/nkp/overview/nkOverview.do?sumryMenuId=CL400

[48] Two Computer Universities was established in 1999. They started to operate their regular education programs in 2000 (Kyung-Joon Song, 2005, p. 18).

North Korea's higher educational institutions for ICT human capital are divided into three goal-based categories. Firstly, the top tier category includes core institutions to train top talented and gifted computer students. This highest tier includes Kim Il Sung University, Kim Chaek University of Technology, Korea Computer Center (KCC)'s College of Information Technology, Pyongsong College of Science, and Kim Il Military University, known as Mirim (Automation) University. In the second tier, there are two Computer Universities in Pyongyang and Hamheung for mid- and high-level ICT experts. Lastly, low-level ICT engineers or technicians have been trained in ordinary several local engineering colleges, such as Huichon University of Telecommunications (희천체신대학 in Korean), Sariwon Geology University (사리원지질대학 in Korean), Pyongyang University of Publication & Printing Industry (평양출판인쇄공업대학 in Korean), Hamheung University of Chemical Industry (함흥화학공업대학 in Korean), Sariwon Industry University (사리원공업대학 in Korean), and Rajin University of Marine Transport (라진해운대학 in Korean).

The aforementioned goal includes a focus on the top five colleges offerings in advanced intensive computer education training courses to talented and gifted students who mainly graduated from top Number One secondary schools. More specifically, the curriculum of these computer colleges is directly connected to top Number One secondary schools. For example, students from Guemseong Number One and Two secondary schools are exempted from a one-year preparatory course required for every new student in Kim Il Sung University and Kim Chaek University of Technology because some of their secondary school classes, such as computer, basic science, and foreign language, are recognized as the equivalent to the preparatory course (Song, 2005, p. 17). As an interesting side note, some students at these top

colleges are awarded a special chance to be exempted from mandatory military service (Choon-Geun Lee, 2014). This is an important, if indirect, point about these top programs.

The top five colleges are also divided into three sub-groups: (1) Kim Il Sung University; (2) Kim Chaek University of Technology, KCC, and Pyongsong College of Science; and (3) Kim Il Military University. Kim Il Sung University is the best college in North Korea in terms of every field, such as its reputation, the quality of teachers and students, and the curriculum. Its graduates have been automatically seen as national leaders. Therefore, only gifted students with "good" family backgrounds, are admitted to the university. Many members at the top of the North Korean elite, including Kim Jong Il and Kim Jong Un, are alumni of Kim Il Sung University. It is therefore expected to have excellent faculty, academic resources, and students. Since 1999, its talented computer students have been trained in the College of Computer Science, which was originally the Faculty of Automation in 1977 and the Faculty of Computer Science in 1997.[49] The university established the Information Center in 1997 that supports computer education activities and develops software programs for the College of Computer Science. It also has the Information Technology Institute, described to serve the following functions:

> [A]ims to positively contribute to the digitization and modernization of education and scientific research in the university and national economy by closely combining scientific research on information technology with software development and update the country's information industry. It tries to introduce diverse IT products into international markets. It dominates local market in the field of IP phone service system, vaccination program, face

[49] For more information, see the website of Kim Il Sung University. http://www.ryongnamsan.edu.kp/univ/success/depart/11

> information processing system and online meeting system and its face information processing technology can match the world's quality products.[50]

Thus, as the potential national leader graduates of Kim Il Sung University go to KWP, military, universities, KCC, and other higher level entities in the society (ROK Unification IT Forum, 2015, pp. 73, 83).

The second goal-category includes sending some gifted computer students from top Number One secondary schools to the College of Computer Science, Kim Chaek University of Technology, the College of Information Technology, KCC, or Pyongsong College of Science. Kim Chaek University of Technology is the number one technology university specializing in engineering. As a research center, KCC plays a key role for developing ICTs and managing ICT infrastructure. It also has the three education programs, the College of Information Technology, the Ph.D. School, and the Information & Technology Professional School (Song, 2005, pp. 26–27).[51] Pyongsong College of Science also trains selected computer students who pass its own math, physics, and foreign language tests at least two times (Song, 2005, p. 29). These three schools have solid educational infrastructure, programs, and systems for gifted students served by quality researchers and research centers. Bright students who are not at the top of their class, but have good family backgrounds are allowed to enter these schools. Graduates become field computer scientists who work at KCC, the Academy of Science, computer-based research centers, or other state-led ICT companies (ROK Unification IT Forum, 2015, p. 72).

---

[50] For more information, see the website of Kim Il Sung University. http://www.ryongnamsan.edu.kp/univ/success/institute/27

[51] The College of Information Technology is for undergraduates. The Ph.D. School trains Ph.Ds. The Information & Technology Professional School is viewed as the re-education organization for ICT experts and technicians who have already a lot of work experience.

In the third goal-category stands Kim Il Military University, also known for playing a key role in fostering military ICT human capital. It was established based on Mirim (Automation) University, a military academy. Thus, it is sometimes called its old name, Miram or Mirim Automation University. It is suspected of cultivating cyberwarriors who work in the North Korean military in cyberoperations, including the areas of electronic warfare, cyber espionage and intelligence, and hacking (Sunny Lee, 2011, p. 8; Feakin, 2013, p. 72).

Secondly, North Korea has trained its mid-level computer experts to build its ICT industry, mainly focused on hardware, via two Computer Universities in Pyongyang and Hamheung. When North Korea established several intensive computer education programs in universities in the 1980s, two colleges of Electronic Computers were opened up in Pyongyang and Hamheung (in 1985). One of the two shifted its name from Pyongyang College of Electronic Computers to Pyongyang Computer University in December 1999. It was first called the Pyongyang High Physics School in 1960, Pyongyang High Physics Special School in 1974, and then Pyongyang High Electronic Computers Special School in 1977 (Cho, 2012b). Hamheung Computer University (named in 1999) was originally Hamheung College of Electronic Computers (Cho 2012a). These two universities were designed to train computer experts only. They also have a preparatory college program, which includes students selected in the 3rd grade of Number One secondary schools. After finishing the preparatory college program, these students enroll in the regular major at the computer universities or computer science departments in other top universities, including Kim Il Sung and Kim Chaek universities (Choon-Geun Lee, 2014, p. 20). However, there is evidence to suggest that the level of these two schools is lower than that of previously discussed top universities. First of all, the curriculum is focused on hardware, rather than software (Song, 2005, p. 29). This means that after graduating, most students in the

universities go into jobs focused hardware, instead of software ones which are of primary interest to the North Korean government. Their students also primarily come from local Number One secondary schools, which are behind those in Pyongyang. Third, these universities lack doctoral programs. In other words, as teaching-based universities, these institutions are limited in their capacity to cultivate high-quality ICT human capital. Finally, the quality of the faculty in the two universities are also behind that of the faculty in the aforementioned top universities. One official propaganda video clip revealed that Hamheung Computer University has very few faculty members with a Ph.D. (*Ugly person Kim Heung-Kwang in an academic scholar's skin*, 2016).

Lastly, computer science or computer-related departments in ordinary universities are in charge of training low-level ICT human capital. These schools do not have intensive courses and adequate computers for students. Also, they have limited academic resources, including faculty. Moreover, the universities in this last category are severely limited in their capacity to foster ICT human capital because they are mainly located in local areas (Choon-Geun Lee, 2014, p. 22). Students in these schools are just required to take several basic-level computer courses. Thus, they are not recognized as computer programmers. As technicians or ICT-skilled people, these graduates work in several industries: factory automation, transportation, power plants, among others. Huichon University of Telecommunications, which is located in a local industrial area, is a good illustration of this last category. The university changed its name from Huichon University of Technology in 2003 in order to signal its aim to develop ICT human capital. Contrary to the universities in the two other categories, universities in this category try to balance theory and practice in order to prepare students who will enter these ICT fields in the future. Thus, having work experiences is more important than increasing computer programming skills for students at these universities (Choon-Geun Lee, 2014, p. 22).

2.4.4 *Kim Jong Un's ICT Policy for Cyber Human Capital*

Since the 1980s, North Korea has created state-led intensive educational systems to foster an ICT elite. It selects gifted and talented teenagers, and then provides special programs for them. First, these young people are trained at the Number One secondary schools. Then, they are taught advanced computer courses at top universities. This appears to be an efficient way to cultivate many ICT experts in North Korea, which has limited financial, educational, and infrastructural resources. However, the development of this system raises two critical questions: where is the ICT human capital and what is the ICT human capital doing in the state?

Given its small ICT industry and the international economic sanctions against it, North Korea does not have a sufficient number of jobs to hire all of the ICT experts who graduate from this intensive elite education system. This means that some experts could work in cyberoperations that work toward achieving North Korea's national interest: regime survival. Moreover, the state can mobilize programmers who work in state-led companies for the purpose of cyberoperations because there is no clear line between public and private in North Korea. A story about a North Korean defector who worked in North Korea's private ICT sector demonstrates this reality (Sam Kim, 2018). The defector had a good family background and was selected by the government to study computer science in a college due to his strong test scores. He was even sent to a Chinese college to broaden his knowledge of computer technologies. After his college years, he was assigned to work at a state-affiliated agency, creating office software. Before he could settle into this job, he was moved to China. At that time, he did not know he was on a mission in China. His job was not to conduct software research; he became a poor, low-paid laborer ordered to make money for his country via hacking gambling sites, collecting digital

game items, snatching credit card numbers, installing ransomware on corporate servers, and conducting other illegal online activities (Sam Kim, 2018).

This section has focused on an intensive, elite educational system for ICT human capital during the Kim Jong Il era (1994–2011) due to the lack of recent primary and secondary sources. Despite that, Kim Jong Un's North Korea (2011–) also has also had a similar education system for fostering ICT experts. Since his inauguration in 2011, the state has once again granted privileges to scientists. North Korea has built new and modern streets, districts, buildings, and houses, such as Unha (Galaxy) Scientists Street in September 2013 (Korean Central News Agency, 2013; Stimmekoreas, 2013), Wisong (Satellite) Scientists Residential District in November 2015 (Dave Lee, 2015), and Mirae (Future) Scientists Street in November 2015 (Yonhap News Agency, 2016) to encourage scientists. These are all in Pyongyang. These new areas include housing and community centers for scientists and their families, as well as research facilities. Moreover, while Kim Jong Un has continued his father's core science policies, such as the Five Years Plan for Science and Technology, the Policy for Computer Numerical Control (Tae-Hee Park, 2017), and the modernization of its intranet, the state has begun new businesses for cyber education systems, cyber medical treatment programs, and electronic payment systems (Lee & Kim, 2015, p. 4). It is no secret that Kim Jong Un has tried to make its ICT industry more developed (Lee & Kim, 2015, p. 6).

2.5 CONCLUSION

The empirical evidence presented about the development of North Korea's cybercapability over the last 30 years provides a unique opportunity to see why and how the state has the capability of carrying out massive and complicated cyberoperations. In summary, there are three important findings. First, the evidence provided a chance to look at the asymmetric way of

Pyongyang as an authoritarian regime to develop ICTs, which is different from the ICT development of ordinary democratic countries. The evidence illustrates why North Korea started to focus on ICT advancements. Second, the empirical findings show the amount, types, and quality of North Korea's ICTs. The third finding is that the origin and core of Pyongyang's development of an aggressive cybercapability is to advance its national interests. These three findings provide the following challenges for the rest of the world.

First of all, the North Korean case illustrates how a closed country has entered the information age. Information technologies are recognized as a double-edged sword for authoritarian states. On the one hand, new technologies can accelerate economic growth. On the other hand, these technologies can also threaten closed-state regimes. This does not mean, however, that the state strives to maintain distance from the developments of an information age. North Korea also heavily focuses on developing ICTs for the last four decades, though its ways go wrong.

The Kim dictator family has pursued information technology advancements not to achieve economic prosperity, but rather to achieve its ultimate goal, regime survival. There is no doubt that despite North Korea's intensive, state-controlled policies, including educational system reformation, the development of the ICT sector has not progressed as the state might have hoped. This is because the closed characteristics of its communication system clash with the internet's emphasis on freedom of information. This clash has created a paradoxical situation in which North Korea has limited ICTs and ICT infrastructure. North Korean citizens are not allowed to access the internet for fear it would harm the regime. However, Pyongyang has many skilled ICT professionals who have emerged from its intensive education programs in science and technology. This gap between abundant, highly educated, and skilled ICTs professionals and

underdeveloped ICT sector is increasing. Then, there are growing international concerns about the focus of North Korea on cyberoperations against the outside world. Thus, it shows that the increase in cybercapability of North Korea can be understood as a strategic tool only for regime survival.

This is the first challenge. Despite this "dictator's dilemma," authoritarian states recognize the internet as a strategic tool. While the regime prevents its citizens from accessing harmful sources through strong censorship programs, the regime employs the positive aspects of ICTs for itself. Thus, if the international community wants to weaken North Korea's censorship programs for freedom of information and world peace in cyberspace, it should make a strategy. Specifically, ordinary North Korean people need to be exposed to the internet in order to undermine the North Korean regime.

Next, it appears that North Korea only connects to the outside world in cyberspace only to advance its strategic goals. The regime has developed ICTs and constructed ICT infrastructure. North Koreans can use 3G mobile services with smartphones and tablet PCs. However, they are only allowed to access North Korean intranet services internally to the country. Despite this limitation, the state has the technical capacity to provide adequate internet access for its citizens.

Unlike ordinary North Koreans, the elite and cyberwarriors can access the outside world through the internet. North Korea owns 1,024 IP addresses and its dot-KP internet top-level domain. Moreover, there are around 1,900 additional IP addresses associated with North Korea. This includes China Unicom's 256 IP addresses. The IP evidence is meaningful because it demonstrates that the state is not isolated and has the potential to be a member of the global internet community. Above all, this evidence corroborates some reports which attributed some aggressive cyberoperations to North Korean IP addresses.

This is another challenge. North Korea and its hacker troops borrow many IP addresses from others to conduct hostile cyberoperations. It is hard to trace North Korean hackers and attribute massive cyberattacks to them directly. Thus, if the international community wants to mitigate North Korea's cyber threats, it should stop some countries and companies from allowing North Korea to use their IP addresses. Also, countries should share information about IP addresses associated with North Korea with others to mitigate North Korea's cyber threats.

Lastly, North Korea's state-led education system to cultivate ICT human capital is the origin and core of its aggressive cyberoperations used to advance it national interests. Although the state's ICT infrastructure is much less advanced than other countries' ICT infrastructure, it has slowly moved forward into the information age. However, its state-led education system for gifted computer students has created a pool of ICT professionals who can be viewed as potential cyberwarriors for the state.

Pyongyang established gifted schools to focus on nurturing talented science students, including those in computer technology, since Kim Il Sung visited the Soviet Union and its satellite states in 1984. Since the 2000s, its secondary schools for gifted children have offered special classes only for talented ICT students who are sent to computer science departments in top universities in North Korea after graduation. Everyone from the education system cannot be categorized as cyberwarriors who have targeted networks around the glove. They can be viewed, however, as the potentials who will work directly or indirectly for the regime's cyberoperations associated with its political goals at some point.

This is the third challenge. North Korea's ICT infrastructure is comparatively underdeveloped. Infrastructure underdevelopment does not mean, however, that North Korea cannot carry out massive and complicated cyberoperations. It has many skilled cyber

professionals from its state-led intensive education system. Thus, the international community should monitor North Korea as a potential and an active cyber threat to other countries in cyberspace.

To conclude, North Korea is not a hermit kingdom isolated from the information age. This authoritarian state has developed and constructed a restricted and limited cyberspace that does not allow its ordinary citizens to access the internet out of fear it would harm the regime. Domestically, well-secured intranet services are provided for its public and private sectors. Despite that, the state seems to use several IP ranges to access the outside cyber world for its cyberoperations. Pyongyang has steadily fostered ICT professionals through its state-led intensive education system for gifted computer students. It is important to note that the ICT experts are the core source of North Korea's capacity to carry out aggressive cyberoperations against the outside world.

Chapter 3. NORTH KOREA'S CYBER PROXY WARFARE STRATEGY

3.1 INTRODUCTION

On December 7, 2014, a spokesperson for North Korea's National Defense Commission denied responsibility for an attack on Sony Pictures Entertainment but stated that it "might be a righteous deed of the supporters and sympathizers" responding to the North's call to the world to turn out in a "just struggle" against U.S. imperialism (Associated Press, 2014). It was the first North Korean official response to the suspicion that the state hacked Sony in November 2014. The report came through the Chosun Central News Agency, a vehicle to spread the views of the regime. Also, the spokesperson of the Commission added that the film, *The Interview*[52], would "hurt the dignity of the supreme leadership of the DPRK (Fifield, 2014).

Who were the supporters and sympathizers working for the suspected North Korean-sponsored hack? What drove these non-state actors to conduct the cyberattack on behalf of the state, in the face of danger? These questions were asked in many policy and technical reports; academic journals; and news articles which sensationalized the role of state-associated patriotic hackers, cyber (or digital) militia or mercenaries, and state-sponsored or pro-government hackers (defined as cyber proxies) (Applegate, 2011; Coats, 2018; Group-IB, 2017; Kallberg & Rowlen, 2014; Maurer, 2018; Shinkman, 2016; Sigholm, 2013).

This chapter seeks to answer the following question: How has Pyongyang accomplished its hostile cybermissions without being traced and punished? In other words, what is North Korea's central cyber strategy? This is also the response to an unsolved issue from the last chapter: What

[52] *The Interview* is a 2014 American action comedy of Sony Pictures Entertainment depicting the assassination of the North Korean leader, Kim Jong Un.

role do a large number of sophisticated IT professionals, trained in state-led intensive gifted computer education programs, play in terms of North Korea's cyber strategy?

This chapter argues that North Korea provides a case study of the fact that cyberspace has become a new venue for state-led proxy warfare. "Proxy warfare"[53] is traditionally understood as the involvement of principals, mainly state actors, indirectly in an armed conflict by employing third parties, states or non-state actors, as proxies wishing to archive their mutual strategic goals (Mumford, 2013, p. 1). More specifically, a proxy-warfare strategy is revitalized in cyberspace by the characteristics of manmade space—anarchical states, anonymity, and a lack of boundaries. In cyberspace, this strategy uses information technologies such as fake IP addresses, proxy servers, hop points, and VPNs.

The empirical evidence from the North Korean case shows that a proxy-warfare logic has been applied to state cyberwarfare strategy. It is defined as cyber proxy warfare in this dissertation. State actors prefer to delegate their monopoly authority over violence to online non-state actors who conduct their aggressive cyberoperations. These non-state actors, who are connected to states and their political interests, are understood as cyber proxies: pro-government or state-sponsored hackers, sometimes including official intelligence groups or the military. Moreover, North Korea's cyber-proxy-warfare strategy plays a crucial role in keeping the regime's distance from what are arguably North Korean-related cyberoperations. Thus, this chapter contends that as a state-sponsor, North Korea actively enjoys proxy warfare by using its cyberwarriors as proxies for achieving national goals in cyberspace while simultaneously avoiding tracking and punishment.

[53] [Cyber] proxy warfare and [cyber] proxy war are interchangeable in this research.

Ultimately, this chapter also aims to answer how North Korea employs its sophisticated IT human capital developed by state-led gifted-education programs. As detailed in the last chapter, North Korea began to develop its IT human capital through gifted-educational systems in the 1980s. It does not have sufficient public and private IT sector capacity, however, to accommodate the number of highly educated IT professionals. This means that North Korea's IT human capital is used to engage in cyber proxy warfare.

From a general perspective, proxy relationships between state actors and state or non-state actors have a long history. From the Greek city-state to the feudal state of the Middle Ages, and finally to the modern nation-state, states have hired proxies to help achieve their strategic goals (Maurer, 2018, p. 29). Andrew Mumford claims that the proxy relationships have been particularly prevalent since 1945, as the shadow of nuclear war ensured more acute selectivity in conflict engagement given the consequences of a potential nuclear exchange. During the Cold War, the United States and the Soviet Union commonly engaged in proxy warfare and frequently used proxies to further their strategic goals and ideologies (Bar-Siman-Tov, 1984; Hughes, 2012; Towle, 1981; Westad, 2005). Moreover, since the end of the Cold War, proxy non-state groups with external support have not only played a critical role in fueling intra- and interstate conflict, but have also quantitatively dominated proxy relationships (Borghard, 2014, 4; Cunningham, Gleditsch, & Salehyan, 2013; Salehyan, 2010; Sarkees & Schafer, 2000). Around 48% (214) and 50% (223) of the 443 rebel groups and 446 governments operating in armed conflicts between 1945 and 2011 had explicit or alleged external support mainly from states (Cunningham et al., 2013, p. 527).

From a theoretical perspective, proxy warfare is driven by reasons of maximizing interest, while at the same time minimizing risk. Principal states have hired non-state actors as proxies to

avoid engaging in direct, costly, and bloody warfare, while also seeking to further their own national interests through conflict (Mumford, 2013, p. 11). According to Ariel I. Ahram, proxy relationships are also viewed as a phenomenon where states delegate their monopoly authority over violence to their proxies (Ahram, 2011). This refutes Max Weber's definition of the state as having the monopoly authority over the legitimate use of force (Weber, 1919). In other words, although the state has become tied to this monopoly over violence, very few have effectively possessed it (Maurer, 2018, p. 3).

The proxy warfare literature is not a perfect way to explain cyber proxy warfare, but is a good start to account for states' use of proxy warfare strategy in aggressive cyberoperations. Cyber proxy warfare theory shares the same baseline assumption and major components of the proxy warfare literature. The literature assumes that state actors can employ third parties as proxies for their own interests whenever they need them in the anarchical international system. Cyber proxy warfare is in line with this assumption. Cyber proxy warfare can also be explained with the major components of the proxy warfare literature, such as cause, types of proxy relationships, ways of assistance, control mechanisms. For example, state actors conduct both traditional proxy warfare and cyber proxy warfare for little or no attribution and plausible deniability.

However, the literature and cyber proxy warfare diverge in one critical respect: the natural, physical world is very different from the artificial, virtual world that was created by scientists and information technologies. In this context, Thomas Rid (2013b) argued that non-destructive cyber weapons differ from destructive physical weapons though whether cyber weapons have destructive power or not is controversial. Thus, the assumption and components of the proxy

warfare literature are borrowed in this study but revised to be more generally applicable to cyber proxy warfare based on information technologies and the difference between the two worlds.

This chapter illustrates how states use proxies for their cyberoperations with a single case study, North Korean-associated cyberoperations. The case was selected because the state is (1) among the top cyber threats to the United States and other countries, along with China, Russia, and Iran (Coats, 2018, pp. 5–6); (2) has conducted many massive cyberattacks; and (3) provides sufficient evidence about cyber proxy relationships. Thus, the case of North Korean cyberattacks is perfect for understanding how state actors use cyberspace to maximize their national interests as well as how the North Korean regime avoids being traced and punished as it carries out its hostile cyberoperations. Therefore, the chapter makes two interrelated arguments about state's aggressive cyber strategies. First, states have employed cyber third parties to achieve their national goals. In the case of North Korea, the state has delegated monopoly authority over violence to its cyber non-state actors whether they are government officials or not. Since 2009, North Korean cyber proxies have carried out massive, well-organized, and sophisticated cyberattacks against the outside world; these attacks are connected to national interests of the state under a strong command, control, and surveillance system.

Second, North Korea's aggressive cyber proxy warfare strategy shows that cyberspace has become a new strategic battlefield among states, along with four natural domains, land, sea, air, and space. There is a controversy over whether cyberwar actually fits the definition of war. According to one perspective, cyberwar is imminent (Arquilla & Ronfeldt, 1993). This first group of scholars has emphasized the dangers of cyberwar since the 1990s. Some scholars and policymakers have depicted potential cyber threats as a "cyber-Pearl Harbor" (Bumiller & Shanker, 2012; Wirtz, 2017). This group's influence peaked with Richard Clarke and Robert

Knake's book, *Cyber War* (2010) that contributed to raising public governmental, and academic awareness about the importance of cybersecurity (Sharp, 2017, pp. 1–2).

More recently, some scholars have begun to criticize these ideas about cyberwar. Specifically, Thomas Rid claimed that cyberattacks are different from conventional warfare because they fail to meet all three aspects of Carl von Clausewitz's definition of war[54] as violent, instrumental, and attributable to one side as an action taken in pursuit of a political goal (Rid, 2013a). Therefore, Rid argued that "cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future" (Rid, 2013a, p. xiv).

This chapter also joins this debate about state-led cyber proxy warfare theory by focusing on actors and their intentions. Empirical evidence about North Korean-associated cyberattacks refutes Rid's argument. North Korea, illustrates how states have aggressively employed cyberspace as a national strategic battlefield using chosen cyber proxies for their national interests. The chapter argues that as cyberattacks are the state's instrument, these are an act of violence designed to compel adversaries to bend to its will.

The chapter proceeds as follows: section 3.2 reviews principal-agent (P-A) theory and its relationship with proxy warfare literature in order to shed light on the origin of cyber proxy warfare. Section 3.3 develops the concept of cyber proxy warfare based on the classic proxy warfare components. The primary assumption and major aspects of cyber proxy warfare are the same as those of proxy warfare literature. Despite that, the classic proxy warfare components are revised to be more generally applicable to cyber proxy warfare because of the differences between the physical and virtual worlds.

[54] Clausewitz defined war as an act of violence intended to compel our opponent to fulfill our will (Clausewitz, 2007).

Section 3.4 provides an overview of North Korean-associated cyberoperations. In the first half, it summarizes the chronology of major North Korean-associated cyberoperations. Then, it offers a typology for cyberoperations based on the state's short-term goal as a common criterion. Section 3.5 details North Korea's cyber proxy warfare strategy. It consists of four sub-categories: anarchy, anonymity, and North Korea's non-state actors; information technologies and cyber proxy warfare strategy; non-state actors, front companies, and the North Korean regime; and North Korea's control mechanism for cyber proxy warfare. These four themes illustrate how North Korea uses non-state actors in cyberspace to maximize their national interests without being traced and punished. The chapter concludes with a discussion of the implications of North Korea's cyber proxy warfare.

3.2 Proxy Warfare Literature: Violating Monopoly Violence Authority of Modern States

The principal-agent literature was initially developed in the field of economics to investigate more general questions of incomplete information- and risk-sharing between employers and employees (Moe, 1984, p. 756). Broadly speaking, a principal-agent relationship is one of the oldest and commonest codified modes of social interaction in which principals consider making contractual agreements with agents in the hope that, on behalf of them, agents will subsequently take proper activities for achieving desired outcomes of principals (Kiser, 1999, p. 146; Moe, 1984, p. 756; Ross, 1973, p. 134). A principal-agent relationship primarily aims to increase efficiency for the principal through a particular capability of a hired agent in a specific task (Borghard, 2014, p. 26). The agent also seeks to gain financial or other compensation directly from the principal or indirectly from the task (Prendergast, 1999).

The relationship model has been most commonly applied in other social science areas, especially security studies and war history, under the name of *proxy warfare*. Many armed conflicts between states; between states and non-state actors and vice versa; and between non-state actors have occurred due to a proxy relationship. Specifically, states have been centered in the proxy warfare because they afford to hire other actors for achieving their goals. Tim Maurer (2018, p. 29) argues that states have employed proxies to help achieve their goals beginning with Greek city-state, to the feudal state of the Middle Ages, and finally to the modern state. On the one hand, theoretically, in Chinese military thought, the third tactics of the Thirty-Six Stratagems[55] is to "kill with a borrowed sword" (Taylor, 2013, pp. 22–24). This school of thought emphasizes that when attacking an opponent, it is better to use the strength of a third party than one's own strength. In practice, however, Thucydides's *History of the Peloponnesian War* said that warring city-states used to employ non-state actors, such as mercenaries and volunteers (Mynott, 2013). State actor's use of proxy mechanisms is a permanent feature of the contemporary international landscape. Prominent examples include the Cold War; civil wars in the Middle East and Africa; and terrorism across the globe (Bar-Siman-Tov, 1984; Craig, 2012; Innes, 2012; Towle, 1981).

The proxy relationship repudiates Max Weber's famous definition of modern states as "a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory" (Weber, 1919). While Weber's definition has since been amended and revised, the core emphasis on a state's monopoly authority over the legitimate use of violence remains unaltered (Ahram, 2011, p. 7). According to his idea, the modern state can be

[55] The Thirty-Six Stratagems is one of the Chinese military classics. It mainly focuses on the use of cunning and deception on the battlefield. Recently, it is known as the basis of Chinese business strategy. For more information about that, see the following article. Tung, R. L. (1994). Strategic Management Thought in East Asia. *Organizational Dynamics*, *22*(4), 55–65.

understood as the unilateral actor who maintains public order within its territory using the constabulary force as well as the defense force for the purpose of national security. However, contrary to this ideal theory, history demonstrates that the modern state has delegated its monopoly over violence to third parties as proxies, including other states and non-state actors. Michael Mann noted that "most historic states have not possessed a monopoly of organized military force and many have not even claimed it" (Mann, 1986, p. 11). In this regard, Ariel Ahram (2011) argued that only a few states have ever actually sought a complete monopoly over military force, much less possessed it because states have engaged continuously in negotiation, collaboration, and domination of external and internal challengers to assert and maintain a hold on power. Furthermore, he supported up his argument with one of the four proxy relationship combinations[56], states and state-sponsored non-state militias, is ubiquitous in the civil conflict of late-developing states (Ahram, 2011, p. 9).

In the information age, cyberspace has become a new venue for conflicts. Joseph Nye, Jr. has been worried that the virtual world was designed as an open system forty years ago with little attention to security by computer experts and specialists (Nye, 2011, p. 18). More recently, national security experts have viewed the virtual space as a fifth military operational domain, along with other natural domains of land, sea, air, and space (Lynn, 2010). Since then, many counties have devised defense strategies, along with building new regular cyber commands and armies, to defend their critical public and private networks (Obama, 2010; U.S. DoD, 2011). This means that states have prepared for potential regular wars against cyber armies of hostile countries.

[56] As detailed in section 3.3.2, these are four combinations of principals and agents: (1) State(s) - State(s); (2) State(s) - Non-state Actor(s); (3) Non-state Actor(s) - State(s); and (4) Non-state Actor(s) - Non-state Actor(s).

States have not been faced with cyberattacks directly from nation-states and their regular cyber militaries, despite their cyber preparedness based on the traditional concept of a national defense strategy. On the contrary, states have only faced massive, irregular cyber threats originating from non-state cyber actors backed by other states (Coats, 2018; Geers, Kindlund, Moran, & Rachwald, 2014). In other words, states prefer to use proxies to engage indirectly in conflict because of plausible deniability. In this regard, a 2018 U.S. intelligence report, *Worldwide Threat Assessment of the U.S. Intelligence Community* (2018, pp. 5–6), begins with an emphasis on the threat of state-sponsored cyberattacks as the top national security priority. This emphasis illustrates that a new abstract concept, state-led cyberwarfare, has materialized and been realized in the different way: cyber proxy warfare; a state delegates its monopoly over legitimate violence to non-state cyber proxies to act on its behalf, based on principal-agent theory. Moreover, proxy warfare strategies in the virtual world are more attractive than ones in the real world due to the anonymous and borderless characteristics of the anarchical cyber domain, as illustrated in the following sections.

3.3 A New Framework for Cyber Proxy Warfare

It would be a mistake to neglect the past, as Mark Twain said: "History does not repeat itself, but it often rhymes."[57] States have a long history of delegating their monopoly over legitimate violence to a proxy to act on its behalf, as illustrated in the previous section. In the information age, cyberspace has become a new place for the devolution of state monopoly authority over violence to a proxy actor to occur. This means that although traditional and cyber proxy warfare exist in very different worlds—the real and virtual—there are some areas of

[57] This is often attributed to Mark Twain. However, there is no compelling evidence for the attribution.

critical overlap: the anarchical nature of international politics, anonymity, a borderless world, the importance of non-state actors, and the mechanism of a proxy relationship. Thus, this chapter conceptualizes cyber proxy warfare theory based on traditional proxy warfare literature.

3.3.1 *Premise: Causes of Cyber Proxy Warfare*

Anarchy is a central concept of international relations theory: it is the idea that the world lacks any supreme authority or sovereign (Art & Jervis, 2017, p. 7; Axelrod, 1984, 4; Waltz, 1979, p. 88). The concept is understood as a fundamental foundation of realist, liberal, neorealist, and neoliberal paradigms of international relations. Some of the paradigms (mainly (neo)-realism) use the term *anarchy* to signify a world in chaos, disorder, or conflict; others recognize it just as a reflection of the order of the international system, in which there is no central authority above independent states (Grieco, 1988, p. 486; Keohane, 1984; Milner, 1991, pp. 68–74; Powell, 1994, pp. 329–334). Despite these differences, all of these paradigms assume that in an anarchic state, there is no strong hierarchical superior and coercive power that can resolve disputes between countries, enforce laws between them, or create order in the system of international politics. Proxy warfare literature has also been developed under this idea, though it is not mentioned explicitly. In the proxy warfare literature, while sponsor states have illegally hired proxies to conduct their armed conflicts, no central authority can properly punish the sponsors. Thus, the anarchical nature of international politics is the fundamental baseline assumption of proxy warfare.

Cyberspace is a new anarchical space between states. When the internet was created approximately 50 years ago, a small, village-like community formed around it, comprised mainly of computer experts and specialists who knew one another (Nye, 2011, p. 18). Since then, the virtual domain has expanded with no central authority. Some international organizations, such as

ICANN (Internet Corporation for Assigned Names and Numbers), IANA (Internet Assigned Numbers Authority), IAB (Internet Architecture Board), and IETF (Internet Engineering Task Force), have played a vital role in the evolution of the internet by developing standards, technology, and recommendations, deploying infrastructure and services, and addressing other significant issues (Paul, Bhuimali, & Shivraj, 2016). Nevertheless, none of these organizations have control over the entire virtual world in order to mitigate any military conflicts and disputes that should arise. Moreover, the online space is dominated by computer experts and was designed as an open system with little attention to security (Nye, 2011, p. 18). Thus, security is a secondary priority to maximizing positive aspects of cyberspace, which include global societal, economic, and political prosperity.

The anarchical nature holds its place firmly in both proxy and cyber proxy warfare with two foundational concepts, anonymity and no temporal and spatial borderless. These two aspects of cyberspace support sponsor-actors in hiding their identities behind proxies with ease. The growing the role of non-state actors in cyberspace also makes it even more chaotic.

Anonymity

Being anonymous refers to "a person cannot be identified according to any of seven dimensions of identity knowledge, that is, the person's legal name, location, pseudonyms that can be linked to the person's legal name or location, pseudonyms that cannot be linked to specific identity information but that provide other clues to identity, revealing patterns of behavior, membership in a social group, or information, items, or skills that indicate personal characteristics" (Kang, Brown, & Kiesler, 2013, p. 2658). In proxy warfare literature, anonymity can be defined as a sponsor's tactical way of hiding the aforementioned identifiable clues about itself behind its third-party proxies. Technically, a principal tries to keep anonymous by

employing an agent who would be willing to undertake the responsibility of the principal in an armed conflict. In a proxy relationship, the principal provides a variety of supports for its agent, such as the provision of material and non-military assistance (Mumford, 2013, pp. 61–75). The agent then seeks to achieve shared goals with its principal by becoming directly involved in an armed conflict (Mumford, 2013, p. 103). In this process, the principal keeps a distance from its agent as well as the armed conflict in order to stay anonymous. The proxy agent simultaneously denies its relationship with the sponsor principal to protect the principal's anonymity (Krishnan, 2017).

In traditional proxy warfare, the anonymity of sponsor principals is not only an ideal concept but also an open secret. In the real world, it is extremely difficult to hide sponsors' identities. Despite active efforts to hide their exchanges between sponsors and proxies, the flow of physical supports from sponsors to proxies can be traced to some degree through resources such as funds, weapons and equipment; and other non-military assistance. For example, it is public knowledge that the CIA has used in the three primary means to provide weapons and materials for proxy private military organizations: (1) outdated U.S. military equipment that has been decommissioned, (2) equipment acquired from partner countries, and (3) equipment acquired from the gray arms market through CIA front companies or freelance arms merchants (Krishnan, 2018, p. 63). Thus, dark relations in traditional proxy warfare can be viewed as an open secret.

Nevertheless, both principals and agents do not confirm their secret yet open relationship. Despite these open secrets, sponsors have enjoyed indirect involvement in conflicts by hiring proxies because there is a higher possibility to avoid direct engagement through repeated denials of involvement. It is challenging to reveal a proxy relationship with decisive evidence. Moreover, it is difficult to implement punishment against sponsors instead of proxies. Thus,

while the anonymity of proxy warfare is not entirely secured, it is sufficient enough to hinder the international community from taking proper actions against these indirect military strategies: proxy warfare. The Syrian Civil War (2003–) is a good example. Although the United States, Russia, and other countries have been indirectly involved in the ongoing, multi-sided armed conflict, they have escaped responsibility for the conflict.

The anonymous component of proxy warfare operates almost perfectly in cyberspace. When the new virtual space was invented, users were not required to reveal their identity. In the initial stages of cyberspace, it was just a small, virtual community among computer scientists and specialists who knew one another. Since then, anonymous communication has been viewed as the cornerstone of an overtly anti-establishment internet culture that promotes information sharing and free speech (Davenport, 2002, p. 33). As Jessica Beyer argues in her book, *Expect Us* (2014, pp. 3–4), higher levels of anonymity within online communities with low levels of formal regulation and minimal access to small-group interaction has a positive relationship with political mobilization.

In practice, anonymity across applications is difficult to achieve for most users. First, online activities of average internet users across the globe can be traced and linked to their identities, including name, location, IP address, and other affiliations. They can enter the internet world through local ISPs (Internet Service Providers) after purchasing internet services with their real identities. Internet users are then required to share their personal information with website operators, including private and public entities, when they try to register those websites to get more services and information. Finally, internet users' online activities, linked to their personal information, are stored somewhere online, as well as in the IT devices they used or linked during their online activities. In addition, some countries, such as China and Russia, recognize

cyberspace as part of their sovereign territories which must be monitored and controlled (Heam, 2014, p. 117; Pallin, 2017, p. 23; Raud, 2016, p. 7). These countries have built strong censorship programs—such as the Great Firewall of China—to weaken the anonymous characteristics of cyberspace under the guise of national security (Karatzogianni, 2015, p. 46).

Despite these technical and political challenges, there are many technical and political ways to increase online anonymity. The first is a technical way to hide identity. In the simplest case, an online actor posts an article on a website, sends an e-mail to other users, and communicates with them using a falsified name. In cyberspace, users are allowed to create unlimited fake accounts or identities. Therefore, it is not difficult to also fake an IP address via falsified, anonymous, or pseudonymous servers. Anyone can hide their real identity online if they have technical skills, such as the above-described skills. Professional hackers, including state-sponsored cyber proxies, use Dynamic DNS (DDNS),[58] proxy servers,[59] virtual private network servers (VPNs),[60] or hop points[61] to hide their identities. The activities are generally illegal, however.

The second method of securing online anonymity is political. Some actors are allowed to falsify their identities with the aforementioned technical skills under the connivance, cooperation, or support of states who retain sovereign power online. In other words, although

---

[58] Domain Name System (DNS) only works with static IP addresses. However, Dynamic DNS, or 'DDNS,' is designed to support changing (dynamic) IP addresses. DDNS providers allow authorized users to control the IP address assignment of a domain. Users can access this IP address assignment through the provider and make changes as needed. Hackers can use DDNS, which makes identifying the source of malicious network traffic more difficult for the victim or investigators (Shields, 2018, 8-9).

[59] A proxy server originally acts as an intermediary for requests from clients who seek resources from other servers. However, a proxy server also allows hackers to go online under fake IP addresses.

[60] Virtual private network (VPN) services were developed to allow remote users and branch offices to access their private corporate applications and resources. VPNs encrypt traffic between the IP address of a real user and the VPN's server before connecting to the internet. Internet users secure their transactions with a VPN, to avoid geographically restrictions of some servers and websites and censorship programs of states. Some of them use VPNs to connect to proxy servers in order to protect their personal identity and location or to stay anonymous on the Internet.

[61] Hop points refers to computers used by unwitting victims that have been compromised by hackers. Hackers use the compromised computers as part of their infrastructure for further computer intrusions. (Shields, 2018, p. 9).

intentional identity falsification in order to violate laws is not allowed, states enable state-led actors to hide their real identities in order to advance national interests in the virtual world. In this way, states' proxy warfare strategies can be perfectly accommodated in cyberspace through technical skills and states' intentions. States can hire anonymous third-party actors or pretend to be anonymous non-state actors in order to pursue the state's political and financial goals in cyberspace.

Temporal and Spatial Borderless

Direct armed conflicts between two or more actors require them to move their combatants, weapons, and equipment to military targets or the frontline. These military maneuvers take a great deal of time. Even if both warring sides do not share borders, they can be faced with more complicated time and space challenges. They sometimes need to cross seas to get to battlefields by using ships. The parties to conflict also must receive permission from uninvolved states to pass through or over their lands, seas, or skies. These natural and artificial barriers can delay or block strategic maneuvers. Moreover, temporal and spatial restriction create the logistical issues. Warring parties can have difficulties maintaining communication or supply lines to their military units located in remote battlefields due to natural terrain limitations or artificial borders.

In contrast to direct conflict scenarios, sponsors can overcome the aforementioned time and space limitations by employing remote proxies in proxy warfare scenarios. Proxies located in troubled regions fight against mutual opponents alone on behalf of their sponsors who want to keep physical and political distance from the conflict. Sponsors are only required to support their proxies with funds, weapons, equipment, and other non-physical assistance, including military training and the development of ideal political conditions. History demonstrates that strong Western powers have engaged in civil wars on other continents (Africa, Asia, and South

America) without sending their mass military units to those locations (Bar-Siman-Tov, 1984; Craig, 2012; Innes, 2012; Towle, 1981). However, given the three ways the CIA provides weapons and materials to its proxies[62], it is undeniable that it takes time for sponsors to covertly send funds and weapons to proxies who may be located far away (Krishnan, 2018, p. 63). Space issues, such as natural barriers and borders of other countries, also hinder sponsors from sending material supports to proxies. Thus, although proxy warfare can overcome some time and space limitations of conventional wars, it does not entirely overcome these challenges.

The virtual world is entirely different from the physical world with respect to temporal and spatial restrictions. In the 1960s and 1970s, virtual space was designed as a neutral as well as temporally and spatially borderless world (Goldsmith & Wu, 2006, p. 23). There is no time and space restrictions of the real world in cyberspace. Information travels online at the speed of light. In the blink of an eye, one internet user can send an email to a friend living on the opposite side of the earth. Theoretically, cyberspace is a borderless space, not under the control of any single sovereign country. When sending an email, for example, the sender does not need to consider space issues, even if their email passes through several servers located in sovereign territories. On the whole, online users are not restricted by time and space challenges.

Cyberspace is viewed as an ideal battlefield for a proxy warfare strategy because it does not have temporal and spatial restrictions. First, physical meetings and exchanges between sponsors and proxies are optional in the case of a cyberoperation. Though seeking proxies, making contracts, issuing operational orders, and other critical activities happen in cyberspace, the location of the actor for proxy warfare is relatively unimportant. A sponsor can contact its remote

[62] The CIA has used in the three primary ways to provide weapons and materials for proxy private military organizations: (1) outdated U.S. military equipment that has been decommissioned, (2) equipment acquired from partner countries, and (3) equipment acquired from the gray arms market through CIA front companies or freelance arms merchants (Krishnan, 2018, p. 63).

proxies through a variety of methods: encrypted emails, social networking services, cyber dead drops,[63] VPNs, DDNS, or hop points.

In addition, sponsors do not have to account for temporal and spatial issues when funds and cyber weapons are transferred to proxies. Cyber proxy warfare is also a relatively low-cost operation. In general, cyber weapons are malware, hacking tools, or coding sources of targets. Contrary to guns or rockets used in physical warfare, malware, hacking tools, or computer knowledge can be shared between sponsors and proxies online right before the operation begins. Hacker or computer-expert cyber proxies may sometimes operate without any additional resources from sponsors. This means a professional hacker in a cyber proxy warfare operation can be the equivalent to hundreds of militias in a physical proxy warfare scenario. Sponsors and proxies do not need to expend energy exchanging funds or weapons online. These limited interactions also play a critical role in reducing the risk of exposing the relationship between sponsor and proxy.

Lastly, cyberoperations targeting critical networks or computers of the opposing party can be conducted without any military maneuvers. Cyber proxies pass through several independent networks, IP addresses, or computers to attack its targets. The aforementioned DDNS, VPNs, hop points, or other computer techniques enable this process. Because this process occurs rapidly, it cannot be easily blocked by territorial issues. On the contrary, the process increases the chances that sponsors' identities and purposes will remain undetected. In sum, the lack of

[63] A dead drop, called a dead letter box, is a method of espionage tradecraft used to pass items or information between two related actors, such as two agents, a case officer and an agent, or an agent and a double spy, using a secret location. Thus, the actors are not required to meet directly and thereby maintaining operational security. The cyber dead drop is a kind of online version of the traditional dead drop. For example, a cyber proxy can download a directive that is hidden in a normal open website by its sponsor.

temporal and spatial limits in cyberspace matches the core assumption of traditional proxy warfare which is to hide sponsors' identities.

Despite the ostensible borderless internet, Jack Goldsmith and Tim Wu expressed their concern over the attempt of governments to erect internet borders in their book, *Who Controls the Internet* (2006). States have built online borders to control internet activities, and thus enforcing their laws, by exercising coercion within their cyber sovereign territories under the guise of national security. It is not a healthy state of affairs for non-state actors, such as activists or hacktivists, who are not related to states or even stand against governmental authority. On the contrary, however, it is beneficial for state-related actors. For example, while a state allows its cyber proxies to use advantages of the temporal and spatial borderless online world for its cyberoperations, it protects its proxies from opposing parties by using its online territorial sovereignty. Paradoxically, building cyber-state sovereignty provides the ideal conditions for state-related cyber proxies who enjoy a temporally and spatially borderless online world.

The Growing Role of Non-state Actors

Conventional wisdom views states as primary actors in wars. States have also played key roles in proxy warfare. Sometimes they are sponsors, and other times they are proxies. Despite their dual role, state actors are not only one in proxy warfare. Non-state actors also play a critical role in proxy relationships. In their new correlates of war project (COW), Meredith Reid Sarkees and Phil Schafer (2000, p. 123) focused on the increasing number of non-state actors who have the motivation and the capacity to engage in warfare both within traditional states and across state borders. They created an expanded typology of wars, as shown in Table 3.1; since World War II, a growing number of armed conflicts (or important combatants) do not fit comfortably within the initial COW's dichotomous typology of international wars and civil wars (Sarkees &

Schafer, 2000, p. 127). Their expanded typology, based on data from all wars between 1816 and 1997 sheds light on the importance of non-state actors as well as state actors.

Table 3.1. The Correlates of War Project's Two Typologies of War

Traditional Typology	Expanded Typology
I. International Wars A. Interstate Wars B. Extra-systemic Wars	I. Inter-State Wars (type 1) II. Extra-State Wars A. State vs. dependent non-state (type 2) B. State vs. independent non-state (type 3)
II. Civil Wars	III. Intra-State Wars A. Civil Wars 1. For central control (type 4) 2. Over local issues (type 5) B. Inter-Communal (type 6, in development)

Source: Sarkees & Schafer, 2000, 128.

When all actors in domestic and international politics are ideally divided into two categories, non-state actors can be understood as the opposite of states. *The Oxford Dictionary* states that a non-state actor is an individual or organization that has significant political influence but is not allied to any particular country or state ("Non-state Actor," n.d.). According to the U.S. National Intelligence Council's (2007, p. 2) report, *Nonstate Actors*, non-state actors are viewed as "non-sovereign entities that exercise significant economic, political, or social power and influence at a national, and in some cases international, level." The report also categorizes non-state actors into three groups: multinational corporations, non-governmental organizations, and super-empowered individuals (The U.S. NIC, 2007, p. 2). In a broad sense, the report characterizes non-state actors as not only autonomous from the structure and machinery of the sovereign state but also as influential individuals or organizations in domestic as well as international areas (Josselin & Wallace, 2001, pp. 2–3).

In a narrow sense, proxy warfare literature defines non-state actors as armed organizations that have the motivation and the capacity to engage in warfare on behalf of their sponsors. In this context, the literature has focused on paramilitaries, terrorist groups, militia groups, anti-government forces, and more recently on private security companies that have been utilized as proxies (Ahram, 2011; Craig, 2012; Krishnan, 2018; Mumford, 2013). In a few cases, those organized non-state groups have been sponsors. Unorganized individuals or groups are not considered potential proxies. Moreover, the literature considers it crucial whether non-state actors are equipped with physical arms or not. Thus, non-state actors in the traditional proxy warfare literature are required to have physical military power as well as be organized to fight against other armed groups or countries.

Contrary to traditional proxy warfare, cyber0proxy warfare follows a more broad definition of non-state actors. Like conventional proxy warfare, cyber-proxy warfare may also prefer more powerful, organized groups that are equipped with cyber arms. Well-trained, controlled, and organized groups will be useful for mass and complicated cyberoperations. Despite this fact, individuals or unorganized groups may also participate in cyberoperations. Broadly speaking, the role and performance of individuals in the information age is growing in importance in every field (Zhang, Johnson, Seltzer, & Bichard, 2010; Zúñiga, Jung, & Valenzuela, 2012). Even the internet has empowered ordinary individuals on the margins of society (Mehra, Merkel, & Bishop, 2004). This means that individuals across the globe can use the internet to easily participate in diverse economic, social, and political activities. In addition, an individual online user cannot be viewed as one unorganized, weak actor in cyberoperations. According to John Arquilla, David Ronfeldt, and Michele Zanini (1999, p. 81), the rise of the internet means that "[cyber] power is migrating to nonstate actors, who are able to organize into sprawling multi-

organizational networks." Arquilla et al. emphasized that unorganized, non-state individual actors are thought to be more flexible and responsive than state or organized and hierarchical actors in a cyberwar or netwar situation (1991, p. 81).

The differences in cyber weapons compared to traditional arms lowers the barrier to entry for organized cyber groups, and even individual internet users. Non-state actors in the physical world use instruments of harm that range from the nuclear bomb to the human body trained in martial arts; their utility ranges from destroying an entire city to protecting one single person (Rid, 2013a, p. 36). However, weaponized code or malicious software in cyberoperations are different from physical weapons. Malicious code or software generally do not destruct anything directly. When non-state cyber actors use those weapons online, they have a very little chance of seeing the blood of others. They are not likely to have a guilty conscience. In addition, cyber non-state actors sometimes do not need to possess special weapons or computer skills in order to carry out cyberoperations. For example, one internet user can participate in a cyberoperation taking down a critical network, server, or website by clicking a mouse button several times to access one of the three, along with other individuals, at the same time. Thus, every online non-state actor, including individuals, can intentionally or unintentionally turn into a potential cyber combatant on behalf of a sponsor.

The Cause of Cyber Proxy Warfare

In *On War*[64], a Western military classic, Clausewitz (2007) defined war is an act of violence intended to compel our opponent to fulfill our will, directed by political motives and morality (p. 13). The ultimate goal of proxy wars is the same. However, there is a critical difference between

[64] Carl von Clausewitz's *On War* was originally published in 1832 in German. This study cites an English translated version.

regular and proxy wars in the way they seek to further strategic and ultimate goals. Contrary to regular wars, primary actors in proxy wars are reluctant to engage in direct, physical conflict against their opponents. This situation raises a more reliable way to distinguish the cause of proxy war from that of other regular wars by asking the following question: Why do as sponsors state actors prefer the indirect engagement in a conflict by hiring third parties, proxies, wishing to achieve their strategic goals?

In his book, *My Enemy's Enemy* (2012), Geraint Hughes listed specific factors that encourage sponsor states to initiate or assist proxy wars: political constraints on direct military action, security, casualty sensitivity, ideological solidarity, conflict avoidance, assisting a military campaign, intelligence-gathering, nationalist/religious ties, revenge, and preserving or enhancing spheres of influence (Hughes 2012, pp. 22–35). In *Proxy Warfare*, Andrew Mumford (2013) simplified the above factors with his definition of proxy wars: "the logical replacement for states seeking to further their own strategic goals yet at the same time avoid engaging in direct, costly, and bloody warfare" (p. 11). In other words, proxy wars have occurred when sponsors—primarily state actors—seek to maximize their interests via an indirect conflict while minimizing potential negative costs from the conflict.

The negative costs from direct engagement in an armed conflict can be divided into two categories: internal and external resistance. In the case of internal resistance, direct conflicts or interferences require primary actors to increase military expenditures. This would worsen the fiscal health of the actors. Direct military engagements also demand of enormous sacrifices of blood and property. In addition, citizens must consider the morality of their state's direct, armed conflict. Thus, these listed negative costs could threaten the position of leaders or ruling groups who ignite direct conflicts. These cause internal resistance. It is possible that the negative costs

outweigh the benefits of the conflicts. For instance, a famous ancient Chinese military text, Sun Tzu's *The Art of War*[65] (2000), is about how to fight wars without actually having to engage in a battle. *The Art of War* also emphasizes that several consecutive war victories could cause the fall of a nation due to heavy military expenditures and a decreased labor force. It reminds a paradoxical Western story, called a "Pyrrhic Victory"[66]: a victory that imposes such a devastating toll on the victor that it is tantamount to defeat. These two Eastern and Western stories demonstrate that it is important to avoid negative costs originating from unnecessary, direct battles.

The second category is international resistance (external) to armed conflicts. Human history shows that wars, especially the two world wars, have caused tremendous physical and psychological damage to the world, as well as to individuals. Thus, the international community has made efforts to circumvent other potential wars and minimize the damage from unwanted wars. In this vein, the international community has created international treaties on the laws of war, such as the Geneva Convention and Hague Conventions. Based on these treaties, the United Nations and its sub-organizations were established to keep world peace. The U.N. Charter bans any armed threat or use of armed force against another state. From an academic perspective, Michael Walzer's book, *Just and Unjust Wars* (2006), used a modern, secular theory of "just war" in an attempt to ascertain any reasons that might justify war and the ethical limits on the conduct of a war. Despite the controversy over his standards used to distinguish just wars from unjust ones, the book illustrates how international actors who enter into unjust and unnecessary

[65] It is known that Sun Tzu's *The Art of War* was originally published around 5th century BC in Chinese. This study cites an English translated version.

[66] Pyrrhic victory is named after Pyrrhus, king of Epirus, whose army suffered immense losses in defeating the Romans at the Battle of Heraclea in 280 BC and the Battle of Asculum in 279 BC. These losses later led to his defeat and death (Denson, 1999).

wars could be faced with international resistance (Walzer, 2006). At least in a theoretical sense, the international community has not allowed its members to resort to using armed force to maximize their interests. The international community has imposed economic and military sanctions against those states which violate international treaties on the laws of war or use armed force unjustly.

There are two prominent examples of international resistance. First, George W. Bush's justification of the Iraq War that began in 2003 was criticized by the international community. The war occurred as part of a declared war against international terrorism and Iraq's sponsorship of the September 11th attacks. The Bush administration justified its invasion of Iraq based on its need to eliminate Iraq's weapons of mass destructions (WMDs). However, the existence of Iraq's WMDs was never confirmed. Second, Islamic State of Iraq and Syria (ISIS) has been almost collapsed by the coalition forces because its aggressive armed conflicts have caused international indignation. In the 2010s, the group and its territorial area were growing due to the power vacuum in a part of the Middle East. However, the international community did not stand by and let the group violate international rules. These two examples from state and non-state actors illustrate that the direct use of armed force without justification may be faced with international resistance.

The use of proxy warfare to circumvent domestic/international resistance is commonly associated with hostile and aggressive cyberoperations. Cyberspace is understood as the fifth domain in which states have competed with each other to maximize national interests, along with other four natural domains (land, sea, air, and space). While states have listed cyber threats as a top security priority, they have simultaneously established organizations within military and secret government agencies in charge of cyber conflicts with others (Coats, 2018; U.S. DoD,

2015a). Some security experts have argued that an offensive rather than defensive cyber strategy is a better way to defend national security (Clarke & Knake, 2010). In the process of conducting aggressive cyberoperations, however, states are reluctant to escalate avoidable tensions with others. This means that when states pursue their national interests on the new virtual battlefield, they can circumvent domestic/international resistance by hiding their identities. In line with a definition of proxy warfare, state's actors seek to maximize their interests—including defending national security—by hiring the third parties in cyberspace while minimizing their political, financial, and other costs originating from direct and aggressive cyberoperations.

3.3.2 *The Practice of Cyber Proxy Warfare*

Two Types of Principal-Agent Relationships

As the name suggests, proxy warfare is focused on actors and their relationships. Thus, it is critical to grasp who engages in proxy relationships in order to understand the mechanisms by which proxy warfare occurs. This section addresses the following questions: Who becomes a principal and an agent in a proxy relationship? How does the distance between the principal and agent vary in a proxy relationship? The first part of this section explains four combinations between a principal and an agent. The second part of this section analyzes the three different types of distance between the two sides.

Before considering the four principal agent combinations, the actors in these scenarios must be identified. The major actors in proxy warfare can be identified as three different types: Actor A, Actor B, and Actor C. Actors A and B are primary actors who form the backbone of proxy relationships. They take hostile action against Actor C (a passive actor), their shared target. In this proxy relationship, Actor A becomes a principal by hiring third-party Actor B, who is supposed to impose a cost on or influence Actor C to do what Actor C would otherwise not do

(Maurer, 2018, p. 32). Actor B is involved directly in an armed conflict with the support of Actor A. The relationship between the two active actors (A and B) can be understood as the crucial asymmetric combination to be analyzed. Then, the dichotomy of players of international relations, states and non-state actors, in a broad sense, can be fallen into three of them. Thus, two Actors, A and B, and the two players, state and non-state actors, make four combinations of the proxy relationship detailed in Table 3.2. The proxy relationship is built between two or more states (Relationship I), between states and non-state actors, and vice versa (Relationship II and III), and between groups of non-state actors (Relationship IV). These four identifiable types of relations between these actors that have shaped the dynamics of proxy warfare in the past and present.

Table 3.2. Four Combinations of P-A Relationships in Proxy Warfare

Principal-Agent Relationship		Actor *b*: Third Party, Agent (Proxy)	
		State(s)	Non-state Actors(s)
Actor *a*: Principal (Sponsor)	State(s)	I. State(s) - State(s)	II. State(s) - Non-state Actor(s)
	Non-state Actors(s)	III. Non-state Actor(s) - State(s)	IV. Non-state Actor(s) - Non-state Actor(s)

∗ Actor *c*: Opponents of Principal-Agent Relationship

Principals on the benefactor side are required to provide various material/non-material assistances for proxy agents on the beneficiary side. On the contrary, a potential proxy is expected to receive support from a powerful sponsor based on mutual trust, once it made a secret and informal contract with a principal. This means that principals are required to have sufficient and continuous support capabilities for a chosen agent in a proxy warfare situation. Thus, in this regard, two state-led proxy relationships are pervasive: state-state (I) and the state and non-state

(II). A state-state proxy relationship (I) has been viewed as the traditional proxy strategy. Strong states have sponsored relatively weak states. World War I and II are good examples of this category. Moreover, the category I relationship was the main Cold War strategy of two superpowers, the United States and the Soviet Union (Bar-Siman-Tov, 1984). During the Cold War era, both hired weak states in an effort to circumvent mutually assured destruction that would come from direct conflict with one another (Mumford, 2013, p. 3). Thus, the combination of the Cold War with proxy warfare is viewed as the mainstream of proxy warfare literature (Bar-Siman-Tov, 1984; Craig, 2012; Mumford, 2013).

Tim Maurer (2018) argues that of the four proxy relationships detailed in Table 3.2, the most relevant to international affairs today is the state and non-state proxy relationship (II) (p. 31). Mumford (2013) has also illustrates the importance of the category II relationship by exploring the details of a category II case: East African Wars by non-state actors who were hired by Sudan and Uganda (1986–1999) after another category I case occurred (pp. 57–60). Since the end of the Cold War, the category II relationship has attracted more attention by proxy warfare scholars because non-state actors have played increasingly important roles in international affairs. In regions experiencing power vacuums—such as Syria, Iraq, and Libya—local non-state armed groups have protected their territory and fought against state or other non-state actors.

Although non-state actors are relatively weaker than state actors in terms of support capability, they have become the benefactor in categories III and IV in Table 3.2. In a narrow sense, there is only one prominent case of category III in which a former rebel group, RCD (The Congolese Rally for Democracy; Rassemblement Congolais pour la Démocratie in French), provided the Burundian government with valuable intelligence in the 1990s (Sarkees & Schafer, 2000, pp. 629–630). Broadly speaking, the literature on ‘weak states’ and organized crime

provide plenty of examples of a non-state and state proxy relationship (III) whereby a state is employed as a proxy by an organized crime group. In the literature, category III can be applied to some countries where state institutions function mainly as mechanisms for officials to achieve their personal (private) gain (Avant, 2005, 24). Kimberley Thachuk (2005), an intelligence analyst who focuses on transnational threats, further described this hollowing out of state institutions:

> terrorists and organized criminals have duped and suborned individuals in governments into virtually selling their sovereignty so as to create 'state of convenience' from which to conduct international operations… In other words, rather than being agents of government in their official capacities, individuals are the government. (pp. 143–146)

Atanas Atanasov, a member of the Bulgarian parliament and a former counterintelligence chief, also argued that while other countries have the mafia, the mafia has Bulgaria (Naím, 2012, p. 105).

Table 3.3. Possibility for Each Combination of P-A

	Proxy Warfare	Cyber Proxy Warfare
I. State(s) - State(s)	High (*Permanent)	Low
II. State(s) - Non-state Actor(s)	High (*Permanent)	High (*State-sponsored Cyberoperations)
III. Non-state Actor(s) - State(s)	Low, but Possible	Low
IV. Non-state Actor(s) - Non-state Actor(s)	High (*Since the end of the Cold War)	High (*Cybercrimes)

While it is difficult to name cases of the fourth relationship (IV) between non-state actors due to the covert and blurred nature of this relationship, the fourth category is one of the most

crucial relationship types for understanding proxy warfare over a longer period of time. Above all, the category illustrates the fact that proxy warfare is not required to include a state at all. Through an empirical case, Mumford (2013) emphasized that this category IV relationship is essential in the age of non-state actors and networked terrorism: "the establishment of global al-Qaeda 'franchises' has distinctly affected the mode by which regional conflicts can be influenced by the proxy involvement of such networked cells, particularly at the behest of with the cooperation of 'rogue states'" (p. 8). Furthermore, when ISIS had a parastatal position, it indirectly engaged in local conflicts in the Middle East and Africa via small, local rebel proxy groups who secretly pledged allegiance to ISIS. Although the fourth relationship does exist, Types I and II (led by state actors) are more clear, prevalent, and measurable than Type III and IV, which are sponsored by non-state actors due to the size and scale of proxy warfare.

These four relationship combinations can be applied to cyber proxy warfare. Both state and non-state actors have played critical roles in cyberspace. Each actor can easily make a secret and informal contract with another for cyber proxy operations based on borderless temporal and spatial characteristics. However, according to the empirical evidence on massive and organized cyberoperations,[67] the state and non-state proxy relationship (II) is more prevalent than others for a few reasons. First, non-state actor-led cyberattacks without states used to be categorized as cybercrimes. In general, these are not massive and complicated operations. Moreover, these attacks are more focused on short-term financial benefits than long-term political gains. Thus, the non-state actors can be classified only as cybercriminals.

[67] The following list includes empirical evidence about massive and organized cyberoperations. Russia-associated non-state actors conducted cyberoperations against the critical infrastructure of Estonia, Georgia, Ukraine, and the United States. The United States and Israel were accused of conducting the Stuxnet attack on Iranian nuclear facilities. North Korea has been arguably suspected of causing several massive, organized cyberoperations, such as the 2009 Sony hack and the 2017 WannaCry ransomware attack.

Second, on the sponsor's side, a state prefers non-state actors to states as its proxy. Chosen proxies are vulnerable in cyberspace to sponsor states as sovereign powers. In contrast to traditional proxies, cyber proxies equipped with cyber arms cannot operate as independent entities who can later engage in resistance against their principals. Whether a state is strong or weak, a state actor in international relations is technically an independent sovereign entity that cannot be easily controllable by others. This means that hiring state actors as proxies is not a good option for sponsors who are pursuing aggressive cyber proxy operations. Therefore, it is reasonable to assume that states (Actor A) are more likely to employ non-state actors (Actor B), under their sovereign powers to compel opponents (Actor C), to fulfill the preference of other two actors, primarily Actor A. In this vein, well-known massive and organized cyber proxy operations that associate with political interests of some states, such as Russia, China, North Korea, and Iran, arguably fall into the state and non-state proxy relationship (II).

The second question to be addressed in this section relates to the three distance degrees between the principal and agent. Maurer (2018) suggested three main types of the proxy relationship to illustrate a spectrum of control and detachment between the principal and agent: delegation, orchestration, and sanctioning (p. 42). His classification system is borrowed in this study but revised to be more generally applicable to the distance between state and non-state actors in cyber proxy warfare. Measuring the distance between a principal, Actor A, and an agent, Actor B, is essential to understanding the mechanism of proxy warfare. The distance is also a critical indicator of the characteristics, scale, intensity, or duration of proxy warfare. Three classifications of the relationship between principal and agent can be ordered by distance: delegating, encouraging, and sheltering (Table 3.4).

Table 3.4. Three Distance Degrees between Principals-Agents

		Delegating	Encouraging	Sheltering
Distance Degrees between P-A		Close *Hierarchical relationships	Medium *Horizontal Relationships	Far *No Linear Relationships
Role of Agents		Active	Partially Active	Passive
Control Mechanism: (1) Screening and Selection, (2) Monitoring, (3) Punitive Measures		High	Medium	Low
Plausible Deniability of Principals	Proxy Warfare	Low	Medium	High
	Cyber Proxy Warfare	High or Low	High or Medium	High

In the narrow sense, proxy warfare relationships can be only understood through delegating, in which a sponsor delegates authority to a proxy to act on its behalf through covert and informal contracts. Principal-agent theory rooted in concepts of delegation in economics and other social science fields, including security studies (Kiser, 1999; Moe, 1984; Ross, 1973). Delegating diverges from the other two models, encouraging and sheltering, due to three assumptions. The first assumption is that the delegation relationship is not official, but formed based on contracts (covert or open) (Maurer, 2018, p. 43). Making contracts brings the principal and agent closer together than the other two models. Based on a contract, each actor in this relationship expects active and explicit mutual exchanges that while a sponsor provides military or non-military assistance for a proxy, a proxy maximizes a sponsor's interests through a direct conflict on behalf of its sponsor. In other words, one actor shares active support and clear mutual targets and interests with another in the delegating model. Thus, sponsors can enable their proxies to conduct clear, massive, complicated, and effective military operations against mutual targets that would maximize the interests of sponsors. Lastly, sponsors have access to imperfect, but real control mechanisms: (1) screening and selection; (2) monitoring; and (3) punitive measures, prior to and during delegating in order to reduce risks of the agency problem (see Table 3.4). In the latter two

relationships, encouraging and sheltering, principals can also have access to three control mechanisms. However, in the two relationships, a principal only has the limited capability to punish a proxy because they have never exchanged explicit materials or mutual targets actively based on a contract. Therefore, in general, delegating describes hierarchical relationships between sponsors and proxies (Maurer, 2018, p. 46).

Delegating cannot illustrate all possible proxy relationships. Contrary to the delegating model, some actors passively use proxy mechanisms to maximize their interests, while they keep a distance from third parties. A principal does not seek to make a contract with an agent. Some of them do not provide direct assistance for their third parties. Sometimes the third parties do not realize that they are employed as proxies by other actors. Although the relationships between principals and agents are weak without tangible contracts, these relationships also behave like the archetypal proxy relationship, delegation. In this regard, Daniel Byman (2005) emphasized that open and active proxy relationships are blessedly rare, and have decreased since the end of the Cold War (p. 117). Therefore, Encouraging and Sheltering models can fall into proxy relationships, along with delegating.

The encouraging model attracts voluntary participation from other third-party actors in a conflict by providing them with ideational and material support in pursuit of political goals (Maurer, 2018, p. 45). In an encouraging relationship, a sponsor emphasizes the ideational dimension, such as nationalism and religion, to encourage proxies to participate in a conflict on its behalf. A sponsor prefers to encourage a proxy who has correlated goals or targets originating from the shared ideational values between them. Political scientists Kenneth Abott and his co-authors argued that correlated goals between the encourager as a sponsor and the volunteer as a proxy are “constitutive of their relationship” (Abbott, Genschel, Snidal, & Zangl, 2015, p. 18). In

other words, the hiring mechanism (voluntary) in an encouraging relationship diverges from that of a delegating one. While proxies acknowledge the importance of material support from sponsors, they place correlated goals based on ideational values over other benefits. Therefore, in terms of the correlated goals, encouraging describes horizontal relationships between the sponsor and proxy. It also means that an encourager principal has limited capability to punish its proxies when their goal diverges from that of their own.

The third model, sheltering, is a looser proxy relationship than the encouraging model. In this weak proxy relationship, proxies' malicious activities are based on passive and indirect support from a sponsor who stands by in spite of having the capacity to control the proxies. Their relationships are not formed based on contracts and mutual material or ideational exchanges. The sponsor and proxy ostensibly do not share correlated goals in pursuit of political interests. Thus, sheltering can be understood as the least passive support proxy relationship that is formed or run with the connivance of a sponsor. Moreover, one or more of the following three different factors can drive a sponsor's toleration of a proxy's malicious activity within its controllable range. First, sheltering occurs when a proxy's malicious activity does not pose a threat to a sponsor while simultaneously increasing a sponsor's self-interests. Second, a sponsor's toleration is more cost-effective than its active support. Last, sheltering involves a discrepancy between the sponsor's projected capacity or aspirational status and its de facto capacity and power (Maurer, 2018, p. 47). However, contrary to the previous two relationships, this loose relationship between principal and agent cannot be measured as a linear relationship. It seems like that one actor on the principal enjoys malicious activities, including a conflict with its opposite, of another side without direct support and direction or the shared goals.

These three degrees of distance can be applicable to cyber proxy warfare led by mainly sovereign states. First, as a principal actor, a sovereign state can delegate its monopoly over legitimate violence to cyber-proxy non-state actors under a contract to conduct aggressive cyberoperations that would benefit the state itself. The cyber principal can have access to more strong control mechanisms because cyber proxies are vulnerable to their sponsors in the real world. This means that cyber proxies and their cyberoperations in delegating relationships are controllable under the direction of sponsors. Thus, these proxies can conduct complicated, massive, and intended cyberattacks on targets with full support from sponsors. For instance, some non-state actors pursuing political goals organized massive cyberattacks with complicated hacking tools, which small, non-state cybercriminals could not undertake. The non-state actors are not conventional regular army combatants under the laws of war, but cyberwarriors who are closely related to or hired by principals through contracts. Sometimes principals disguise themselves as proxies. This also includes cyber "false flag." A false flag means a covert operation designed to deceive. The term "false flag" origins from a pirate ship that flew a flag of a state as a disguise to prevent its victims from fleeing or preparing for battle. In cyberspace, false flags also refer to tactics used in covert cyberoperations by a perpetrator to deceive or misguide attribution. For a false flag, the perpetrator intentionally provides its fake origin, identity, movement, and coding or exploitation patterns.

Second, a sponsor can intentionally encourage other actors with correlated goals. For example, many Russian internet users, including professional hackers, were encouraged under the guise of Russian nationalism to participate in the 2007 and 2008 cyberattacks on Estonia and Georgia.

Third, some states do nothing as non-state cyber actors conduct malicious activities that might indirectly benefit these states. In this regard, it is suspected that the Chinese government does not take action against individual Chinese and North Korean hackers (operating inside China) who conduct cyber espionage against the United States.

The Ways of Assistances to Proxies

The primary goal of assistance in proxy warfare is to equip, arm, and train a proxy to fight against a common target on behalf of a sponsor (under a covert contract). Moreover, while a proxy can benefit indirectly from its direct involvement in a conflict, it can also be directly rewarded with assistance from a sponsor. Thus, types of assistance can be understood as everything needed to strengthen and benefit a proxy in the course of pursuing the sponsor's goals. Nevertheless, these types of assistance can be broadly divided into two categories: material and non-material support.

First, material assistance is real and tangible support necessary for a proxy to be ready to engage in a fight. Material assistance to a proxy includes a broad range of items: military weapons, equipment, foodstuffs, providing human capital, and providing financial aid (Mumford, 2013, pp. 61–75). Military weapons and equipment, such as arms, ammunition, and other military technology, directly enable a proxy group to arm itself. Sending human capital can expand the size of the warring fraction. Principals use this is a primary way to convince others to fight on their behalf. However, it is not easy to supply these materials directly as the exchange can expose a sponsor's relationship with its proxy. Others can easily trace transfers of tangible materials.

In this regard, financial aid is a more attractive and flexible option for both the sponsor and proxy. Money transfers to a chosen agent provide more cover for a sponsor than supplying

weapons, for example (Mumford, 2013, pp. 65–66). In this case, a principal does not need to gather weapons for the proxy. A proxy can also use the money for various purposes, such as purchasing weapons, equipment, and food; hiring combatants; paying wages; constructing basecamps and buildings; and forming relationships with other friendly actors. Despite these benefits, money transfers can be traced. A proxy is likely to have difficulty buying the aforementioned materials itself in a troubled area as well as from other entities, including the international community. In general, proxies may not be eligible members of the international community, and therefore cannot participate in international trade. Thus, balancing between supplying real materials and sending money is vital in preparing a proxy to be ready to fight on behalf of a sponsor.

Second, while non-material support is not a direct way to arm a proxy, it essential for proxy warfare strategy in a big picture sense. It can be understood as an indirect way to strengthen a proxy and its military operations. It ranges from sharing military training programs, doctrine, and strategy, to making political ideas and policies, to setting up a favorable international opinion, and to psychological support, including boosting morale and motivating its combatants (Mumford, 2013, pp. 67–69). These can be summed up as "soft power," an international politics concept which Joseph Nye conceptualized as "the ability to get what you want through attraction rather than coercion or payments" (Nye, 2004, x). Members of a proxy group could become professional combatants through a sponsor's military training programs. Leaders of a proxy group could command their troops with the sponsor's military doctrine and strategy. Favorable international opinions could legitimate the aggressive activities of a proxy unit in a conflict. Moreover, the sponsor's psychological support could provide a sense of security for a proxy unit.

Therefore, indirect non-material support can be recognized as another pillar, along with direct material assistance, which enables a proxy to fight on behalf of a principal.

A cyber proxy is also in need of the same material and non-material assistance from a principal. Material assistance enables cyber proxies to target computers or networks of others on behalf of a sponsor through funding IT infrastructure, IT equipment, and cyber weapons, such as hacking tools and malware. Non-material support, however, especially sovereign protection, has played a more pivotal role in cyber proxy warfare. Armed cyber proxies with virtual weapons and fighting skills are vulnerable to physical power. While cyber proxies and their malware are everywhere in the virtual space, proxy's physical bodies and IT devices are located in a physical place belonging to sovereign territory. This means that when their identity and locations are exposed, they cannot resist against a sovereign power in their particular location. Therefore, in order for cyber proxy warfare to be successful from a sponsor's point of view, cyber proxies and their illegal behaviors in cyberspace must be directly and indirectly protected and guaranteed by a sovereign power.

Proxy's Autonomy

Problems of agency are critical points of discussion in principal-agent theory in every social science field, including economics, sociology, and political science. An agency problem is defined as a conflict of interest inherent in any relationship where one party is expected to act in another's best interest (Eisenhardt, 1989, p. 58; Ross, 1973, p. 134). In general, the problem stems from adverse selection or moral hazard of proxies, the imperfect alignment of interests or information asymmetries between principals and agents, or the mixture of two or more of the aforementioned causes (Fama, 1980, pp. 299–300; Moe, 1984, pp. 754–756). For instance, although a proxy makes a contract with a sponsor to pursue interests of its sponsor as well as its

own under the sponsor's assistance, the proxy is incentivized to take actions that run against the preference of its sponsor. Thus, principals must design mechanisms for screening, monitoring, and incentivizing agents to mitigate this critical problem (Milgrom & Roberts, 1992, p. 168; Moe, 1984, pp. 754–7).

Proxy warfare literature based on principal-agent theory cannot be divorced from the agency problem. Erica Borghard (2014, pp. 25–31) highlightes that the problem is the best among the core assumption of P-A theory that can be applied to proxy warfare literature. More specifically, she argues the clandestine and informal nature of a proxy warfare relationship between a principal and agent increases the possibility of agency loss (Borghard, 2014). Throughout proxy warfare literature, the agency problem has been presented as a sponsor's loss of control on their remote proxies at the end of an operation. Despite principals' control mechanisms, weak and unofficial relationships between both actors under clandestine and informal contracts give remote proxies a certain degree of autonomy.

An informal relationship between a sponsor and proxy, based on a secret contract, hides the identity of a sponsor at the beginning of the relationship, but it also weakens the sponsor's control capabilities. In proxy warfare literature, sponsors' assistance to proxies can enhance the autonomy of proxies. Funds and weapons from sponsors expand the size of armed proxy groups or proxy states and make them more skillful. These well-equipped militia groups or states can become an independent local power in troubled areas. Moreover, on some occasions, a proxy group could be incentivized to take action against their sponsors or their interests as a form of self-help; as the proxy groups have expanded power, their interests have changed, diverging from the sponsor's preference. In other words, sponsors' financial and military assistance can make their proxies uncontrollable.

In contrast to the physical world, it is difficult for cyber proxies to betray their sponsors. A cyber proxy relationship is similar to conventional proxy relationships in that it is based on a clandestine and informal contract. Nevertheless, even after becoming powerful online through sponsors' assistance, cyber proxies cannot become independent entities for three reasons: they only wield power in cyberspace; they reside in the sovereign territories of sponsors; and they pretend to be third parties when in reality they are sponsors' employees.

First, despite their powerful online activities, the capability of cyber proxies does not extend to physical power they might use to protect themselves. With funds from sponsors, cyber proxies can conduct cyberoperations against targets with ICT equipment and infrastructure, places, legal protection, and cyber weapons, such as malware, backdoor information about targets, or hacking tools, provided from sponsors. These types of assistance make cyber proxies powerful in cyberspace. However, this assistance does not separate proxies from sponsors. While proxies are armed and equipped in the virtual space, they are still just unarmed civilians who cannot take action that diverge from their sponsor's preferences. In other words, a sponsor's assistance to cyber proxies does not help promote proxy autonomy from the sponsor.

Second, cyber proxies are vulnerable to sovereign power. While cyberspace is a new domain, it is not separate from the real world. Although cyber proxies conduct their operations online, they, their ICT devices, and their infrastructure are located in a specific place under the control of a state's sovereign power. It follows that a state has sufficient control mechanisms over cyber proxies within its sovereign territory. Even though cyber proxies can conduct their operations abroad, they are in need of the sovereign protection of a sponsor. Namely, on the one hand, they can only go to other countries, which have a good relationship with their sponsor. On the other hand, they should go back to its sponsor's territory from other countries, where they

conducted cyberoperations, immediately after the operations in order to avoid the investigation of victim countries. Thus, as cybercriminals, proxies cannot escape the umbrella of their sponsor's sovereign power.

Lastly, the anonymous and borderless characteristics of the virtual world enable official employees of sponsors to pretend to be a third-party proxy. The official employees can also attack targets with fake nicknames, IP addresses, hacking tools, VPNs, DDNS, or hop points, like other cyber proxies. However, they are sponsors themselves or under official contracts with sponsors already. This means that those in the last category have little chance of betraying their sponsors or pursuing their own interests.

Unlike conventional proxies, cyber proxies cannot threaten their sponsors because they have so little autonomy. When traditional proxies need financial and military assistance to be powerful, they make clandestine and unofficial contracts with principals based on their common interests. However, there are many cases in which the proxy became powerful enough to resist their sponsor (after receiving supports); at that point, the proxy's interests had diverged from those of the sponsor (Borghard, 2014). The sponsor's assistance was sufficient enough to arm and equip proxies to survive in troubled areas. Although cyber proxies also receive support from their sponsors, they cannot become independent entities who can stand against their sponsors. Support provided for cyberoperations only allows cyber proxies to go to war in cyberspace. Therefore, it is understood that because cyber proxies have little autonomy, they are effectively subordinate to their sponsors.

Sponsor's Control Mechanisms

In traditional proxy warfare, clandestine and informal relationships between sponsors and proxies have required sponsors to limit proxies' autonomy because this autonomy can cause an

agent problem. These control mechanisms can be broken into three stages: screening and selection, monitoring, punitive Measures. While the three stages cannot guarantee sponsor control traditional proxies, these three stages are more applicable to cyber proxy warfare strategy.

In the first stage, screening and selecting controllable proxies is the primary condition for both traditional and cyber proxy operations. Sponsors need proxies who are not only easily armed, equipped, and trained with their assistance, but also have mutual interests. Despite these needs, the relationship is useless if proxies will break these contracts with sponsors later. Daniel Byman and Sarah E. Kreps (2010) said that a principal will select agents whose own preferences are naturally suited to those of the principal in order to minimize loss of agency (p. 10). According to Idean Salehyan (2010), the screening process involves searching for proxies "who share ethnic, religious, and linguistic kinship ties to the state… ethnic kin are more likely to share the patron's preferences, or at least be perceived to do so" (p. 505). A sponsor will search for plausible proxies with common interests in order to reduce the risk of losing them later. Thus, in the case of both traditional and cyber proxy operations, sponsors prefer controllable and less powerful proxies over less controllable but more powerful ones.

In the second stage, where proxies are armed and proxy operations commence, sponsors begin to control their proxies through a passive method—monitoring—which ranges from requiring audits and reports from proxies to so-called "fire alarms," which involved other third parties who warn a sponsor about an agent's unexpected behavior (Byman & Kreps, 2010, p. 10; Maurer, 2018, p. 44; Salehyan, 2010, p. 502). For instance, media and non-government organizations often play the latter role by documenting violent activities by proxies during a conflict. However, effective monitoring cannot be achieved in reality. In a proxy warfare

strategy, sponsors are supposed to keep a physical distance from their proxies in order to deny their involvement in a conflict. During operations, sponsors have only one option to monitor whether their remote proxies take proper actions for their shared goals or not while taking a step back. Sponsors can signal to proxies to correct mistakes the proxies made during the operation. However, passive signals are not a strong enough mechanism to change the behavior of proxies. Proxies are likely not only to miss, but also ignore, sponsor signals. In addition, it is difficult for sponsors to send messages to proxies while avoiding attention, mainly from the international community. Furthermore, timing presents a difficult issue for sponsors. Sponsors can reveal their dissatisfaction with and complaints about proxies after the operations, but by then it is too late. Thus, monitoring is just a passive control mechanism to correct the direction of operations led by proxies.

In the last stage, sponsors can try to control their proxies through various punitive measures, including reductions in material or non-material assistance, abandoning the proxy altogether, and arresting or killing the proxy. Compared to monitoring, these control methods are tangible, decisive, and sometimes permanent. However, it is difficult for a principal to officially punish a proxy due to their covert relationship. A sponsor must keep a distance from a proxy-led conflict in order to maintain plausible deniability. Furthermore, any punishment would work only in the case of some small or weak proxies who are not ready to be independent of their sponsors. In other words, sometimes a principal cannot punish an uncontrollable proxy who can survive on its own in a troubled area. Moreover, a principal should consider that continuous resistances by a well-armed proxy are hampering its efforts to punish. Thus, these punitive methods are also not the best way to control proxies.

Contrary to traditional proxies, these punitive measures can be applied to cyber proxies. These new, virtual agents cannot grow into independent entities separate from a principal. While agents are armed and equipped with material and non-material support from sponsors in cyberspace, they are not armed to resist against their sponsors in the real world. This means that when a principal wants to punish a cyber proxy who betrayed them, the proxy cannot avoid punishment. Therefore, the lack of cyber proxy autonomy makes them more dependent on principals. Moreover, these tangible control mechanisms make cyber proxy warfare strategy more attractive to state actors as principals than traditional proxy warfare strategy.

3.3.3 *Consequences: Attribution/Retaliation/Deterrence*

Attribution can be defined as the art of answering a question. As the initial action doing attribution is determining the identity of the perpetrator involved in any of hostile activities ranging from a crime to a massacre in order to impose responsibility on the perpetrator. It is also at the core of all forms of coercion and deterrence—international and domestic—to prevent the recurrence of similar hostile activities (Rid & Buchanan, 2015, p. 4).

Proxy relationships are formed to make it more difficult to attribute the cause, source, or origin of an armed conflict to a specific actor; a sponsor wants to avoid potential domestic or international risks from the result of an attribution connected to the sponsor itself. A sponsor employs a proxy to shift all the responsibility of armed conflict to the proxy. The hired agent actively claims the credit for a conflict. However, the attribution problem has not been extensively discussed in proxy warfare literature. Proxy warfare scholars have focused on other topics, such as covert operations or plausible deniability.

Attribution is a critical aspect of cyber proxy warfare. It has been recognized as the primary issue at hand in the resolution of many cybersecurity problems including individual deviant

behaviors, crimes, and state-associated operations (Lupovici, 2014; Rid & Buchanan, 2015; Robinson, Jones, & Janicke, 2015). In the information age, diverse actors have participated in a countless number of activities in the new anarchical domain of cyberspace which ideally guarantees the anonymity and movement of information. Thus, the intrinsic nature of cyberspace makes the attribution process difficult. For example, law enforcement agencies struggle with attribution of cybercrimes. Cybercriminals and criminal groups have enjoyed the anarchical characteristics of the virtual space in order to avoid legal punishment. In other words, law enforcement agencies have difficulty finding evidence in order to attribute a cybercrime to a specific individual or organization.

In this context, it seems that state actors' national interests have also benefited from the cyberoperations attribution problem. A large number of cybersecurity studies pay attention to attribution problem as the primary burden in mitigating cyber threats (Kello, 2013, p. 33; Lupovici, 2014, p. 339; Rid & Buchanan, 2015). According to Jon R. Lindsay (2013), penetrators can disguise themselves in various technical ways, such as "aliased accounts, multiple user identities, forged or stolen credentials, obfuscated file properties, strong encryption, proxy servers, virtual private networks [VPNs], and the ability to route attacks across multiple organizational and international jurisdictions," (p. 377) to obscure the origin of attack. Furthermore, Amir Lupovici (2014) points out that state actors face technical challenges (p. 399). For example, cybersecurity experts could not find definitive evidence of Russia's engagement in the cyberattack on Georgia during the confrontation between these two countries in August 2008 (Deibert, Rohozinski, & Crete-Nishihata, 2012).

These technical challenges hinder defenders from attributing state-associated cyberattacks to a suspect actor. Moreover, proxy warfare strategy intensifies the attribution problem due to two

key factors. First, using a cyber proxy actor's name is one technical way to obscure the origin of a cyberattack. Second, a hired proxy actor can also use one or more technical ways to hide its own identity. This helps a sponsor keep a distance from its proxy as well as the cyberattack. Ultimately, the collaboration between cyber proxy strategy and other technical challenges can generate a significant synergy effect for sponsor states who want to avoid internal and external risks. Therefore, the core of a cyber proxy warfare strategy is for a sponsor to hire cyber proxies in order to avoid attribution. For example, private cybersecurity company FireEye's effort to trace advanced persistent threat (APT)[68] groups sheds light on some state actors, especially China, Russia, and North Korea, who have given direction and support to the APT groups in order to disturb attribution process of defenders (FireEye, n.d.).

3.4 Overview: North Korea-associated Cyberoperations

3.4.1 *A Brief History of North Korea-associated Cyberoperations*

North Korea's cyberoperations began to attract public attention in the late 2000s. In the beginning, state cyberwarriors targeted critical infrastructure and websites of other countries with a destructive, but simple hacking method known as a "DDoS attack" (Jong-Hwan Shin, 2013). As time went on, North Korea's cyberoperations' methods and targets became increasingly complicated and diverse based on its goals and interests. Moreover, North Korea's malicious cyberactivities have had a significant impact on the national security of other countries, mainly South Korea and the U.S.

[68] APT stands for advanced persistent threat. It is a broad term used to describe a cyberattack campaign in which an intruder, or group of intruders, establishes an illicit, long-term presence on a network or computer in order to mine highly sensitive data of victims (Incapsula, n.d.).

North Korea's cyberoperations was not one of the global issues until July 2009. North Korea started to carry out cyberoperations. Hackers or hacker groups allegedly associated with Pyongyang tested "logic bombs"[69] on South Korea in 2007, sent Trojan horse[70] email to South Korean military officers in 2008, and hacked South Korea's Chemical Accident Response Information System (CARIS) in 2009. Despite having a major impact on South Korean society, these hacking incidents did not attract global attention.

In July 2009, when important websites in the United States and South Korea were taken down by DDoS attacks, the illegal activities of North Korean-affiliated hackers started to attract public attention, including the attention of security experts and political leaders across the globe. As shown in Table 3.5, on July 4, 2009, the first wave of the DDoS attacks (July 4–5) targeted twenty-one government websites as well as websites of U.S-based private financial and media companies. Victims of its second wave (July 6–7) included U.S. and South Korean government and private websites. The third (July 8–9) and fourth (July 9–10) waves followed and shut down several public and private websites in the United States and South Korea. More interestingly, the July 2009 DDoS Cyberattacks marked a significant turning point for South Korea's cyber-threat policy. The attacks accelerated the establishment of Republic of Korea's Cyber Command on January 1, 2010 based on South Korea's Military Reform Plan 2020 (Min-Seok Kim, 2009; ROK Military Reform Committee, 2005). Since then, despite the efforts of the two countries, North Korea continued to carry out several DDoS-based cyberattacks against South Korea: March 2011

[69] A logic bomb refers to "malicious application logic that is executed, or triggered, only under certain (often narrow) circumstances (Fratantonio et al., 2016).

[70] Trojan horses or Trojans are a type of malware that is disguised as legitimate software. They can be understood as impostors, which claim to be something desirable but, in fact, are malicious. Trojans are different from true viruses because they do not replicate themselves, as viruses do. Trojans' malicious codes can be employed by hackers trying to gain access to targets' or victims' systems (Kaspersky Lab, n.d.; Symantec, 2016).

DDoS attacks on several websites, including U.S. Forces in Korea, Cyberattacks on Nonghyup Bank in April 2011, DarkSeoul in March 2013, and the 6/25 Cyber Attacks in June 2013.

Table 3.5. Timeline of the July 2009 DDoS Cyberattacks

	Date (EST)	Major Targets
1st Wave	July 4 - 5, 2009	21 U.S. government websites, several financial and other websites
2nd Wave	July 6 - 7, 2009	14 U.S. and 12 South Korean government websites, financial and cybersecurity companies in the two states
3rd Wave	July 8 - 9, 2009	1 U.S. and 15 South Korean government websites, U.S. Forces in Korea, and other private sectors
4th Wave	July 10 - 11, 2009	7 South Korean government websites and other private sectors

Source: *Jong-Hwan Shin, 2013, p. 43*.

During this period, North Korea's tactics for cyberattacks evolved. The state started to use types of Advanced Persistent Threat (APT) for its cyberoperations, along with DDoS attacks. Russia-based cybersecurity company Kaspersky Lab discovered an ongoing North Korean APT cyber campaign in March 2013 which targeted the ROK Ministry of Unification, two think tanks, the Sejong Institute, the Korea Institute for Defense Analyses (KIDA), and a South Korean logistics company, Hyundai Merchant Marine (Tarakanov, 2013). Kaspersky Lab Malware researcher, Dmitry Tarakanov, dubbed this APT campaign "Operation Kimsuky" because the two master email accounts that control the campaign were registered by "kimsukyang" and "Kim asdfa" (Infosecurity, 2013).

While researcher Tarakanov said what he found was the early stages of an unsophisticated but extensive and highly targeted campaign, he attributed it to North Korea based on some evidence: the compilation path string contained Korean hieroglyphs; they targeted South Korea's websites only; the drop box mail accounts iop110112@hotmail.com and rsh1213@hotmail.com were registered with the *kim* names ("kimsukyang" and "Kim asdfa"; and ten IP-addresses used

by the Kimsuky operators were all registered in the two Chinese provinces adjacent to North Korea (Tarakanov, 2013). “Kimsuky” was still detected by cybersecurity companies after the campaign (AhnLab Security Emergency Response Center, 2014).

The 2014 Sony hack astonished the U.S. government and its citizens, as well as others around the world. On November 24, 2014, confidential data from Sony Pictures Entertainment was leaked to the internet by a hacker group who called themselves the Guardians of Peace (GOP). The data included personal data of company employees and their families: salaries; social security numbers; email exchanges between employees, scripts and various versions of unreleased new movies in production at Sony; as well as other information (Siboni & Siman-Tov, 2014, p. 1). At the same time, Sony’s networks were attacked with destructive malware (Novetta Threat Research Group, 2016, p. 21). Although GOP claimed to take credit for the hack, the Federal Bureau of Investigation (FBI) held North Korea responsible for the attack (Federal Bureau of Investigation, 2014).

North Korea has also been accused of being behind financial benefits-related cyberoperations designed to ensure regime survival, such as hacking banks and cryptocurrency exchanges; spreading ransomware; and selling malware or hacking tools across the globe. Two interesting examples are the SWIFT-related bank heists known as the Bangladesh Bank Robbery and the WannaCry ransomware attack which took place in 2016 and 2017 respectively.

The first bank robbery occurred between February 4th and 5th in 2016. North Korea-associated hackers attempted to steal $951 million U.S. dollars from Bangladesh Bank, the central bank of Bangladesh, when the bank’s offices were closed, via the Federal Reserve Bank of New York. The hackers managed to compromise Bangladesh Bank’s computer network and to observe the transfers process. Then they gained access to the bank’s credentials for payment

transfers. They used these credentials to authorize around three dozen requests to the Federal Reserve Bank of New York to transfer funds from the account of Bangladesh Bank to accounts in Sri Lanka and the Philippines. Fortunately, the hackers only succeeded in completing 5 of the transactions, with $20 million U.S. dollars traced to Sri Lanka (all recovered) and $81 million U.S. dollars traced to the Philippines (approximately $18 million U.S. dollars recovered). The FBI and several security companies, including Symantec and BAE Systems, said that North Korea-based hacking group was probably behind the cyberattack (Barrett & O'Keeffe, 2016; Symantec Security Response, 2016b).

Second, computers running older Microsoft Windows operating systems around the world were targeted through an exposed vulnerable SMB port by WannaCry ransomware between May 12–15, 2017. More than 200,000 computers in 150 countries (including, China, Russia, the United Kingdom, and the United States) were affected; victims included hospitals, telecommunications companies, banks, and warehouses. It is known as the 2017 WannaCry ransomware attack. Data in the targeted computers were encrypted. Individuals, organizations, or companies who wanted to recover their computers and data were demanded to pay a ransom or lose everything. Following the claim of Symantec and Kaspersky Lab that the code had some similarities with that previously used by a North Korea-sponsored hacker group, Brad Smith, president of Microsoft, said he believed North Korea initiated the ransomware attack (GReAT, 2017; Harley, 2017; Symantec Security Response, 2017b). Moreover, in December 2017, the United States, the United Kingdom, Japan, Canada, and New Zealand, among other countries, officially held North Korea responsible for the attack (Ministry of Foreign Affairs of Japan, 2017; U.K. Foreign & Commonwealth Office, 2017; The White House, 2017a).

North Korea has also tried to earn money by selling malware or hacking tools. North Korean IT experts, including state-sponsored hackers, have been sent to China and Southeast Asian countries to make illegal software programs. In 2011, the Seoul metropolitan police agency arrested four South Korean criminals and one Chinese criminal. They had hacked online gaming sites and had collaborated with North Korean hackers who worked in Chosun Rungrado Trading Company (조선릉라도무역총회사 in Korean) under the control of North Korea's spy agency's Unit 39 after graduating from Kim Il Sung University (Associated Press, 2011). The police agency pointed to the Korea Computer Center as another alleged culprit. In 2013, three South Koreans were arrested for operating an illegal home trading system website tied to North Korean hackers (Dong-Un Kim, 2013). According to the South Korean prosecution, North Korean hackers provided hacking tools and malware for the site. Thus, those North Korea-led cybercrimes can be recognized as one source of money under its economically isolated condition.

As a new trend, these three stories show that there has been an important change in the target and purpose of North Korea's cyberoperations. North Korea has widened its target countries beyond South Korea and the U.S. In these cases, cyberoperations place more weight on financial targets rather than critical infrastructure ones. The change means that North Korea has recently started to focus on a more short-term goal: earning money. Despite that, the new trend needs to be analyzed alongside North Korea's larger goal of regime survival. These attacks appear to be just financially driven attacks. However, the recent pressure of international economic sanctions against North Korea and its nuclear programs has led the state to conduct cybercrimes to earn money. In other words, the new trend also contributes to North Korea's ultimate political goal of regime survival through hostile, aggressive cyberoperations.

Nevertheless, the North Korean regime has still conducted cyberattacks on critical infrastructure of its enemies since the late 2000s in pursuit of this larger goal of regime survival. It is undeniable that North Korea's current hacks against financial entities, including cryptocurrency exchanges, have attracted attention from around the world. Sometimes, however, these financially motivated hacks turn attention away from North Korea's traditional targets, critical national infrastructure. In December 2014, blueprints and test data for Korea Hydro & Nuclear Power (KHNP), the South Korean nuclear operator, were leaked by North Korea-associated hackers who identified themselves by the name "Who Am I," claiming they were protesting against nuclear facilities (Joint Investigation Group, 2015). The hackers leaked the information over social media, presumably to try to create public panic and to disrupt South Korean energy policies. Even though South Korean officials claimed that only non-critical nuclear data was leaked in the breach, it cannot be overlooked that the South was exposed to the potential risks of blackout as well as radioactive contamination (Park & Beyer, 2017). In addition, FireEye (2017) said that North Korea hackers tried to hack U.S. electric companies in 2017. Table 3.6 illustrates twenty major North Korea's cyberoperations that had significant impacts on the national security of other countries, mainly South Korea and the U.S.

Table 3.6. A Short History of North Korea-associated Cyberoperations

Date (Local Time)		Name: Suspected Victim(s)	Technique/Tool	Aim[71]
1	7/4 – 7/9/09	July 2009 Cyberattacks: U.S. and South Korean government, financial, and media websites	DDoS (Symantec Security Response, 2016a)	Cyber Sabotage
2	3/4/11	3.4 DDoS Attacks: South Korean media, financial, and critical infrastructure, U.S. Forces Korea	DDoS (McAfee, 2011)	
3	4/12/11	Cyber Terror on NH Bank: South Korea' National Agricultural Cooperative Federation (Nonghyup Bank)	DDoS, Malware (Rahn Kim, 2011)	
4	3/20/13	3.20 Cyber Terror (Dark Seoul): South Korean broadcasters and financial Companies	DDoS, Malware (Sherstobitoff, Itai Liba, & Walter, 2013)	
5	3/1/13	Operation Kimsuky: Ministry of Unification, Sejong Institute, and Korea Institute for Defense Analyses	Spear Phishing & Phishing (Tarakanov, 2013; Alyac, 2018)	Cyber Espionage
6	6/25/13	6.25 Cyber Terror: South Korean government and news media websites, U.S. Forces Korea	DDoS, Malware (Symantec Security Response, 2013)	Cyber Sabotage
7	7/1/14	Compromise of the Seoul subway system: Seoul Metro	Watering hole (Hyun-Jeong Lee, 2015; Choi, 2015)	
8	11/1/14	The 2014 Sony Hack: Sony Pictures Entertainment	Spear Phishing, Malware (The White House, 2015; Shields, 2018)	Cyber Espionage
9	12/9/14 - 03/12/15	Hacking on KHNP (Korea Hydro & Nuclear Power)	Phishing, Malware (Joint Investigation Group, 2015)	
10	10/1/15	None: Members of the National Assembly	N/A (Shim, 2015)	
11	2/4 - 2/5/16	SWIFT-related Bangladesh bank heists: Bangladesh Central Bank, Tien Phong Bank, Banco Del Austro	Exploit, Watering hole, Malware (GReAT, 2017)	Cyber Finance-driven Operations
12	8/1/16	None: Email accounts of South Korean diplomats, journalists, and security officials	Spear Phishing (Hyung-Jin Kim, 2016; Pauli, 2016)	Cyber Espionage
13	8/4 - 9/23/16	The South Military Intranet hack: South Korea Military	Malware (Fifield, 2017)	
14	Oct. 2016	SWIFT-related Polish bank heists: Polish Bank	Watering hole, malware (Symantec Security Response, 2017a)	Cyber Finance-driven Operations
15	2016-2017	Targeting of U.S. Military Contractor: Lockheed Martin	Spear phishing, Malware (Shields, 2018)	Cyber Espionage
16	4/22/17-Early July/17	Compromise of Cryptocurrency Exchanges: Cryptocurrency exchanges in South Korea	Spear phishing, Malware (McNamara, 2017)	Cyber Finance-driven Operations
17	5/12-5/15/17	The WannaCry Ransomware: Worldwide	Ransomware (Symantec Security Response, 2017b)	
18	May, 2017	Targeting of Middle Eastern Organization: Egyptian company Orascom	Spear phishing, exploit, malware (FireEye, 2018)	Cyber Espionage
19	9/22/17	Targeting of U.S. electric companies: U.S. Electric Companies	Spear phishing (FireEye, 2017)	Cyber Sabotage
20	10/1-10/12/17	Compromise of Far Eastern International Bank in Taiwan: Far Eastern International Bank	Ransomware (BAE Systems, 2017)	Cyber Finance-driven Operations

* This table does not include cases of North Korea's cyber psychological warfare and selling malware and hacking tools.

[71] Aims of North Korea's cyberoperations will be detailed in the following chapter 3.4.2.

3.4.2 *Typology and Objectives of North Korea's Cyberoperations*

Typologies are a useful way to understand the goal of North Korea's cyberoperations and to manage them. However, there are no typologies that use clear criteria for North Korea's cyberattacks. Thus, this section explores a new typology based on a common standard: the short-term goals of the state's cyberoperations. Moreover, the typology illustrates that the short-term goals have contributed to North Korea's ultimate political goal, regime survival.

North Korea has ceaselessly conducted cyberoperations against the rest of the world, mainly South Korea and the United States, mainly since the late 2000s. As detailed in Figure 3.1, Lim et al. (2013, p. 16) classified its cyber threats into ten categories based on studies of other scholars: (1) Distributed Denial of Service (DDoS) [disrupting network service]; (2) Advanced Persistent Threat (APT); (3) Cyber Terrorism [destroying infrastructure]; (4) Cyber Espionage; (5) Cyber Intelligence Activities; (6) Internet Trolls; (7) Cyber Psychological Warfare with propaganda websites; (8) Manipulating Public Opinion; (9) Propaganda; and (10) Cyber Unification Movements.[72] These ten classifications show the diversity of North Korea's cyberactivities and the importance of cyberoperations for the state.

However, there is no consistency in Lim et al.'s typology. First, their standard of the classification is ambiguous. At least three different standards, types, purposes, or authors of cyberattacks, were applied in order to divide the types of North Korea's cyberattacks. Some of the categories also overlap. For example, types of North Korea's cyberoperations from category (6) to (10) can be combined under the name of (7) "cyber psychological warfare." Category (2),

[72] Lim and his co-researchers cited Yoon Kyu-sik's *North Korea's Cyber Warfare: The Capability and Threat* (2011) and Lee Sang-ho's *North Korea's Cyber-Based Psychological Warfare and South Korea's Deterrent Options* (2011) for their categories on North Korea's cyberoperations.

APT attacks, may also include Category (4), cyber espionage. Moreover, Category (3), cyber terrorism, narrowly defines terrorism as acts that only destroy infrastructure. Although there is no universally agreed definition of terrorism, it is broadly viewed as "the [systematic] use of force or violence or the threat of force or violence to change the behavior of society as a whole through the causation of fear and the targeting of specific parts of society in order to affect the entire society" (Garrison, 2004, p. 273). Cyber terrorism could include other categories, such as (1) and (2), because in these categories there is the systematic use of violence to cause fear in the greater society to make change in that society as well. Thus, the ambiguity of the existing typology is driving the need to make a new clear typology under common criteria.

Thomas Rid's simplified classification scheme is helpful in designing a new typology. For reasons of simplicity, Rid (2013a) suggests only three categories are necessary for classifying cyberoffenses: sabotage, espionage, and subversion (p. 10). All three aggressive online activities may involve states as well as private actors. He also uses these three divisions as a tool to emphasize his main argument that there is no cyberwar in the information age. This is a central difference from my argument that state-led cyberwar is real.

According to Rid, in contrast to the use of physical violence, such as guns and explosives, sabotage "is not ultimately focused on the human body as a vehicle to the human mind" (Rid, 2013a, p. 57). First and foremost, [cyber] sabotage refers to the attempt to "impair a technical or commercial network system and to achieve a particular effect by means of damaging that system" (Rid, 2013a, p. 57). He defines cyber espionage as "the clandestine collection of intelligence by intercepting communications between computers as well as breaking into somebody else's computer networks in order to exfiltrate data" (Rid, 2013a, p. 81). Lastly,

[cyber] subversion attempts "to undermine the trustworthiness, the integrity, and the constitution of an established authority or order" (Rid, 2013a, p. 116).

This study borrows Thomas Rid's simple classification system in creating a typology of Pyongyang's offensive cyberoperations; it has been revised, however, to be more generally applicable to these types of operations. Based on empirical data detailed in the last chapter, this study divides North Korea's aggressive cyberoperations into four types: sabotage, espionage, psychological warfare, and finance-driven operations. As shown in Figure 3.1, this new typology primarily focuses on the difference between an attack's short-term goals. Each short-term goal can also contribute to North Korea's ultimate long-term goal of regime survival.

Figure 3.1. New Short-term Goal-based Typology of North Korea's Cyberoperations

Typology (Lim et al., 2013, p. 16)
I. Distributed Denial of Service (DDoS) II. Advanced Persistent Threat (APT) III. Cyber Terror IV. Cyber Espionage V. Cyber Intelligence Activities VI. Internet Troll VII. Cyber Psychological Warfare VIII. Manipulating Public Opinion IV. Propaganda V. Cyber Unification Movements

Short-term Goal-based Typology	Long-term Goal
Type 1. Cyber Sabotage (Lim et al.'s categories I, II, III) : Disrupting network service, sabotaging critical infrastructures, deleting database, or taking sites	Regime Survival
Type 2. Cyber Espionage (II, IV, V) : Compromising sensitive public and private information & intellectual property	
Type 3. Cyber Psychological Warfare (VI, VII, VIII, IV, V) : Manipulating public opinion by spreading mis/disinformation	
Type 4. Cyber Finance-driven Operations (II) : Stealing cryptocurrencies & money	

First, cyber sabotage (type 1) aims to disrupt network services or IT devices and to impair a network system in order to achieve political goals. It also includes deleting database and total site takeovers. For example, North Korea-affiliated hackers conducted several massive DDoS attacks

in 2009, 2011, and 2013 that made an IT device or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet. This is a classic strategy of North Korean cyberwarriors used to spread fear in targeted countries.

Second, cyber espionage (type 2) refers to clandestine attempts to collect sensitive public or private information by intercepting communications between IT devices as well as penetrating targeted computer networks. In late 2014, North Korea-affiliated hackers leaked Sony Pictures Entertainment's confidential data, including executive salaries, copies of unreleased Sony films, personal information about Sony Pictures employees and their families, as well as e-mails between employees (The White House, 2015). Moreover, according to evidence collected by the FBI, North Korea attempted to collect data about the Terminal High Altitude Area Defense (THAAD), a missile-defense system (Shields, 2018, p. 96). Throughout 2016 and 2017, North Korea hackers sent spear-phishing emails to various employees of Lockheed Martin, the primary contractor for THAAD (Shields, 2018, p. 96).

Third, cyber psychological warfare (type 3) aims to manipulate public opinion by spreading misinformation and disinformation. It is pervasive. North Korean cyber psychological operations date back to its first official propaganda website, Korea Central News Agency (Chosun Tongsin, www.kcna.co.jp), which was opened in January 1997. Since then, North Korea has continued to manipulate South Korea's public opinion as they conduct disinformation campaigns and disseminate propaganda. The 2016 ROK Defense White Paper emphasized that "North Korea engaged in a war of public opinion and cyber psychological warfare as part of its scheme to instigate social unrest in the South" (ROK MND, 2016, p. 25). According to an unknown South Korean official, North Korea operates several teams that generate distorted online comments and

fake news through web portals and social media platforms as they aim to split South Korean society along ideological lines (Ho-Jun Kim, 2016). North Korean-run propaganda websites are used for the same purpose (K. Sung, 2017). Some experts on North Korea argue that North Korea's online activities increase during election periods of South Korea (Jung, 2018).

Recently, North Korea started to focus its cyber psychological operations on foreign countries' online streaming or social network services. The South Korean government does not allow its citizens to access North Korean propaganda websites. Internet users cannot technically visit those websites with IP addresses belonging to South Korea. The South Korean government's efforts have been weakened by North Korea's new strategy of using global online streaming and social network services. North Korea has three YouTube channels. Two of them are Korean language channels, Red Star TV (붉은별 TV in Korean),[73] operated by the Korean Central News Agency, and DPRK Today (조선의 오늘 in Korean).[74] One English channel is called North Korea Today.[75] As of January 2019, 12,351 YouTube users had subscribed Red Star TV, which has 1,616 videos, including Kim Jong-un's 2019 new year message. During the same time period, DPRK Today had 11,212 YouTube subscribers and 9,979 videos that focused on the life of North Korean citizens. The last channel, North Korea Today provides extra information about videos in English. It had 32,308 YouTube subscribers and 2,001 videos in January of 2019. Experts on North Korea have said these YouTube channels are operated by the North Korean regime because individual North Korean citizens cannot access the

[73] The Red Star TV. (n.d.). Retrieved January 8, 2019, from YouTube website: https://www.youtube.com/channel/UCJ7i-yFvuzn9FbUdU77WKcA. However, the Red Star TV account of YouTube has been terminated due to a legal complaint (accessed on April 22, 2019)
[74] DPRK Today. (n.d.). Retrieved January 8, 2019, from YouTube website: https://www.youtube.com/channel/UCndGz3c8ImJ216C4kZMxaWA. However, DPRK Today account of YouTube has been terminated due to a legal complaint (accessed on April 22, 2019).
[75] North Korea Today. (n.d.). Retrieved April 22, 2019, from YouTube website: https://www.youtube.com/channel/UCNaH2TGwop7CHZvnj0t3yjA.

internet (D. Kang, 2019). More interestingly, Red Star TV collects advertising income and accepts donations (KCNA, n.d.). It is suspected this is a method used to soften the blow of international economic sanctions.

Furthermore, the South Korean government cannot ban its citizens from watching videos of these three North Korean propaganda channels and from sharing the contents of propaganda websites via their social networking services. The government has a national security law to manage North Korean propaganda sites. However, the law can only regulate its citizens and domestic companies. Thus, the South Korean government does not have the legal authority to regulate North Korea's propaganda channels and videos on foreign websites. Moreover, as of January 2019, DPRK Today has its own Korean language-based Instagram account (@dprktoday) with 16,584 posts and 1,827 followers. A South Korean TV news station said that most of the followers are South Korean citizens, sharing DPRK Today's posts with their accounts (Kang D., 2019). North Korea also has English versions of Instagram (@everydaydprk) and Facebook (@EverydayDPRK) accounts with the ID name "Everyday DPRK." Approximately 120,000 Instagram users follow the Instagram account, which has uploaded 315 posts in English. Approximately 1,800 Facebook users follow the Facebook account which was created on October 1, 2014. This new trend shows that North Korea's cyber psychological strategy keeps evolving as ITs continually improve.

Last but not least, cyber finance-driven operations (type 4) are a means of evading sanctions and obtaining hard currencies to fund the regime (McNamara, 2017). In a narrow sense, it refers to the online attempt to raise large sums of money by targeting financial institutions, such as banks, cryptocurrency exchanges, and countries' financial governing bodies. Recently, FireEye discovered a financially motivated North Korean hacker group and named it APT38. FireEye's

report, *APT38: Un-usual Suspects* (2018), argues that APT38 is a financially motivated North Korean regime-sponsored group responsible for conducting destructive attacks against financial institutions, as well as some of the world's largest cyber heists. The group also sells malware, hacking tools, and online gaming items to others; it also commits cyber fraud in order to make money. More interestingly, it is believed that the application of increasingly restrictive and numerous financial sanctions against Pyongyang probably encouraged cyber finance-driven operations (Fraser, Plan, Cannon, & O'Leary, 2018, p. 12).

Table 3.7. New Short-term Goal-based Typology and North Korean Major Examples

	Type 1. Cyber Sabotage	Type 2. Cyber Espionage	Type 3. Cyber Psychological Warfare	Type 4. Cyber Finance-driven Operations
2009	July 2009 Cyberattacks		Since 1997, con't	
2010				
2011	3/4 DDoS Attacks, Cyber Terror on NH Bank,			
2012				
2013	3/20 Cyber Terror (Dark Seoul), 6/25 Cyber Terror	Operation Kimsuky		
2014	Compromise of the Seoul subway system	The 2014 Sony Hack, Hacking on KHNP		
2015		The 2015 Cyber Espionage		
2016		The 2016 Cyber Espionage, Intrusion into the South Military 's Intranet, Targeting of U.S. Military Contractor (Lockheed Martin)		SWIFT-related Bangladesh bank heists, SWIFT-related Polish bank heists
2017	Targeting of U.S. electric companies	Targeting of Middle Eastern Organization,		Compromise of Cryptocurrency Exchanges, The WannaCry Ransomware Attack, Compromise of Far Eastern International Bank in Taiwan

The new typology illustrates how North Korea's offensive cyberoperations contribute to the state's long-term political goal of regime survival. In the late 2000s and the early 2010s, as shown in Table 3.7, North Korea-associated hackers used to focus on disrupting network services, resulting in inconvenience and fear in targeted countries. In the mid-2010s, however, these hackers began to conduct cyberoperations clandestinely to collect important information to contribute to the regime (Table 3.7). For example, North Korean hackers tried to access Lockheed Martin's networks by spreading spear-phishing emails to its employees. The aim of this operation was to steal information about the U.S.-South Korea alliance's missile defense program that would threaten North Korea's nuclear program.

Since the late 2010s, North Korean hackers have focused on financially motivated operations. It is believed the application of increasingly restrictive and numerous financial sanctions against Pyongyang probably encouraged its hackers to raise large sums of money. Along with the three other types, cyber psychological warfare remains at the core of North Korea's cyberoperations. North Korea has only two types of websites. One is websites for business. The other is Korean language-based propaganda websites to praise the regime and its dictators. Given that North Korean citizens cannot access the internet, those propaganda websites target South Korean citizens. Moreover, it is known that North Korea has cyber psychological warfare units to manipulate South Korean public opinion.

As demonstrated above, North Korea's offensive cyberoperations can be divided into four types: cyber sabotage, cyber espionage, cyber psychological warfare, and cyber finance-driven operations based on the different short-term goals. Despite these short-term objectives, the four types of cyberoperations contribute to the regime's long-term goal of survival in different

contexts. In the late 2000s and the early 2010s, the North Korean regime started to conduct cyberoperations, focusing on sabotage and psychological warfare. However, as time passed, it began to widen its spectrum of cyberoperations to espionage and finance-driven operations. More specifically, diplomatic factors or perceived insults against the regime can bring about North Korean cyber sabotage and psychological operations against specific countries. The regime's recent financial needs are also a reason for its cyberoperations against global financial institutions.

3.5 North Korea's Cyber Proxy Warfare Strategy

Several massive cyberattacks have been attributed to North Korea. These cyberattacks can be categorized into the four types discussed in the previous section (cyber sabotage, cyber espionage, cyber psychological warfare, and cyber finance-driven operations). However, as the state has employed non-state actors, it has effectively avoided punishment by victim states and the international community. This is the essence of North Korea's aggressive cyber strategy. Thus, this section illustrates how the state has tried to ensure its own survival through cyber proxy warfare, or the use of non-state actors to carry out its operations. This section of the chapter begins with the relationships between anarchy, anonymity, and North Korea's non-state actors. Then it shows how information technologies enable the state to use a cyber proxy warfare strategy. The third section includes stories about North Korean non-state cyberwarriors, front companies, and the North Korean regime. Finally, North Korea's control mechanisms which enabling cyber proxy warfare are discussed.

3.5.1 *Anarchy, Anonymity, and North Korea's Non-state Actors*

Traditionally, the North Korean regime has used the anarchical nature of the international system to ensure its survival. On October 9, 2006, North Korea tested its nuclear weapons for the first time. The international community attempted to halt North Korea's nuclear program with a carrot and stick approach through the Six-Party Talks[76] and international economic sanctions. Since then, however, the North has not only ignored the unenforceable efforts of the international community, but also has continually developed nuclear weapons with five more nuclear tests on May 25, 2009; February 12, 2013; January 6, 2016; September 9, 2016; and September 3, 2017 (Kristensen & Norris, 2018, p. 45). This illustrates that the anarchical nature of the international system cannot force the North Korean regime to give up its aggressive nuclear strategy.

North Korea-associated cyberoperations have verified that cyberspace is a new anarchical venue for North Korea's aggressive national strategy. An anonymous and borderless cyberspace offers the state ample opportunities to pursue its aggressive cyber proxy warfare strategy. First, in a broad sense, cyberattacks relating to North Korea's political interests have been arguably conducted by its anonymous state-sponsored hackers. Some of these hackers are cyberwarriors belonging to North Korea's military, intelligence groups, state-run institutions, or companies. They have led massive, sophisticated cyberattacks on the outside world. On June 25, 2013, a series of cyberattacks—including the DDoS attacks—on the South Korean government, South Korean news media websites, and U.S. Forces in Korea were carried out by multiple perpetrators (Symantec Security Response, 2013). The South Korean government attributed the attacks to

[76] The Six-Party Talks were a series of multilateral negotiations held intermittently since 2003. Six countries, China (Chair), Japan, North Korea, Russia, South Korea, and the United States, have participated in the talks for the purpose of dismantling North Korea's nuclear program. However, in 2009, Pyongyang decided to no longer participate in the Six-Party process. In subsequent years, other members, notably China, have called periodically for a resumption of the Talks (Davenport, 2018).

North Korea's Lab 110, which is affiliated with the Reconnaissance General Bureau (RGB),[77] a military spy agency controlled by the regime's Defense Ministry (HP Security Research, 2014, p. 50). The Lab had already been accused of conducting cyberattacks in July 2009 (Associated Press, 2009).

Other North Korean cyberwarriors are working at state-run companies, such as Chosun Rungrado Trading Company and Chosun Expo Joint Venture (Chosun Expo), which are both allegedly controlled by Lab 110 (Shields, 2018). They have carried out cyberattacks and cyber finance-driven operations, such as operating or hacking online games, to raise money for their regime (Associated Press, 2011; Dong-Un Kim, 2013). However, in both cases, cyberwarriors have behaved as anonymous personae to protect themselves even to protect their state sponsor, North Korea.

There are a few, but important cases in which North Korea-related actors actively revealed themselves to be hacktivists responsible for a cyberattack. In the first case in 2011, the "Whois Team" claimed its credit for the 3.20 Cyber Terror through computer-defacement graphics (Baumgartner, 2014; Shields, 2018, p. 131). Second, the 2014 Sony hack was clearly connected to the North Korean regime's political interests in banning Sony Pictures Entertainment from releasing a film, *The Interview*. From the outset, the "Guardian of Peace" (GOP) group claimed its credit for the hack in order to divert the U.S. government's investigation of the real author of the attack, North Korea itself.

Last, in late 2014, KHNP was hacked by a group claiming to be anti-nuclear activists. The group is called "John" because it posted warnings with accounts named 'john_kdfifj1029' on

[77] The RGB is North Korea's primary foreign intelligence service, responsible for collection and clandestine operations. The RGB is comprised of six bureaus with compartmented functions including operations; reconnaissance; technology and cyber; overseas intelligence; inter-Korean talks; and service support.

Twitter and “Jenia John” on Facebook (Lee & Chung, 2015). This hacker group intentionally revealed its accounts in order to create distance from the North Korean regime. However, according to a South Korean prosecutor and cybersecurity experts, the anti-nuclear group is related to North Korean hackers who conducted the 3.20 Cyber Terror in 2013 and the 2014 Sony hack (Lee & Chung, 2015; Song & Lee, 2014). The hacker group shared leaked information through a website, pastebin.com, that GOP already used in the Sony hack; The hacker group also accessed the internet with specific IP addresses that hackers from the 3.20 Cyber Terror and the Sony hack used (Lee & Chung, 2015; Song & Lee, 2014). Revealing the names of the group is an active strategy to disconnect the hacks with the real sponsor, the North Korean regime.

In the majority of cases, North Korea-associated hackers have not revealed their names. Cybersecurity experts in states and companies analyze and categorize massive cyberoperations based on similarities in coding patterns, malware, and IP addresses. In the course of analyzing and categorizing, they gave North Korea-related actors different diverse names, such as DarkSeoul, Lazarus, APT 37, APT 38, Lab 110, Group 123, Hidden Cobra, Nickel Academy or Reaper. For example, some of the names are from malware elements that North Korean hackers created (Strom, 2018). Also, cybersecurity companies named North Korean hacker groups APT 37 or APT 38 according to their naming rules for hackers or hacker groups.

Naming each cyberattack is an effective way to manage each case and to trace the real identity of hackers through accumulated data. Paradoxically, it can also be understood as North Korea’s passive strategy to keep a distance from its cyberoperations using unknown state-sponsored hackers. For example, different states or private institutions give one same case different names. The United States Computer Emergency Readiness Team (US-CERT) uses

Hidden Cobra to distinguish North Korean malicious activities from others, including the 2014 Sony hack and the 2017 WannaCry ransomware attack (US-CERT, n.d.). A cybersecurity report, "Operations Blockbuster: Unraveling the Long Thread of the Sony Attack," named a hacker group Lazarus in order to attribute it to North Korea (Novetta Threat Research Group, 2016). Since then, many cybersecurity companies and institutions and state entities have used the name "Lazarus" for a specific North Korean hacker group. Symantec argued that there are strong links between Lazarus and the WannaCry ransomware attack (Symantec Security Response, 2017b).

In addition, FireEye's recent report, *APT 38: Un-usual Suspects* (2018), tries to subdivide Lazarus, the so-called Hidden Cobra, into three different groups based on the characteristics of missions: Lazarus, APT 38, and TEMP.Hermit. While the Lazarus operates for political purposes, activities of APT 38 and TEMP.Hermit are motivated by financial and military goals. Whether North Korea intends or not, this passive strategy naturally has led others to provide random names for its hackers. Paradoxically, however, while naming North Korea-associated hackers appears to be an effective way to trace them based on accumulated data, random and different names for the same North Korean hacker group help North Korea and its hackers hide their relationship to one another.

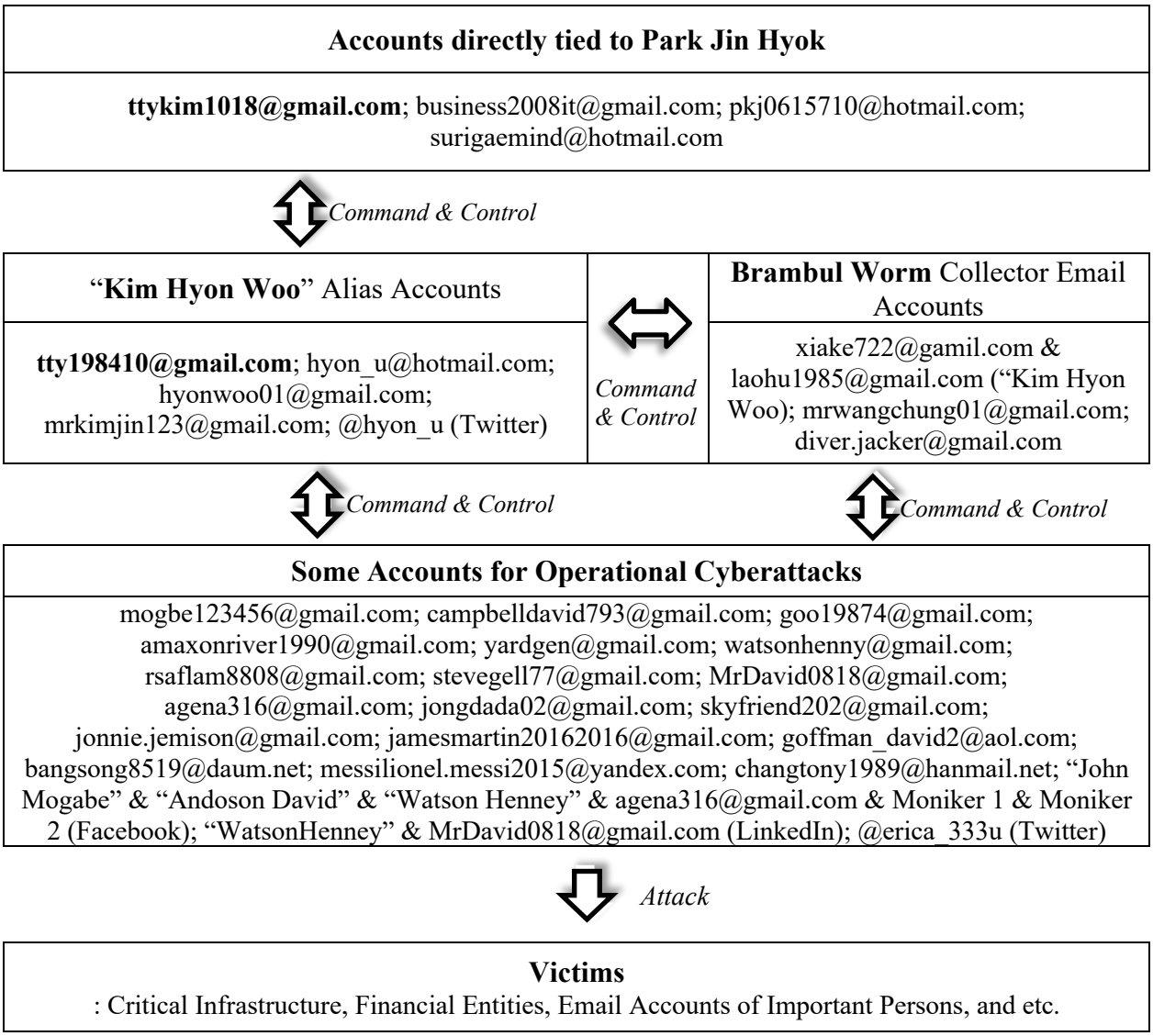
3.5.2 *Information Technologies and Cyber Proxy Warfare Strategies*

The malicious use of some information technologies enables North Korean hackers to hide their real identity and relationships with the North Korean regime. These hackers mainly use fake IP addresses, VPNs, DDNS, compromised computers, hop points, and anonymizing proxy services for their aggressive cyber proxy warfare strategy. These technologies systematically frustrate attribution efforts.

Temporal and spatial barriers do not limit the malicious activities of North Korea-associated hackers in cyberspace. Whether they are located in their country or not, they can easily carry out cyberoperations with diverse email and website accounts, IP addresses, proxy servers, and computers across the globe. First, according to the *Criminal Complaint Against Park Jin Hyok* (2018), North Korean hackers used over fifty email accounts for cyberoperations, such as the 2014 Sony hack and the 2017 WannaCry ransomware attack. As shown in Figure 3.2, these hackers created gmail, outlook, and hanmail[78] accounts with fake identities before its sophisticated cyberattacks, such as Anderson David, Watson Henny, John Mogabe, and Kim Hyon Woo (Shields, 2018). Some of these accounts were used for reconnaissance missions to target networks (Shields, 2018, p. 140). North Korean hackers used other email accounts from those for reconnaissance missions to send spear-phishing emails to employees of the target[79] (Shields, 2018, p. 21). Moreover, the fake identities and email accounts were used to create social media accounts on Facebook and Twitter (Shields, 2018, p. 127). North Korean hackers have created new accounts with the identity of various aliases of email services that global IT companies operate. They have also consistently changed their accounts to avoid being tracked by victim states and private cybersecurity companies.

[78] It is from one email service of a South Korean web portal, Daum.
[79] tty198410@gmail.com associated with the alias "Kim Hyon Woo."

Figure 3.2. North Korea's Cyberoperations' Mechanism with Its Email/SNS Accounts[80]



* These email or social networking service accounts were accessed via North Korean or North Korea-related IP Addresses.

Source: Shields, 2018, pp. 173–5.

Second, North Korea hackers have carried out cyberoperations with diverse IP addresses, proxy servers, and computers. North Korean hackers have accessed these aforementioned email and social media accounts through their own IP addresses as well as others from China, the

[80] SNS stands for Social Networking Service. These accounts were accessed directly by North Korean IP Address or from North Korean IP Address through a Proxy Service. These were also accessed by an arguably North Korea-related IP address. Some of them were accessed through same computers or devices (Shields, 2018, p. 174).

United States Switzerland, Germany, the United Kingdom, and the Netherlands. North Korean hackers have mainly conducted cyberattacks with IP addresses assigned to North Korea or allocated to it via Chinese Unicom, Dalian, China. The first set of IP addresses is 175.45.176.0–175.45.179.255, registered to a company, Star Joint Venture Co., Ltd. in Pyongyang, North Korea (Jun, et al., 2015, p. 53). The other IP range is 210.52.109.0–210.52.109.255, registered to China Unicom, which is a company located in China, but leased to North Korea (Jun et al., 2015, p. 53). In addition, North Korean cyber proxies have accessed their accounts via other IP addresses across the glove. A specific IP address located in the Netherlands had been used to access a North Korean email account, business2008it@gmail, in November 2014 and January 2015, to access ttykim1018@gmail.com in February 2015, and to access another Chosun Expo Account, surigaemind@hotmail.com in February 2015 (Shields, 2018, p. 153). The email accounts ttykim1018@gmail.com and business2008it@gmail.com were also accessed from several different IP addresses in Germany, the United Kingdom, and the United States between August 27 and November 24, 2014 (Shields, 2018, p. 153).

Third, VPNs, DDNS, compromised computers, hop points, and anonymizing proxy services help North Korean cyber proxies conceal their true location. Internet technology company Recorded Future found that North Korean internet users were accessing their gmail accounts, logging into Twitter, and making online purchases with bitcoin via VPNs (Insikt Group, 2017). Then, DDNS used to target the Bangladesh Bank in 2016 were controlled by computer devices of North Korean-related hackers via North Korean IP addresses (Shields, 2018, p. 64). Compromised computers infected by a piece of malware, known as "Brambul Worm"[81] were

[81] Brambul malware is a brute-force authentication worm that spreads through Server Message Block (SMB) shares. SMBs enable shared access to files between users on a network. The malware typically spreads by using a list of hard-coded login credentials to launch a brute-force password attack against an SMB protocol for access to a

used as hop points in order to command and control the malware being used in two intrusions, the Bangladesh Bank heist and the watering hole attack in Poland in 2016 (Group-IB, 2017; Shields, 2018, p. 14).

During the July 2009 DDoS Cyberattacks, 435 Command and Control (C&C) servers located in 61 countries ordered attacks on 36 critical websites of the United States and South Korea from 110,000 zombie computers (Byung-Min Oh, 2010; Choe & Markoff, 2009). Won Sei Hoon, head of South Korea's National Intelligence Service, told lawmakers in October 2009 that the DDoS attacks were traced to a Chinese IP address of North Korea's Ministry of Post and Telecommunications (Beom-Hyeon Kim, 2009). In 2011, the 3.4 DDoS attacks occurred when 746 overseas C&C servers across 70 countries ordered 100,000 zombie computers to attack critical South Korean websites. South Korea's Police Cyber Bureau blamed North Korea because some of the C&C servers used in the DDoS attacks overlapped with those of the July 2009 DDoS Cyberattacks. As of the early 2016, analytics company Novetta's (2016) report on the Lazarus Group identified IP addresses of C&C servers used by the Lazarus Group located in the United States (29%), Taiwan (7%), China (7%), India (5%), Italy (5%), Thailand (4%), and others (43%) (p. 27). The use of diverse, unknown IP addresses, proxy servers, compromised computers, and several techniques to conceal the true location of North Korean hackers as non-state actors appears to be an effective method to hide the relationship between specific cyberoperations and North Korea for proxy warfare in cyberspace.

Cyberspace is a new operational venue for North Korea's proxy warfare. No authority punishes North Korea's illegal activities in an anarchic cyberspace. North Korea can easily hide its real identity by using anonymous cyber actors when it conducts offensive cyberactivities

---

victim's network. For more information see: US-CERT. (n.d.). Hidden Cobra: Joanap Backdoor Trojan and Brambul Server Message Block Worm. Retrieved January 4, 2019, from https://www.us-cert.gov/ncas/alerts/TA18-149A

against the outside world. Diverse IT technologies, such as fake IP addresses, VPNs, DDNS, compromised computers, hop points, and anonymizing proxy services enable North Korea-associated hackers to keep a distance from their state sponsor. Moreover, these technologies allow hackers to overcome temporal and spatial limitations. Thus, cyberspace is an ideal location for proxy warfare and North Korea's offensive cyber strategy.

3.5.3 *Non-state Actors, Front Companies, and the North Korean Regime*

North Korea has employed cyber proxies in order to achieve its national interests. As detailed in Chapter 2, these cyber proxies have been nurtured and trained through North Korea's state-led intensive ICT education programs in Number One Secondary schools, top universities, and military institutions. These trained professionals have then been assigned to the DPRK's military, intelligence groups, IT-related institutions, IT-related universities, or state-run companies. After conducting reconnaissance activities, these professionals have played a central role in conducting massive, sophisticated, and well-organized cyberattacks against state-sponsored designated targets. However, these professionals have officially revealed themselves as non-state actors with the purpose of keeping a distance from the North Korean regime. In addition, as the private sector does not exist in North Korea, it is believed that all North Korean cyberwarriors and their missions are closely connected to the regime.

According to the FBI, a federal warrant was issued by the Central District of California United States District Court for Park Jin Hyok (박진혁 in Korean), also known as Pak Jin Hek, for his role in several cyberattacks, including the 2014 Sony hack, 2016 Bangladesh Bank heist, the WannaCry ransomware attack, and attacks on other financial and defense industries (FBI, 2018). Although the U.S. Department of Justice's (DoJ) criminal complaint noted that one or more subjects had been involved, Park is the only one identified in the complaint (Shields, 2018).

North Korea's political and financial goals were the motives for these attacks. The Sony hack was designed to suppress the film, *The Interview*, which undermined the new supreme leadership of the DPRK, Kim Jung Un. Park and his conspirators attacked the Lockheed Martin Corporation to collect information about its missile defense program, THAAD, designed to detect and shoot down North Korea's nuclear weapons. Following the increase in the international sanctions against North Korea based on its nuclear programs, other financially motivated cyberattacks have been carried out. Although Mr. Park is the only one who is charged by the DoJ, the politically motivated cyberattacks show that Park Jin Hyok and his fellow cyber proxies are directly connected to the North Korean regime.

Park Jin Hyok is a North Korean programmer who was dispatched to Dalian, a city which borders North Korea in Liaoning province, China. He arrived in late 2010 or early 2011 in China to work for Chosun Expo, which is a North Korean regime front company, and continued to work in Dalian until late 2013 or early 2014, when he returned to North Korea shortly before the Sony hack (Shields, 2018, p. 144). According to information attached to his particular email on January 10, 2001, Park was born on August 15, 1984 and had been employed starting in 2002 as an online game developer in Chosun Expo after graduating from Kim Chaek University of Technology (Shields, 2018, p. 143). This university's computer science department, along with North Korea's other top universities, especially Kim Il Sung University, has been suspected of training hackers. His resume also included foreign language skills in English and Chinese and programming language skills in Java, php, jsp, and flash, Visual C++ (Shields, 2018, p. 143). In the beginning, the DPRK's cyber proxy and other programmers in Chosun Expo participated in some non-malicious software and information technology projects for paying clients (Shields, 2018, pp.142–143). Despite the fact that he was trained in Visual C++ which was used in

numerous malware samples, including WannaCry and nearly all 32-bit North Korean malware samples, he appeared to be an ordinary North Korean IT professional working in China (Shields, 2018, p. 143).

However, Park Jin Hyok's email and social media activities with his real name (in China and North Korea) illustrate he played a critical role in cyberattacks sponsored by the North Korean regime. He accessed his four Chosun Expo-related personal email accounts, surigaemind@hotmail.com, ttykim1018@gmail.com, pkj0615710@hotmail.com, and business2008it@gmail.com, all four connected to his alias, Kim Hyon Woo, and many other email and social media accounts used for major North Korea-associated cyberattacks. For example, two of the four email addresses, surigaemind@hotmail.com and business2008it@gmail, were accessed by a particular Switzerland IP address that was also used to access accounts used for spear-phishing on May 18, 2015 and August 10, 2015 (Shields, 2018, p. 140). Furthermore, FBI special agent Nathan P. Shields found that according to access logs, ttykim1018@gmail.com (created on October 27, 2008) had been accessed by IP addresses located in the United States, the United Kingdom, Germany, and other countries via proxy services, VPNs, or hop points for North Korea's cyberoperations (Shields, 2018, pp. 149–152). There is no evidence that Park Jin Hyok had ever traveled to the United States, the United Kingdom, or Germany.

In the early 2000s, Chosun Expo was created as an e-commerce and lottery website joint venture between North Korea and South Korea (Kwak, 2016). While the South Korean business partner withdrew from the venture, North Korea maintained the business which is to develop mobile and computer game software; gambling-related products; search engines; and network technology (Shields, 2018, p. 136). Before its closure in January 2016, its website indicated it

was developing a cryptocurrency exchange solution and big data analytics software (Jin-Kyu Kang, 2016). Officially, its employees, including Park Jin Hyok, worked for paying clients on software and information technology projects.

In reality, Chosun Expo is one of the North Korea's front companies used in the state's cyber proxy warfare activities. IT professionals from North Korea have been hired by the front company in order to further North Korea's interests. FireEye's (2018) report, *APT 38: Un-usual Suspects*, emphasizes that Park Jin Hyok and his hacker colleagues belong to two North Korean front companies: Chosun Expo Joint Venture in Dalian, China, and Chosun Baeksul Trading Company in Shenyang, China. More interestingly, these companies have been affiliated with one of the North Korean hacking organizations, known as "Lab 110" (or Bureau 110), since at least 2002 (Shields, 2018, pp. 5, 133, 171). Lab 110, also called the Technology Reconnaissance Team, was suspected of carrying out the July 2009 DDoS attacks against South Korea and the United States (Murauskaite, 2014).

It is believed that the 6th Technical Bureau in North Korea's Reconnaissance General Bureau (RGB) controls Lab 110 (Fraser et al., 2018). RGB has been responsible for North Korea's asymmetric and clandestine operations, especially cyberattacks (Office of the Secretary of Defense, 2015, p. 14). Although it is subordinate to the Ministry of People's Armed Forces, it reports directly to the North Korean National Committee (NKNC), formerly known as the National Defense Commission; the NKNC is the highest guiding organ of the military in North Korea—a country where the military dominates. The chairman of the NKNC, Kim Jong Un, directly controls the RGB. The RGB formed "Office 91" as the headquarters of North Korea's hacking operations (Gause, 2015). It also has another cyber organization, Unit 121, linked to DarkSeoul, known as the 3.20 Cyber Terror in 2013 (Jun, LaFoy, & Sohn, 2014). This alleged

hierarchical structure illustrates that Park Jin Hyok and co-conspirators of the front company, Chosun Expo, are professional cyber proxies hired by the North Korean regime.

3.5.4 *North Korea's Control Mechanism for Cyber Proxy Warfare*

North Korea's robust control mechanism enables the regime to successfully carry out cyber proxy warfare operations that are tied closely to its national interests. First, North Korean cyberwarriors must pass strict state screening processes. Second, cyberwarriors activities are monitored and controlled by several layers of the North Korean surveillance system. Lastly, North Korea deploys various punishment methods to enhance hacker performance.

North Korea's closed Communist system includes a detailed selection and screening process. Broadly speaking, North Korean cyberwarriors are able to travel abroad, like other ordinary workers dispatched to foreign countries. Despite several useful techniques to conceal the true location of North Korean hackers, such as foreign IP addresses, proxy servers, hop points, and VPNs, conducting cyberoperations abroad has distinct advantages. In addition to better IT infrastructures, foreign cyberoperations increase cyberwarriors plausible deniability capabilities. Around 58,000 North Korean workers in 50 foreign countries have been selected through strict several screening processes to prevent them from escaping (Han, Lee, Do, Hong, & Kim, 2018, pp. 414–416). This means that most North Korean workers dispatched to foreign countries come from members of Korean Workers' Party (KWP) as well as the Pyongyang middle class; both groups are loyal to the North Korean regime (Han et al., 2018, pp. 415–416). In addition, it is believed that these workers are required to bribe officials because moving abroad holds out the promise of increased income (Han et al., 2018, pp. 415–416).

In a narrow sense, North Korean cyberwarriors consist of IT professionals who passed a more strict screening process than other ordinary North Koreans who work in other countries. In

January 2016, Chosun Expo's website stated that it employed approximately 50 computer programmers in their 20s and 30s who had graduated from Kim Il Sung University, Kim Chaek University of Technology, and Pyongyang University of Fine Arts (Jin-Kyu Kang, 2016). Park Jin Hyok is also a graduate of Kim Chaek University of Technology. As detailed in Chapter 2, these three universities are well known as top universities in North Korea. Only gifted students from good family backgrounds are admitted to these universities. Given these facts, it is believed that North Korean cyber proxies who work in front companies in North Korea, China, or other countries are strongly tied to the regime based on their family origin and loyalty to it.

Cyber proxy monitoring is implemented through a variety of methods. Via several layers of surveillance, North Korean cyber proxies are subject to intense scrutiny and control by the regime. In a broad sense, North Korea operates its strict monitoring system for all citizens. First, North Korean does not guarantee freedom of movement. *Freedom in the World 2018* points out that forced internal resettlement is routine and emigration is illegal. All foreign travel—whether for work, trade, or educational opportunities—is strictly controlled by the regime (Freedom House, 2018).

Second, North Korea has a centralized dictatorial political and economic system. A private sector does not exist. All citizens are required to register with one or more cell groups of Korean Workers' Party (KWP) (ROK Ministry of Unification, n.d.-e). The KWP and its central or local cell groups control all daily activities (Institute for Unification Education, 2017, pp. 146–8). Third, North Koreans, including workers abroad, have been monitored by agents of the State Security Department (SSD) and the Ministry of People's Security; these agencies track down anti-party or rebellious citizens (ROK Ministry of Unification, n.d.-e). SSD is the state's autonomous secret police agency who reports directly to the supreme leader. It is responsible for

internal security. The Ministry of People's Security is the law enforcement agency of North Korea who monitors the public distribution system and operates the prison system.

North Korean hackers and their online activities are more strictly controlled and managed by these aforementioned monitoring systems. They are not allowed to move to another place or to change their job without the regime's permission. One former North Korean hacker, alias Jong Hyok, said that he majored computer science department at a top university, even though his dream was to become a medical doctor (Sam Kim, 2018). Along with other computer programmers from top schools, Jong Hyok was then sent to China to earn money for the state through illegal activities (Kim Sam, 2018). North Korean cyber proxies dispatched to other countries all live together with other team members in the same houses or buildings, like other ordinary North Koreans working abroad. Some of these workers are spies sent to monitor workers, including cyberwarriors (Lee, Oh, & Lee, 2017, p. 73). This is an effective way to monitor all citizens living abroad. Even ordinary workers monitor one another (Lee et al., 2017, p. 73).

Jong Hyok lived with other cyberwarriors as well as state spies, called "bodyguards" (Sam Kim, 2018). North Korean hackers are also placed under 24-hour surveillance under the command of chief delegate from KWP. On Saturdays, North Koran hacker Jong Hyok and his peers in the same unit had two-hour meetings led by a government official to discuss the philosophies of the Kim dictatorship(s) as well as any new ideological tenets dispensed by Kim Jong Un (Sam Kim, 2018). Park Jin Hyok was also controlled and monitored by the strict surveillance system. May and September 2011 email exchanges between Park Jin Hyok and another person saved in a ttykim1018@gmail.com account illustrate that cyber proxies, including

Mr. Park, were required to secure special permission to leave China and to permanently return to North Korea (Shields, 2018, pp. 146–147).

Punishments can take a variety of forms. All North Korean workers are forced to work hard for the state, not themselves (Lee et al., 2017, p. 73). Some workers in foreign countries are required to make a certain amount of money for the North Korean regime. Moreover, although they work in shabby surroundings, North Korean workers in foreign countries are not allowed to express dissatisfaction with their country, regime, and work conditions. In some minor offenses, such as failing to meet the requirement, they could mean being sent home (Sam Kim, 2018). Serious offenses, such as not showing sufficient fealty to the country or skimming profits, could result not only in repatriation, but also hard labor at a factory or farm; this is known as "revolutionization" (Sam Kim, 2018). Even more serious offenses could lead to the death penalty, which was the case for some Kim family members, such as Kim Jong Nam and Jang Song Thaek. North Korea cyber proxies are not different from other ordinary workers in foreign countries. The former North Korean hacker, Jong Hyok, said that he worked hard to make around $100,000 U.S. dollars a year as a way to show his fealty to the regime (Sam Kim, 2018).

North Korea applies proxy warfare to its offensive cyber strategy. The state has delegated its monopoly authority over violence to cyber proxies in order to achieve its national interests. The proxies are IT professionals trained in North Korea's state-led intensive ICT education programs in Number One Secondary schools, top universities, and military institutions. As fake civilian IT professionals, they work for state-led front companies. However, these companies indirectly are under the control of North Korea's governmental organizations. Activities of their IT employees are monitored by its systemic surveillance programs designed to raise the efficiency of cyber

proxy warfare. Thus, in practice, these professionals can be identified as North Korea's cyberwarriors who work for state interests.

3.5.5 *North Korea's Freedom from Attribution, Punishment, and Deterrence*

The criminal complaint against a North Korean hacker, Park Jin Hyok, paradoxically verifies that a cyber proxy strategy works well for Pyongyang. North Korea's cyber proxy warfare makes attribution extremely difficult. A senior official in U.S. Department of Justice said that the complaint makes it clear the hacker worked with other conspirators to affect all of North Korea-associated cyberattacks listed in the complaint (Barrett, 2018). Despite this fact, Mr. Park is the only individual charged in the complaint. In other words, the complaint does not directly hold the North Korean regime responsible for such cyberattacks.

Since its 2009 DDoS attacks on critical U.S. and South Korean infrastructure, North Korea continues to be blamed as the source of cyberattacks. Before the 2014 Sony hack, victim countries only blamed hackers working for the North Korean regime (Han, 2011; Beom-Hyeon Kim, 2009; R. Kim, 2011). Private cybersecurity companies supported the claims of those countries with scientific evidence (McAfee, 2011; Sherstobitoff, Itai Liba, & Walter, 2013; Symantec Security Response, 2009; Tarakanov, 2013). However, their efforts were fruitless in terms of punishing North Korea. The DPRK denied all claims of the victim countries.

The 2014 Sony hack was a turning point in countermeasures against North Korea-related cyberattacks. The United States warned that it would take tough action against such aggressive cyberoperations. The FBI accused North Korea of the Sony hack on December 19, 2014 (FBI National Press Office, 2014). It found the data deletion malware used in this attack was linked to other malware the FBI knew to be previously developed by North Korean hackers (FBI National Press Office, 2014). This was the first time the U.S. government blamed a state for a particular

cyberoperation (Noh, 2014). On that day, U.S. President Barack Obama insisted in his year-end press conference a briefing with reporters that "[North Korean hackers] caused a lot of damage," and "We will respond proportionally, and we'll respond in a place and time and manner that we choose" (Obama, 2014). Moreover, while the U.S. Department of Defense Cyber Strategy (2015) confirmed that the Sony hack was "one of the most destructive cyberattacks on a U.S. entity to date," it said that the hack "further spurred an already ongoing national discussion about the nature of the cyber threat and the need for improved cybersecurity" in the military defense area (p. 2).

The U.S. government's response was understood as laying the groundwork for decisive, massive retaliation against North Korea. Some senior U.S. officials and experts on North Korea said the Obama administration was considering several countermeasure options, such as conducting cyber retaliations, imposing financial sanctions, re-designating North Korea as a state sponsor of terrorism, and increasing U.S. military capability in South Korea against North Korea (Northam, 2014). Secretary of State John Kerry said North Korea's actions were a "brazen attempt by an isolated regime to suppress free speech and stifle the creative expression of artists beyond the borders of its own country" (Kerry, 2014). U.S. Senator Robert Menendez (D-NJ), Chairman of the Senate Foreign Relations Committee, also sent a letter to John Kerry urging him to consider re-designating the DPRK as a state sponsor of terrorism in wake of the Sony hack (Menendez, 2014).

While perhaps a coincidence, North Korea lost its connection to the internet only hours after President Obama declared that on Friday December 19, 2014, the United States would launch a "proportional response" to the Sony cyberattacks (Perlroth & Sanger, 2014). For example, as of December 28, 2014, some of the major North Korean propaganda websites, such as

Uriminzokkiri (www.uriminzokkiri.com) and Ryomyong (http://www.ryomyong.com), whose severs were based in China remained inaccessible ("Major N. Korean Websites," 2014). In a December 27, 2014 statement, the National Defense Commission of North Korea lashed out at the United States, blaming it for disruptions that cut off the nation's already-limited internet connections. The statement also called President Obama a "monkey" for urging the film studio to release *The Interview*, a comedy depicting the assassination of the North Korean leader, Kim Jong Un via the North's state-run Korean Central News Agency (Fackler, 2014). However, the U.S. administration sidestepped the issue about whether it was involved in bringing down the North's internet connectivity to the outside world (Sanger & Schmidt, 2015). It is still unclear who is responsible for this disruption.

The Obama administration's verifiable actions against North Korea in response to the Sony hack exceeded previous warnings. On January 2, 2015, President Obama signed an executive order authorizing sanctions against three North Korean organizations and ten individuals. The White House said the new penalties were a "proportional response" to North Korea's "ongoing provocative, destabilizing, and repressive actions and policies" (Francis, 2015). According to the new sanctions, three North Korean government entities—the RGB, North Korea's primary intelligence agency; the Korea Mining Development Trading Corporation, Pyongyang's main arms dealer; and the Korea Tangun Trading Corporation, responsible for procurement and technology connected to North Korean defense research and development—were not allowed to run businesses with American companies and individuals (Francis, 2015). In addition to the three entities, ten individuals with connections to the Korea Mining Development Trading Corporation have not also access the American financial system, and any assets they had inside the United States are now frozen (Francis, 2015). However, some experts cast doubt on the new penalties

with comments that the Obama administration overestimated the impact of sanctions (Sanger & Schmidt, 2015). All three North Korean entities had already been punished by previous sanctions (Francis, 2015). The *New York Times* emphasized that six decades of similar sanctions designed to isolate North Korean have not stopped it from developing nuclear weapons, launching terrorist attacks on the South, testing missiles, or maintaining large prison camps (Sanger & Schmidt, 2015).

Since Obama's sanctions, North Korea-sponsored hackers and hacker groups have still carried out cyberattacks. The criminal complaint against Park Jin Hyok detailed what the hackers did and how they were connected to each other and to each cyberattack. The complaint was supported by scientific and circumstantial evidence collected and analyzed from the FBI and other U.S. law enforcement entities, private cybersecurity companies, individual computer scientists, and other countries (Shields, 2018, p. 2). The complaint also illustrated that the hackers worked for the North Korean regime and its national goals. Nevertheless, the U.S. Department of Justice only indicted Park Jin Hyok and Chosun Expo, the front company for which he worked. On September 6, 2018, Treasury Secretary Steven Mnuchin then announced that the Department of the Treasury's Office of Foreign Assets Control also designated only Mr. Park and Chosun Expo under Executive Order 13722 based on the criminal complaint (Office of Public Affairs, DoJ, 2018). In other words, these efforts failed to deter North Korea from conducting cyberattacks led by its cyber proxies on the United States and other countries. Moreover, this punishment was far weaker than other U.S. or U.N. sanctions imposed in response to North Korea's nuclear programs.

North Korea's cyber proxy warfare strategy dictated this outcome of the criminal complaint. The state delegated its monopoly authority over violence to individuals as well as front

companies far from itself for cyberoperations. Although the criminal complaint revealed that Chosun Expo hired Mr. Park and other North Korean hackers working for Lab 110 under the control of North Korean intelligence agency RGB, it did not verify a direct connection between the attacks and the regime. The regime has been successfully protected by artificial connections and layers between an individual, the front company, and the regime under a cyber proxy warfare strategy. Moreover, North Korean cyber proxies used the anonymous and borderless characteristics of cyberspace to conceal their identities and their relationship with their sponsor.

It is critical to investigate both ends to identify real actor or actors behind cyberattacks. One end is victims or targets who are attacked by state-led cyber proxy operations. Law enforcement agencies of victim states can usually access targeted devices or networks. These devices and networks are under state sovereignty. The challenge is that victim states cannot investigate the starting point of the cyberattacks, where proxy hackers physically resided or passed through in a virtual sense. The starting point includes IT infrastructure or devices the hacker used for cyberattacks. In general, this starting point is more likely than the endpoint to contain evidence linking North Korea-cyber proxies to North Korea. Thus, there is no evidence about the cyberattacks starting point in the criminal complaint against Park Jin Hyok, especially with regards to North Korea and China.

The starting points of state-led cyber proxy cyberattacks have been protected by state sovereignty. North Korea hackers have conducted cyberoperations only in North Korea, China, and other friendly countries. North Korea is an entirely closed country that foreigners cannot access without state permission. The state has not joined many international treaties or organizations (such as Interpol) that would hurt its regime.

It is also difficult to secure cooperation from China and other countries friendly to North Korea in order to investigate North Korean hackers located in their sovereign territories. Since the July 2009 Cyberattacks, despite South Korea's law enforcement agencies' repeated requests, China has not assisted investigations into the North Korea-related cyberattacks. For instance, in 2015, China declined the request of South Korea's Joint Investigation Team for Hacking on KHNP to access the starting point of the hack. The team said that hackers who penetrated KHNP accessed a VPN service using Chinese IP addresses allocated to Shenyang near North Korea, along with North Korea's own IP addresses (Han-Sol Kim, 2015). However, the team were not able to confirm whether hackers directly used the Chinese IP addresses or not due to China's decline to cooperate with the investigation.

Several efforts, including South Korea's accusations, Obama's sanctions, and the 180-page criminal complaint against Park Jin Hyok, appear to have failed in deterring North Korea from conducting cyberattacks. As North Korea has employed third-party, non-state actors for its offensive cyber strategy, it has avoided responsibility and punishment from the international community, including victim states. Therefore, conducting cyber proxy operations can be clearly viewed as a clever aggressive strategy for this isolated state which wants to use cyberspace to ensure regime survival without being punished.

3.6 CONCLUSION

How has the North Korean regime accomplished its hostile cyberoperations without being traced and punished? North Korea has been accused of conducting several massive and complicated cyberattacks against the rest of the world. Despite this, the state has still denied responsibility through a new proxy warfare strategy in cyberspace. The empirical evidence from North Korea's cyberoperations illustrates that a proxy warfare logic has been applied to a

cyberwarfare strategy. Thus, this chapter concludes that Pyongyang conducts cyber proxy operations to achieve its national goals while keeping a distance from its responsibility for its malicious activities in the virtual world. Three main findings follow from the case of North Korea's hostile cyberoperations.

First, this chapter proves cyberspace is a new venue for proxy warfare. Proxy warfare has been pervasive. States have employed third parties as proxies to achieve their strategic goals. The anarchic international system offers sufficient conditions for proxy relationships. However, there are some challenges for sponsors in a classic proxy warfare situation, such as physical barriers and control mechanisms over proxies. Contrary to the real world, however, cyberspace can overcome these challenges. In other words, for state actors, proxy warfare is perfectly realized in the virtual world due to artificial characteristics of the space—an anarchical environment, anonymity, and an absence of boundaries—and using information technologies—such as fake IP addresses, proxy servers, hop points, and VPNs. This is called cyber proxy warfare.

Second, North Korea provides the best example of cyber proxy warfare in practice. North Korean IT human capital used for cyber proxy state operations, trained by state-led intensive gifted computer education programs, is disguised to appear as non-state actors in cyberspace. These cyber warriors work for the North Korean regime in their state, China, and other Southeast Asian countries. In practical terms, proxy hackers are employees for North Korea's front companies, which are directly controlled by Lab 110. Lab 110 is also affiliated with the Reconnaissance General Bureau (RGB), North Korea's military spy agency, managed by the regime's Defense Ministry. Several layers between North Korea's proxy hackers and the state protect the regime from potential punishment by the international community.

Last, this chapter offered an opportunity to examine North Korea's cyberoperations patterns. Beginning with DDoS attacks, Pyongyang targeted critical infrastructure of its primary enemies, South Korea and the United States, to achieve its long-term political goal of regime survival. Since recent international economic sanctions against North Korea and its nuclear programs, North Korean proxy hackers have focused on financial entities for short-term financial gain. However, this focus does not indicate that North Korea is reluctant to conduct cyberattacks in pursuit of its long-term goal. The North Korean regime still targets critical infrastructure of other countries, along with international financial banks, institutions, and cryptocurrency exchanges. Moreover, these short-term financial gains also contribute to North Korea's long-term political goals.

Chapter 4. NORTH KOREA'S CYBER UNCERTAINTY AND REGIONAL SECURITY DYNAMICS

4.1 INTRODUCTION

In comparison to conventional military power, cyberpower is viewed as a doubtful strategic tool to maintain and alter the balance of power; and to resist or impose disputed outcomes (Gartzke, 2013). Some scholars view cyber threats merely as a phantasm because it attracts the attention of policymakers but has no effect in reality (Kello, 2013, p. 10). Political scientist Erik Gartzke (2013) contends that cybercapability is unlikely to serve as the final arbiter of power games between states in an anarchical world; therefore, it should not be considered in isolation from more conventional military capabilities (p. 42). Overall, these skeptics believe that cyberoperations are a less powerful tool than conventional military capabilities, making them ineffective for achieving political goals.

Despite the skeptics, North Korea's uncertain cyberactivities in recent years seem to indicate that cyber power of the state has already become one of its strategic tools for pursuing national interests. These cyberactivities include DDoS (Distributed Denial of Service) attacks against South Korea and United States' governments and private websites; the spread of WannaCry ransomware designed to encrypt computer data and demand ransom payments around the world; as well as recent hacking of international financial entities, including cryptocurrency exchanges. Clearly, states and military alliances have organized, planned for, and responded to the uncertain malicious activities in the virtual world. In the *Cyberspace Policy Report* published in November

2011, the U.S. military officially declared cyberspace as the fifth domain of war, after the physical domains of land, sea, air, and space (U.S. DoD, 2011).

On June 14, 2016, NATO Secretary General Jens Stoltenberg also said in an interview published by German newspaper The *Bild*, that "A severe cyberattack may be classified as a case for the alliance. Then NATO can and must react [to a massive cyberattack on any of its allies]" (Shalal, 2016). Two days before the interview, NATO also officially confirmed that cyberspace is an official operational domain of warfare, along with physical domains (Baldor, 2016). Similar to traditional military operations, aggressive activities in cyberspace cause fear and raise security concerns. Thus, this chapter analyzes North Korea's uncertain activities in cyberspace to shed light on how much a state's cyber buildup impacts regional and world security dynamics.

Cyberspace is becoming increasingly important in nearly every aspect of daily life (Jordan, 1999). National security and warfare are no exception. Cyberspace has become one of the most important topics in national security. In the 1990s and the 2000s, information technology was simply used to augment conventional warfare. However, cyberspace made by the technology is now viewed as an independent domain of warfare.

Information technology attracted the attention of military experts under the name of electronic warfare during the Gulf War (Aug. 2, 1990–Feb. 28, 1991). Coalition troops led by the United States paralyzed the defense system of Iraq via electronic warfare before the main assault began. This strategy recalls Sun Zhu (2000): "it is that in war the victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory" (p. 13). In the Gulf War, information technology played an important role in conventional warfare, but still remained supplementary.

Since the 2000s, information technology has started to become independent of conventional warfare. Terms such as “information warfare,” “cyber warfare,” and “cyber war” frequently began to appear in the media and academia. Moreover, during this period, militaries recognized cyberspace as an operational domain of war. Carl von Clausewitz (2007) defined war as “an act of force to compel enemy to do our will” (p. 13). According to this definition of war, states and their militaries officially accepted that cyberspace activities have sufficient power to compel a state to bend to the will of others.

In this regard, there is a growing literature on the topic of national security in cyberspace. Beginning in the 1990s, some scholars warned of the dangers of cyberoperations to national security (Arquilla & Ronfeldt, 1993; Bumiller & Shanker, 2012; Clarke & Knake, 2010; Wirtz, 2017). While these scholars contributed to raising public, governmental, and academic awareness about the importance of cybersecurity, they were viewed as fearmongers because they did not have sufficient empirical evidence to support their arguments (Sharp, 2017, pp. 1–2). After Russia’s cyberattacks on Estonia in 2007, however, empirical data about state-led cyberoperations began to accumulate. Many scholars have since focused on technical aspects of cybersecurity and cyberwarfare (Applegate, 2011; Qin et al., 2007; Weedon, 2015). Their studies provide practical guidance for cybersecurity experts, including military personnel who carry out cyberoperations.

In relation to cyberspace, others have studied issues of military doctrine (Colarik & Janczewski, 2012; Monaghan, 2015); national cyberpolicy and strategy (Ciolan, 2014; Czosseck, et al., 2013; Joubert, 2012; Libicki, 2009); and domestic and international laws (DeLuca, 2013; Gervais, 2012; Goldsmith, 2015; Schmitt & Vihul, 2014; Stinissen, 2015). These studies are useful for political leaders, policymakers, and other elite groups who are interested in

cybersecurity issues. However, using the language of security studies, relatively few scholars have explored the relationship between conventional forms of national security and cybersecurity (Buchanan, 2016; Junio, 2013; Rid & Buchanan, 2015; Sharp, 2017; Valeriano & Maness, 2014). Those who have engaged in this research have also presented available empirical evidence to support their arguments more systematically.

Using the traditional language of security studies, this study also joins this small group of scholars by examining whether a state's building of its cybercapability causes fear and uncertainty among other countries. In other words, can the development of states' cybercapability increase fear, insecurity, and even change regional security dynamics in comparable ways to the development of traditional military power and alliances in the security dilemma? The security dilemma involves one country taking steps to increase its security, thereby inadvertently threatening the security of other countries with what appears to be offensive actions. By analyzing North Korea's uncertain activities in cyberspace, this chapter demonstrates how much a state's cyber buildup impacts regional and world security dynamics. This chapter also argues that states' cyber capabilities are as powerful as conventional military capabilities; this, in turn, creates the security dilemma and resulting changes in regional security dynamics.

The chapter's central argument is supported by a single case study: North Korea's uncertain cybercapability and ambiguous intentions about increasing that capability. A revolution in military affairs (RMA), sometimes described as the military-technical revolution, has led to change in and uncertainty over future characteristics of warfare, the security of the region, and even that of the rest of the world (Cohen, 1996, p. 37; Kihl, 2002, p. 60). RMA includes the increased adaptation of information technology for military use to advance states' political goals

(Cohen, 2004; Kihl, 2002, p. 60). North Korea is an exemplar of a country using information technology to reach its national goal, survival. Moreover, North Korea's developing cybercapability causes fear and uncertainty in other countries, mainly South Korea and the Korean Peninsula, increasing the security dilemma between the two Koreas.

North Korea started to develop its cybercapability in the 1980s through its state-led intensive education programs for gifted computer students, as detailed in Chapter 2. Officially, the state tried to develop hardware and software programs. However, the isolated state, North Korea, from others does not match the core concept of cyberspace to connect networks to each other for supporting an infinite creativity across the world (Jordan, 1999, p. 21). The IT human capital developed from state-led intensive computer education programs has not advanced the economy or North Korean society. Moreover, the North Korean regime does not allow its ordinary citizens to access the internet. The internet appears to be a potential threat to the authoritarian regime. Thus, this paradoxical situation raises a serious concern about the role of North Korea's surplus IT human capital.

At the outset, it must be acknowledged that there are two controversial issues. The first is a controversy over whether North Korea's development of cybercapability is a defensive action or not. According to the strict definition of the security dilemma, clearly offensive actions of a state do not cause the security dilemma. Therefore, it is useless to differentiate defensive actions from hostile acts originating from states who are willing to change the status quo of the international system. The actions generated by openly hostile states are understood as a security problem, rather than a security dilemma. Thus, from this perspective, North Korea's development of cybercapability, which is a demonstration of dissatisfaction with the status quo, can be viewed as intentional aggressive actions to increase the Korean Peninsula's security problem.

In spite of this security problem rather than a security dilemma, North Korea's development of its cybercapability is an ambiguous action that causes uncertainty, resulting in a cybersecurity dilemma. Since the end of the Cold War, North Korea has increased its conventional military power, including nuclear weapons. The state used to cause armed provocations with its conventional military capability. However, North Korea's cybercapability cannot be clearly divided into defensive and offensive actions. While massive cyberattacks across the globe have been attributed to North Korea, it has successfully denied and avoided responsibility. North Korea's development of its cybercapability is also ostensibly a tool to develop its society and economy. Therefore, in a broad sense, North Korea's ambiguous intentions in its development of a cybercapability is not a security problem, but rather a security dilemma for South Korea.

This study also focuses on the South Korean military's defensive response to North Korea's uncertain cybercapability. Perhaps more importantly, when South Korea strengthens its defensive cybercapability and forms cyber alliances, the cybersecurity dilemma is transferred to Northeast Asia. In other words, South Korea's defensive efforts inadvertently decrease the security of other countries in the region. Thus, the North Korean case illustrates the cybersecurity dilemma.

Second, this study does not argue that the Korean Peninsula cybersecurity dilemma is the only cause of conflict between the United States and China or between the United States and Russia in cyberspace. The United States was already in competition with China and Russia in the virtual space before North Korea's cyber threats. China has conducted cyber espionage operations to steal cutting-edge technology, including defense-related technologies. Russia has also carried out aggressive cyberoperations on critical U.S. networks, mainly the 2016 Democratic National Committee email leak, to revive its past glory (U.S. DHS, 2016). However,

this chapter does not examine the three states' complex cyber conflicts with one another. On the contrary, this study only aims to emphasize how two former Cold War blocs encounter each other during the course of the spread of the cybersecurity dilemma from the Korean Peninsula to the Northeast Asia region.

The study proceeds as follows: section 4.2 explores the origin of the cybersecurity dilemma on the Korean Peninsula. Section 4.3 introduces classic security theories: the security dilemma and offense-defense theory. Section 4.4 bridges the gap between the aforementioned theories and cybersecurity to name and explain the cybersecurity dilemma. Section 4.5 presents empirical evidence illustrating the existence of the cybersecurity dilemma. The two primary responses of South Korea to the dilemma are detailed in sections 4.5.1 and 4.5.2. Lastly, the expansion of the dilemma to the Northeast Asia region is discussed in section 4.5.3. The chapter concludes with a summary discussion and suggestions for future research.

4.2 The Evolution of Northeast Asian Regional Security Challenges

Pyongyang's traditional method of maintaining its regime has been to increase its military capability. In doing so, regional security uncertainty and instability on the Korean Peninsula has increased over time. North Korea-led security dynamics in the region began with its conventional arms buildup, including increasing the size of regular and special military forces as well as chemical and biological weapons production. Since the end of the Cold War, North Korean has begun to develop nuclear weapons, creating both regional and global security instability. In response to this uncertainty, South Korea and other countries in or near the region have also increased their military power against North Korea's military. The regional dynamics caused by the increase in North Korea's conventional military capacity supports the international relations theory of the "security dilemma." Moreover, these regional security dynamics are being

transferred to cyberspace as Pyongyang develops its cybercapacity. This transfer of security dynamics may be viewed as an example of a classic security dilemma in the virtual world. These theoretical issues will be detailed in the following two chapters.

The Cold War East-West confrontation remains a reality on the Korean Peninsula. Since the Korean War was triggered by the Cold War in 1950, the Peninsula has been divided into two parts, South Korea and North Korea. The first side includes South Korea, the United States, and Japan. The other side includes North Korea, China, and Russia. This ideologically based division has been the source of regional security dynamics. More precisely, uncertain military action provoked by survival needs has led to an arms race which can, in turn, lead to open conflict.

Beginning in the late 2000s, these regional security dynamics have expanded to cyberspace. As detailed in Chapter 2, North Korea began to develop its cybercapability in the 1980s as a tool for regime survival. Since then, the uncertain actions of the North in cyberspace have threatened other countries in the Northeast Asia region. During the first stage, South Korea began to increase its defensive cybercapability against North Korea's uncertain cyber strategy. During the second stage, the cyber arms race spread to all interested parties in the region, as each Korea began to cooperate with its traditional partners. Paradoxically, there was a classic confrontation between the Eastern and Western Blocs around North Korea's uncertain aggressive cyber strategy. Thus, the uncertainty of the Korean Peninsula in cyberspace and the unintended consequences of the uncertainty illustrate that the security dilemma is still valid in the information age.

Defensive actions of a state to increase its national security decrease the security of others. This security dilemma may result in military tension and even unplanned wars. The North Korean case, however, does not meet this narrow definition of the security dilemma. North

Korea's military buildup has been understood as an offensive strategy to attack the South and other Western states. It is a security problem. In a broad sense, however, North Korea's aggressive military buildup can be viewed as a defensive way to increase its national security in the face of threats from Western states. However, North Korea's actions have threatened South Korea's national security, creating a security dilemma on the Korean Peninsula. In a broader context, North Korea's increasing cybercapability is the source of the cybersecurity dilemma in the region. Regardless of North Korea's intentions, North Korea's development of cybercapability can be seen by South Korea as an unavoidable, uncertain threat.

Since the creation of the North Korean state in 1948, the regime has sought to have a strong military for survival by itself based on *Juche* ideology, translated as self-reliance, that founder Kim Il Sung (1912–1994; in office from 1948–1994) created. The Soviet Union and China assisted the regime when it was first established. After the Korean War (June 1950–July 1953), however, the North Korean regime believed that the changes in the two allies would threaten its existence. Following the death of Joseph Stalin in March 1953, China and the U.S.S.R. experienced several dramatic changes: de-Stalinization,[82] a peaceful coexistence with Western countries, an acceptance of a variety of socialist systems within the Eastern Bloc, and the rise of China along with Mao Zedong (ROK Ministry of Unification, n.d.-c). Kim Il Sung's response to these shifts was to establish a self-reliance ideology of *Juche* as a theoretical underpinning of the Kim family dictatorship.

North Korea's *Juche* includes four principles: (1) an ideology of self-reliance (*Juche*), (2) political independence (*Chaju*), (3) economic independence from foreign influences (*Charip*), and (4) military independence from imperialists (*Chawi*). Following the fourth principle, North

[82] De-Stalinization consisted of a series of political reforms, removing key institutions that helped Stalin hold power: the cult of Stalin's personality, the Stalinist political system, and the Gulag labor-camp system.

Korea adopted Four Military Lines in 1962: (1) arm the entire population, (2) fortify the entire country, (3) train the entire army as a "cadre army," and (4) modernize weaponry, doctrine, and tactics (Scobell & Sanford, 2007, p. vii). Article 60 of North Korea's Constitution says that "the State shall implement the line of self-reliant defense, the import of which is to arm the entire people, fortify the country, train the army into a cadre army and modernize the army on the basis of equipping the army and the people politically and ideologically" (DPRK Constitution, 1998). Thus, Kim Il Sung chose *Juche* self-reliance ideology to emphasize the necessity of an arms buildup for regime survival.

North Korea's second leader, Kim Jong Il (1941–2011; in office 1994–2011), focused more on military power than his father. In the mid-1990s, Kim Il Sung's successor, Kim Jong Il, adopted the Military First Policy, known as *Songun* in Korean, to overcome its post-Cold War isolation. The Military First Policy was the driving principle behind North Korea's politics and economy; the Korean People's Army was prioritized both in affairs of state and in resource allocation. It also guided North Korea's international interactions. It was under this policy that North Korea started to develop nuclear weapons as the best way to ensure regime survival.

While North Korea's arms buildup based on Kim Il Sung's Four Military Lines and Kim Jong Il's Military First Policy increased its national security, it decreased South Korea's national security. North Korea's military power was viewed as a threat by South Korea. South Korea responded to North Korea's military-focused policies by developing its own military power as a defense mechanism. Although South Korea should have invested more money on economic development after the end of the Korean War, it instead steadily increased its military expenditures (see Appendix: Yearly Defense Budget Comparison of ROK Military). According to World Bank statistics, South Korea's military expenditures accounted for 7.2% of its 1960

GDP (The World Bank, n.d.-a). Table 4.1 shows that as of 2017, South Korea's military expenditures as 2.6% of its GDP was still relatively higher than other countries in the world. South Korea's biannual *Defense White Paper* says that higher military expenditures have resulted from threats from its main enemy, North Korea.

Table 4.1. The 15 Countries with the Highest Military Expenditures in 2017

Rank		Country	Spending, 2017 ($ b.)	Change, 2008–17 (%)	World share, 2017 (%)	Spending as a share of GDP (%)	
2017	2016					2017	2008
1	1	U.S.A.	610	*-14*	*35*	*3.1*	*4.2*
2	2	China	[228]	*110*	[*13*]	[*1.9*]	[*1.9*]
3	4	Saudi Arabia	[69.4]	*34*	[*4.0*]	[*10*]	*7.4*
4	3	Russia	66.3	*36*	*3.8*	*4.3*	*3.3*
5	6	India	63.9	*45*	*3.7*	*2.5*	*2.6*
6	5	France	57.8	*5.1*	*3.3*	*2.3*	*2.3*
7	7	U.K.	47.2	*–15*	*2.7*	*1.8*	*2.3*
8	8	Japan	45.4	*4.4*	*2.6*	*0.9*	*0.9*
9	9	Germany	44.3	*8.8*	*2.5*	*1.2*	*1.3*
10	10	South Korea	39.2	*29*	*2.3*	*2.6*	*2.6*
11	13	Brazil	29.3	*21*	*1.7*	*1.4*	*1.4*
12	11	Italy	29.2	*-17*	*1.7*	*1.5*	*1.7*
13	12	Australia	27.5	*33*	*1.6*	*2.0*	*1.8*
14	14	Canada	20.6	*13*	*1.2*	*1.3*	*1.2*
15	15	Turkey	18.2	*46*	*1.0*	*2.2*	*2.2*
Total top 15			1,396	..	*80*	..	..
World total			1,739	*9.8*	*100*	*2.2*	*2.4*

[ ] = SIPRI[83] estimate; GDP = gross domestic product

Source: Tian, Fleurant, Kuimova, Wezeman, & Wezeman, SIPRI Fact Sheet, May 2018.

Table 4.2 illustrates the arms race between the two Koreas. As of 2018, North Korea has 1,280,000 soldiers and diverse weapons. South Korea has approximately 599,000 soldiers. The

[83] SIPRI stands for Stockholm International Peace Research Institute, which was established in 1966. SIPRI is an independent international institute based in Stockholm, Sweden, dedicated to research into conflict, armaments, arms control and disarmament. Based on open sources, SIPRI provides data, analysis and recommendations to policymakers, researchers, media, and the interested public across the world. For more information about SIPRI, see, https://www.sipri.org/about (SIPRI, n.d.).

two Koreas have large-scale militaries compared to the size of their populations, 51.47 million in South Korea and 25.49 million in North Korea as of 2017 (The World Bank, n.d.-b).

Table 4.2. Comparing Military strengths of the Two Koreas
(As of December 2018)

Category				South Korea	North Korea
Troops	Army			464,000	1,100,000
	Navy			70,000 (including 29,000 Marine Corps troops)	60,000
	Air Force			65,000	110,000
	Strategic Force			-	10,000
	Total			599,000	1,280,000
Major Forces	Army	Units	Corps	13 (including Marine Corps)	17
			Divisions	40 (including Marine Corps)	82
			Maneuver Brigades	31 (including Marine Corps)	131
		Equipment	Tanks	2,300 (including Marine Corps)	4,300
			Armored Vehicles	2,800 (including Marine Corps)	2,500
			Cannons	5,800 (including Marine Corps)	8,600
			MLRS/MRLs	200	5,500
			Ground-to-ground missiles	60 launchers	100 launchers
	Navy	Surface	Combatants	100	430
			Amphibious ships	10	250
			Mine warfare vessels (minesweeping boats)	10	20
			Support and auxiliary vessels	20	40
		Submarines		10	70
	Air	Combat aircraft		410	810
		Surveillance & control aircraft		70	30
		Transport aircraft		50	340
		Trainers		180	170
	Helicopters (army/Navy/air Force)			680	290
reserve troops				3,100,000	7,620,000

* Units and equipment of the Marine Corps are included in the number of units and equipment of the army to compare military strength between the two Koreas; North Korean cannon numbers do not include 76.2 mm guns that are infantry regiment-level artillery; The table above is a result of quantitative comparisons based on disclosable data, as qualitative assessments are limited.
Source: ROK MND, The 2018 Defense White Paper, December 2018a, p. 244.

In addition to the arms race between the two Koreas, North Korea's potential military threats have led to stronger cooperation between the United States and South Korea based on

their Mutual Defense Treaty.[84] The South Korean president, Rhee Syng-man (1875–1965; in office 1948–1960), delegated the command authority of the South Korean military in peacetime as well as wartime to the commander of the United Nations Command during the Korean War on July 14, 1950 (Seoyeon Yoon, 2015). This was a rational action for the South to take, which was weaker than the North during the Korean War. However, the United States still maintains operational control authority in wartime for mutual defense against North Korea's military threats. Also, according to the treaty, the United States stationed its large-scale military forces in South Korea. South Korea has therefore built a strong military force and formed the alliance with the United States against military uncertainty about North Korea's arms buildup.

Multilateral corporation has also responded to the uncertainty generated by North Korea's nuclear weapons program on the Korean Peninsula. The international community attempted to find a peaceful resolution to this security concern through the Six-Party Talks[85] attended by China (Chair), Japan, North Korea, Russia, South Korea, and the United States. The talks tried to halt North Korea's development of nuclear weapons in exchange for energy aid, including two proliferation-resistant light-water reactors sponsored by South Korea, Japan, and the United States (Davenport, 2018). At the same time, the United Nations Security Council has imposed sanctions on North Korea since North Korea's first nuclear test in 2006 ("UN Documents for DPRK," n.d.). However, despite these diplomatic efforts and sanctions, North Korea has still developed nuclear weapons.

---

[84] Mutual Defense Treaty Between the United States and the Republic of Korea was signed on October 1, 1953. The agreement commits the two countries to provide mutual aid if either faces external armed attack. Then, it allows the United States to station military forces in South Korea in consultation with the South Korean government.

[85] The Six-Party Talks were a series of multilateral negotiations held intermittently since 2003. China (Chair), Japan, North Korea, Russia, South Korea, and the United States attended the talks for the purpose of dismantling North Korea's nuclear program. (Davenport, 2018)

The third dictator of North Korea, Kim Jong Un (1983–present; in office 2011–present), has continued this emphasis on the military. In 2012, North Korea proclaimed itself a "nuclear state" through a revision of the DPRK's constitution, listed on its official "My Country" propaganda website:

> Amid the collapse of the world's socialist system and the vicious anti-Republic oppressive offensive by the imperialists' joint forces, Comrade Kim Jong Il honorably defended the gains of socialism which is Comrade Kim Il Sung's lofty legacy through military-first politics; changed our fatherland into a politically and ideologically powerful state that is invincible, a nuclear state, and a militarily powerful state that is indomitable; and paved a brilliant main road in building a powerful state. (Hayes, 2012)

On March 31, 2013, during a plenary session of the Party Central Committee (PCC), North Korea adopted a parallel economic and nuclear weapons development policy, known as *Byungjin* in Korean (Cheon, 2013, p. 1). Moreover, while Kim Jong Un retains Kim Il Sung's Four Military Lines, he created the Four-Point Strategic Lines: (1) to arm the entire population, (2) to fortify the entire country, (3) to train the entire army as a "cadre army," and (4) to modernize weaponry, doctrine, and tactics (Scobell & Sanford, 2007, p. 31). These lines were announced at the North Korean People's Army's buildup at the third Political Convention for Battalion Commanders and Commissars in November 2014; it is believed these lines are closely connected with heavy militarization (Dong-Yub Kim, 2015, p. 95). The state has also trained defense scientists and developed military industry in order to support Kim Jong Un's military policy (ROK Ministry of Unification, n.d.-d).

North Korea's parallel economic and nuclear weapons development policy increases the uncertainty on the Korean Peninsula and the world more generally. South Korea is still increasing military expenses to maintain a large-scale military against North Korea's potential provocation, including nuclear and missile tests. The South has also delayed a shift in its wartime command in cooperation with the United States to increase its national security. However, since 2018, the North Korean regime has begun to negotiate with the United States and South Korea governments about denuclearization of the Peninsula due to stiff sanctions. North Korea wants to receive financial support from the international community in response to its denuclearization process. Despite that, it is uncertain whether North Korea will accept the international community's requirements, especially the United States' stipulations. These negotiations show that the development of North Korea's nuclear weapons is a powerful bargaining chip rather than a real offensive strategy.

In contrast to the politics of nuclear weapons, North Korea's cybercapability provides a more effective method for achieving regime survival. As detailed in Chapter 2, Pyongyang realized the importance of IT technology in the 1980s when Kim Il Sung visited its communist allies in the Soviet Union and the Eastern bloc; the regime began to focus on computer education for the young. Since then, North Korea has made efforts to foster IT human capital through state-led intensive elite education systems. However, in reality, there is not a sufficient IT infrastructure or private IT sector to employ all of North Korea's computer experts. Moreover, IT policies of the North Korean regime are different from those of other countries. All ordinary North Korean people are not allowed to access and use the internet for private purposes. Thus, it is suspected that unlike other countries' IT experts, North Korean IT human capital operates as cyberwarriors who conduct cyberoperations for the regime.

Beginning in the late 2000s, North Korea arguably began to conduct cyberoperations. The July 2009 Cyberattacks on several vital websites of the United States and South Korea marked the start of North Korea's cyberoperations. A variety of cyberattacks followed. The 2014 Sony hack showed that Pyongyang could directly use cyber power for achieving its political goals. It is believed that the state hacked Sony Pictures Entertainment to prevent the release of the film, *The Interview*, which is about the assassination of Kim Jong Un. Since the international community's strong economic sanctions against its nuclear programs, North Korea-affiliated hackers have begun to target financial institutions, such as Bangladesh Bank and cryptocurrency exchanges. The state carried out the WannaCry ransomware attack for financial purposes. However, North Korea has still attacked networks of critical infrastructure and conducted cyber espionage against other countries for political purposes. All of these events mean that North Korea has threatened others' national security in cyberspace.

North Korea has created a security dilemma with the arms buildup for its regime survival. Since the end of the Cold War, it has begun to develop nuclear weapons, threatening the region and even the world as a whole. The security dilemma is still valid in cyberspace as North Korea increases its cybercapability, which creates uncertainty among other countries. The next section discusses classic international relations theories, especially the security dilemma and offense-defense theory, to conceptualize the impact of North Korea's cyber arms buildup on Northeast Asian regional security dynamics.

4.3 IR Theories of Bilateral and Regional Security

A crucial challenge for international relations theorists is explaining how empirical examples of regional insecurities escalate under conditions of mutually shared interest in non-confrontation or non-aggression. These cases have been described by international relations

scholars and policymakers as "security dilemmas." The security dilemma is one of the most important theoretical ideas that explains the source of increased tension and security dynamics between countries; this increased tension can create conflict even when neither side really desires it (Tang, 2009, p. 587).

According to defensive realists,[86] World War I is a classic case of the security dilemma; though there is a controversy over the origins of the War,[87] an offense-defense dynamic was at work in the case. The security dilemma caused escalating tension between Western countries, triggering World War I. David Lloyd George, British Prime Minister during the war, wrote in his 1933 memoirs that "the nations [European powers] slithered over the brink into the boiling cauldron of war without any trace of apprehension or dismay" (George, 1933, p. 49). He also added that "the nations backed their machinery over the precipice … not one of them wanted war" (George, 1933, p. 52).

Defensive realism summarizes the origin of World War I as follows. Britain, France, and Russia formed the Triple Entente in 1907 primarily as a counterweight to the German-led Triple Alliance (Austria-Hungary and Italy) formed in 1882 (Schmitt, 1924).[88] The Triple Entente

[86] Realism is mainly divided into two groups concerning explaining the cause of World War I. The first is defensive realists focus on the security dilemma. According to the dilemma, they contend that European powers were relatively satisfied with their status quo, mainly worried about their national security, and primarily taking defensive measures, causing unintended World War I. The second is offensive realists, arguing that World War I was driven by maximizing power of European countries with regional hegemonic ambitions.

[87] In recent years, some international security scholars contend that the argument of an accident (or "sldie") is incorrect for some reasons (Hamilton & Herwig, 2003). For instance, German elite groups just preferred a local war against France and Russia in the Balkans while they never sought and expected a broader European war involving Great Britain (Lieber, 2007, p. 156). This view, of course, accepts that Germany played a significant role in the outbreak of the war and assigns Germany a greater share of the blame. Moreover, in recent years, some scholars place the blame on the United Kingdom, Russia, Austria-Hungary, or France for the origins of World War I (Ferguson, 1999; McMeekin, 2011; Wawro, 2014). This discussion is to search for 'bad guys' and 'good guys' in a complex world though it also provides the public with in-depth analyses of the cross-continental motivations for statesmen to turn a small diplomatic crisis in the Balkans into the First World War (Neiberg, 2018).

[88] More information about the Triple Entente and the Triple Alliance see, Schmitt, B. E. (1924). Triple Alliance and Triple Entente, 1902–1914. *The American Historical Review*, *29*(3), 449–473.

increased the insecurity of the Triple Alliance by creating fears of encirclement. This, in turn, led Germany to an arms buildup. The Triple Entente saw this increased arms production as preparation for war. Each side was unable to differentiate defensive behaviors from offensive ones. Moreover, Robert Jervis (1976) asserts that the vicious circle is an immediate cause of the outbreak of war in 1914 (p. 94). He also emphasizes that at the time the offense dominance captured European powers: "Each of the continental powers believed that the side that struck first would gain a major military advantage" (Jervis, 1976, p. 94). Thus, according to defensive realists, undistinguishable intentions of each side and offense dominance caused World War I.

The following section outlines the classic security dilemma and applies it to a similar phenomenon in the information age called the *cybersecurity dilemma*. First, it gives an overview over the security dilemma. Then it presents the main theoretical framework of this chapter by introducing Robert Jervis' offense-defense theory, which evaluates the intensity of the dilemma, and provides empirical examples for the theory. Lastly, it discusses theoretical and methodological debates about the framework of this study and how well it applies to real-world examples.

4.3.1 *The Classic Security Dilemma*

In the 1950s, political scientist John H. Herz coined the term "security dilemma" (Herz, 1950, 1951, 1959). At the same time, historian Herbert Butterfield independently used the term to illustrate a state's action that is exposed to uncertainty (Butterfield, 1950, 1951). Herz and Butterfield argued that many countries recognized the importance of their survival during and after the two world wars. Therefore, states have pursued survival with every means available to them. However, other countries have view pursuing survival of a state as an aggressive way to threaten their survival.

The Cold War had played a key role in attracting scholars' attention to the security dilemma. States' survival instincts became particularly noticeable after the beginning of the Cold War in the late 1940s, which had divided the world into the two opposing sides. Many scholars used the security dilemma to illustrate the tension between the Free World and Communism (Collins, 1998; Jervis, 2001; Kydd, 2005). In other words, the security dilemma theory developed over the course of the Cold War (Byoung-Won Min, 2012, pp. 34–35). Moreover, since the end of the Cold War, the dilemma has attracted security studies scholars' attention as it has expanded its boundaries to other new transnational security areas, such as terrorism (Byoung-Won Min, 2012, pp. 41–45).

Structural and psychological problems of international relations are two main sources of the security dilemma. First, Butterfield and Herz focused on uncertainty as the main structural cause originating from the anarchical nature of the international system. They conceptualized the security dilemma as a situation in which states pursue their own survival under the anarchical international system. Butterfield emphasized that the ultimate source of the dilemma is uncertainty and fear, which is derived from inevitable "Hobbesian fear" (Butterfield, 1950, p. 155; 1951, p. 22). Therefore, such uncertainty over others' intentions, which could cause war, was viewed as the tragic result of "man's universal sin" (Butterfield, 1950, p. 155; 1951, p. 22).

Herz took Butterfield's ideas and formally conceptualized it as the security dilemma which results from the structural problem of the international system, namely anarchy. Before Herz and Butterfield, some scholars, such as G. Lowes Dickinson, claimed that international anarchy characterizes international relations and causes the insecurities of nation-states (Zaidi, 2018, p. 61). In the 1970s, Kenneth Waltz argued in his book, *Theory of International Politics* (1979), that the anarchical nature of the international system is the most prominent feature of world

politics. In the internal realm, states monopolize the legitimate authority to use violence and practically provide protection for their citizens against illegitimate violence (Waltz, 1979, pp. 103–4; Milner, 1991). In contrast, however, in the external realm, the world lacks any supreme authority, sovereign, or coercive power which can resolve conflicts or enforce law or order in the system of international politics (Waltz, 1979, pp. 103–4; Milner, 1991). It therefore follows that in the anarchical international system, states are required to seek ways or methods to ensure survival. In this regard, Dickinson said that the anarchy gives rise to arms races between states (Zaidi, 2018, p. 61). In alignment with these scholars, Hertz argued that the ultimate source of the security dilemma is anarchy—the lack of "a higher unity" (Herz, 1950, p. 157).

Herz focused on the structural dilemma of the security problem that stems from fundamental social interactions between states. More important, individual states cannot resolve the dilemma by themselves. Herz emphasized the tragedy of international politics where states in the world were ridden with conflicts as they went to wars in the early 20th Century. In this context, he then demonstrated how difficult it is to find a solution to the dilemma. Beginning with the 1940s invention of the nuclear bomb and the emergence of a bipolar world, the dilemma has become pertinent and valid as way to explain the tragic events rooted in the Cold War (Herz, 1959).

In the 1970s, Jervis' psychological approach brought the security dilemma into the mainstream of structural international relations theories. He argued that the dilemma results from a psychological problem, along with the structural problems of the international system. Jervis defined the security dilemma as one of the means by which a state tries to increase its security while unintentionally decreasing the security of others: "one state's gain in security often inadvertently threatens others" (Jervis, 1978, pp. 169–170). Jervis also emphasized that "even if they [states] can be certain that the current intentions of other states are benign, they can neither

neglect the possibility that the others will become aggressive in the future nor credibly guarantee that they themselves will remain peaceful" (Jervis, 2001, p. 36). Jervis indicates that states' misinterpretations animate the dilemma. Thus, states unintentionally threaten others with their actions because they are frequently unable to understand how others who do not know their intentions will perceive their behavior (Buchanan, 2016, p. 19).

Jervis' emphasis on misperception as the second source of the security dilemma illustrates that international conflicts result from unintended and undesired consequences of states' actions (Jervis, 1976, p. 66). Before him, Herz already claime that a structural problem—the anarchical nature of the international system—causes the dilemma. This structural limitation forces states to seek to have a strong desire for their defense, resulting in the dilemma. In addition to this structural problem, Jervis showed that national decision-makers' psychological limitations also lead to the structural security dilemma. Jervis demonstrates a kind of realistic pessimism about international politics: "if each state pursues its narrow self-interest with a narrow conception of rationality, all states will be worse off than they would be if they cooperated" (Jervis 1976, p. 67).

In a security dilemma, states build a strong military and form alliances for defensive purposes. First, a state's arms buildup is a natural way to protect itself against hostile actions of others. Each state increases military expenditures and then invests in developing military technologies, producing more weapons, establishing more troops, and recruiting more military personnel. Thus, the arms buildup is an understandable way to ensure a state is prepared to defend itself against attacks of others in the face of the structural and psychological uncertainties of the international system. For example, Germany and Britain built up their military before the start of World War I (Jervis, 1976, pp. 68–70).

Second, military alliances are another reasonable way to secure national security. The security dilemma might force states to form new alliances or to strengthen existing alliances. Glenn H. Snyder (1984) argued that under the security dilemma, alliances will form for two reasons: (1) a state may be unsatisfied with the amount of security it has and it can increase security substantially by allying with friendly countries if its adversaries abstain from alliances; (2) a state, fearing that others will not abstain, will ally in order to avoid isolation or to preclude partners from allying against it (p. 462). For example, before World War I, Western powers repeatedly formed and dissolved alliances with one another under the security dilemma.

In this context, *alliances* refer to several types of international defense cooperation. In *Alliance Politics* (1997), Snyder offered a relatively narrow definition: "alliances are formal associations of states for the use (or nonuse) of military force, in specified circumstances, against states outside their own membership" (p. 2). Melvin Small and J. David Singer (1969) divided formal alliances into the three types: defense pact (Example: NATO, 1949); a non-aggression or neutrality treaty (Hitler-Stalin treaty, 1939); and entente (Great Britain-France, 1904). However, Stephen M. Walt's *The Origins of Alliances* (1987) broadly defined alliances as "a formal or informal relationship of security cooperation between two or more sovereign states" (p. 12). In a broader context, international cooperation military alliances in terms of defense are divided into three types: an alignment, a coalition, and an alliance[89] (Krause & Singer, 2001, p. 16). Thus, although states seek more closed relationships with their partners to defend themselves under the security dilemma, alliances can be understood as a variety of international cooperation measures

[89] Although the three terms are closely related, and even interchangeable in many cases, the three terms focus on different things. "An alignment is usually understood as any general commitment to cooperation or collaboration… A coalition is characterized by the commitment of two or more states to coordinate their behavior and policies in order to perform particular functions or pursue specific goals… An alliance is based on a written, mostly voluntary, formal agreement, treaty, or convention among states pledging to coordinate their behavior and policies in the contingency of military conflict" (Krause & Singer, 2001, p. 16).

designed as collective security between states, organizations, or both in order to increase their security.

However, building a strong military and forming alliances between states for defensive purposes paradoxically leads to a vicious circle of escalating tension. According to the definition of the security dilemma, although these actions are purely defensive, increasing the security of a state causes similar defensive actions of others, therefore deepening the dilemma. Thus, in general, the vicious circle becomes an arms race. These competitions sometimes result in regional security uncertainty, and even unplanned wars between states.

Though the term, the security dilemma, was coined by Herz and Butterfield in 1950s, Jervis brought the term into the mainstream of structural international relations theories in the 1970s. The defensive actions of a state can be divided into two types: an increased arms buildup and alliance formation. Paradoxically, however, these defensive actions may appear to be offensive actions to others. Therefore, it is likely that the security dilemma becomes a vicious circle between states, even resulting in unwanted wars. In the following section, it is discussed whether the security dilemma can be overcome.

4.3.2 *The Theoretical Framework: Offense-Defense Theory*

The security dilemma can be understood as a structural and psychological security problem that threatens the peace of a state, a region, and even the world. In this regard, the following key question emerges: can states increase their security without unintentionally decreasing the security of others and risking conflict? In response to this question, Jervis (1978) offered offense-defense theory in an effort to control the security dilemma, though it is impossible to overcome the dilemma in the anarchical international system completely.

According to his offense-defense theory, the security dilemma can be divided into four different worlds by intensity (Jervis, 1978). Moreover, he argued that according to the intensity of the dilemma, a major war could be avoided (Glaser & Kaufmann, 1998, p. 44; Jervis, 1978, p. 193). Two crucial variables are involved in offense-defense theory. These are whether the defense or the offense has the advantage and whether defensive weapons and policies can be distinguished from offensive ones (Jervis, 1978, pp. 196–187). In other words, the first variable is *offense-defense balance*. The second is *offense-defense differentiation*. Both can be combined into the four different worlds.

The first variable, offense-defense balance, is divided into two situations, offense-dominated or defense-dominated worlds. An offense-dominated world means that destroying the other country's army and taking its territory is easier than defending one's own army and territory (Jervis, 1978, p. 187). In contrast, in the defense-dominated world, defensive actions–protecting and holding one's territory–has the advantage over offensive ones–destroying others' armies and taking their territories (Jervis, 1978, p. 187).

The security dilemma is at its most vicious in the offense-dominated world, where "the only route to security lies through expansion" (Jervis, 1978, p. 187). Belief that offensive actions have a higher security incentive lead to following results: "war will be profitable for the winner"; "wars are expected to be both frequent and short"; "when wars are quick, states will have to recruit allies in advance"; and "if wars are frequent, statemen's perceptual thresholds will be adjusted" (Jervis, 1978, pp. 189–190). States easily choose offensive strategies to increase their security when the offense has the advantage. On the contrary, there is no security dilemma when the defense is dominant. In this regard, a state that fears attack is reluctant to launch a preemptive military action but instead focuses on the readiness for receiving an attack (Jervis, 1978, p. 187).

In a defense-dominated world, a state is unlikely to go to wars that can be won only at enormous cost (Jervis, 1978, p. 190). In this world, states will choose to cooperate while avoiding an arms race.

The second major variable is offense-defense differentiation. It changes how strongly the security dilemma operates. If weapons and policies of a state that increase national security also provide the offensive capability, they can decrease the security of others (Jervis, 1978, p. 199). However, on the contrary, if they do not, the security dilemma does not operate (Jervis, 1978, p. 199). This means that when states are able to differentiate defensive behaviors of others from their offensive ones, there is no security dilemma between countries.

Jervis (1978) argues that if the power of the defense is the same as that of the offense, the differentiation between them leads status-quo states to behave in defensive ways that are distinct from destructive ones of aggressors (Jervis, 1978, p. 199). In this regard, when the defense is superior to the offense, there are three beneficial consequences:

> First, status-quo powers can identify each other, thus laying the foundations for cooperation… Second, status-quo states will obtain advance warning when others plan aggression… Third, if all states support the status quo, an obvious arms control agreement between them is a ban on weapons that are useful for attacking. (Jervis, 1978, pp. 199–201)

Thus, in offense-defense differentiation, whether defensive weapons and policies can be distinguished from offensive ones is also important in measuring the intensity of the security dilemma.

According to the combination of the two variables, the intensity of the security dilemma can be divided into four worlds, as detailed in Table 4.3.

Table 4.3. Four Worlds

	Offense Has the Advantage	Defense Has the Advantage
Offensive Posture Not Distinguishable from Defensive One	*First World* - Doubly dangerous	*Second World* - Security Dilemma, but security requirements may be compatible
Offensive Posture Distinguishable from Defensive One	*Third World* - No security dilemma, but aggression possible - Status-quo states can follow different policy than aggressors - Warning given	*Fourth World* - Double stable

Source: Jervis, 1978, p. 211.

The first world is the situation in which the offense has an advantage over the defense and offensive posture is indistinguishable from a defensive one. This world is the worst scenario for states. A state can only increase its security with threatening others. On the other hand, it is hard to increase its security through defensive actions for a state (Jervis, 1978, p. 211). Arms races and military alliances are the best route to protection in the situation. These competing states are likely to be trapped in a vicious circle of escalating tension. Incentives to attack first will turn military tension between states into wars. The world will become unstable. Thus, this world can be explained as follows: the security dilemma is very intense; states are placed in a doubly dangerous situation; and states have a little chance to cooperate with others.

Jervis introduces one empirical case, which is close to the first world. The case is Europe before the First World War. During this period, European powers' decision-makers thought that the offense has the advantage over the defense and saw little difference between offensive and

defensive behaviors of others (Jervis, 1978, p. 212). Thus, the Triple Alliance and Triple Entente became enemies.

The second world is that offensive and defensive postures cannot be distinguished, but the defense has the advantage. Although the security dilemma operates under these conditions, it does not operate as strongly as in the first world (Jervis, 1978, p. 212). In other words, the dilemma in the second world is intense but not as intense as in the first one. In such a case, a state might be able to increase its security without threatening and endangering the security of others. Jervis (1978) says that "to assume that the apparently excessive level of arms indicates aggressiveness could therefore lead to a response that would deepen the dilemma and create needless conflict" (p. 212) in the world. However, he believed that empathy and skilled diplomacy could avert the dilemma (Jervis, 1978, p. 212). Moreover, the advantageous position of the defense means that a state can often maintain a high degree of security with a lower number of arms than that of its expected opponent (Jervis, 1978, p. 212).

The second world is common in history. Offensive operations are usually harder than defensive ones due to the strength of natural and artificial fortifications. However, holding purely defensive positions is difficult because the offensive capability also supplements fortifications (Jervis, 1978, p. 212). Under this condition, Jervis says that "a world of either ICBM (Intercontinental ballistic missile)'s or SLBM (Submarine-launched ballistic missile)'s in which both sides adopted the 'Schlesinger Doctrine' would probably fit in this category" (Jervis, 1978, p. 212).[90]

[90] The Schlesinger Doctrine was a major realignment of U.S. nuclear strike policy that was announced in January 1974 by the US Secretary of Defense, James Schlesinger. The doctrine emphasized the need for a greater range of nuclear capabilities in order to give a broader range of choices to the U.S. President (Baylis, 2005, p. 61).

The third case is the world where offensive and defensive behaviors are distinguishable, but the offense has an advantage over the defense. There may be no security dilemma, but there are security problems (Jervis, 1978, p. 213). The security dilemma is not intense, but security issues exist. The dilemma does not appear if states publicly obtain defensive weapons and equipment that do not decrease the security of others (Jervis, 1978, p. 213). However, aggression is still possible because the offense has the advantage over the defense. Even though the second world is safe, states are likely to encounter unwanted conflicts with others at some future time because offensive behavior has an advantage.

This third world is not likely to occur. Therefore, Jervis assumes that a hypothetical nuclear world would fit the third category. The assumed nuclear world would be one in which both sides relied on SLBM's, and in which anti-submarine warfare techniques were very active (Jervis, 1978, p. 213). This means that on the one hand, a state could show its lack of desire to attack the other by stopping from threatening its submarines if it did not feel threatened by the other. On the other hand, if it felt threatened by the other, it could strike the other first because the offense has the advantage.

The last world is the case where the offense and the defense are distinguishable and defensive behavior has the advantage over offensive one. States have no reason to strengthen offensive capabilities and states easily distinguish whether the actions of others are offensive or defensive (Jervis, 1978, p. 214). The security dilemma has very little or no intensity in the fourth world. This means that the situation is doubly safe.

Jervis provided one ideal case to explain the fourth world. He assumed that doubly safe world would have existed in the early 20th century if European powers' decision-makers had understood the intentions of another side and differentiated offensive activities from defensive

ones. In that case, establishing impregnable defense systems could guarantee the safety of France and Germany (Jervis, 1978, p. 214). Jervis concluded that "there would have been no competitive mobilization races reducing the time available for negotiations" in the assumed world (Jervis, 1978, p. 214).

4.3.3 *Theoretical and Methodological Debates*

Some scholars continue to raise questions about the utility of the offense-defense theory. The first question arises around the ambiguity of the definition of one of the two theory's major variables, the offense-defense balance (Lynn-Jones, 1995, p. 672). Jack S. Levy (1984) argues that the offense and the defense are distinct only by military technology and perhaps tactics that would affect the possibility of war, but not by national policies (p. 223). Thus, he defines the balance as the offensive/defensive balance of military technology. Moreover, the ambiguity of the offensive/defensive distinction is detailed "in terms of the defeat of enemy armed forces, territorial conquest, protection of population, tactical mobility, the characteristics of armaments, attack/defense ratios, the relative resources expended on the offense and the defense, and the incentive to strike first" (Levy, 1984, pp. 222–30). Glaser and Kaufmann (1998) claimed that the ambiguity results in inconsistent application and testing of the theory (p. 44).

Moreover, critics contend that the theory contains following inherent flaws as well: "offense-defense balance cannot be measured because the outcomes of wars are so uncertain"; "that ingenuity, not structural constraints, determine the balance; that state behavior is determined by perceptions, not the 'objective' offense-defense balance; and that offense and defense cannot be distinguished" (Glaser & Kaufmann, 1998, pp. 1, 16).

Despite this criticism, the theory is useful in assessing the intensity of the security dilemma between states in cyberspace. Contrary to those in the traditional space, two major variables of

offense-defense theory in the virtual space can be more clearly defined and measured due to the characteristics of anonymity and absences of boundaries in the new space. Thus, the following section links the security dilemma and behaviors of states in cyberspace. Then, it places the cybersecurity dilemma on one of the four worlds via Jervis' theory to emphasize the danger of cyber uncertainty between states.

4.4 Cyber Uncertainty and the Pinpointing Security Dilemmas

As a variant on the classic security dilemma, the cybersecurity dilemma can be defined as a situation where one state takes steps to secure itself in cyberspace, thereby inadvertently threatening other states' national security with what appears to be offensive action (Buchanan & Williams, 2018). Can this variant explain security tensions and conflicts between countries in cyberspace? In other words, does a country's increasing cybercapability or alliance formation unintentionally cause fear in other countries? Furthermore, can these efforts to improve national security cause changes in regional security dynamics? In order to answer the questions, this section will theorize the cybersecurity dilemma through two main components of the classic security dilemma, the cause and the reaction. The intensity of the cybersecurity dilemma is then analyzed with the offensive-defensive theory.

4.4.1 *The Conceptual Linchpin of the Cybersecurity Dilemma*

Two main causes of the security dilemma—structural and psychological problems—are also valid in understanding tensions between states in cyberspace. The characteristics of cyberspace make these causes valid. This artificial space is anonymous, anarchical, and borderless. No one individual or entity controls or regulates the virtual world. Cyberspace was invented based on the concept of anonymity and has continued to operate in the same vein. Every border between

actors in the space is ambiguous. These characteristics make the security dilemma useful in explaining states' uncertainty and fear of others in cyberspace; this can result in cyber arms races and military alliances. These vicious cycles of escalation between countries may also lead to unplanned conflicts in the virtual world.

Cyberspace is a new anarchical space for states. There is no higher entity to control and monitor security issues in the virtual world. Cyberspace governance is not the product of an institutional hierarchy, but rather comes from "the decentralized, bottom-up coordination of tens of thousands of mostly private-sector entities across the globe" (Masters, 2014). Moreover, cyberspace is not subject to international laws that mitigate international disputes between states. The anarchical cyberspace means that states are exposed to the uncertainty that is derived from a structural problem of cyberspace. It is likely that in the anarchical nature of cyberspace, countries increase their security by building their own cybercapability and forming cyber alliances with friendly countries, while simultaneously unintentionally threatening the security of others.

A psychological problem also animates the security dilemma in cyberspace. A state is frequently unable to understand how other states who do not know its intention will perceive its behavior in the space. The problem comes from the ambiguity of actors themselves and their behaviors and purposes. This makes it more difficult for a victim country to attribute a state-led cyberattack to a specific country.

The ambiguity of cyber actors themselves increases the cybersecurity dilemma between states. Cyberspace is designed to promote diverse activities of everyone ranging from individual users to state actors without revealing their real identity. Moreover, some actors who conduct malicious activities in cyberspace intentionally hide their identity to avoid being traced. State actors can also engage in this behavior. In this regard, the *Worldwide Threat Assessment* of the

U.S. Intelligence Community (2018) emphasized that state-sponsored cyberattacks threaten national security (p. 5). Then it is difficult to differentiate between national security threats and crimes in cyberspace. There are blurred borders between them. Cybercrimes in the private sector can influence national security. Thus, these two ambiguities make states fearful of unknown online activities led by unidentified actors. This ultimately leads to the cybersecurity dilemma.

The consequences of the cybersecurity dilemma are the same as that of the classic security dilemma. Security experts and policy decision-makers view cyberspace as the fifth domain of conflict between countries. Cyberspace can be employed by states to pursue their national interests and goals. In this regard, when states are unaware of the intentions of others' activities in cyberspace, they can become uncertain and fearful. This, in turn, leads states to ensure their survival by strengthening self-defense capabilities and forming military alliances for cybersecurity. In other words, these two responses to the cybersecurity dilemma are the same as those to classic security dilemma.

The first response of a state to the uncertainty in cyberspace is to increase its self-defense cybercapability. States make laws to allow the military to defend their virtual spaces and facilities within their sovereign territories. They also create cybersecurity budgets connected to national security. They also train cyberwarriors and increase troop numbers in preparation for cyberwarfare. For example, U.S. Cyber Command (USCYBERCOM) was established under U.S. Strategic Command (STRATCOM) in mid-2009. On May 4, 2018, USCYBERCOM became the DoD's 10th unified combatant command, which is at the same level as STRATCOM and other unified combatant commands (Lange, 2018). A four-star general is the leader of the military's cyberwarfare organization, USCYBERCOM. USCYBERCOM has roughly 6,200 personnel (USCYBERCOM Public Affairs, 2018). The commander also is in charge of the

nation's largest spy agency, the National Security Agency (NSA), which includes approximately 38,000 military and civilian personnel, as well as approximately 17,000 contractors (Nakashima, 2018).

The other major response of a state to the fear of others in cyberspace is to increase its national security through cyber military alliances and partnerships with other states. Cooperation between countries for cybersecurity is necessary because cyberspace is a borderless space. Cyber cooperation between states can be categorized in three ways.

First, two states can agree to cooperate with each other for cybersecurity. This is called bilateral cyber cooperation. The second is the multilateral cyber partnership. NATO is one good example for that. NATO said that cyber defense is part of its core task of providing collective defense (NATO, 2018). It pursues cyber cooperation based on its own classic collective defense strategy. Another example is Five Eyes, which is the world's leading intelligence-sharing network between Australia, Canada, New Zealand, the United Kingdom, and the United States. Cybersecurity is one of its main challenges (Dabbagh, 2017). Last, there are many meetings led by international organizations to strengthen cooperation between countries, private companies, and both. One example is the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE, n.d.). U.N. G.G.E. will be detailed in Section 4.5.2.

The two main causes of the classic security dilemma still hold true in cyberspace. A state's defensive steps to secure itself inadvertently threatens other states' national security with what appears to be offensive actions in anarchical cyberspace. Psychological factors also increase the cybersecurity dilemma. The ambiguity of actors themselves and actions and purposes in borderless cyberspace is likely to cause a state to misunderstand others' intentions. Finally, the

cybersecurity dilemma leads states to strengthen their self-defense capability and cooperation for cyber defense. The intensity of the cybersecurity dilemma will be tested with Jervis' offense-defense theory in the following section.

4.4.2 *An Application of the Offense-Defense Theory to the Cybersecurity Dilemma*

This section assesses whether states need to strengthen their self-defense capability and cooperation with others to ensure security for themselves in cyberspace. Jervis' offense-defense theory is useful to test the intensity of the cybersecurity dilemma for this purpose. The first half of the section discusses whether the offense has the advantage in cyberspace. The latter half examines whether defensive actions of states can be differentiated from offensive ones in the virtual world.

The first major variable, offense-defense balance, can be applied to cyberspace. From the perspective of a conventional military, defensive forces have the advantage over offensive ones in regular warfare. Defensive forces occupy an advantageous place by watching opponents and their maneuvers before these opponents arrive. Moreover, they can prepare for battle while also resting in the occupied location. This location, which has stable supply lines, is surrounded by artificial forts and/or natural obstacles.

In contrast, offensive forces are disadvantaged in a conventional war scenario. They must travel a great distance from their countries or central military camps. Therefore, they must maintain long supply lines to provide support. They must deploy their forces in a less-than-ideal location that is also monitored by defensive forces. Moreover, soldiers in the offensive forces do not have sufficient time for rest and preparation before battle. In this regard, Sun Tzu's *The Art of War* (2000) emphasized that "the rule is, not to besiege walled cities if it can possibly be avoided" (p. 8). He also added that "the preparation of mantlets, movable shelters, and various

implements of war [against walled cities], will take up three whole months; and the piling up of mounds over against the walls will take three months more" (Sun Tzu, 2000, p. 8). Thus, offenders pay more to prepare for war than defenders. According to Lanchester's laws of combat, offenders need more troops than defenders under the same set of conditions in modern warfare (Lepingwell, 1987).

However, this traditional military scenario is not applicable to cyberoperations. The offense clearly has the advantage over the defense in cyberoperations. There are three primary asymmetric reasons for this difference. First, offensive cyber actions are less expensive than defensive cyber ones. This is an asymmetric cost. Offensive operations are also easier to conduct than defensive ones in cyberspace due to the scope of what is to be defended: cyberspace. This is an is asymmetric scope. The last reason is that offensive cyberoperations (and operators) are exposed to relatively low risk, thus causing an asymmetric risk between offense and defense.

The first point is asymmetric cost. Defensive national cybersecurity operations require much more money than offensive operations. A state must train and hire many cybersecurity experts to defend critical IT infrastructure. These professionals are different than traditional military personnel trained in boot camps. States must establish new training centers and programs for cybersecurity experts. Moreover, the private sector is closely linked to national security. Thus, states must attend to private sector cybersecurity issues and cooperate with the private sector to ensure national security. These factors increase defensive costs and efforts, especially when compared to offensive operations

On the other hand, offensive cyberoperations cost much less than defensive cyber ones. Cyberattack offenders do not need to establish gigantic military training centers and camps to train cyberwarriors. They are not required to equip cyberwarriors with expensive weapons and

tools. Moreover, they do not need to transport troops to battle zones with vehicles, airplanes, or ships. Cyberwarriors need high-quality computers and IT infrastructure for their missions in the virtual world. States have the relatively easy task of hiding their cyber proxies to avoid being traced. Thus, offensive cyberoperations are understood as a low-cost, high-impact tool for achieving national interests of states (Lipton, Sanger, & Shane, 2016).

The second asymmetric issue is scale and scope. Traditionally, militaries defend their physical borders against adversaries. However, there are no clear borders between countries in cyberspace. IT devices, networks, and facilities are all connected to one another. The border between public and private sectors is blurred. Cyberattacks on the private sector can easily threaten a state's national security. Accordingly, a state must defend traditional security boundaries, such as borders and public sectors, as well as important private sectors and individuals in the case of cybersecurity. Cybersecurity experts from a state cannot defend against all of cyberspace. The space is infinite. In contrast to defensive operations, cyber offenders can choose one of many targets for their surprise attacks. Thus, a state is required to spend more on a cyber defensive strategy compared to offensive strategy. For example, in the case of the Sony Pictures Entertainment hack (2014), a private global company and their employees became a threat to U.S. national security (U.S. DoD, 2015a). This illustrates how the private sector or individual citizens are not separate from national security when it comes to cybersecurity.

The last point is asymmetric risk. State-led cyberattacks seem to be a cost-effective tool to protect national interests. Russian cyberoperations have threatened national security of other countries across the globe. The 2016 U.S. presidential election was threatened by the Russian government and its hackers. In the case of North Korea, its cyberattacks on global financial entities and cryptocurrency exchanges are understood as a way to avoid international economic

sanctions against its nuclear program. However, some states, including Russia and North Korea, have not faced actual punishment for their malicious activities, such as cyberattacks on critical infrastructure of other countries. This means that cyber offenders are at a relatively low risk of exposure compared to the benefits achieved by their cyberattacks. In this regard, countries across the globe are at risk of state-led cyberattacks under these conditions of asymmetric risk. Therefore, these three asymmetric factors lead to offense-dominated world, increasing the intensity of the cybersecurity dilemma.

The second major variable, offense-defense differentiation, is applicable to state-led cyberoperations. In traditional security studies, state actions and activities can be categorized generally as offensive or defensive. Developing, producing, and deploying fighters or tanks increases a state's offensive capability. An anti-ballistic missile defense system, such as the Terminal High Altitude Area Defense (THAAD), is clearly a defensive weapon designed to shoot down short- medium- and intermediate-range missiles. However, a state's intention is sometimes unclear. For example, reconnaissance aircraft can be used for both offensive and defensive purposes.

Despite these differences in conventional forms of defense and offense, the defense is entirely indistinguishable from the offense in cyberspace for three reasons. First, a state's increased cybercapability cannot be monitored. A state does not require a vast territory and resources to develop a cybercapability. Cybersecurity experts can develop a state's cybercapability and strategy in one small room. In addition, final outcomes are not tangible or physical. Cyber tools do not need to be physically moved for offensive and defensive operations. Therefore, other states have difficulty in monitoring a state's malicious offensive actions in

cyberspace. Thus, it is impossible to differentiate a state's offensive cyberactivities from its defensive ones.

Offense and defense are also indistinguishable in cyberspace because many cyber weapons are dual-use. Cyberwarriors generally use normal computers, IT devices, and IT infrastructure. These tools are the same as those of ordinary internet users. Sophisticated offensive cyberoperations require malicious software programs, hacking tools, or computer viruses. These malicious tools, however, are not categorized as military tools for war. Also, these offensive tools are not unveiled before their use in aggressive cyberoperations. Thus, it is challenging to distinguish an offensive cyber tool for a state-led cyberattack from other normal software programs. Furthermore, according to mission characteristics, state cyberwarriors are not always required to use special cyber weapons. In some cases, they use normal software programs to hack or to infiltrate their target networks and devices.

Finally, offense and defense are also indistinguishable in cyberspace because of two ambiguities regarding actors and the purpose of cyberattacks. First, cyberspace is an anonymous space. Therefore, it is difficult to identify state-sponsored hackers and cyberwarriors of military or intelligence agencies in cyberspace. Moreover, these hackers intentionally use many techniques, such as spoofing, VPNs, and fake IP addresses to hide their real identities and their connections to particular states. Second, in some cases, state-led cyberattacks are similar to malicious activities of cybercriminals and terrorists. For example, North Korea spread ransomware targeting financial entities and cryptocurrency exchanges in a similar way to cybercriminals with a focus on financial gain. Thus, it is likely that states can misunderstand the intentions of others and fail to differentiate offensive activities of states from malicious ones of

cybercriminals due to the ambiguity of actors' identities and purpose. In sum, offensive cyberspace activities are not distinguishable from defensive ones.

Table 4.4. The Intensity of the Cybersecurity Dilemma

	Offense Has the Advantage	Defense Has the Advantage
Offensive Posture Not Distinguishable from Defensive One	*First World* **** Cybersecurity Dilemma*** - Security Dilemma: Doubly dangerous	*Second World* - Security Dilemma, but security requirements may be compatible
Offensive Posture Distinguishable from Defensive One	*Third World* - No security dilemma, but aggression possible - Status-quo states can follow different policy than aggressors - Warning given	*Fourth World* - Double stable

Source: Jervis, 1978, p. 211.

As shown in Table 4.4, the cybersecurity dilemma belongs to the first world of offense-defense theory, which is doubly dangerous for states. In cyberspace, the offense has the advantage over the defense. To make matters worse from the defense's perspective, an offensive posture is indistinguishable from defensive posture. Thus, states are likely to be fearful of the uncertain activities of others in cyberspace. Moreover, this fear drives them to increase their own defensive cybercapability. However, this increase in defense can paradoxically threaten others, resulting in the security dilemma in cyberspace. The following four sections offer empirical evidence from the Korean Peninsula to illustrate this cybersecurity dilemma. Furthermore, the cybersecurity dilemma on the Peninsula displays emerging regional (and even Northeast Asian) security dynamics in the information age.

4.4.3 *North Korea's Cybercapability Development and the Interlocking Cybersecurity Dilemma*

North Korea's cybercapability development increases opponent states' uncertainty, thereby creating a cyberspace security dilemma. Two of Jervis'(1978) "offense-defense theory" variables can be applied to North Korea's cybercapability. First, North Korea clearly has the offensive cyberoperations' advantage in the "offense-defense balance." The state's cyberspace is limited in the sense that it is disconnected with the outside world. Ordinary North Koreans cannot access the internet for private purposes. They are only allowed to use its closed intranet service, Kwangmyong. Therefore, North Korea's IT infrastructure is relatively protected from cyberattacks by other countries, private hackers, or cybercriminals. This limited vulnerability means that North Korea does not need to develop a cyber defensive strategy and programs which require massive financial and human capital investments.

Under these conditions, North Korea can focus its limited resources on developing cyberwarriors, cyber strategy, and techniques for offensive operations in cyberspace. Moreover, North Korea's offensive cyberoperations are not under any international sanctions. North Korea and its cyberwarriors are not in danger in any way. In other words, the state has enjoyed asymmetric benefits in cost, efforts, and risks in cyberspace with the goal of achieving regime survival. The North Korean regime has the offense advantage in cyberspace.

The second variable is "offense-defense differentiation." North Korea is one of the most closed and secretive nations on earth. It is hard to know precisely what the state is doing within its territory. These characteristics are combined with cyberspace, which is anarchical, anonymous, and unobserved. Moreover, hardware devices and software programs are dual-use goods, used for civilian purposes but which may also have military application. Finally, the link between cyberwarriors and the state is unclear.

In such a unique situation, North Korea's offensive and defensive activities become virtually indistinguishable from one another. North Korea officially promotes its economy through information technologies and highly educated IT human capital (Cuthbertson, 2018). However, their IT products are also dual-use. It is therefore unknown whether the state is developing IT products only for its national economy. In reality, however, North Korea's private IT sectors do not have the capacity to employ the number of IT professionals trained by state-led, intensive education programs for gifted computer students. It is therefore unclear how the state uses its surplus IT human resources. North Korea's civil computer experts can always conduct offensive cyberoperations on behalf of the state with a simple command. Therefore, North Korea's actions, cybercapability, use of its IT human capital and technologies remain unobservable. In other words, North Korea's offensive posture is not distinguishable from its defensive one. In summary, the cyber uncertainty that North Korea creates is placed in Type 1 in offense-defense theory. It is doubly dangerous: (1) offense has the advantage and (2) an offensive posture is not distinguishable from a defensive one.

North Korea has created a security dilemma on the Korean Peninsula with its arms buildup for its regime survival. Since the end of the Cold War, it has begun to develop nuclear weapons, threatening the region and even the world. The security dilemma is still valid in cyberspace as North Korea increases its cybercapability which is viewed with uncertainty by other countries. The following section discusses how the cybersecurity dilemma works on and near the Korean Peninsula through the presentation of empirical data. Two of the three in the following section are the unintended defensive consequences of South Korea in response to perceived threats generated by North Korea's cybercapability development. The last one of the three is to illustrate

the expansion of the cybersecurity dilemma to the Northeast Asia region in the course of strengthening defensive cybercapability and forming cyber alliances of South Korea.

4.5 Presentation of Evidence from the Korean Peninsula

North Korea's increased cybercapability creates uncertainty and fear on the Korean Peninsula. According to "offense-defense theory," North Korean malicious cyberactivities make other countries in and near the region, especially South Korea, feel threatened. North Korea's cyber offense has the advantage, and its offensive posture is not distinguishable from a defensive one. Thus, the dangerous situation leads South Korea to increase its cyber self-defense capability and strengthen its military partnerships with other countries. It is a cybersecurity dilemma between the two Koreas. This cybersecurity dilemma is transferred to the entire Northeast Asia region as South Korea strengthens its defensive cybercapability and forms cyber alliances. This section presents evidence of the cybersecurity dilemma from the Korean Peninsula.

4.5.1 *South Korea's First Response: An Increase in Self-Defense Capability*

South Korea's development of defensive cybercapability is the product of uncertainty generated by North Korea's cyberspace activities. According to "offense-defense theory," the South Korean government feels threatened by North Korea's uncertain cyberactivities. Beginning in the late 2000s when Pyongyang's creation of cyber uncertainty began to threaten Seoul, South Korea's military began to build its defensive cybercapability. First, since 2008, South Korea's biannual *Defense White Paper* included North Korea's cybercapability as one of the threats to its national security (ROK MND, 2008). Second, South Korean established the ROK Cyber Command in 2010 (Sang-Hun Lee, 2011). Third, it augmented budgets to increase its defensive cybercapability. Fourth, it has made an effort to develop human capital for

defensive cyberwarfare. Fifth, in 2015, the Blue House, the executive office and official residence of the President of South Korea, hired a senior cyberwarfare expert as a secretary to the President. Sixth, the military started to cooperate with other governmental organizations and private sectors in South Korea to defend cyberspace. Lastly, the military encouraged patriotic hackers to join its efforts for national security. These seven empirical facts illustrate how the South Korean military develops its defensive cybercapability in response to the North Korean-created security dilemma.

The first fact concerns South Korea's Ministry of National Defense's (ROK MND) specifications that cyberattacks were a threat to national security. For the first time in December 2008, the ROK MND's *Defense White Paper* said that "The most notable changes in the security environment today is the rise of complicated and multifarious transnational and non-military threats besides conventional military threats. Threats such as terrorism, the proliferation of WMDs, cyberattack, etc. have become universal, encompassing wide areas" (ROK MND, 2008, p. 10). The statement reflects South Korea's military intentions to engage in serious military issues that would threaten its national security in cyberspace. In other words, the ROK MND started to categorize cyberspace as a new domain for military operations.

In addition, the 2008 *Defense White Paper* warned that North Korea was likely to carry out cyberattacks on South Korea's critical infrastructure that would harm national security. It stated that "North Korea is reinforcing the capability to execute modern [cyber] warfare. This is evidenced by the construction of a command automation system and by the cultivation of computer hackers for cyber warfare" (ROK MND, 2008, p. 27). The report was issued approximately seven months before North Korea conducted its first massive and complicated DDoS attacks on critical websites of the United States and South Korea. Since the 2008 Paper,

South Korea's *Defense White Papers* have emphasized that (1) North Korea has many professional cyberwarriors working in entities that are similar in size to the U.S. Cyber Command and (2) these cyberwarriors have threatened national security. Above all, repeated statements about North Korea's cyber threats have played an essential role in the development of South Korea's defensive cybercapability.

North Korea's uncertainty in cyberspace has also accelerated the establishment of the ROK Cyber Command. Seven months after the ROK MND's 2008 *Defense White Paper*, several important websites of the U.S. and South Korean governments were shut down by North Korea's DDoS attacks in July 2009 (Choe & Markoff, 2009). The attacks accelerated an ongoing national discussion about the establishment of a military command responsible for cyberwar. After these discussions, the ROK Cyber Command was created in January 2010 (Sang-Hun Lee, 2011).

The South Korean government failed to make progress in forming a military cybersecurity command before the DDoS attacks. Since the early 2000s, cybersecurity experts in South Korea have argued that the South Korean government must establish a new entity to defend critical infrastructure, such as the Blue House and MND, against state-led cyberattacks (Gwi-Geun Kim, 2004, 2006; Young-Tae Park, 2004). Despite this need, the government did not have specific plans to build a military command until 2009. In June 2009, the ROK MND released a revised 'the Defense Reform 2020' that includes a plan to establish 'Cyber Defense Command' by 2012 (ROK MND, 2009). That was only one tangible blueprint for creating a ROK Cyber Command until then. However, the ROK MND just left it at tentative.

Moreover, this plan to establish a Cyber Defense Command was criticized. A non-governmental organization argued that it was an attempt to increase the size of the South Korean military based on virtual threats in cyberspace, which are not plausible (Jeong-Wan Kim, 2009).

The group also said that the attempt to establish a new command does not meet the direction of the Defense Reform, which tries to downsize the South Korean military overall (Jeong-Wan Kim, 2009). They viewed this as an attempt at offensive action against others (Jeong-Wan Kim, 2009). Nevertheless, the ROK MND pressed ahead with its plan to form a new military cyber entity due to potential cyber threats to national security.

Although the plan was challenged, the ROK military succeeded in establishing its Cyber Command in January, 2010 (Sang-Hun Lee, 2011). The ROK MND proposed its plan to form a new command for cyberwar immediately following the July 2009 DDoS attacks. Then, the pre-announcement of the revised bill of 'Defense Intelligence Agency Directive' for the command was released during the period from December 8 to 10, 2009 (Jeong-Wan Kim, 2009). The revised bill was a useful strategy to avoid the delay that would be required by the creation of a new bill. According to Article 5 of the Presidential Decrees, titled "General Principles about Defense Organizations and Size," the Minister of National Defense can form a new organization and provide a mission to the newly established command under the control of the existing entity. Thus, the ROK MND chose to establish the Cyber Command as a new branch of the National Defense Intelligence Command as it revised "Defense Intelligence Agency Directive."

Since January 2010, the ROK Cyber Command under the National Defense Intelligence Command has operated its missions in cyberspace with around 500 personnel, including military officers, non-commissioned officers, enlisted soldiers, and civilian workers in the military. A brigadier general was commissioned as the commander. The ROK MND followed this with a new President Decree 26101, "National Defense Cyber Command Directive," to allow the Cyber Command to be promoted in status from under the control of the National Defense Intelligence Command to under direct command of the ROK MND (ROK MND, 2017). It also led to the

promotion of the cyber commander from brigadier general to major general. The South Korean government planned to double the size of the Cyber Command. However, as of 2017, it is believed that the Command has only approximately 600 personnel for defensive cybermissions against North Korea and others (Ki-Noh Sung, 2017).

Third, the change in the defensive cyberoperations budget ROK military provides clear evidence of the cyberarms buildup. The cyberoperations budget is not available to the public. Despite this, budgetary change can be indirectly observed through the Budget for Defense Information Security, which is a part of the National Defense Informatization Budget[91] (Da-In Oh, 2018c). The Budget for Defense Information Security consists of sub-budgets for network security, software security, hardware security, counter-cyberoperations, security management, and crypto equipment. This budget is also used to train defensive cyberoperations personnel (Da-In Oh, 2018c). It is an unclassified part of the entire ROK Cyber Command budget.

Since the July 2009 DDoS attacks, the ROK MND has steadily increased the ROK Cyber Command's defensive cyberoperations budget. As shown in Table 4.5, the Budget for Defense Information Security has grown within the National Defense Informatization Budget, which has been fixed at approximately $500 million U.S. dollars. In response to the July 2009 DDoS attacks, the ROK military appropriated 23.2 million dollars for defensive cyberoperations in 2010. In 2014, the budget was drastically cut back because it was suspected that some members of the Cyber Command engaged in the opinion-rigging scandal for the 18th President Park Geun-hye and the ruling party (Soo-Ho Lee, 2016). In 2019, the military doubled the Budget for Defense Information Security from 23.2 to 55.6 million dollars.

[91] The National Defense Informatization Budget includes several sub-budgets for constructing ICT infrastructure, operating ICT infrastructure and devices, telecommunication and internet fees, broadband convergence networks, and defense information security.

Table 4.5. ROK National Defense Budgets for Informatization and Information Security

*1,128.29 KRW = 1 USD (As of Feb. 18, 2019)

	Military Expenditure		Budget for Informatization		Budget for Information Security	
	USD at Constant 2019 Prices (KRW)	Share of GDP	USD at Constant 2019 Prices (KRW)	Share of Military Expenditure	USD at Constant 2019 Prices (KRW)	Share of Budget for Informatization
2019	41.4 billion (46.7 trillion)	2.51 %	445.6 million (502.7 billion)	1.08 %	49.3 million (55.6 billion)	11.06 %
2018	38.3 billion (43.2 trillion)	2.38 %	400.6 million (451.9 billion)	1.05 %	35.2 million (39.7 billion)	8.79 %
2017	35.7 billion (40.3 trillion)	2.33 %	418.2 million (471.7 billion)	1.17 %	33.6 million (37.9 billion)	8.03 %
2016	34.4 billion (38.8 trillion)	2.37 %	465.8 million (525.3 billion)	1.35 %	million (41.9 billion)	7.98 %
2015	33.2 billion (37.5 trillion)	2.39 %	482.2 million (543.8 billion)	1.45 %	37.1 million (38.3 billion)	7.04 %
2014	31.65 billion (35.7 trillion)	2.4 %	457.8 million (516.5 billion)	1.45 %	21.9 million (24.7 billion)	4.78 %
2013	30.4 billion (34.3 trillion)	2.4 %	449.4 million (507.0 billion)	1.48 %	29.6 million (33.4 billion)	6.59 %
2012	29.3 billion (33.0 trillion)	2.39 %	443.7 million (500.6 billion)	1.52 %	22.9 million (25.8 billion)	5.15 %
2011	27.8 billion (31.4 trillion)	2.36 %	419.0 million (472.7 billion)	1.51 %	21.1 million (23.8 billion)	5.03 %
2010	26.24 billion (29.6 trillion)	2.34 %	381.1 million (430.0 billion)	1.45 %	23.2 million (26.2 billion)	6.09 %
2009	25.3 billion (28.5 trillion)	2.48 %	366.4 million (413.4 billion)	1.45 %	5. 8 million (6.54 billion)	1.58 %
2008	23.6 billion (26.6 trillion)	2.41 %	380.3 million (429.0 billion)	1.61 %	N/A	N/A

Source: ROK National Defense Committee Budget Report, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018; Fiscal Year 2019 ROK MND Budget Proposal, 2018;ROK MND Personnel Operating Budget Division, The Change in ROK Defense Budget, 2019; Ho, 2011; Soo-Yeon Ko, 2012; Kyeong-min Lee, 2009; Soo-Ho Lee, 2016; ROK MND, In 2012, Defense Informatization Budget Will Be Increased, 2011; Hye-Kwon Shin, 2013, 2015; Sae-Rom Yang, 2016.

The 2019 Budget for Defense Information Security increased sharply by 39%. The 2018 Budget was 39.7 million dollars. The budget's share of the total Budget for Informatization[92] increased from 8.79% in 2018 to 11.06% in 2019, as detailed in Table 4.5. According to the ROK MND, the Budget for Defense Information Security increased rapidly for following several

[92] South Korea's military expenditures is 40.5 billion USD in 2018 and 42.0 billion USD in 2019.

reasons. The Cyber Command increased personnel expenses for civilian workers in the military from 14.2 million dollars in 2018 to 20.5 million dollars in 2019 (Da-In Oh, 2018b). It was understood that the Command would hire highly professional civilian cybersecurity personnel with an increased budget. The Cyber Command will also use 12.1 million dollars to strengthen its cybercapability (Da-In Oh, 2018b). The construction of a cyberoperations command system and surveillance reconnaissance operations system accounts for 1.4 million dollars (Da-In Oh, 2018b). Upgrading the cyber defense operations system and building cyber offense and defense training centers accounts for 1.1 and 8.8 million dollars (ROK MND, 2018d). The Cyber Command emphasized that it will invest a large portion of its budget to construction a cyberbattlefield simulation training center (ROK MND, 2018d). Therefore, this increase in the Budget for Defense Information Security indicates that the South Korean government is attempting to build sufficient defensive cybercapability against North Korea's cyber threats as it feels threatened by North Korea-led cyberattacks.

Fourth, the ROK MND strives to develop cyberwarriors for the Cyber Command. It is challenging to hire skilled cybersecurity experts from existing military schools, boot camps, or private IT sectors. First, existing military schools and boot-camp systems are designed to train military professionals only for traditional security purposes. Second, employment at military organizations is not an attractive prospect for civilian cybersecurity experts. The salary of military personnel is lower than IT employees working in the private sector. It is generally believed that military personnel work in much poorer conditions. For example, military personnel are required to work 8 am to 5 pm; they have little flexibility in scheduling their working hours. This led the ROK MND to build a new program to develop cybersecurity professionals with the goal of creating state-led defensive cyberoperations.

The Department of Cyber Defense is a new program to train undergraduates to become cyberwarriors; this program addresses a shortage of IT professionals who can work at Cyber Command. In June 2011, the ROK MND made an agreement with Korea University at Seoul to train cybersecurity experts (Korean University Admissions Office, 2012, p. 204). The Department of Cyber Defense was designed to cultivate cybersecurity experts from all computer science fields. The ROK MND provides financial support to the department through the Budget for Defense Information Security.

Since its inception in 2012, 30 students are accepted by this department every year (Min-Hyung Lee, 2011). The department turned out the first cohort in 2016. Four-year, full-tuition scholarships are awarded to all students admitted to the program (Chun, 2013). They each receive an additional 500-dollar monthly stipend (Min-Hyung Lee, 2011). More importantly, graduates from the Department of Cyber Defense are required to serve seven years as military officers at the Cyber Command (Korea University Department of Cyber Defense, 2018). As all South Korean young men have to serve as enlisted soldiers for approximately 18 months, this requirement of 7 years of service is not as onerous as it might appear. The students also have opportunities to pursue M.A. or Ph.D. degrees during their military service at the Graduate School of Information Security, Korea University (So-Yeob Kim, 2011). Therefore, the admission rate for the Department of Cyber Defense is the second highest after that for the Medical School in Korea University, which is one of the top private colleges in South Korea (Won-Sang Lee, 2017). The new program has benefits for both students and the government: (1) gifted computer students have access to a high-quality education system without financial burdens, and (2) the Cyber Command has access to a sufficient pool of well-trained cybersecurity.

Fifth, the Blue House of the President of South Korea hired a senior cyberwarfare expert as a secretary to the President in March 2015 (Joo-Hyung Lee, 2015). The Cybersecurity Secretary in the National Security Office to the president has a mission of advising the president about small and large-scale cyberattacks; cybercrimes; and cyber incidents that threaten public and private sectors. Above all, the secretary was given the task of coordinating the work of several governmental organizations, military, spy agencies, police, public services, for cybersecurity (Yoo-Ji Lee, 2015). It was considered that the cooperation between the listed entities against cyber-related issues has long been insufficient.

The creation of the position of the Cybersecurity Secretary, along with their mission, indicates that the South Korean government understands how cyber threats can harm national security. The secretary belongs to the National Security Office, which is in charge of national security. Most members of this office come from the military, spy agencies, and diplomatic services (Byung-Chul Won, 2018). The office aims to bridge the gap between the president and national security- and diplomatic-related agencies.

A total of three cyber experts have been assigned to work with the Cybersecurity Secretary. Two were from ROK Cyber Command. They served as army generals before. The other expert arrived from South Korea's spy agency, the National Intelligence Service (NIS). He was the director of a bureau for science and technology. These experts' backgrounds indicate that this new position is designed to increase military-centered national security against cyberattacks. In 2018, the government changed the title from the Cybersecurity Secretary to the Cyber Information Secretary (Byung-Chul Won, 2018). This change caused controversy because of fears that it undermined the state's defensive cybercapability (Chun-Sik Park, 2018). However, the government said the Cyber Information Secretary would be responsible for data and

information management in cyberspace, in addition to maintaining the previous mission of the Cybersecurity Secretary (Byung-Chul Won, 2018).

In January 2015, another mode to bolster cybersecurity was made when South Korean President Park Geun-Hye appointed civilian cybersecurity expert, Lim Jong In, as the Special Advisor in Security to the President (Se-Ah Min, 2015). This was a remarkable event because traditional security experts from the military, NIS, or the Ministry of Foreign Affairs had been chosen for the Special Security Advisor to the President in the past. After receiving his Ph.D. in cryptology, Dr. Lim became a professor in the Division of Information Security & Graduate School of Information Security at Korea University. He was the president of the Korea Institute of Information Security and Cryptology, chairperson of the Advisory Committee for Digital Forensic Science in Supreme Public Prosecutors' Office, and the Chief of the Financial Security Technical Committee. His appointment was criticized because Dr. Lim's expertise was limited to cyber-related issues, though national security includes conventional security issues as well (Oi-Hyun Kim, 2015). He was in office for a short time: 13 months, from January 2015 to March 2016. Nevertheless, this was a meaningful appointment in that state decision-makers acknowledged the need for cybersecurity under the general umbrella of national security.

Sixth, the ROK military cooperates with public and private sectors in the state in pursuit of its defensive goals in cyberspace. According to the National Emergency Management Basic Guidance (Presidential Decree 342), the National Cybersecurity Policy Coordination Meeting controls and manages all matters connected with cybersecurity-related issues and trends (Tae-Kyu Kim, 2018; The Office for Government Policy Coordination, 2016b). More specifically, the National Security Office in the Blue House leads a meeting for cooperation between private and public sectors, including the military. The meeting was held in December 2016 when North

Korea's cyber threats—such as the South Military Intranet hack, hacks of military contractors, and the spread of spear phishing emails—were on the rise (The Office for Government Policy Coordination, 2016b). At this meeting, the head of the National Security Office asked 14 participant governmental organizations to minimize the anxiety of citizens about cybersecurity as they made an unified counter-action system between governments and organizations against North Korea's cyberattacks (The Office for Government Policy Coordination, 2016a). The meeting was attended by 13 governmental organizations, such as the MND, the National Police Agency, Supreme Public Prosecutors' Office, and other governments. The head of the National Security Office conducted the meeting to discuss the best methods and strategies to secure cyberspace in response to the North Korea-related cyberattacks (Kyung-Ae Kim, 2018). The participants pledged to work closely on making cyberspace safe by sharing information about threats with other participants (Kyung-Ae Kim, 2018).

The National Cybersecurity Policy Coordination Meeting is significant. Since 2005, the South Korean NIS has held the National Cybersecurity Strategy Meeting according to the National Cyber Security Management Regulation (ROK NIS, 2013). Participants are the same as those at the National Cybersecurity Policy Coordination Meeting (ROK NIS, 2013). However, NIS's Meeting has been led by the head of the NIS who focuses heavily on intelligence missions. Moreover, the National Cyber Security Management Regulation does not state that cyberattacks, cybersecurity, and cyber threats are a part of cyberwar (ROK NIS, 2013). This indicates that it is likely that the meeting includes analysis of North Korea's cyber-threat issues with NIS' interests and purposes. It is also possible that the ROK military cannot play a leading role in defending cyberspace under the command and control of the NIS. Therefore, the National Cybersecurity Policy Coordination Meeting, led by the head of the National Security Office, is a more

comprehensive way than the NIS's meeting to deal with North Korea's cyber threats. The National Security Office can act in cooperation with various governmental organizations of the state without being biased toward the NIS.

In addition to these changes, the ROK MND seeks to organize cyber-reserve forces in order to cooperate with public and private sectors. The military has accepted the importance of cybersecurity experts (Kyung-Tak Lee, 2018). On condition of anonymity, a scholar on cybersecurity emphasized that "it is important to employ civilian IT human capital in response to multiple simultaneous cyber threats happening in a variety of places across the country" (Kyung-Tak Lee, 2018). Military facilities, government agencies, and critical national infrastructure are no longer the only cyberattack targets. This is a reason the military is interested in establishing cyber-reserve forces. For example, in the case of the United States, its military announced the plan to establish cyber-reserve forces in October 2012 (Kyung-Tak Lee, 2018). Moreover, the Japanese government decided to outsource some of cyber-defense missions to private security companies (Kyung-Tak Lee, 2018). At the same time, the Japanese government considered making a short-term program to enlist civilian cybersecurity experts in the Japanese Self-Defense Forces (Kyung-Tak Lee, 2018).

The ROK MND began to discuss organizing cyber-reserve forces in depth with the Ministry of Science, ICT, & Future Planning in a working group meeting on October 26, 2016. This was a project plan to create new reserve forces, consisting of dischargees who worked at the ROK Cyber Command, the Army/Navy/Air Force CERT (Computer Emergency Response Team), and other cyber-related divisions or bureaus in the ROK MND and the National Police Agency. According to the plan, members of reserve forces will be supposed attend cyberwarfare training centers for mandatory reserve duty training (Gwi-Geun Kim, 2016). While they are working as

civilians during peacetime (Kyung-Tak Lee, 2018), they can be mobilized to conduct cyberoperations just in case of an emergency, such as the outbreak of war (Gwi-Geun Kim, 2016).

In order to achieve the project plan under discussion, the two Ministries divided their missions into two parts. First, the ROK MND planned to evaluate the possibility and effectiveness of cyber-reserve forces, review existing laws, and determine the necessity of new laws. Second, the Ministry of Science, ICT, & Future Planning planned to consider ways to establish cyberwarfare training centers and to develop education programs (Gwi-Geun Kim, 2016). However, the establishment of these reserve forces has been delayed. Nevertheless, the project plan has been still discussed (Kyung-Tak Lee, 2018). Furthermore, the ROK MND strives to make programs to train their human cybersecurity capital in cooperation with the Ministry of Science, ICT, & Future Planning. The military and private IT companies will work together to apply new information technologies from private sectors to cybersecurity defense (Tae-Jin Kim, 2017).

Last but not least, the ROK MND has strived to cultivate and encourage patriotic hackers to join its national security efforts in cyberspace. Firstly, the ROK military has held several different levels of hacking competitions not only to attract public attention to the importance of cybersecurity but also to cultivate talented cybersecurity experts. The "White Hat Contest" has been held by the ROK MND, Cyber Command, and NIS every year since 2013. It is one of the top four hacking competitions[93] in South Korea. More interestingly, the military differentiates its contest from other hacking competitions as questions of the contest cover military tactics and

[93]The top four hacking competitions in South Korea are 'Secuinside' sponsored by a private white hackers union, HARU; 'Codegate' by a private cybersecurity company, Softforum; Hacking Defense Contest (HDCON) by Korea Internet & Security Agency (KISA); and the White Hat Contest.

North Korea's hacking trends, along with other normal hacking-related questions (Jong-Tack Oh, 2018). In 2018, the title of the contest was changed to 'National Defense Cybersecurity Contest' to emphasize the importance of national cybersecurity (Jong-Tack Oh, 2018).

In addition to the White Hat Contest, all three armed forces of South Korea have hacking competitions. The army has the Army Hacking Defense Contest for military personnel as well as civilian cybersecurity experts and students (Seong-Uk Park, 2016). The Navy has the Navy Hacking Defense Contest only for naval officers and sailors (Choi, 2018). The two contests have been held by the headquarters of the two armed forces since the July 2009 DDoS attacks of North Korea (Chang, 2016; Choi, 2018; Seong-Uk Park, 2016). The ROK Air Force has also held the Contest for Air Force Cyber Warrior only for air force personnel since 2015 (Chang, 2016). The military spy agency, the Defense Security Command, has a hacking contest for all military personnel with the help of KISA (Korea Internet & Security Agency) (Kyung-Ae Kim, 2013).

Secondly, the ROK MND holds several cybersecurity academic conferences. For example, approximately 500 cybersecurity experts from civil and public sectors participated in the 2018 military-sponsored Cybersecurity Conference, titled "National Cyber Threats and the Role of the Military" (Tae-Young Noh, 2018). There were several significant papers, including "Recent Trends on Attacks of Enemy Hacker Groups," by ESTsecurity; "Cyber Threats and Cyber Kill Chain," by the National Security Research Institute; "Cyber Self-Defense Technology," by the Electronics and Telecommunications Research Institute; and "Recent Trends on Cyber Weapon System and Technology," by the National Defense and Science Institute (Tae-Young Noh, 2018). The ROK MND has also sponsored private sector-led academic associations, such as the Korea Information Assurance Society and their conferences. This demonstrates there is an effort

to use public sector theories, technologies, and experiences in pursuit of national cybersecurity defense against state-led cyberattacks, especially North Korea's cyber threats.

These seven efforts of the South Korean military illustrate that the military has pursued the cyber arms buildup against the uncertainty originating from the development of North Korea's cybercapability. South Korea's cyber arms buildup began in the late 2000s when North Korea conducted massive, complicated DDoS attacks on several critical websites of the United States and South Korea. The buildup is one of the two primary responses to uncertainty under the cybersecurity dilemma. The other consequence of the cybersecurity dilemma—alliance formation—will be discussed in the next section.

4.5.2 *South Korea's Second Response: The Increase in Military Partnerships*

In building cyber defense against North Korea's creation of cyber uncertainty, the South Korean military has attempted to increase its national security by strengthening existing partnerships and forming new relationships with other countries, along with increasing its self-defense capability discussed in the previous section. Thus, this section provides empirical evidence about the South Korean military's efforts to increase its defensive cybercapability in cooperation with other countries or international organizations. During the Cold War era, the Korean Peninsula was a place of confrontation between the Western and Eastern blocs. The Western bloc (maritime powers) consisted of the United States, Japan, and South Korea. The Eastern bloc (continental powers) included China, the Soviet Union, and North Korea. The consequence of the conflict between the two groups has been the division of the Korean Peninsula since the end of World War II. Despite the end of the Cold War, the confrontation has continued on the Peninsula. Paradoxically, the tension between the two sides has moved to cyberspace as North Korea develops its cybercapability. In other words, the cybersecurity

dilemma North Korea created on the peninsula has been transferred to the entire Northeast region where the two Cold War powers face each other. South Korea's cyber-alliance formation efforts can be divided into three types: a bilateral military alliance, partnerships between maritime powers, and multilateral cooperation.

Bilateral Cyber Military Alliance between South Korea and the United States

The longstanding U.S.-South Korea alliance has been a bulwark against communist expansion in the Northeast Asia region for the last seven decades. The Mutual Defense Treaty between the United States and the ROK signed on October 1, 1953, two months after the signing of the Korean Armistice Agreement,[94] serves as the backbone of the military alliance. The treaty has allowed the United States to station military forces in South Korea in consultation with the South Korean government. In practice, the two nations established the ROK-U.S. Combined Forces Command in 1978. Since then, the militaries of the two nations have held several meetings and held combined military exercises to increase allied forces' capabilities; this has also served as a communication method against potential traditional military threats in the region.

Since the increase North Korean-generated cyber uncertainty beginning in the early 2010s, the bilateral alliance included cyber issues as one of the collaborative defense missions. The 2011 Joint Communique of the 43rd U.S. ROK Security Consultative Meeting (SCM)[95] was the first official signal of cyber defense cooperation between the two countries. The SCM is the

[94] The Korean Armistice Agreement brought a halt to the fighting in the Korean War (June 25, 1950–July 27, 1953).
[95] The SCM meeting is usually held just after the MCM meeting. Two chairs of the joint chiefs of staff of South Korea and the U.S. have a discussion about common practical security issues. The South Korean Minister of National Defense and U.S. Secretary of Defense issue the common communique based on the discussion of the two chairs.

annual regular military talk between the U.S. Secretary of Defense and the ROK Minister of National Defense on behalf of the presidents of the two countries.

The 2011 Joint Communique affirmed the need for the two governments to strengthen cooperation concerning the protection of cyberspace (ROK MND, 2012, p. 382). The military heads of the two countries agreed to establish a bilateral strategic policy dialogue on cybersecurity issues to discuss new ways for the ROK and the United States to confront the challenges posed by increasing threats in cyberspace (ROK MND, 2012, p. 382). The 2012 Joint Communique of the 44th SCM announced the launch of the "U.S.-ROK Cyber Policy Consultations" as a "whole-of-government" approach, mainly led by the U.S. Department of State and the ROK Ministry of Foreign Affairs (ROK MND, 2012, p. 386). Moreover, in taking note of the second ROK-U.S. Cyber Policy Consultations held in Washington D.C. in July 2013, the defense heads of the two nations welcomed the signing of the terms of reference for the "Cyber Cooperation Working Group" (CCWG) on September 5, 2013 (ROK MND, 2014a, p. 288). The Cyber Cooperation Working Group purely focuses on military issues with the following sentence: "[the Group] endeavors to strengthen cooperation in information sharing, cyberpolicy, strategy, doctrine, personnel, and exercises to improve their collective readiness against various cyber threats" (ROK MND, 2014a, p. 288). However, this cyber cooperation has not fully materialized. For example, the sentence of the 2014 Joint Communique of the 46th SCM over the Cyber Cooperation Working Group is the same as that of the 2013 Joint Communique.

Since the 2014 Sony hack, the ROK Ministry of National Defense and the U.S. Secretary of Department State have deepened their cybersecurity defense discussions during the SCM meeting. In the 2015 Joint Communique of the 47th SCM, the two officials emphasized that

CCWG manages the alliance's joint cyber trainings, exercises, and enhanced cyber military education (ROK MND, 2016, p. 294). In the 2016 Joint Communique of the 48th SCM, both countries decided "to create a ROK-U.S. Cyber Task Force to study how the Republic of Korea and the United States can better synchronize and enhance their combined cooperation in cyberspace within the alliance construct" through regular bilateral engagements of the CCWG (ROK MND, 2016, p. 298). Moreover, the communique stated that both countries are also committed to advancing ROK-U.S. cooperation in science and technology to identify new and innovative means of countering the North Korean threat (ROK MND, 2016, p. 298). Finally, in 2018, both countries agreed to reorganize their respective cyber command through active information sharing (United States Forces Korea, p. 2018). This allowed the two countries to promote cybersecurity cooperation that would strengthen alliance cyber capabilities as the scope and scale of mutual cybersecurity threats increased (United States Forces Korea, p. 2018).

In addition, strengthening cybersecurity cooperation was also one of the essential agendas in the U.S. and ROK summit meeting. There were at least four significant moments between presidents of the two countries about cybersecurity defense. On May 7, 2013, Park Geun-Hye and Barack Obama stated that both countries would strengthen their efforts to promote cybersecurity in the Joint Declaration in Commemoration of the 60th Anniversary of the Alliance between the Republic of Korea and the United States of America (Office of the Press Secretary, 2013). This is significant because it was the first official statement of two countries' presidents about cybersecurity. In April 2014, according to the *Joint Fact Sheet: The United States-Republic of Korea Alliance: A Global Partnership*, the summit meeting between two countries affirmed their commitment to pursue "a common vision of an open, interoperable, secure, and reliable cyberspace that cyberspace" through increased cooperation between their

computer security incident response teams as well as their militaries (Gyu-Ryun Kim, 2014, pp. 50–51).

In the second visit of President Park Geun-Hye to the United States in October 2015, presidents of both countries mapped out a specific cooperation plan for cybersecurity. The *Joint Fact Sheet* stated that both countries decided to create "a White House-Blue House cyber coordination channel to further strengthen and complement the deep and broad bilateral cyber cooperation that already exists" (Office of the Press Secretary, 2015b). Their cooperation would include:

> (1) enhancing information sharing on cyber threats, particularly to critical infrastructure; (2) strengthening collaboration on investigation on cyber incidents; (3) deepening military-to-military cyber cooperation; and (4) encouraging collaboration on cybersecurity research and development, education and workforce development, and cooperation on technology between cybersecurity industries. (Office of the Press Secretary, 2015b)

Like the partnership between former Presidents Park and Obama, Moon Jae-In and Donald Trump have also emphasized the importance of cyber cooperation between both countries. In the joint statement between Moon and Trump on June 30, 2017, both countries committed to strengthening cooperation to fight against "North Korea's dangerous and destabilizing malicious cyberactivities" (The White House, 2017b). This indicates a recognition of North Korea as their common enemy in cyberspace, along with traditional military domains.

The aforementioned high-level cyber cooperation talks were followed by working group meetings between South Korea and the United States. There were three important cyber working group meetings: the U.S.-ROK Cyber Policy Consultations, the Korea-U.S. Integrated Defense Dialogue, and the Cyber Cooperation Working Group. The first is the U.S.-ROK Cyber Policy

Consultations, which was mentioned in the 43rd SCM in 2011 for the first time (ROK MND, 2012). The consultations are a "whole-of-government" cybersecurity approach mainly led by the U.S. Department of State and the ROK Ministry of Foreign Affairs (ROK MND, 2012). The consultations meetings were held in September 2012 (first), July 2013 (second), August 2014 (third), June 2016 (fourth), and June 2018 (fifth). The fifth consultations in 2018 included the Departments of State, Commerce, and Defense, as well as the FBI (Office of the Spokesperson, 2018a; ROK Ministry of Foreign Affairs, 2018). The Deputy Assistant Secretary for Cyber and International Communications and Information Policy was the head of the U.S. delegation. The chief delegate of South Korea was the Ambassador for International Security. The ROK participants included the Ministries of Foreign Affairs, Defense, and Science and ICT; the Supreme Public Prosecutors' Office; the Korea Internet & Security Agency; and the National Police Agency (ROK Ministry of Foreign Affairs, 2018).

Since the first meeting in 2012, the U.S.-ROK Cyber Policy Consultations have included several discussions of cybersecurity issues, including the protection of national internet and communications networks; building confidence in cyberspace; countermeasures against cybercrimes; and North Korea's cyber terror. The 2012 participants chose to focus on countermeasures against North Korea's cyber terror as the major agenda item. In 2016, before the fourth meeting, South Korea's Ministry of Foreign Affairs clarified that the ROK and the United States have shared information about major cyberattacks and cyber threats, including the 2014 Sony hack and the Cyberattack on Korea Hydro and Nuclear Power (Hyo-Jeong Kim, 2016). Although the official announcement of the fifth meeting (2018) did not attribute several cyberattacks to North Korea, the agendas of the meeting—the WannaCry ransomware attack and hackings on cryptocurrency exchanges—showed that their main topic was North Korea's cyber

threats. Thus, these agendas of the U.S.-ROK Cyber Policy Consultations illustrate that state-level cyber threats are not only connected to defense areas, but also related to private and other public fields.

The second cyber working group meeting is the Korea-U.S. Integrated Defense Dialogue (KIDD). The KIDD is a semiannual working group meeting between the ROK Ministry of Defense and the U.S. Department of Defense. The KIDD has been led by the ROK Deputy Minister for Defense Policy and the U.S. Principal Deputy Assistant Secretary of Defense for Asian & Pacific Security Affairs. It was established by the 43rd SCM in 2011 to strengthen cooperation between working groups for every field in defense (ROK MND, 2012, pp. 380–381). In other words, the dialogue was designed to manage every national defense-related working group meetings between two countries.

Cybersecurity has been regarded as one of the important agendas of KIDD since its inception. In 2011, the ROK Deputy Minister for Defense Policy said that two countries have a plan to strengthen cooperation in cyberspace because cyberspace became a conflict domain between countries (Choi, 2012). During the sixth KIDD in September 2014, both countries blamed North Korea for conducting repeated cyber psychological warfare and cyber provocations (ROK MND, 2014c). Since then, the U.S. and ROK militaries have affirmed they will enhance their defensive cooperation against North Korea's aggressive cyberoperations as well as pervasive cyber threats across the globe (U.S. DoD, 2015b, 2018a, 2018b, 2018c). The annual SCM has adopted these KIDD agreements. Thus, KIDD is a more military-focused working group meeting than the U.S.-ROK Cyber Policy Consultations.

The third cyber working group meeting is the U.S.- ROK Cyber Cooperation Working Group (CCWG). CCWG was designed to discuss mainly national defense focused cybersecurity

issues, unlike the previous two working group meetings. Although the U.S.-ROK Cyber Policy Consultations thematically focuses on cyber issues only, it was led by the Ministry of Foreign Affairs in cooperation with other public areas. The Korea-U.S. Integrated Defense Dialogue was led by the military, but cybersecurity is one of the many national defense related agendas. Thus, CCWG is understood as a working group meeting that focuses on military-related cyber issues only.

Since its first meeting in February 2014, the CCWG—only designed for cybersecurity issues in defense—has been led by high-ranking military officers or defense department officials of the United States and South Korea (ROK MND, 2014b). In September 2013, both sides established that the CCWG would be held two times per a year, beginning in 2014 (Jin, 2017, p. 9; ROK MND 2014a, pp. 57–58). The first, second, and third CCWGs were held in February 2014, February 2015, and October 2015 (ROK MND, 2014b; ROK MND, 2015). The high-ranking officials of both countries shared practical ideas and ways to strengthen their cooperation for cybersecurity in the field of defense (ROK MND 2014a, pp. 57–58). A report of a member of the ROK National Assembly said that in 2015, the U.S. and ROK militaries made a new practical rule about information sharing for cyber threats (Jin, 2017, p. 9). However, since then, the two militaries have not announced what they did during the CCWG. Despite that, the 2016 Joint Communique of the 48th SCM and the 2017 Joint Communique of the 49th SCM stated that CCWG has played a critical role in enhancing cooperation for cyber issues (ROK MND, 2016, 2018). Thus, it is believed that although details about agendas of CCWG remain unannounced, CCWG is the most practical of the other working groups between the United States and South Korea for national defense cyber cooperation.

The U.S. and ROK militaries also have joint military exercises for defensive cyberwarfare. One day prior to the first CCWG held on February 7, 2014, the South Korean government announced that the U.S. Armed Forces in Korea and ROK Joint Chiefs of Staff had conducted a Table Top Exercise (TTX) against potential cyberattack scenarios on February 6, 2014 (ROK MND, 2014b). Using the TTX, they attempted to ascertain their weaknesses as well as practical agenda items for CCWG (ROK MND, 2014b). They had two more TTX in July and October in 2015 (ROK MND, 2015). During this exercise, they discussed countermeasures of the U.S. and ROK military alliance against cyberattacks on nuclear power plants and combined and Joint Command, Control, Communications, Computers and Intelligence (C4I) systems (ROK MND, 2014b). These two TTXs were held before the 2015 CCWG as well. These joint military exercises indicate that the bilateral U.S. and ROK alliance has engaged in practical cooperation for their defensive cybersecurity. Moreover, it is believed that cyber working groups between the U.S. and ROK militaries have discussed practical ways and methods to secure common interests in cyberspace based on the result of TTX (ROK MND, 2014b).

Triangle Cyber Partnerships between South Korea, Japan, and the United States

North Korea's cyber uncertainty has led to the increase in defensive cooperation between South Korea, Japan, and the United States. The historical antagonism between South Korea and Japan has hindered the two countries from agreeing to establish a direct military alliance for the last several centuries. Without a sincere apology by Japan for its invasion of Korea and exploitation of Koreans, the two countries cannot make progress toward a direct military partnership. However, both countries have indirectly cooperated with each other against various military threats in Northeast Asia under the auspices of the United States. North Korea's cyber uncertainty is one of the main concerns between these three countries in the information age.

The U.S. government has strengthened its military partnership with the Japanese government to deter North Korea's cyber provocations. The U.S. DoD emphasizes its relationships with Japan and the Republic of Korea against North Korea cyber threats, which is one of the top four cyber threats from China, Russia, Iran, and North Korea (Joint Chiefs of Staff, 2015; U.S. DoD, 2011, p. 7). The 2016 U.S. President's Cybersecurity National Action Plan also stated that the U.S. government would take action to deter and disrupt malicious activity in cyberspace in concert with its allies and partners around the world (Office of the Press Secretary, 2016).

In this regard, the United States-Japan Cyber Dialogue has been held since 2013. According to the official statement of the sixth KIDD on July 26, 2018, the United States and Japan share "a common commitment to ensure an open, interoperable, reliable, and secure cyberspace and confront emerging cyber challenges" (Office of the Spokesperson, 2018b). In addition, the two countries have cooperated with each other for cybersecurity, including the establishment of cyber working group meetings, joint cyber military exercises, shared cybersecurity technologies, and exchange programs for cyber experts (Sangbae Kim, 2017, p. 132; Gi-Lim Shin, 2015).

In April 2015, the U.S. and Japanese governments also updated their guidelines for Japan-U.S. defense cooperation. According to remarks by President Obama and Prime Minister Abe of Japan at a joint press conference after the summit, they planned to expand their cooperation to cyber threats and those in space (Office of the Press Secretary, 2015a). The Guideline for Japan-U.S. Defense Cooperation includes Chapter VI, "Space and Cyberspace Cooperation." Section B of Chapter VI specifies that "the two governments will share information on threats and vulnerabilities in cyberspace in a timely and routine manner, as appropriate" (Japan Ministry of Defense, 2015). Moreover, the section B also said that two government agreed to consult closely

and take proper actions to respond together when Japan is under serious cyberattacks that threaten Japanese national security (Japan Ministry of Defense, 2015).

The bilateral cooperation for cybersecurity between the U.S. and Japanese governments is also linked to the effort of the ROK-U.S. bilateral alliance to deter North Korea's cyber threats. On January 5, 2017, Deputy Secretary of the U.S. State Department, Deputy Ministers of the ROK, and Japanese Ministries of Foreign Affairs reaffirmed the importance of the meeting between their cyberpolicy experts held on December 19, 2016, along with that of their cooperation in response to North Korea's nuclear threat (Office of the Spokesperson of U.S. State Department, 2017). In the 2016 meeting, U.S.-ROK-Japan cybersecurity experts "consulted trilaterally in Washington, D.C. regarding the cybersecurity of critical infrastructure, including a discussion of cyber trends and threats to critical infrastructure as well as a scenario-based discussion on responding to malicious cyber activities" (Ministry of Foreign Affairs of Japan, 2016; U.S. Embassy in Korea, 2016). Many government cyber experts in the field from the three countries participated in the meeting (Ministry of Foreign Affairs of Japan, 2016; U.S. Embassy in Korea, 2016). In June 2017, presidents of the United States and South Korea emphasized their alliance to promote United States-ROK-Japan trilateral cooperation. Moreover, President Trump and President Moon affirmed that trilateral security and defense cooperation contributes to enhanced deterrence and defense against the DPRK threat, including cyber threats (The White House, 2017b).

On July 27, 2018, the U.S. government hosted a trilateral meeting of cyber experts with South Korea and Japan on cybersecurity in Washington, D.C. The three countries committed to promoting an open, interoperable, reliable, and secure cyberspace (Office of the Spokesperson, 2018c). They also reaffirmed their commitment "to advancing trilateral cooperation to enhance

international cyber stability, deter malicious activities in cyberspace, and counter cyber threats, including from state actors" (Office of the Spokesperson, 2018c). At the end of its official announcement about the trilateral working group meeting, the U.S. Department of State underlined that "the meeting builds on President Trump's, Prime Minister Abe's, and President Moon's commitment to enhancing cyber cooperation" (Office of the Spokesperson, 2018c). This indicates that despite the historical antagonism between South Korea and Japan, the U.S.-ROK-Japan relationship has made defensive efforts to enhance cooperation in response to North Korea's creation of cyber uncertainty.

Multilateral Security and Cooperation

The South Korean government strives to increase its national security for cybersecurity through multilateral security and cooperation. South Korea's multilateral security and cooperation can be divided into three activities for cyber defense (Yoo & Lee, 2013, pp. 2–5). The first is to participate in international organizations or meetings that make international laws and norms to regulate malicious activities in cyberspace. The second is that the South Korean government and its military have played a leading role in international conferences or working group meetings for cybersecurity against state-associated malicious activities in cyberspace. The last is that they have joined combined defensive cyber exercises with militaries of other countries.

In terms of the first activity, the South Korean government has actively participated in international organizations or meetings to make international laws and norms to regulate malicious activities in cyberspace. The best example is the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). The issue of information security has been on the UN agenda

since Russia first introduced a draft resolution in the First Committee of the UN General Assembly in 1998 (UNODA, n.d.). The UN GGE and its six working groups were established in 2004 to study emerging threats in information security and create international norms for responsible state behavior in cyberspace (Maurer & Taylor, 2018; "UN GGE," n.d.). Government officials of 25 participant countries from around the world are members of UN GGE (Ji-hye Yoo, 2014).

Since 2004, there have been five UN GGEs: the first UN GGE (2004–2005), the second (2009–2010), the third (2012–2013), the fourth (2014–2015), and the fifth (2016–2017) ("UN GGE," n.d.). South Korea participated in four UN GGEs, except for the third ("UN GGE," n.d.). The UN GGE contributed to cyber cooperation among countries with two major achievements: "outlining the global cybersecurity agenda, and introducing the principle that international law applies to the digital space" ("UN GGE," n.d.). However, In June 2017, the fifth UN GGE ended without a consensus about its efforts to advance international norms for responsible state behavior in cyberspace (Maurer & Taylor, 2018). Nevertheless, it is significant since it shows that many leading countries around the globe are working hard together to solve a variety of cybersecurity issues. Moreover, the South Korean military regards UN GGE as important. It is planning to create rules of cyber engagement based on the result of UN GGE at the end of 2018 (Gwi-Geun Kim, 2018).

The South Korean government and its military have also played a leading role in international conferences or working group meetings to increase national cybersecurity against state-associated malicious activities in cyberspace. The MND of South Korea founded an annual multinational security dialogue meeting, "Seoul Defense Dialogue" (SDD), for high-level talks to enhance military confidence building and the security environment of the Asia Pacific region.

The first SDD ("Cooperation for Security & Peace") was held on November 14, 2012. Since then, the vice minister-level and other senior defense officials; security advisers in the region; and some international organizations have participated in SDD (E. Kim, 2012). At the seventh SDD in 2018, there were many senior defense officials and security advisers from 48 countries, including European and Middle East countries, as well as representatives from four international organizations (ROK MND, 2018b).

Establishing a cyber working group within the SSD was proposed at the first 2012 SDD, where 15 countries and two international organizations attended.[96] The Cyber Working Group has been held since the third SDD in 2014. The Cyber Working Group in SDD was designed to discuss countermeasures against cyber threats that its members face. Thus, it is believed that the working group led by the South Korean military can be viewed as a way South Korea is attempting to bolster national cybersecurity through exchanges and cooperation for secure cyberspace between its member countries (Jin, 2017, p. 9).

The Cyber Working Group of the SDD is growing over time. In 2015, approximately 60 senior officials and cybersecurity experts from 20 countries participated in the second Cyber Working Group (M. Park, 2018; ROK MND, 2018c). At the fifth Cyber Working Group, there were around 100 senior officials and cybersecurity experts from 31 countries and two international organizations (M. Park, 2018; ROK MND, 2018c). Moreover, their themes are critical in terms of military participation. For example, participants of the fifth Group meeting had a panel discussion about three main themes: the "Role of the Military in Cybersecurity,"

[96] Participants of the first SDD were the United States, Japan, China, Russia, Canada, New Zealand, Australia, Indonesia, Singapore, Vietnam, Thailand, Philippines, Malaysia, India, and two international organizations (the EU and NATO).

"Focus Areas to Advance Cyber Capability," and an introduction section for cybersecurity policies of some countries (ROK MND, 2018b).

In addition to the South Korean military-led Cyber Working Group of the SDD, the South Korean government has actively participated in multilateral security meetings for cybersecurity hosted by other countries or organizations. The second is the Global Conference on Cyberspace (GCCS), which was created by the United Kingdom in 2011 to discuss cyber issues in depth. It was an annual meeting in the beginning. Moreover, South Korea was the host country for the third GCCS in 2013 (ROK Ministry of Foreign Affairs, 2013). There were around 1,600 attendees from 87 countries and 18 international organizations. The most significant outcome of the third GCCS is "the Seoul Framework for and Commitment to Open and Secure Cyberspace, which highlights the importance of universal internet access, emphasizes that the same rights that people have offline must also be protected online" (Association for Progressive Communications, 2015). The Seoul Framework reaffirmed the conclusion of the 2011 London conference that existing norms and international law apply to cyberwarfare and that states should ban non-state actors from launching cyberattacks from their sovereign territory (Mazanec, 2015, p. 253). Since the third Seoul conference, GCCS has been held once every two years. In 2017, the fifth GCCS conference was held from 23 to 24 November 2017 in New Delhi, India (Internet Society, n.d.).

Third, there were two more prominent examples of South Korea's leading role in cooperating with other countries with the goal of increasing national security in cyberspace. The South Korean government played a crucial role in adopting the Seoul Communique, which emphasizes the importance of cybersecurity in protecting nuclear facilities and sensitive

information about them, in the 2nd 2012 Seoul Nuclear Security Summit[97] (Office of the Press Secretary, 2012; The 2012 Seoul Nuclear Security Summit, 2012). The South Korean government also seeks to cooperate with the EU on cybersecurity through the "Framework Agreement between the EU and the Republic of Korea."[98] Article 37 of this framework, titled "Combating Cyber Crime," affirmed South Korea and the EU's commitment to enhance "cooperation to prevent and combat high technology, cyber and electronic crimes and the distribution of terrorist content via the internet through exchanging information and practical experiences in compliance with their national legislation within the limits of their responsibility" (Delegation of the EU to the ROK, 2016). Article 37 also added that "[they] will exchange information in the fields of the education and training of cybercrime investigators, the investigation of cybercrime, and digital forensic science" (Delegation of the EU to the ROK, 2016). These statements demonstrate that North Korea's cyber threats are not limited to Northeast Asia. Moreover, it also illustrates that in order to prevent North Korea's cyber threats and spread of uncertainty, South Korea should strengthen cooperation with other entities and countries around the world.

Last but not least, South Korea has joined combined cyber exercises with the military of other countries for defensive cyberoperations. There are three key examples. The first is the Cyber Defense Exercise Locked Shields led by The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Locked Shields is not a Capture The Flag (CTF) exercise, but an annual military cyber defense exercise held since 2012 (Da-In Oh, 2018b). Attendees of Locked

[97] The Nuclear Security Summit (NSS) is a biannual world summit, aimed at preventing nuclear terrorism as one of the greatest threats to international security. The first summit was held in Washington D.C. on April 12–13, 2010.
[98] The new 2010 framework agreement between the EU and South Korea was titled the "Framework Agreement between the EU and the Republic of Korea" based on their previous agreements.

Shields are from cyber experts from the military as well as civil sectors from NATO's member countries.

The National Security Research Institute of the Republic of Korea participated in the 2018 Cyber Defense Exercise Locked Shields (CCDCOE, 2018).[99] South Korea is the first Asian country to attend Locked Shields of the NATO CCDCOE (CCDCOE, 2018). The Institute also signed an MOU with CCDCOE to supply training equipment for Locked Shields (Da-In Oh, 2018a). In the 2018 Locked Shields exercise, approximately 1,000 cyber experts from 30 countries participated (Ranger, 2018). The attendees were divided into several different teams (Calatayud, 2017; Ranger, 2018). The Blue Team played the role of Berylia's Rapid Cyber-reaction Team. Berylia was a small fictional country for the Locked Shields exercise. The Red Team was the in-game malignant hackers who attacked Berylia. The White Team was responsible for overseeing the exercise, and the Yellow Team was tasked with situation awareness. The Green Team was in charge of the physical and online infrastructure of Locked Shields. According to the fictional game scenario, Berylia's Rapid Cyber-reaction Team—the Blue Team—played the role of handling large-scale, coordinated cyberattacks from the Red Team, which caused severe disruptions to the electric power grid, 4G public safety networks, drone operations, and other critical infrastructure components of Berylia (Ranger, 2018).

The second example is the Multinational Experimentation (MNE) led by the U.S. military and NATO. MNE was designed in 2001 to prepare countermeasures against diverse current and future military threats. The MNE series chose military experimental topics and published handbooks, manuals, and guidebooks through seminars, workshops, and the development of

[99] Locked Shields 2018 was organised by CCDCOE in cooperation with the Estonian Defence Forces, the Finnish Defence Forces, the Swedish Defence University, the British Joint Army, the United States European Command, CERT.LV, National Security Research Institute of the Republic of Korea and Tallinn University of Technology (CCDCOE, 2018).

response models. The South Korean military began to attend MNE in 2006. Furthermore, senior military officers and cybersecurity experts from ROK Joint Chiefs of Staff and Cyber Command participated in the Multinational Experimentation 7 (MNE7) campaign (2011–2012), which focused on cyber threats (MNE, 2012, 2013). The MNE series were replaced by The Multinational Capability Development Campaign (MCDC) series after the conclusion of MNE7. The activities of the MCDC series is closed to the public.

The last example is an annual Cyber Drill of The Asia Pacific Computer Emergency Response Team (APCERT). The military does not lead the APCERT Cyber Drill. However, it is essential to improve cooperation, response, and information sharing among Computer Security Incident Response Teams (CSIRTs) in the region in response to malicious activities in cyberspace. The Korea Internet & Security Agency (KISA), which works closely with the South Korean military, has actively participated in the Cyber Drill since its inception. As of 2018, 27 CSIRTs from 20 countries—Australia, Bangladesh, Brunei Darussalam, the People's Republic of China, Chinese Taipei, Hong Kong, India, Indonesia, Japan, Korea, Lao People's Democratic Republic, Macao, Malaysia, Mongolia, Myanmar, New Zealand, Singapore, Sri Lanka, Thailand, and Vietnam—participated in the drill, titled “Data Breach via Malware on IoT” (Hong Kong-CERT, 2018).

The South Korean military tries to increase its national security by strengthening existing partnerships and forming new relationships with other countries in cyber defense against North Korea’s creation of cyber uncertainty, along with increasing self-defense capability discussed in the previous section. Thus, this section provides empirical evidence about the South Korean military’s efforts to increase its defensive cybercapability in cooperation with other countries or international organizations. The Korean Peninsula in the Northeast Asia region was a

confrontation place between the Western and Eastern blocs during the Cold War era. The Western bloc maritime powers consisted of the United States, Japan, and South Korea. The Eastern bloc continental powers included China, the Soviet Union, and North Korea. The consequence of the conflict between the two groups has been the division of the Korean Peninsula since the end of World War II. Despite the end of the Cold War, the tensions still run high on the Peninsula. Paradoxically, the tension between the two sides has transferred to cyberspace as North Korea develops its cybercapability. In other words, the cybersecurity dilemma North Korea made on the peninsula has been transferred to the entire Northeast region, where the two powers face each other. South Korea's efforts to create cyber alliances or partnership formations can be divided into three categories: the bilateral military alliance with the United States, partnerships between three maritime powers in Northeast Asia, and multilateral cooperation around the globe.

In addition to its first response, increasing cyber self-defense capability, South Korea's second response to North Korea's creation of cyber uncertainty has been to strengthen existing military partnerships with traditional allies and to form new cooperation with other countries or international organizations around the globe. However, South Korea's two defensive efforts against North Korea's creation of cyber uncertainty have paradoxically generated another cybersecurity dilemma from the continental bloc in the region, consisting of North Korea, China, and Russia. Thus, another cybersecurity dilemma resulting from new cyber partnerships between three continental powers will be discussed in the following section.

4.5.3 *The Expansion of the Cybersecurity Dilemma to Northeast Asia*

Cyberspace is a new place for cooperation between North Korea, China, and Russia. China and Russia have threatened U.S. national security in cyberspace (Coats, 2018, 2019).[100] The 2015 Sino-Russian Cybersecurity Agreement marked further cooperation between them in cyberspace (The Russian Government, 2015). The framework of the agreement was largely borrowed from their previous agreement under the Shanghai Cooperation Organization,[101] emphasizing mutual assurance on non-aggression in cyberspace, but added novel language protecting internal sovereignty in cyberspace (Margolin, 2016; Roth, 2015). The agreement challenges U.S. dominance in the international system as well as cyberspace, which puts emphasis on internet freedom under the guise of cyber sovereignty. The disparity between the United States and Sino-Russian cooperation resulted in the failure to agree on a consensus in its efforts to advance international norms for responsible state behavior in cyberspace in the 2016/2017 UN GGE (Grigsby, 2018). Furthermore, China and Russia have allowed North Korea to conduct malicious activities in cyberspace. It is known that the Chinese government is dissatisfied with the strengthening of defensive cooperation between South Korea, the United States, Japan, and other Western-centric countries and organizations against North Korea's creation of cyber uncertainty. The development of North Korea's cybercapability with the help

[100] China arguably has conducted cyber espionage operations on public and private sectors of the United States. For example, it is believed that China has developed its science and technologies based on its cyber espionage operations. The Russian government was also accused of hacking the U.S. Democratic National Committee.
[101] The creation of Shanghai Cooperation Organisation (SCO), a Eurasian political, economic, and security alliance, was announced on June 15, 2001 in Shanghai, China by the leaders of China, Russia, Kyrgyzstan, Kazakhstan, Tajikistan, and Uzbekistan. It includes 8 member states, 4 observer states, 6 dialogue partners, and 4 guest attendances. Eight member states are the aforementioned six countries and India and Pakistan. Four observer states are Afghanistan, Belarus, Iran, and Mongolia. Six dialogue partners are Turkey, Armenia, Azerbaijan, Cambodia, Nepal, Sri Lanka. Then, 4 guest attendances are ASEAN, CIS (the Commonwealth of Independent States), Turkmenistan, and the United Nations. For more information about SCO, see, http://eng.sectsco.org.

of China and Russia leads to the expansion of the cybersecurity dilemma to the Northeast Asia region where traditional maritime and continental powers have been in conflict.

China's Continuous Support for North Korea's Malicious Activities in Cyberspace

China has played a vital role in connecting an isolated country, North Korea, with the outside world. China has been recognized as the main gateway to North Korea. This relationship remains constant and relevant, even in the information age. China has helped North Korea develop its cybercapability, resulting in North Korea's generation of uncertainty in cyberspace.

North Korea has sent its gifted computer students to China for higher education (Sam Kim, 2018). Chinese IT companies have provided materials, resources, and technologies for North Korea to build ICT infrastructure for the internet, intranet, and wireless communications (Taylor, 2017). In addition, experts on North Korean IT have said that North Korea produces IT products, including computers, cellular phones, and Tablet PCs with imported critical parts from China (Jong Sun Kim & Choon-Geun Lee, 2014, p. 19; Yonho Kim, 2014; Williams, 2013).

North Korean hackers can conduct aggressive cyberoperations via China and its IT infrastructure. Since 2010, China Unicom has provided an internet connection to North Korea (Madory, 2017). The Chinese company was the only internet-service provider for Pyongyang prior to mid-2017 when a major Russian telecommunications company appeared to have begun providing an satellite internet access to North Korea (Williams, 2017). Despite several rounds of economic sanctions on North Korea due to its tests of nuclear weapons and missiles, North Korea and its hackers are still able to access the internet via China Unicom.

North Korea has its own and borrowed IP addresses that enable it to participate in diverse activities in cyberspace. The state has used these IP addresses for its online propaganda activities as well as hostile cyberoperations which increase the cybersecurity dilemma. As of 2019, North

Korea has its one block of 1,024 IPv4 addresses, running from 175.45.176.0 to 175.45.179.255 (Asia-Pacific Network Information Centre, n.d.-b). The block of 1,024 IP addresses was registered to Star Joint Venture in 2010, a company with links to the government in Pyongyang (Williams, 2010).

However, these resources are still insufficient for North Korea to conduct its cyberoperations. According to Asia-Pacific Network Information Centre (APNIC), the North Korean regime has borrowed IP addresses owned by other entities. China Unicom owns one of the prominent IP address blocks that North Korea has borrowed. The block contains 256 IP addresses and runs from 210.52.109.0 to 210.52.109.255 (Asia-Pacific Network Information Centre, n.d.-a). According to the *Criminal Complaint Against Park Jin Hyok* (2018) written by the FBI, North Korean hackers used some IP addresses of the two blocks for their malicious activities in cyberspace, including the 2014 Sony hack. This indicates that North Korean hackers have carried out aggressive cyberactivities via a Chinese internet service provider and its IP addresses. Moreover, the Chinese government indirectly allows Pyongyang to conduct malicious cyberactivities through its IT infrastructure.

In addition to the issue of Chinese IP addresses, many North Korean hackers and IT experts are working in China in order to conduct their malicious activities. The FBI revealed that North Korean front companies in China are bases for Pyongyang's cyberattacks against the outside world (Shields, 2018). Hackers living in China can use the superior IT infrastructure to conduct their online operations. North Korean hackers also develop and sell malicious software programs, such as hacking tools, in China (D.-U. Kim, 2013). In other words, state-sponsored hackers commit cybercrimes in a similar way to other crimes. For example, four South Korean and one Chinese criminal hacked some online gaming sites, collaborated with North Korean

hackers who work at Chosun Rungrado Trading Company (조선릉라도무역총회사 in Korean) under the control of North Korea's spy agency's Unit 39 after they graduated from Kim Il Sung University (Associated Press, 2011).

Despite North Korea's malicious cyber activities via its IT infrastructure and within its sovereign territory, the Chinese government has not cooperated with the South Korean government in regulating North Korean hackers under its direct influence. South Korean enforcement agencies announced that North Korean hackers used to reside in some Chinese cities closed to North Korea and to conduct cyberattacks through Chinese IP addresses (Gi-Hong On, 2014). However, the Chinese government has not allowed South Korean agencies to investigate the origins of North Korean cyberoperations (Han-Sol Kim, 2015). The FBI also pointed out that North Korean front companies and their employees (North Korean hackers), carried out malicious activities in cyberspace, such as the 2014 Sony hack, while inside Chinese territory (Shields, 2018). Thus, it seems that North Korean hackers and their illegal online activities have been protected by the Chinese government, whether intentionally or otherwise.

China is reluctant to see an increase in South Korea's defensive cybercapability in cooperation with other countries, especially the United States. In the early 2010s, the U.S. government asked its traditional allies, including South Korea, Japan, and Australia, to strengthen cooperation for cybersecurity (Ho-Cheol Sung, 2015). However, it is estimated that at that time, the South Korean government hesitated to join the cyber cooperation with its allies (primarily the United States) due to the relationship with China. In 2015, a South Korean official said that its government could not respond to the offer of the U.S. government to make a new alliance model for cybersecurity properly because it was concerned about China's potential

strong opposition to the new partnership between the United States and South Korea in the Northeast Asia region (Ho-Cheol Sung, 2015).

This South Korean official also added that this cyber alliance issue was the same as the deployment of the United States' THAAD weapon system in the territory of South Korea (Ho-Cheol Sung, 2015). China claimed that the long-range THAAD X-band radar could monitor North Korea as well as the northern part of China (Swaine, 2017). The Chinese Minister of Foreign Affairs Wang Yi said that "[the monitoring scope of its X-Band radar] will reach deep into the hinterland of Asia, which will not only directly damage China's strategic security interests, but also do harm to the security interests of other countries in this region" (PRC Ministry of Foreign Affairs, 2016). The Chinese government then imposed unofficial political and economic sanctions against South Korea to force it to abandon cooperation with the United States for the deployment of THAAD in South Korea. Thus, it is believed that close cooperation between South Korea and the United States for cyber defense against North Korea's production of cyber uncertainty can paradoxically threaten China's national security, resulting in the cybersecurity dilemma in the region between traditional Western and Eastern blocs.

North Korea's Reunion with Russia in Cyberspace

The North Korean regime also cooperates closely with the Russian government in the information age. Russia is also one of the three main gateways to enter North Korea. North Korea shares a border with three countries: China, Russia, and South Korea. Russia's border with North Korea is shorter than the other two. It is just 11 miles, following the Tumen River and its estuary in the far northeast (Taylor, 2018). Despite this short border, North Korea and Russia have been both important to each other for the last 70 years: Russia has contributed to the establishment and survival of North Korea since the 1940s (Suk Ryul Yu, 1987, Zhebin, 1995).

North Korea has been recognized as the outpost for the expansion of communism in Northeast Asia (Suk Ryul Yu, 1987, p. 76). Their cooperation remains important in the information age.

North Korea relied on the Soviet Union to develop science and technology for its survival. Since its establishment in the late 1940s, North Korea had accepted Russia's advanced science and technology developments. The Soviet Union's electronic calculator technology, which is the basis of ITs, was transferred to North Korea after the Korean War (Bo-Mi Kim, 2013; Kim & Lee, 2001, pp. 27, 39; Lee & Hwang, 2004, p. 77). The Soviet Union sent its scientists to North Korea to develop science and technology since the end of World War II (Kang, 2007, pp. 46, 64–66; Kim & Lee, 2001). At the same time, North Korean scientists who studied in the Soviet Union also returned to their home country and led to the development of basic science and technology (Kang, 2007, pp. 84–85, 92–95; Kim & Lee, 2001, pp. 68, 128). Thus, the Soviet Union's scientists and North Koreans who studied in the Soviet Union played a crucial role in the advancement of electronic engineering as the foundation of IT-related science and technology (Kang, 2007, pp. 328–329).

North Korea started to focus on the development of cybercapability after witnessing the Soviet Union's emphasis on the importance of ITs in the 1980s. During his visit to the Soviet Union, Kim Il Sung saw that the Soviet Union paid attention to computer education programs for young people. Since then, the North Korean regime has initiated state-led intensive computer programs for young and gifted science students (Cho, 2004, pp. 57–60; Korea Development Institute, 2001, p. 65). IT human capital cultivated by these education programs are regarded as the primary source of North Korea's aggressive cyberoperations.

In September 2017, a major Russian telecommunications company, TransTeleCom, appeared to have begun providing an internet connection to North Korea (Williams, 2017). Amid

diplomatic fallout between North Korea and China, its only major partner, Russia, tried to position itself to be a stronger North Korean ally, reaching out to provide North Korea with an internet connection (Park & Newton, 2017). As a result, North Korea has two internet lines to access cyberspace because China Unicom still provides an internet connection to Pyongyang. The new change in the capacity of North Korea's internet traffic gives the state more flexibility.

Russia has not actively participated in the international sanctions against North Korea as a result of its nuclear programs. China was also reluctant to join the sanctions in the beginning. However, due to pressure from the United States, China started to join the international community to punish North Korea. In this period, North Korea turned toward Russia, which refused to join the punishment. Russia has still supported North Korea's access to cyberspace.

Moreover, it is suspected that North Korean IT experts are conducting malicious activities in cyberspace inside Russian territory (Office of Foreign Assets Control, 2018). Two cybersecurity experts on North Korea and Russia, Donghui Park and Matthew Newton (2017), claimed that Russia might embolden Pyongyang and its hackers to launch more destructive cyberoperations, causing the expansion of the cybersecurity dilemma in the Northeast Asia region. They also added that "[s]tronger cooperation between the two raises the possibility that they will even collaborate on cyberattacks themselves, which would be devastating for the international community" (Park & Newton, 2017).

The cybersecurity dilemma on the Korean Peninsula resulting from North Korea's creation of cyber uncertainty has expanded to the Northeast Asia region, where two ideological blocs used to compete with one another. One consists of the United States, Japan, and South Korea. The other is made up of China, Russia, and North Korea. North Korea is developing cybercapability for survival, thus creating uncertainty in cyberspace. This uncertainty has

threatened South Korea's national security and led to the cybersecurity dilemma on the Peninsula. In response to North Korea's cyber threats, the South Korean government started to increase its self-defense cybercapability. It also began to strengthen its existing relationships with traditional allies and make new partnerships with friendly countries. Paradoxically, the effort to increase South Korea's national security in cyberspace has allowed the cybersecurity dilemma on the Peninsula to spread throughout Northeast Asia as it revitalizes the Cold War confrontation between the two blocs.

China and Russia have continued to provide assistance to North Korea in the information age. The two countries have challenged U.S. dominance in the international system as well as cyberspace. In this regard, they are reluctant to see the cooperation between South Korea, the United States, other Western-oriented countries, as well as international organizations for cybersecurity in response to North Korea's cyber threats in the Northeast Asia region. They also have helped North Korea develop its aggressive cybercapability. Major Chinese and Russian telecommunications companies have provided internet connections to North Korea. Moreover, it seems that North Korean hackers and their malicious online activities within the sovereign territories of the two countries have been protected by the Chinese and Russian governments, whether intentionally or otherwise. Currently, the traditional Easter and Western blocs have threatened each other in cyberspace and created the cybersecurity dilemma which results in a vicious circle of arms races and alliance formation in Northeast Asia.

4.6 Conclusion

How much does a state's cyber buildup impact regional and world security dynamics? Some scholars cast doubt on cyber power as a strategic tool for states, compared to conventional military power (Gartzke, 2013; Kello, 2013). Overall, skeptics view cyberoperations as a less

powerful tool, making them ineffective for political goals. However, empirical evidence from North Korea's cybercapability buildup illustrates that uncertain activities of the state in cyberspace cause countries to become fearful, thus creating the security dilemma and resulting changes in regional security dynamics. Based on empirical findings, this chapter claims that a state's cybercapability can be as powerful as a state's conventional military capability.

North Korea's development of cybercapability reduces the security of neighboring countries. Pyongyang's intention to enhance cybercapacity is ambiguous for the outside world. It is hard for other countries to understand the goals and purposes of North Korea's activities in the virtual world due to the characteristics of cyberspace and information technologies. North Korea's actions cannot be closely monitored in this artificial space. Moreover, information technologies are dual-use goods generally used for civilian purposes, but may also work for malicious cyber activities.

South Korea has responded to North Korea's creation of cyber uncertainty. First, the South began to increase its self-defense capacity in cyberspace. The state officially announced that North Korea's cybercapability was one of the threats to its national security. This, in turn, led to further actions including the establishment of the ROK Cyber Command, an increase in budgets for defensive cybercapability, the creation of new positions for cybersecurity in the Blue House, and the creation of new relationships with individual cyber experts and private sectors. These concrete actions to increase defensive cybercapability are responses to the cybersecurity dilemma.

The South Korean government has also attempted to increase its national security by strengthening existing partnerships and forming new relationships with other countries in the pursuit of cyber defense against North Korea, along with a growing self-defense capability.

South Korea's efforts to create cyber alliances can be seen in three different actions: (1) a bilateral military alliance with the United States, (2) partnerships with maritime powers (Japan and the United States), and (3) multilateral cooperation around the globe. As cyberspace is borderless, these efforts can be understood as a reasonable way to secure the national security of a state, along with the increase in self-defense cybercapacity.

South Korea's defensive actions against North Korea's cyber uncertainty inadvertently leads to the transfer of the cybersecurity dilemma on the Korean Peninsula to Northeast Asia as a whole. The Korean Peninsula has been a place of confrontation between the Western bloc—the United States, South Korea, and Japan—and Eastern bloc—China, Russia, and North Korea—of the Cold War. Despite the end of the Cold War, the confrontation has continued. Furthermore, the tension between the two sides has moved to cyberspace as North Korea develops its cybercapability. Cyberspace becomes a new place for cooperation between North Korea, China, and Russia against the partnership of South Korea, the United States, and Japan. China and Russia allow North Korea to conduct its malicious cyber activities in response to defensive actions of their counter-partners, whether intentionally or otherwise. Therefore, this chapter argues that through the application of the traditional security dilemma to cyberspace, a state's cyber buildup has sufficient power to change regional and world security dynamics, along with other conventional military capacities.

Chapter 5. CONCLUSION

5.1 SUMMARY

This dissertation aims to answer this question: Why and how did North Korea become a world-class cyber-threat actor? This question is puzzling because North Korea appears to be undeveloped in science and technology, as well as being isolated in a digital age. However, empirical data about North Korea challenges the image of North Korea as technologically undeveloped. Thus, on the basis of empirical evidence, this dissertation argues that since the 1980s, Pyongyang has focused on the importance of cybercapability, developed ITs, constructed IT infrastructure, cultivated IT human capital, and conducted hostile cyber proxy operations against the rest of the world in pursuit of its national interests. This research also claims that the malicious activities of North Korea in cyberspace increase fear and insecurity among other countries which can also have an impact on regional security dynamics.

Chapter 2 demonstrated that North Korea has sufficient IT infrastructure and human capital to conduct hostile cyberoperations against the outside world in pursuit of its national goals. The Kim dictator family has officially emphasized the importance of information technology for regime survival. The country has policies to boost ITs without allowing its people to access the open digital world which would harm its authoritarian regime. In other words, society is disconnected from the outside world in cyberspace but has its own internal and closed network systems. Moreover, North Korea's intensive education programs for gifted computer students are the core of North Korea's hostile cybercapability. It is suspected that IT human capital developed by these education programs plays a critical role in aggressive cyberoperations of the regime, threatening the national security of other countries and resulting in changes in regional security dynamics.

North Korea's cyber strategy is detailed in Chapter 3. North Korea has been accused of conducting many massive and complicated cyberoperations since the July 2009 DDoS attacks. However, the state has denied and avoided its responsibility for covert operations in cyberspace by adopting a classic proxy warfare strategy. Pyongyang achieves its strategic outcome without being traced or punished by employing non-state actors as proxies to carry out cyberattacks.

North Korea-associated hackers keep a distance from their sponsor country as they disguise themselves as online non-state actors, such as cyber hacktivists or criminals. The proxy warfare strategy is revitalized in cyberspace by using the characteristics of the artificial space (an anarchical nature, anonymity, and an absence of boundaries) and using information technologies (fake IP addresses, proxy servers, hop points, and VPNs). For example, employees of North Korea's front companies in China hid their identities and conducted cyberoperations to contribute to the political goals of the North Korean regime. However, the front companies were directly controlled by North Korea's Lab 110, which is affiliated with the Reconnaissance General Bureau (RGB) military spy agency, managed by the regime's Defense Ministry.

Chapter 4 provides an empirical examination of the power of states' cyber capabilities as the strategic tool in the field of national security. North Korea's creation of cyber uncertainty causes fear among other countries in Northeast Asia. This uncertainty and fear lead those countries to increase their defensive cyber capabilities. However, this increase in defensive capability also inadvertently decreases the security of other countries in the region. Thus, this vicious circle illustrates that a state's cyber capabilities have sufficient power as a strategic tool to compel others to do their will, and even to change regional and world security dynamics.

5.2 Bridging Gap between Classic IR Theories and Cybersecurity

This research uses traditional IR and security theories to approach a new security phenomenon. It assumes that cybersecurity issues share some common features with traditional security ones. This does not mean this study accepts every traditional theory without question. Therefore, this research borrows three useful classic theories and revises them to understand new security issues in the virtual world which is unique and different in comparison to the physical world.

The first theory applied in this dissertation is the *dictator's dilemma*. Dictators are worried about freedom of information which could harm their regimes. In this regard, they also recognize that ITs, including the internet, could weaken their positions in their authoritarian countries. However, despite the potential risk, the findings illustrate that dictators accept ITs for their political and economic goals while using strong censorship programs to monitor their citizens. North Korea is an extreme case in that it forbids its people from accessing the internet entirely. Pyongyang uses ITs, however, to conduct hostile cyberattacks against the outside world to ensure regime survival. It is a distorted and asymmetric way of using ITs in authoritarian regimes.

The second theory involves proxy warfare literature. Historically, state actors have indirectly engaged conflicts by hiring third parties as proxies, such as state or non-state actors, in order to achieve their strategic goals. The anarchical international system enables countries to conduct a proxy warfare strategy in the real world. For states, a classic proxy warfare strategy is even more beneficial in the virtual world due to the characteristics of cyberspace (its anarchical nature, anonymity, and absence of boundaries) and using information technologies (fake IP

addresses, proxy servers, hop points, and VPNs). Thus, conventional literature sheds light on how state actors conduct cyberoperations for their national interests, summarized in Chapter 3.

The last empirical chapter applies the third theory, the *security dilemma*, to understand the power of states' cyber capabilities. A state's defensive actions designed to increase its national security paradoxically decrease the security of other states. The dilemma results from the uncertainty about the actions of countries in the anarchical international system. The digital world is also a new uncertain space for countries. States cannot entirely monitor one another in cyberspace. In this regard, one state can easily become fearful of other states' cyber activities, which are indeed not offensive. Therefore, on the basis of the classic security dilemma, Chapter 4 reveals that North Korea's uncertain actions in cyberspace cause fear among and raise security concerns for states; this can then lead to changes in regional security dynamics.

These three theories show that some classic IR theories are applicable in understanding security issues in the digital age. This dissertation does not imply that every traditional IR and security theory can be applied to cybersecurity issues without question. However, it argues that some of the theories are useful in grasping new security phenomena in the virtual world if these theories are carefully revised based on unique and different characteristics of cyberspace as compared to other natural domains of land, sea, air, and space.

5.3 Policy Implications

This study suggests important implications for the international community and policymakers who focus on cybersecurity in public and private sectors. Malicious activities in cyberspace are growing and threaten national security across the globe. More interestingly, these malicious cyber activities have been caused by a variety of unknown actors including non-state actors (individual internet users, cybercriminals, criminal groups, cyber terrorists, terrorist

groups), and state actors. North Korea's case illustrates that an economically weak state has sufficient cyber capabilities to conduct aggressive cyberoperations against the rest of world in pursuit of its national interests. The state even hires and uses non-state actors as third-party proxies for its hostile cyberattacks to avoid its responsibility and potential punishment. Moreover, North Korea's cyber capabilities prove cyber power can change regional security dynamics. Therefore, it is imperative for the international community and policymakers to understand the risk and challenges associated with North Korea's cybercapability buildup and cyberoperations. A few basic lessons follow from this dissertation's findings. The lessons are divided into two parts: (1) understanding national security in the information age, and (2) how to protect national security in the digital wilderness.

5.3.1 *Understanding National Security in the Information Age*

There are six implications from the findings about national security in the digital age. First, cyberspace is a new frontline between countries pursuing their national interests. They are ready to fight one another in this space if it can prove beneficial to their political, societal, and economic interests. Moreover, the anarchical and anonymous nature of cyberspace and a variety of information technologies play a critical role for their cyber competitions.

The anarchical and anonymous virtual space is also a perfect strategic venue for authoritarian countries. In a narrow sense, cyberspace is recognized as a dangerous space for these countries due to freedom of information that could threaten their regimes. However, this negative aspect of cyberspace is not a critical enough issue to prevent them from moving forward in cyberspace. Authoritarian states use strong censorship programs to block their people from sharing negative information about the regime on the internet. These countries utilize malicious

cyber activities as a strategic tool to increase their national goals. North Korea is the perfect example of a regime that uses its cybercapability to pursue hostile goals.

The second implication is that in the digital age, weak states are no longer weaker than strong states in terms of offensive action. North Korea's case shows that weak states can quickly develop their offensive cyber capabilities which threatening other states, especially strong states. Cyber weapons are cheaper than conventional ones. Even personal computers, commercial software, and commercial hardware can be used for cyberattacks. States are not required to build several military camps equipped with a variety of facilities and weapons for training cyberwarriors. On the contrary, weak states can develop their cyber professionals with computers, textbooks, some software programs, and the internet. Even free open sources, such as YouTube, can teach IT professionals how to hack websites.

In some cases, weak states are better at defensive operations than strong states. Weak states, such as North Korea, do not have state-of-the-art information technologies and IT infrastructure that strong states have. This leads to an asymmetric situation between weak and strong states. Weak states do not have many networks and IT infrastructure needed to be secure. In contrast, leading IT countries are required to spend lots of time, effort, and money on protecting their vast IT infrastructure and networks against malicious cyberattacks. Paradoxically, this means that while weak states can be easily equipped with offensive cyber capabilities, massive IT infrastructure and cyberspace of strong countries are vulnerable to cyberattacks.

The third implication is that cyber power is an independent strategic tool for states. In the 1990s, information technologies were used for auxiliary methods in conventional wars. U.S. army forces jammed the warning and guidance systems of Iraqi defense forces by means of ITs to win the Gulf War (Baudrillard, 1995). However, in recent years, cyber methods have proven

their power as a strategic tool to maintain or alter the balance of power and resist or impose disputed outcomes. A state can impose its will on others with independent cyber power from other physical weapons in peacetime as well as wartime. Pyongyang conducts aggressive cyberoperations against the outside world for its ultimate goal, regime survival, without other conventional weapons during peacetime. In addition, North Korea seems to be ready to fight against others in cyberspace during wartime.

The fourth implication is that non-state actors are of higher importance than ever before. The U.S. Department of Defense contributed to the invention of the internet. However, since then, private sectors have mainly expanded and managed cyberspace, while state actors have monitored and controlled their activities. State and non-state actors, ranging from spy agents and military officers to hackers and cybercriminals and terrorists, are working in the private sector-led virtual world. In recent years, many software programs and hardware devices of private companies have also be applied to the defense arena around the globe. Malicious non-state actors, including state-led cyberwarriors, conduct cyberattacks by using various devices, software programs, and internet services provided by private sectors. Thus, the border between public and private areas is blurred in the information age. Furthermore, this means that the role of private IT companies is more important than ever before for national security.

Individual internet users have also played a critical role in national security. It is possible that a genius hacker can harm critical networks of states. This fact raises a critical question: who is a cyber combatant? The answer is that in the digital age anyone can participate in national security issues with or without a contract with a country. Thus, private IT companies and individual internet users should be considered as a key factor in national security and cyberwar.

The fifth and related implication is that although non-state actors have played a critical role in national security, sovereign countries have the authority to control their own areas and non-state actors in cyberspace. It would be a mistake to assume that the virtual world is disconnected from other natural domains. However, cyberspace cannot exist without the real world. This artificial space has been constructed with facilities, infrastructure, and devices, which are physically attached to land, sea, air, and space under the control of sovereign states. For example, fiber optical cables under the ground and sea provide high-speed data connections between devices, servers, buildings, and countries.

People who are living in the physical world access the virtual space with physical devices, infrastructure, and IT services. They are citizens of sovereign countries. When they are absorbed in activities in cyberspace, their bodies cannot move out of the territorial boundary of a state. Although various IT techniques and skills enable hackers to hide their identities in cyberspace, these are not perfect and permanent for their covert cyberoperations and crimes. In general, non-state actors, including hackers, are supposed to follow the laws and rules of their governments. Thus, state sovereign power is still a valid and powerful way to manage and control non-state actors within their territorial boundaries in the information age.

The final implication is that cyber proxy warfare continues to be the best military strategy for both strong and weak states. States seek to increase their national interests in cyberspace—whether strong or weak or democratic or authoritarian—while trying to avoid responsibility for their cyberoperations. Therefore, it is reasonable that state actors are likely to pay attention to the power of non-state actors under their sovereignty when carrying out various state-led cyberoperations.

Together, these six factors present a less-than-sanguine outlook on national security in the digital age, despite the political, economic, and social benefits of ITs. Therefore, new types of national security issues occurring in cyberspace continually challenge policymakers and cybersecurity experts to make creative security policies and plans.

5.3.2 *How to Protect National Security in the Digital Wilderness*

These findings produce four recommendations for national cybersecurity policy. First, cybersecurity issues should be considered the same as traditional security issues. Cyberspace is invisible. Cyberattacks do not directly cause physical violence and bloodshed. Therefore, people tend to be desensitized to cyberweapons and cyberattacks on themselves. However, this dissertation's findings illustrate that state cyber activities are a strategic tool for national interests and can even change regional security dynamics. Thus, cybersecurity is not a sub-category of other conventional security areas, but rather a new national security field. Political leaders and policymakers should cultivate cybersecurity experts to deal with this new security field.

The second recommendation is that a state can increase its national security in cooperation with others, ranging from individual internet users to private IT companies to other countries. A state has the authority to control its cyberspace based on sovereign territorial power. However, the authority of a state is limited because cyberspace is anarchical, anonymous, and borderless. It is challenging for a state to control all areas of cyberspace. Freedom of information and people's rights should be respected in cyberspace. Therefore, state actors should try to attract voluntary participation from individual internet users and private companies. Also, states should enhance partnerships with others to secure cyberspace where there are not any clear borders between states and private sectors.

The third recommendation is that countries must be responsible for malicious cyber activities that are conducted within their sovereign territories. Cyberoffenders, including both individual and state-associated hackers, are physically located in a state when they carry out cyberattacks. State actors have sufficient authority, however, to control and manage their citizens, facilities, ITs, or IT infrastructure with their laws and rules. This means that each state cannot separate itself from malicious cyber actions which originate from its territory. Thus, states should do their best to mitigate cyber threats that are directly or indirectly related to themselves. Moreover, the international community must punish nations, which connive with cybercriminals or their cyberwarriors to conduct illegal cyberattacks and abet them in malicious cyberoperations against other countries.

Finally, states should have and operate well-organized cyber ethics education programs, including diverse content, such as ethical behavior, good manners, legal behavior, and rights and responsibilities in the digital age. Human beings are at the core of all cyber activities because those actions are directly or indirectly produced by them. Also, anyone can easily become a cyberwarrior who might harm national security. Thus, countries need to provide high-quality and continuing education services that are designed to teach all citizens ranging from students to older people. Teaching young students cyber ethics is critical in particular to keep them away from cybercrimes and malicious state-led cyberoperations.

5.4 Looking Forward

This research project presents many avenues for future research. First, the lessons learned from North Korea's case sheds light on the paradoxical trend of authoritarian countries to maximize its national interests in cyberspace, while developing strong online censorship systems. In other words, studying censorship programs of authoritarian states is an important

challenge for future research. Second, the lessons raise questions about the role of non-state actors for protecting national security. For example, contrary to North Korea's non-state offenders, cyber non-state actors can also be recognized as defenders. Last but not least, exploring the responsibility of IT companies and their relationships with states for national security presents another potentially fruitful avenue for future research.

REFERENCES

Abbott, K. W., Genschel, P., Snidal, D., & Zangl, B. (Eds.). (2015). *International organizations as orchestrators*. New York, NY: Cambridge University Press.

AhnLab Security Emergency Response Center (ASeC). (2014). *ASEC report.* (Vol. 51). AhnLab.

Ahram, A. I. (2011). *Proxy warriors: The rise and fall of state-sponsored militias*. Stanford, CA: Stanford University Press.

Alyac. (2018, February 12). *Covert activities of Operation Kimsuky: Its specialized APT attacks are still working* [Malware code analysis report]. Retrieved April 2, 2018, from ESTsecurity Alyac Blog website: http://blog.alyac.co.kr/1536 (Korean)

Applegate, S. D. (2011). Cybermilitias and political hackers: Use of irregular forces in cyberwarfare. *IEEE Security and Privacy*, *9*(5), 16–22.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165.

Arquilla, John, Ronfeldt, D., & Zanini, M. (1999). Networks, netwar, and information-age terrorism. In Z. Khalilzad, J. P. White, & A. Marshall (Eds.), *In strategic appraisal: The changing role of information in warfare* (pp. 75–111). Santa Monica, CA: RAND Corporation.

Art, R. J., & Jervis, R. (Eds.). (2017). *International politics: Enduring concepts and contemporary issues* (13th ed.). Boston, MA: Pearson.

Asia-Pacific Network Information Centre. (n.d.-a). APNIC - Query the APNIC Whois Database: 210.52.109.0 - 210.52.109.255. Retrieved from http://wq.apnic.net/apnic-bin/whois.pl

Asia-Pacific Network Information Centre. (n.d.-b). APNIC Whois Search: “175.45.176.0 - 175.45.179.255.” Retrieved from http://wq.apnic.net/static/search.html

Associated Press. (2009, July 11). North Korea launched cyber attacks, says South. *The Guardian*. Retrieved from http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks

Associated Press. (2011, August 4). South Korea arrests five over gaming scam: “Linked to hackers in North.” *The Guardian*. Retrieved from http://www.theguardian.com/technology/2011/aug/04/south-north-korean-hackers-china

Associated Press. (2014, December 7). North Korea: Sony hack a righteous deed but we didn’t do it. *The Guardian*. Retrieved from

https://www.theguardian.com/world/2014/dec/07/north-korea-sony-hack-a-righteous-deed-but-we-didnt-do-it

Association for Progressive Communications. (2015, April 15). "What is the Global Conference on Cyberspace?" FAQs on the GCCS, The Hague, 16–17 April 2015. Retrieved January 24, 2019, from Association for Progressive Communications website: https://www.apc.org/en/news/what-global-conference-cyberspace-faqs-gccs-hague

Avant, D. D. (2005). *The market for force: The consequences of privatizing security*. New York, NY: Cambridge University Press.

Axelrod, R. M. (1984). *The evolution of cooperation*. New York, NY: Basic Books.

BAE Systems Applied Intelligence. (2017, October 16). Taiwan heist: Lazarus tools and ransomware. Retrieved April 3, 2018, from Threat Research Blog website: http://baesystemsai.blogspot.com/2017/10/taiwan-heist-lazarus-tools.html

Baldor, L. C. (2016, June 14). Air, land, sea, cyber: NATO adds cyber to operation areas. *AP NEWS*. Retrieved from https://apnews.com/b7a8330df0114498a1611257d4cb5d58

Banks, S. (2005). North Korean telecommunications: On hold. *North Korean Review*, *1*, 88–94.

Barrett, B. (2018, September 6). DoJ charges North Korean hacker for Sony, WannaCry, and more. *Wired*. Retrieved from https://www.wired.com/story/doj-north-korea-hacker-sony-wannacry-complaint/

Barrett, D., & O'Keeffe, K. (2016, May 10). FBI suspects insider involvement in $81 million Bangladesh bank heist. *Wall Street Journal*. Retrieved from https://blogs.wsj.com/indiarealtime/2016/05/10/fbi-suspects-insider-involvement-in-81-million-bangladesh-bank-heist/

Bar-Siman-Tov, Y. (1984). The strategy of war by proxy. *Cooperation and Conflict*, *19*(4), 263–273.

Baudrillard, J. (1995). *The Gulf War did not take place*. Bloomington, IN: Indiana University Press.

Baumgartner, K. (2014, December 4). Sony/Destover: Mystery North Korean actor's destructive and past network activity. Retrieved November 5, 2018, from Securelist - Kaspersky Lab's Cyberthreat Research and Reports website: https://securelist.com/destover/67985/

Baylis, J. (2005). British nuclear doctrine: The 'Moscow Criterion' and the Polaris Improvement Programme. *Contemporary British History*, *19*(1), 53–65.

Beyer, J. L. (2014). *Expect us: Online communities and political mobilization*. New York, NY: Oxford University Press.

Bless young heroes in the information age. (2001, May 3). *The Kyowon Sinmun*. (Korean)

Boas, T. C. (2000). The dictator's dilemma? The internet and U.S. policy toward Cuba. *Washington Quarterly*, *23*(3), 57–67.

Boo, H.-W. (2017). An assessment of North Korean cyber threats. *The Journal of East Asian Affairs*, *31*(1), 97–117.

Borghard, E. D. (2014). *Friends with benefits? Power and influence in proxy warfare* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Columbia University).

Bruce, S. T. (2012). *A double-edged sword: Information technology in North Korea*. Honolulu, HI: The East-West Center.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust and fear between nations*. New York, NY: Oxford University Press.

Buchanan, B., & Williams, R. (2018, October 24). A deepening U.S.-China cybersecurity dilemma. Retrieved December 11, 2018, from Lawfare website: https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma

Bumiller, E., & Shanker, T. (2012, October 11). Panetta warns of dire threat of cyberattack on U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Butterfield, H. (1950). The tragic element in modern international conflict. *The Review of Politics*, *12*(2), 147–164.

Butterfield, H. (1951). *History and Human Relations*. London, UK: Collins.

Byman, D. (2005). Passive sponsors of terrorism. *Survival*, *47*(4), 117–144.

Byman, D., & Kreps, S. E. (2010). Agents of destruction? Applying principal-agent analysis to state-sponsored terrorism. *International Studies Perspectives*, *11*, 1–18.

Byun, S.-J. (2011). A review of studies on North Korea's science and technology policy. *Review of North Korean Studies*, *14*(2), 167–216. (Korean)

Calatayud, J. M. (2017, June 18). Locked Shields: The world's largest cyber-war game. *AlJazeera*. Retrieved from https://www.aljazeera.com/indepth/features/2017/05/locked-shields-world-largest-cyber-war-game-170527102554714.html

Carr, J. (2012). *Inside cyber warfare* (2nd ed). Sebastopol, CA: O'Reilly.

Central Intelligence Agency. (n.d.). The world factbook: North Korea. Retrieved June 14, 2018, from Central Intelligence Agency website: https://www.cia.gov/library/publications/the-world-factbook/geos/kn.html

Chacos, B. (2016, February 12). North Korean dictator Kim Jong-un hates freedom, loves his Macs. *PCWorld*. Retrieved from https://www.pcworld.com/article/3032571/macs/north-korean-dictator-kim-jong-un-hates-freedom-loves-his-macs.html

Chae, K.-H. (2013, March 1). The Number One Secondary School fever. Retrieved June 29, 2018, from Unification Korea website: http://unikorea21.com/?p=6879 (Korean)

Chang, M.-S. (2016, March 24). Army & navy hold hacking defense contests in response to North Korea's cyberattacks. *Newsis*. Retrieved from http://www.newsis.com/view/?id=NISX20160324_0013978862 (Korean)

Chen, C., Ko, K., & Lee, J.-Y. (2010). North Korea's internet strategy and its political implications. *The Pacific Review*, *23*(5), 649–670.

Cheon, S.-W. (2013). The Kim Jong-un regime's "Byungjin" (Parallel Development) policy of economy and nuclear weapons and the "April 1st Nuclearization Law." *Korea Institute for National Unification*, *13*(11), 1–7.

Cho, J.-A. (2012a). Hamheung Computer University. In *Encyclopedia of Korean Culture*. Retrieved from http://encykorea.aks.ac.kr/Contents/CategoryNavi?category=contenttype&keyword=단체&ridx=5505&tot=5562 (Korean)

Cho, J.-A. (2012b). Pyongyang Computer University. In *Encyclopedia of Korean Culture*. Retrieved from http://encykorea.aks.ac.kr/Contents/Item/E0070466 (Korean)

Cho, J.-A. (2004). The educational policy of North Korea in the era of Kim, Jung-il. *Asian Journal of Education*, *5*(2), 47–72. (Korean)

Choe, S.-H., & Markoff, J. (2009, July 8). Cyberattacks jam government and commercial web sites in U.S. and South Korea. *The New York Times*. Retrieved from https://www.nytimes.com/2009/07/09/technology/09cyber.html

Choi, J.-S. (2015, October 5). North Korea commanded Seoul subway for five months. *The Chosun Ilbo*. Retrieved from http://news.chosun.com/site/data/html_dir/2015/10/05/2015100500286.html?Dep0=twitter&d=2015100500286 (Korean)

Choi, S.-H. (2018, November 20). Looking for the best cyber warrior. *The Kookbang Ilbo*. Retrieved from http://kookbang.dema.mil.kr/newsWeb/20181121/3/BBSMSTR_000000010024/view.do (Korean)

Choi, Y.-H. (2012, April 28). ROK-US defense meeting warns of North Korea's potential provocation. *The Donga Ilbo*. Retrieved from http://news.donga.com/3/all/20120428/45857198/1 (Korean)

Chun, H.-W. (2013, December 17). A University fosters cyber warriors. *Sisa In*. Retrieved from https://www.sisain.co.kr/?mod=news&act=articleView&idxno=18703 (Korean)

Chung, C.-H. (2006). *Understanding North Korean society*. Seoul, Korea: Minsogwon. (Korean)

Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty first century. A constructivist approach. *The Public Administration and Social Policies Review*, *1*(12), 120–136.

Citizens' Coalition for Democratic Media. (2009, July 10). Increasing doubts about cyber north wind without evidence. *OhmyNews*. Retrieved from http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0001175013 (Korean)

Clapper, J. R. (2014). *[2014] Statement for the record: Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Clapper, J. R. (2015). *[2015] Statement for the record: Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Clapper, J. R. (2016). *[2016] Statement for the record: Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Clarke, R. (2009). War from cyberspace. *The National Interest*, 104, 31–36.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York, NY: HarperCollins Publishers.

Coats, D. R. (2017). *[2017] Statement for the record: Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Coats, D. R. (2018). *[2018] Statement for the record: Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Coats, D. R. (2019). *[2019] Statement for the record: Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Cohen, E. A. (1996). A revolution in warfare. *Foreign Affairs*, *75*(2), 37–54.

Cohen, E. A. (2004). Change and transformation in military affairs. *Journal of Strategic Studies*, *27*(3), 395–407.

Colarik, A., & Janczewski, L. (2012). Establishing cyber warfare doctrine. *Journal of Strategic Security*, *5*(1), 31–48.

Collins, A. R. (1998). GRIT, Gorbachev and the end of the Cold War. *Review of International Studies*, *24*(2), 201–219.

Company Overview of Loxley Pacific Company Limited. (n.d.). *Bloomberg*. Retrieved from https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=47174087

Cooperative Cyber Defence Centre of Excellence. (2018, April 27). NATO won cyber defence exercise Locked Shields 2018. Retrieved December 31, 2018, from CCDCOE website: https://www.ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018

Craig, D. (2012). *Proxy war by African states, 1950–2010* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (American University).

Cunningham, D. E., Gleditsch, K. S., & Salehyan, I. (2013). Non-state actors in civil wars: A new dataset. *Conflict Management and Peace Science*, *30*(5), 516–531.

Cuthbertson, A. (2018, November 20). North Korea is holding an international cryptocurrency and blockchain conference. *The Independent*. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-cryptocurrency-blockchain-conference-pyongyang-a8643391.html

Czosseck, C., Ottis, R., & Taliharm, A.-M. (2013). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. In M. Warren (Ed.), *Case Studies in Information Warfare and Security for Researchers, Teachers and Students* (pp. 72–91). Reading, UK: ACPIL.

Dabbagh, O. (2017, June 26). Cyber security set to dominate at “Five Eyes” meeting in Canada. *SBS News*. Retrieved from https://www.sbs.com.au/news/cyber-security-set-to-dominate-at-five-eyes-meeting-in-canada

Davenport, D. (2002). Anonymity on the internet: Why the price may be too high. *Communications of the ACM*, *45*(4), 33–35.

Davenport, K. (2018, June). The Six-Party Talks at a glance. Retrieved January 7, 2019, from Arms Control Association website: https://www.armscontrol.org/factsheets/6partytalks

Dear Leader Kim Jong Il provided new school buses and equipment for special schools to train computer gifted human capital. (2002, April 11). *The Kyowon Sinmun*. (Korean)

Dear Leader Kim Jong Il sent gifts to students in the computer classes, Guemseong Number One and Two schools. (2001, May 31). *The Kyowon Sinmun*. (Korean)

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia War. *Security Dialogue*, *43*(1), 3–24.

DeLuca, C. D. (2013). The need for international laws of war to include cyber attacks involving state and non-state actors. *Pace International Law Review Online Companion*, *3*(9), 278–315.

Denning, D. (2007). Assessing the computer network operations threat of foreign countries. In John Arquilla & D. Borer (Eds.), *Information strategy and warfare: A guide to theory and practice*. New York, NY: Routledge.

Denson, J. V. (Ed.). (1999). *The costs of war: America’s pyrrhic victories* (2nd expanded ed.). New Brunswick, NJ: Transaction Publishers.

Dewey, C. (2013, February 26). Instagrams from within North Korea lift the veil, but only slightly. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2013/02/26/instagrams-from-within-north-korea-lift-the-veil-but-only-slightly/

DPRK Today. (n.d.). Retrieved April 22, 2019, from YouTube website: https://www.youtube.com/channel/UCndGz3c8ImJ216C4kZMxaWA

DPRKToday, Welcome to Dprktoday (@dprktoday) [Social Networking Service]. (n.d.). Retrieved April 22, 2019, from Instagram website: https://www.instagram.com/dprktoday/

Efron, S. (1999, August 19). Computer chips stacked to master Japanese chess. *The Los Angeles Times*. Retrieved from http://articles.latimes.com/1999/aug/19/news/mn-1595/2

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *The Academy of Management Review*, *14*(1), 57–74.

Everyday DPRK (@everydaydprk) [Social Networking Service]. (n.d.). Retrieved April 22, 2019, from Instagram website: https://www.instagram.com/everydaydprk/

Everydaydprk [Social Networking Service]. (n.d.). Retrieved April 22, 2019, from Facebook website: https://www.facebook.com/EverydayDPRK

Fackler, M. (2014, December 27). North Korea accuses U.S. of staging internet failure. *The New York Times*. Retrieved from https://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html

Fahrion, G. (2011, May 8). Die Pyramidenbauer von Pjöngjang (The pyramid builders of Pyongyang). *The German Financial Times*. Retrieved from http://www.ftd.de/it-medien/it-telekommunikation/:agenda-die-pyramidenbauer-von-pjoengjang/60048145.html

Fama, E. F. (1980). Agency problems and the theory of the firm. *Journal of Political Economy*, *88*(2), 288–307.

FBI. (2014, December 19). *Update on Sony investigation* [Press Release]. Retrieved March 28, 2018, from Federal Bureau of Investigation website: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

FBI. (2018, June 8). *Arrest warrant for Park Jin Hyok*. Retrieved from https://www.fbi.gov/wanted/cyber/park-jin-hyok/@@download.pdf

FBI National Press Office. (2014, December 19). *Update on Sony investigation* [Press Release]. Retrieved April 3, 2018, from Federal Bureau of Investigation website: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Feakin, T. (2013). Playing blind-man's buff: Estimating North Korea's cyber capabilities. *International Journal of Korean Unification Studies*, *22*(2), 63–90.

Ferguson, N. (1999). *The pity of war*. New York, NY: Basic Books.

Fifield, A. (2014, December 7). North Korea denies hacking Sony but calls the breach a "righteous deed." *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/north-korea-denies-hacking-sony-but-calls-the

breach-a-righteous-deed/2014/12/07/508d6991-c242-419c-b71c-59a3d1173766_story.html?utm_term=.38db6212f0b5

Fifield, A. (2017, October 10). North Korean hackers stole U.S. and South Korean wartime plans, Seoul lawmaker says. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/asia_pacific/north-korean-hackers-stole-us-and-south-korean-wartime-plans-seoul-lawmaker-says/2017/10/10/036fb82c-adc6-11e7-99c6-46bdf7f6f8ba_story.html

FireEye. (2017, October 10). North Korean actors spear phish U.S. electric companies. Retrieved April 3, 2018, from FireEye Threat Research Blog website: https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html

FireEye. (2018). *APT37 (Reaper): The overlooked North Korean actor*. Retrieved from FireEye website: https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

FireEye. (n.d.). Who's who of cyber threat actors. Retrieved November 8, 2018, from Advanced Persistent Threat Groups website: https://www.fireeye.com/current-threats/apt-groups.html

Fly Higher. (2003, July 24). *The Kyowon Sinmun*. (Korean)

Former Anonymous hacker doubts North Korea behind Sony Attack. (2014). Retrieved from https://www.youtube.com/watch?v=vWiFtS5F3jc

Foster many specialized people, including computer experts. (2003, May 14). *Rodong Sinmun*. (Korean).

Francis, D. (2015, January 2). Obama slams North Korea with sanctions for Sony hack. Retrieved November 7, 2018, from Foreign Policy website: https://foreignpolicy.com/2015/01/02/obama-slams-north-korea-with-sanctions-for-sony-hack/

Fraser, N., Plan, F., Cannon, V., & O'Leary, J. (2018). *APT38: Un-usual suspects*. Retrieved from FireEye website: https://content.fireeye.com/apt/rpt-apt38

Fratantonio, Y., Bianchi, A., Robertson, W., Kirda, E., Kruegel, C., & Vigna, G. (2016). TriggerScope: Towards detecting logic bombs in android applications. *2016 IEEE Symposium on Security and Privacy (SP)*, 377–396. https://doi.org/10.1109/SP.2016.30

Freedom House. (2018, January 5). *North Korea profile*. Retrieved November 6, 2018, from Freedom in the World 2018 website: https://freedomhouse.org/report/freedom-world/2018/north-korea

French, P. (2007). *North Korea: The paranoid peninsula: A modern history*. London, UK: Zed Books.

Garrison, A. H. (2004). Defining Terrorism: Philosophy of the bomb, propaganda by deed and change through fear and violence. *Criminal Justice Studies*, *17*(3), 259–279.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41–73.

Gause, K. E. (2015). *North Korea's provocation and escalation calculus: Dealing with the Kim Jong-un regime*. Arlington, VA: CNA Analysis & Solutions.

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). *World War C: Understanding nation-state motives behind today's advanced cyber attacks*. Milpitas, CA: FireEye.

George, D. L. (1933). *War memoirs of David Lloyd George, 1914-1915*. Boston, MA: Little, Brown and Company.

Gervais, M. (2012). Cyber attacks and the laws of war. *Berkeley Journal of International Law*, *30*, 525–579.

Glaser, C. L., & Kaufmann, C. (1998). What is the offense-defense balance and can we measure it? *International Security*, *22*(4), 44–66.

Goldsmith, J. (2015). How cyber changes the laws of war. In F. Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations* (pp. 51–61). London, UK: Palgrave Macmillan.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. New York, NY: Oxford University Press.

GReAT. (2017, May 15). Wannacry and Lazarus Group—the missing link? Retrieved July 6, 2018, from Securelist - Kaspersky Lab's Cyberthreat Research and Reports website: https://securelist.com/wannacry-and-lazarus-group-the-missing-link/78431/

Grieco, J. M. (1988). Anarchy and the limits of cooperation: A realist critique of the newest liberal institutionalism. *International Organization*, *42*(3), 485–507.

Griggs, T., & Fidler, S. (2007, July 15). Orascom takes stake in N Korea's Sangwon. *Financial Times*. Retrieved from https://www.ft.com/content/4c0d690c-32ee-11dc-a9e8-0000779fd2ac

Grigsby, A. (2018, November 15). The United Nations doubles its workload on cyber norms, and not everyone is pleased. Retrieved February 22, 2019, from Council on Foreign Relations website: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased

Group-IB. (2017, May 30). *Lazarus arisen*. Retrieved May 30, 2017, from Group-IB website: http://blog.group-ib.com/lazarus

Hachigian, N. (2002). The internet and power in one-party East Asian states. *Washington Quarterly*, *25*(3), 41–58.

Hamilton, R. F., & Herwig, H. H. (Eds.). (2003). *The origins of World War I*. New York, NY: Cambridge University Press.

Han, D., Lee, K., Do, K., Hong, J., & Kim, S. (2018). *The 2018 white paper on North Korean human rights violations*. Seoul, Korea: Korea Institute for National Unification. (Korean)

Han, M. (2011, April 6). ROK police attributes 3.4. DDoS Attacks to North Korea. *Yonhap News Agency*. Retrieved from http://www.yonhapnews.co.kr/society/2011/04/06/0701000000AKR20110406074800004.HTML (Korean)

Harley, N. (2017, October 14). North Korea behind WannaCry attack which crippled the NHS after stealing US cyber weapons, Microsoft chief claims. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/2017/10/14/north-korea-behind-wannacry-attack-crippled-nhs-stealing-us/

Harrison, B. (2017, December 7). How North Korea recruits its army of young hackers. *NBC News*. Retrieved from https://www.nbcnews.com/news/north-korea/how-north-korea-recruits-trains-its-army-hackers-n825521

Hassig, R. C., & Oh, K. (2009). *The hidden people of North Korea: Everyday life in the hermit kingdom*. Plymouth, UK: Rowman & Littlefield Publishers, INC.

Hayes, P. (2012, June 14). The DPRK's nuclear constitution. Retrieved January 15, 2019, from Nautilus Institute for Security and Sustainability website: https://nautilus.org/napsnet/napsnet-policy-forum/the-dprks-nuclear-constitution/

Heam, K. (2014). Hacking, nationalism, democracy and cyberwarfare in the People's Republic of China: A centre / margin perspective. In A. Chong & F. B. Yahya (Eds.), *State, society*

and information technology in Asia: Alterity between online and offline politics (pp. 111–134). Burlington, VT: Ashgate.

Herz, J. H. (1950). Idealist internationalism and the security dilemma. *World Politics*, *2*(2), 157–180.

Herz, J. H. (1951). *Political realism and political idealism: A study in theories and realities*. Chicago, IL: University of Chicago Press.

Herz, J. H. (1959). *International politics in the Atomic Age*. New York, NY: Columbia University Press.

Hong Kong-CERT. (2018, August 3). APCERT Cyber Drill 2018 "Data Breach via Malware on IoT." Retrieved January 24, 2019, from https://www.hkcert.org/my_url/en/articles/18030801

Ho, Y.-J. (2011, October 18). Military will increase the budget for cybersecurity. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=28057 (Korean)

Hodge, M. (2017, May 23). Inside North Korea's 6,000-strong Unit 180 hacking group feared to be behind the NHS ransomware attack. *The Sun*. Retrieved from https://www.thesun.co.uk/news/3633869/north-korea-unit-180-hacking-group-nhs-ransomware/

Holden, C. (1986). Soviets launch computer literacy drive. *Science*, *231*(4734), 109–110.

HP Security Research. (2014). *Profiling An enigma: The mystery of North Korea's cyber threat landscape*. Retrieved from HP website: https://cryptome.org/2014/12/hp-nk-cyber-threat.pdf

Hughes, G. (2012). *My enemy's enemy: Proxy warfare in international politics*. Portland, OR: Sussex Academic Press.

Incapsula. (n.d.). What is APT (Advanced Persistent Threat). Retrieved January 8, 2019, from Web Application Security Center website: https://www.incapsula.com/web-application-security/apt-advanced-persistent-threat.html

Infosecurity. (2013, September 12). Kimsuky: An active North Korean campaign targeting South Korea. Retrieved April 2, 2018, from Infosecurity Magazine website: https://www.infosecurity-magazine.com:443/news/kimsuky-an-active-north-korean-campaign-targeting/

Innes, M. (Ed.). (2012). *Making sense of proxy wars: States, surrogates & the use of force*. Washington, D.C.: Potomac Books.

Insikt Group. (2017, July 25). North Korea's ruling elite are not isolated. Retrieved March 7, 2018, from Recorded Future website: https://www.recordedfuture.com/north-korea-internet-activity/

Insikt Group. (2018). *Shifting patterns in internet use reveal adaptable and innovative North Korean ruling elite* (Technical Report No. CTA-2018-1025). Somerville, MA: Recorded Future.

Institute for Unification Education. (2017). *Understanding North Korea in 2018*. Seoul, Korea: ROK Ministry of Unification. (Korean)

Intelligence, B. S. A. (n.d.). Lazarus & watering-hole attacks. Retrieved May 17, 2017, from BAE Systems Threat Research Blog website: http://baesystemsai.blogspot.com/2017/02/lazarus-watering-hole-attacks.html

Internet Society. (n.d.). Global Conference on Cyber Space (GCCS 2017). Retrieved December 31, 2018, from Internet Society website: https://www.internetsociety.org/events/gccs-2017/

Intezer. (2017, December 12). *Blockbusted: Lazarus, blockbuster, and North Korea*. Retrieved December 12, 2017, from Intezer website: http://www.intezer.com/blockbusted-lazarus-blockbuster-north-korea/

Japan Ministry of Defense. (2015, April 27). The guidelines for Japan-U.S. defense cooperation. Retrieved January 23, 2019, from Japan Ministry of Defense website: http://www.mod.go.jp/e/d_act/anpo/shishin_20150427e.html

Jervis, R. (1976). *Perception and misperception in international politics*. Princeton, NJ: Princeton University Press.

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.

Jervis, R. (2001). Was the Cold War a security dilemma? *Journal of Cold War Studies*, *3*(1), 36–60.

Jin, Y. (2017). *Having a glance at cyberwarfare*. Seoul, Korea: The ROK National Assembly. (Korean)

Joint Chiefs of Staff. (2015). *The national military strategy of the United States of America 2015: The United States military's contribution to national security*. Fort Belvoir, VA: Defense Technical Information Center.

Jordan, T. (1999). *Cyberpower: The culture and politics of cyberspace and the internet*. London, UK: Routledge.

Josselin, D., & Wallace, W. (Eds.). (2001). *Non-state actors in world politics*. London, UK: Palgrave Macmillan.

Joubert, V. (2012). five years after Estonia's cyber attacks: Lessons learned for NATO? *Research Paper*, (76), 1–8.

Jun, J., LaFoy, S., & Sohn, E. (2014). *The organization of cyber operations in North Korea*. Washington, D.C.: The Center for Strategic and International Studies.

Jun, J., LaFoy, S., Sohn, E., & Lewis, J. A. (2015). *North Korea's cyber operations: Strategy and responses*. New York, NY: Rowman & Littlefield.

Jung, Y. (2018, June 29). Lack of South Korean style Korean language of North Korean agents for cyber psychological warfare. *RFA*. Retrieved from https://www.rfa.org/korean/weekly_program/bd81d55c-itc640-acfcd559ae30c220/sciencetech-06282018160531.html (Korean)

Junio, T. J. (2013). *The politics and strategy of cyber conflict* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global (University of Pennsylvania).

Kallberg, J., & Rowlen, S. (2014). African nations as proxies in covert cyber operations. *African Security Review*, *23*(3), 307–311.

Kang, D. (2019, January 8). North Korea's SNS propaganda activities. *TV Chosun*. Retrieved from http://news.tvchosun.com/site/data/html_dir/2019/01/08/2019010890160.html (Korean)

Kang, H.-J. (2007). *History of science and technology in North Korea 1*. Seoul, Korea: Sunin. (Korean)

Kang, J.-K. (2016, January 26). IT company, North Korea's Chosun Expo. Retrieved November 5, 2018, from Digital Hurricane website: http://www.dihur.co.kr/1107 (Korean)

Kang, J.-K. (2018, May). North Korea's security and the cooperation strategy between the two Koreas. *KISA Report*, *2018–5*, 45–50. (Korean)

Kang, Juhee, Ling, R., & Chib, A. (2017). Strategic use of ICTs among North Korean women resettled in South Korea. *The Ninth International Conference on Information and Communication Technologies and Development*, 1–5.

Kang, R., Brown, S., & Kiesler, S. (2013). Why do people seek anonymity on the internet?: Informing policy and design. *Changing Perspectives*, 2657–2666. Paris, France: ACM.

Karatzogianni, A. (2015). *Firebrand waves of digital activism 1994–2014: The rise and spread of hacktivism and cyberconflict*. London, UK: Palgrave Macmillan.

Kaspersky Lab. (n.d.). What is a Trojan virus? - Definition. Retrieved January 8, 2019, from Threats website: https://usa.kaspersky.com/resource-center/threats/trojans

Kello, L. (2013). The meaning of the cyber Revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7–40.

Keohane, R. O. (1984). *After hegemony: Cooperation and discord in the world political economy*. Princeton, NJ: Princeton University Press.

Kerr, J. (2014, October 16). *The digital dictator's dilemma: Internet regulation and political control in non-democratic states*. 1–48. Palo Alto, CA: The Center for International Security and Cooperation in Stanford University.

Kerry, J. (2014, December 19). Condemning cyber-attack by North Korea. Retrieved November 7, 2018, from U.S. Department of State website: //2009-2017.state.gov/secretary/remarks/2014/12/235444.htm

Kihl, Y. W. (1984). North Korea in 1983: Transforming "The Hermit Kingdom"? *Asian Survey*, *24*(1), 100–111.

Kihl, Y. W. (2002). Security on the Korean Peninsula: Continuity and change. *Security Dialogue*, *33*(1), 59–72.

Kim, Beom-Hyeon. (2009, October 30). Head of ROK NIS said North Korea's Ministry of Post and Telecommunications is the origin of DDoS Attacks. *The Hankyoreh*. Retrieved from http://www.hani.co.kr/arti/society/society_general/384886.html (Korean)

Kim, Bo-Mi. (2013). Economic aid from socialist countries in DPRK's post-war reconstruction and the rise of 'Juche", 1953~1955. *The Journal of Asiatic Studies*, *56*(4), 305–340. (Korean)

Kim, Bong-Sik. (2017). Fixed and mobile-cellular telephone services in North Korea and its implications. *ICT & Media Policy*, *29*(10), 1–43. (Korean)

Kim, Dong-Yub. (2015). North Korea's dual policy of nuclear and economic development and military changes. *Review of North Korean Studies*, *18*(2), 77–120. (Korean)

Kim, Dong-Un. (2013, April 7). Brothers collaborated with North Korean hackers for illegal online business. *Maeil Business Newspaper*. Retrieved from http://news.mk.co.kr/newsRead.php?sc=&year=2013&no=264502 (Korean)

Kim, E. (2012, November 15). Seoul defense dialogue discusses WMD, N. Korea. *Yonhap News Agency*. Retrieved from https://en.yna.co.kr/view/AEN20121115003500315

Kim, Gwi-Geun. (2004, July 14). Cyberwarfare between states is not a virtual reality. *Yonhap News Agency*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=001&aid=0000702108&sid1=001 (Korean)

Kim, Gwi-Geun. (2006, May 25). Strong powers develop cyber capabilities as one of the core powers. *Yonhap News Agency*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=001&aid=0001307274&sid1=001 (Korean)

Kim, Gwi-Geun. (2016, May 26). The ROK government will establish cyber reserve forces. *Maeil Business Newspaper*. Retrieved from http://news.mk.co.kr/newsRead.php?sc=50100002&year=2016&no=378204 (Korean)

Kim, Gwi-Geun. (2018, October 14). ROK military, planning to make the rules of cyber engagement. *Yonhap News Agency*. Retrieved from https://www.yna.co.kr/view/AKR20181012158000014?input=1195m (Korean)

Kim, Gyu-Ryun. (2014). *Analysis on the result of the ROK-U.S. summit in April 2014* (No. 2014–03). Seoul, Korea: Korea Institute for National Unification. (Korean)

Kim, Haeyoung. (2014). Stifled growth and added suffering: Tensions inherent in sanctions policies against North Korea. *Critical Asian Studies*, *46*(1), 91–112. https://doi.org/10.1080/14672715.2014.863579

Kim, Han-Sol. (2015, March 17). South Korean prosecution attributed hacking KHNP to North Korea. *The Kyunghyang Shinmun*. Retrieved from http://sports.khan.co.kr/comics/index.html (Korean)

Kim, Hyung-Jin. (2016, August 1). Seoul blames North Korean gov't organization for email scams. *AP NEWS*. Retrieved from https://apnews.com/5a490a275f754bddaa2173d31be3c26c

Kim, Ho-Jun. (2016, October 24). The North operates troll army. *Yonhap News Agency*. Retrieved from http://www.yonhapnews.co.kr/bulletin/2016/10/23/0200000000AKR20161023038000014.HTML (Korean)

Kim, Hyo-Jeong. (2016, June 28). The 4th U.S.-ROK cyber policy consultations will be held in Washington D.C. *Yonhap News Agency*. Retrieved from https://www.yna.co.kr/view/AKR20160628117200014 (Korean)

Kim, Jong Il. (1982). *On the Juche idea*. Pyongyang, North Korea: Foreign Languages Publishing House.

Kim, Jong Il. (1992). *Kim Jong-il's anthology* (Vol. 1–14). Pyongyang, North Korea: Korean Workers' Party Publishing Co. (Korean)

Kim, Jong Il. (1998). A public speaking for workers in the field of education on April 28, 1984: Improving the quality of secondary schools. In J. I. Kim, *Kim Jong Il's Anthology* (Vol. 8). Pyongyang, North Korea: Korean Workers' Party Publishing Co. (Korean)

Kim, Jong Il. (2000). A public speaking for members in the Central Committee of the Workers' Party of Korea on March 3, 1997: Following the revolutionized military spirit. In J. I. Kim, *Kim Jong Il's Anthology* (Vol. 14). Pyongyang, North Korea: Korean Workers' Party Publishing Co. (Korean)

Kim, Jong Il. (2013). A public speaking for members in the Central Committee of the Workers' Party of Korea on January 28, 2001: Improving the quality of the program for computer gifted students. In J. I. Kim, *Kim Jong Il's Anthology* (Vol. 20). Pyongyang, North Korea: Korean Workers' Party Publishing Co. (Korean)

Kim, Jong Sun, & Lee, Choon-Geun. (2014). *An analysis on North Korea's ITs and a cooperation plan for reunification* (No. 142; pp. 1–23). Seoul, Korea: Science and Technology Policy Institute. (Korean)

Kim, Jong Un. (2015, January 1). The 2015 new year address of Kim Jong Un [Full Text]. *The Choson Sinbo*. Retrieved from http://chosonsinbo.com/2015/01/kcna_150101-4/ (Korean)

Kim, Jong Un. (2018, January 1). The 2018 new year address of Kim Jong Un [Full Text]. *The Choson Sinbo*. Retrieved from http://chosonsinbo.com/2018/01/kcna_180101-2/ (Korean)

Kim, Jeong-Wan. (2009, December 17). Can defense "Cyber Command" be established this coming January? *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=18945 (Korean)

Kim, Ji-Young, & Han, C. (2008, December 16). "Koryolink," 3G mobile service. *The Choson Sinbo*. Retrieved from http://nk.chosun.com/news/articleView.html?idxno=6649 (Korean)

Kim, Ju-Jin. (2004, August). A strategy to connect networks of two Koreas by building North Korea's communication networks. *Science and Technology Policy*, *148*, 45–67. (Korean)

Kim, Kyung-Ae. (2013, May 1). The 7th hacking defense contest will be held. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=35911 (Korean)

Kim, Kyung-Ae. (2018, December 20). Several North Korea-related cyberattacks occurred. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=75678 (Korean)

Kim, Kye-Soo, & Lee, Choon-Geun. (2001). The national R&D system and S&T human resources training system in North Korea. *Science and Technology Policy Institute*, *2001–04*, 1–242. (Korean)

Kim, Min-Seok. (2009, July 11). South Korea's Cyber Command will be established next year and in charge of protecting cyber territory. *The JoongAng Ilbo*. Retrieved from https://news.joins.com/article/3682753 (Korean)

Kim, Oi-Hyun. (2015, January 23). Why did the Blue House appoint Lim Jong In as the Special Security Advisor of the President? *The Hankyoreh*. Retrieved from http://www.hani.co.kr/arti/politics/politics_general/674992.html (Korean)

Kim, Rahn. (2011, May 3). NK launched cyber attack on Nonghyup. *Korea Times*. Retrieved from http://www.koreatimes.co.kr/www/nation/2018/03/113_86369.html

Kim, Sam. (2018, February 7). Inside North Korea's hacker army. *Bloomberg.Com*. Retrieved from https://www.bloomberg.com/news/features/2018-02-07/inside-kim-jong-un-s-hacker-army

Kim, Sangbae. (2017). Four neighbouring network-states and South Korea in cyber security: Network structure of powers and strategies of a middle power. *The Korean Journal of International Relationship*, *57*(1), 111–154. (Korean)

Kim, So-Yeob. (2011, August 25). The Department of Cyber Defense, Korea University. *The Chosun Ilbo*. Retrieved from http://news.chosun.com/site/data/html_dir/2011/08/24/2011082401350.html?Dep0=twitter&d=2011082401350 (Korean)

Kim, Sun-Ae. (2007, June 18). The degree of North Korea's Software Technology Is High. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=6542 (Korean)

Kim, Sung-Hwan. (2015, February 3). Is the ‘Christmas Hacking’’ one of the Kimsuky operations?’ *The Hankyoreh21*, *1048*. Retrieved from http://h21.hani.co.kr/arti/economy/economy_general/38919.html (Korean)

Kim, Sung-Jin. (2009, April 16). North Korean defectors accepted to Ph.D. programs in the U.S. *Yonhap News Agency*. (Korean)

Kim, Tae-Jin. (2017, January 16). AI age, cyber reserve forces will be founded. *ZDNet Korea*. Retrieved from http://www.zdnet.co.kr/view/?no=20170116111013 (Korean)

Kim, Tae-Kyu. (2018, December 19). ROK government hold the national cybersecurity policy coordination meeting. *Newsis*. Retrieved from http://www.newsis.com/view/?id=NISX20181219_0000507756 (Korean)

Kim, Yeon-Jeong. (2018, November 5). Cho Myoung-Gyon, “North Korea has 6 million mobile-cellular phone subscribers.” *Yonhap News Agency*. Retrieved from https://news.v.daum.net/v/20181105130122953 (Korean)

Kim, Yonho. (2013, November 26). A closer look at the “explosion of cell phone subscribers” in North Korea. Retrieved July 11, 2018, from 38 North website: https://www.38north.org/2013/11/ykim112613/#_ftnref2

Kim, Yonho. (2014a). *Cell phones in North Korea*. Washington D.C.: US-Korea Institute at SAIS.

Kim, Yonho. (2014b, April 9). North Korea’s Arirang smartphone copies a Chinese one. *VOA Korea*. Retrieved from https://www.voakorea.com/a/1889038.html (Korean)

Kim, You-Yeon. (2014). *A study on the first middle school policy of DPRK* (MA thesis). Retrieved from Korean Research Information Sharing Service. (Ewha Womans University). (Korean)

Kim, You-Yeon. (2017). A comparative study on North Korea’s computer education systems between the Number One and Ordinary Secondary Schools. *The past, present, and future of North Korea’s education*. Daejeon, Korea: Korean Association for Reunification Education. (Korean)

Kim, Yun-Young. (2016). A study on countermeasures to deter North Korean cyber maneuvers against South Korea: Focusing on legal and institutional improvements. *The Journal of Police Policies*, *30*(2), 241-276. (Korean)

Kiser, E. (1999). Comparing varieties of agency theory in economics, political science, and sociology: An illustration from state policy implementation. *Sociological Theory*, *17*(2), 146–170.

Ko, K. (2014). Internet opening up North Korea: Implications and prospects from Cuba's experience. *National Strategy*, *20*(1), 61-93. (Korean)

Ko, K., Jang, S., & Lee, H. (2008). .Kp: North Korea. In F. Librero & P. B. Arinto (eds.), *Digital Review of Asia Pacific 2007-2008.* (pp. 244–250). Retrieved from http://www.deslibris.ca/ID/422877

Ko, K., Lee, H., & Jang, S. (2009). The internet dilemma and control policy: Political and economic implications of the internet in North Korea. *Korean Journal of Defense Analysis*, *21*(3), 279–295.

Ko, Soo-Yeon. (2012, October 10). The 2013 budget for informatization of the South Korean government is 3,296.7 billion won. *The IT Daily*. Retrieved from http://www.itdaily.kr/news/articleView.html?idxno=34182 (Korean)

Korean Central News Agency. (2013). *The housewarming party at the newly constructed Unha Scientists Street* [Video file]. Retrieved from https://www.youtube.com/watch?v=p7tf133vSs8 (Korean)

Korean Central News Agency. (n.d.). *The Red Star TV* [Video file]. Retrieved January 8, 2019, from YouTube website: https://www.youtube.com/channel/UCJtCyB5ayvqhCSqGPdDe7mw

Korea (Democratic People's Republic of)'s Constitution of 1972 with Amendments through 1998. (1998). Retrieved from https://www.constituteproject.org/constitution/Peoples_Republic_of_Korea_1998?lang=en

Korea Development Institute. (2001, January). Review of the North Korean economy. *Korea Development Institute*, *2001–1*, 1–104. (Korean)

Korea University's Admissions Office. (2012, March). *Guidebook for fostering talented persons*. Korea University. (Korean)

Korea University's Department of Cyber Defense. (2018). Admission guide. Retrieved February 19, 2019, from Korea University Division of Information Security & Graduate School of Information Security website: http://gss.korea.ac.kr/ime/info/enter.do (Korean)

Krause, V., & Singer, J. D. (2001). Minor powers, alliances, and armed conflict: some preliminary patterns. In E. Reiter & H. Gartner (Eds.), *Small states and alliances*. Heidelberg, Germany: Physica.

Krishnan, A. (2017). Principal-agent problem in proxy warfare. *The 75th MPSA Annual Conference*. Presented at the 75th MPSA Annual Conference, Chicago, IL.

Krishnan, A. (2018). *Why paramilitary operations fail*. Cham, Switzerland: Palgrave Macmillan.

Kwak, M. (2016, July 5). North Korea transformed two Korea's joint venture website into its own advertisement website. *Yonhap News Agency*. Retrieved from http://www.yonhapnews.co.kr/bulletin/2016/07/05/0200000000AKR20160705179000014.HTML (Korean)

Kydd, A. H. (2005). *Trust and mistrust in international relations*. Princeton, NJ: Princeton University Press.

Lange, K. (2018, May 3). Cybercom becomes DoD's 10th Unified Combatant Command. *DoDLive*. Retrieved from http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/

Lankov, A. (2009). Pyongyang strikes back: North Korean policies of 2002-08 and attempts to reverse "De-Stalinization from Below." *Asia Policy*, *8*(1), 47–72.

Lankov, A. (2013). *The real North Korea: Life and politics in the failed Stalinist utopia*. New York, NY: Oxford University Press.

Lederer, E. M. (2019, March 12). UN probing North Korea sanctions violations in 20 countries. *The Associated Press*. Retrieved from https://www.nytimes.com/aponline/2019/03/11/world/asia/ap-un-united-nations-north-korea-sanctions.html

Lee, Bong-Seok. (2016, March 13). North Korea's Go game software was the best in the past. *Yonhap News Agency*. (Korean)

Lee, Choon-Geun. (2005). *North Korea's science and technology*. Seoul, Korea: Hanul Academy. (Korean)

Lee, Choon-Geun. (2014). *Policies to promote South-North ICT cooperation* (Policy No. 14–28). Sejong, South Korea: Science and Technology Policy Institute. (Korean)

Lee, Choon-Geun., & Kim, Jong-Sun. (2015). *Changes in North Korea's science and technology policy and its implications in the age of Kim Jong Un* (No. 173). Seoul, Korea: Science and Technology Policy Institute. (Korean)

Lee, Dave. (2015, December 10). North Korea's policy to expand the base for science and scientists. *NKtoday*. Retrieved from http://nktoday.kr/?p=9654 (Korean)

Lee, Dave, & Kwek, N. (2015, May 29). North Korean hackers "could kill", warns key defector. *BBC News*. Retrieved from https://www.bbc.com/news/technology-32925495

Lee, Heejin, & Hwang, J. (2004). ICT development in North Korea: Changes and challenges. *Information Technologies & International Development*, *2*(1), 75–87.

Lee, Hyun-Jeong. (2015, October 5). Seoul subway server allegedly hacked by N.K. *The Korea Herald*. Retrieved from http://www.koreaherald.com/view.php?ud=20151005001125

Lee, Hong-Reoul. (2008). Mobile phones in North Korea. *TTA Journal (IT Standard & Certification)*, *117*, 138–143. (Korean)

Lee, Jean H. (2016, January 19). Good luck to @AFP on the wild ride aheadhttps://twitter.com/afp/status/689579045764227072 … [Tweet]. Retrieved July 11, 2018, from @newsjean website: https://twitter.com/newsjean/status/689639913805905920

Lee, Joo-Hyung. (2015, April 5). The Blue House appoints Shin In-sub as the Cybersecurity Secretary. *The Kookbang Ilbo*. Retrieved from http://kookbang.dema.mil.kr/newsWeb/20150405/1/BBSMSTR_000000010031/view.do (Korean)

Lee, Jung-Hun. (2011, June 15). Everyone is happy if North Korea is the cyber offender. *The Hankyoreh21*, *865*. Retrieved from http://h21.hani.co.kr/arti/economy/economy_general/29833.html (Korean)

Lee, Jong-Woon. (2002). North Korea's IT industry and IT cooperation plans between two Koreas. *KIEP World Economy*, *5*(5), 58–71. (Korean)

Lee, Kyeong-Min. (2009, July 10). Request for strengthening information security in defense. *Boan.com*. Retrieved from http://www.boan.com/news/article.html?id=20090710150015 (Korean)

Lee, Kyung-Tak. (2018, June 3). The ROK government does not concern the establishment of cyber reserve forces. *The Digital Times*. Retrieved from http://www.dt.co.kr/contents.html?article_no=2018060402100251041001 (Korean)

Lee, Min-Hyung. (2011, December 6). Four-year tuition waiver and the reason of Korea University's establishment of the first Cyber Defense Department. *The Digital Daily*. Retrieved from http://www.ddaily.co.kr/news/article.html?no=85335 (Korean)

Lee, Sang-Ho. (2011). North Korea's cyber-based psychological warfare and South Korea's deterrent options. *Journal of Korean Political and Diplomatic History*, *33*(1), 263–290. (Korean)

Lee, Sang-Hun. (2011, January 8). Military Cyber Command established. *Yonhap News Agency*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=001&aid=0003063917&sid1=001 (Korean)

Lee, Sang-Sin, Oh, K., & Lee, Y. (2017). *A study on North Korean workers dispatched to foreign countries* (No. 16–04). Korea Institute for National Unification. (Korean)

Lee, Sang-Young. (2010, April 19). The increase in mobile communication capacity and 600,000 subscribers expected in the next year. *The Choson Sinbo*. (Korean)

Lee, Soo-Ho. (2016, December 7). Cybersecurity budget reduction while being attacked. *News1*. Retrieved from http://news1.kr/articles/?2851394 (Korean)

Lee, Sunny. (2011). US security strategy toward North Korea's cyber terrorism. *2011 Dupont Summit*. Washington, D.C.: Carnegie Institution for Science.

Lee, Su-Rak. (2003, December). The status quo about North Korea's project to cultivate information manpower and the prospect. *Science Technology*, *46*. (Korean)

Lee, Won-Sang. (2017, February 13). An analysis on entrance scores of the Seoul National University, Yonsei Univesity, and Korea University in 2017. *Edu-Donga*. Retrieved from http://www.edudonga.com/?p=article&at_no=20170213095158367752 (Korean)

Lee, Yoo-Ji. (2015, July 3). Special Security Advisor of the President, Lim Jong In, "in need of having national cybersecurity strategy & action plans." *The Digital Daily*. Retrieved from http://www.ddaily.co.kr/news/article.html?no=132128 (Korean)

Lepingwell, J. W. R. (1987). The laws of combat? Lanchester reexamined. *International Security*, *12*(1), 89–134.

Levy, J. S. (1984). The offensive/defensive balance of military technology: A theoretical and historical analysis. *International Studies Quarterly*, *28*(2), 219–238.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.

Libicki, M. C. (2012). *Crisis and escalation in cyberspace*. Santa Monica, CA: RAND, Project Air Force.

Lieber, K. A. (2007). The new history of World War I and what it means for international relations theory. *International Security*, *32*(2), 155–191.

Liff, A. P. (2012). Cyberwar: A new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. *The Journal of Strategic Studies*, *35*(3), 401–428.

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

Lim, S., & Hong, S. (2017). Present conditions of North Korean industry and possible reconstruction plans. *Korea's Economy*, *31*, 45–50.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404.

Lipton, E., Sanger, D. E., & Shane, S. (2016, December 13). The perfect weapon: How Russian cyberpower invaded the U.S. *The New York Times*. Retrieved from http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

Local Satellite Internet Services in NORTH-KOREA [Company Website]. (n.d.). Retrieved April 26, 2018, from TS2: Worldwide Satellite Communications website: https://ts2.space/en/satellite-internet-form/NORTH-KOREA

Lupovici, A. (2014). The "attribution problem" and the social construction of "violence": Taking cyber deterrence literature a step forward. *International Studies Perspectives*, 322–342.

Lynn, W. J., III. (2010, September 1). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs*, (September/October 2010). Retrieved from https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

Lynn-Jones, S. M. (1995). Offense-defense theory and its critics. *Security Studies*, *4*(4), 660–691.

Madory, D. (2017, October 2). North Korea gets new internet link via Russia. Retrieved April 25, 2018, from Dyn website: https://dyn.com/blog/north-korea-gets-new-internet-link-via-russia/

Major N. Korean websites remain unstable for 6th day. (2014, December 28). *Yonhap News Agency*. Retrieved from

http://english.yonhapnews.co.kr/news/2014/12/28/0200000000AEN20141228001900315.html

Mann, M. (1986). *The sources of social power: A history of power from the beginning to A.S. 1760*. New York, NY: Cambridge University Press.

Mansourov, A. Y. (2011). *North Korea on the cusp of digital transformation*. Berkeley, CA: Nautilus Institute.

Margolin, J. (2016, December 2). Russia, China, and the push for "digital sovereignty." Retrieved January 25, 2019, from IPI Global Observatory website: https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

Masters, J. (2014, April 23). What is internet governance? Retrieved December 17, 2018, from Council on Foreign Relations website: https://www.cfr.org/backgrounder/what-internet-governance

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. New York, NY: Cambridge University Press.

Maurer, T., & Taylor, K. (2018, March 2). Outlook on international cyber norms: Three avenues for future progress. Retrieved January 23, 2019, from Carnegie Endowment for International Peace website: https://carnegieendowment.org/2018/03/02/outlook-on-international-cyber-norms-three-avenues-for-future-progress-pub-75704

Mazanec, B. M. (2015). *The evolution of cyber war: International norms for emerging-technology weapons*. Lincoln, NE: Potomac Books.

McAfee. (2011). *Ten days of rain: Expert analysis of distributed denial-of-service attacks targeting South Korea* (pp. 1–15). Retrieved from McAfee website: https://securingtomorrow.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf

McMeekin, S. (2011). *The Russian origins of the First World War*. Cambridge, MA: Belknap Press of Harvard University Press.

McNamara, L. (2017, September 11). Why is North Korea so interested in bitcoin? Retrieved April 3, 2018, from FireEye Threat Research Blog website: https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html

Mehra, B., Merkel, C., & Bishop, A. P. (2004). The internet for empowerment of minority and marginalized Users. *New Media & Society*, *6*(6), 781–802.

Menendez, R. (2014, December 19). *Letter to Sec. Kerry on North Korean attacks on Sony*. Retrieved from https://www.foreign.senate.gov/imo/media/doc/12-19-14%20RM%20Letter%20to%20Sec.%20Kerry%20re%20North%20Korean%20attacks%20on%20Sony.pdf

Milgrom, P. R., & Roberts, J. (1992). *Economics, organization, and management*. Englewood Cliffs, NJ: Prentice-Hall.

Milner, H. (1991). The assumption of anarchy in international relations theory: A critique. *Review of International Studies*, *17*(1), 67–85.

Min, Byoung-Won. (2012). The new security dilemma in networked international politics a theoretical analysis. *Peace Studies*, *20*(1), 31-69. (Korean)

Min, Se-Ah. (2015, January 23). Korea University professor Lim Jong In is appointed as the Special Advisor in Security to the President. *Boannews*. Retrieved from https://www.boannews.com/media/view.asp?idx=45142&kind=2 (Korean)

Mina, A. X. (2014). Batman, pandaman and the blind man: A case study in social change memes and internet censorship in China. *Journal of Visual Culture*, *13*(3), 359–375.

Ministry of Foreign Affairs of Japan. (2016, December 20). *Japan-US-ROK experts meeting on cybersecurity of critical infrastructure* [Press release]. Retrieved December 26, 2018, from Ministry of Foreign Affairs of Japan website: /press/release/press4e_001419.html

Ministry of Foreign Affairs of Japan. (2017, December 20). [Press release] Press conference by Foreign Press Secretary Norio Maruyama. Retrieved April 3, 2018, from Ministry of Foreign Affairs of Japan website: /press/kaiken/kaiken4e_000451.html

Moe, T. M. (1984). The new economics of organization. *American Journal of Political Science*, *28*(4), 739–777.

Monaghan, A. (2015). Putin's way of war: The "war" in Russia's "hybrid warfare." *Parameters*, *45*(4), 65–74.

Monsegur, H. (2014, December 18). *Former Anonymous hacker doubts North Korea behind Sony attack*.

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. New York, NY: Public Affairs.

Mozur, P., & Perlez, J. (2018, August 7). China is reluctant to blame North Korea, its ally, for cyberattack. *The New York Times*. Retrieved from https://www.nytimes.com/2017/05/17/world/asia/china-north-korea-ransomware.html

Multinational Experiment. (2012). *Multinational experiment 7 outcome 3: Cyber domain objective 3.4 cyber situational awareness standard operating procedure*. Norfolk, VA: U.S. Joint Chiefs of Staff.

Multinational Experiment. (2013). *Multinational Experiment 7 cyber domain outcome 3. cyber situational awareness. Limited Objective Experiment Report*. Norfolk, VA: U.S. Joint Chiefs of Staff.

Mumford, A. (2013). *Proxy warfare*. Malden, MA: Polity Press.

Murauskaite, E. (2014, September 12). North Korea's cyber capabilities: Deterrence and stability in a changing strategic environment. Retrieved November 5, 2018, from 38 North website: https://www.38north.org/2014/09/emurauskaite091214/

Mynott, J. (2013). *Thucydides: The war of the Peloponnesians and the Athenians* (Trans.). New York, NY: Cambridge University Press.

Naím, M. (2012). Mafia states: Organized crime takes office. *Foreign Affairs*, *91*(3), 100–111.

Nakashima, E. (2018, April 24). Senate confirms Paul Nakasone to lead the NSA, U.S. Cyber Command. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/senate-confirms-paul-nakasone-to-lead-the-nsa-us-cyber-command/2018/04/24/52c95ca4-47e8-11e8-9072-f6d4bc32f223_story.html

Nam, S.-W. (2002). *North Korea's strategy to develop IT industry and building a strong and prosperous country*. Seoul, Korea: Hanul Academy. (Korean)

National Joint Investigation Group on North Korea's Hacking Attack on KHNP. (2015, March 17). *Intermediate investigation result of KHNP cyber terror incident*. The Supreme Prosecutors' Office of the Republic of Korea.

NATO. (2018, July 16). Cyber defence. Retrieved February 4, 2019, from NATO website: http://www.nato.int/cps/en/natohq/topics_78170.htm

Neiberg, M. S. (2018). American entry into the First World War as a historiographical problem. In M. M. Abbenhuis, K. Baird, G. Romano, & N. Atkinson (Eds.). *The Myriad Legacies of 1917: A Year of War and Revolution* (pp. 35–54). Cham, Switzerland: Palgrave Macmillan.

NK Tech. (2008, December 19). Newsletter 182: North Korea's 3G mobile telecommunication company, "Koryolink," started its service. Retrieved July 10, 2018, from NK Tech Briefing website: http://www.nktech.net/inform/nkt_briefing/nkt_briefing_v2.jsp?s_code_cd=&record_no=259 (Korean)

NK Tech. (2009a, May 18). Newsletter 193: The meaning of North Korea's satellite launching and 3G mobile service. Retrieved July 10, 2018, from NK Tech Briefing website: http://www.nktech.net/inform/nkt_briefing/nkt_briefing_v2.jsp?s_code_cd=&record_no=270 (Korean)

NK Tech. (2009b, October 27). Newsletter 203: Mobile phones and games are getting more popular in North Korea. Retrieved July 10, 2018, from NK Tech Briefing website: http://nktech.net/inform/nkt_briefing/nkt_briefing_v2.jsp?s_code_cd=tend&record_no=280 (Korean)

Noh, H.-D. (2014, December 20). The U.S., "North Korea engaged in the Sony hack" and Obama warned "An eye for an eye." *Yonhap News Agency*. (Korean)

Noh, Tae-Young. (2018, November 9). ROK MND holds defense cybersecurity contest. *The Asia Economy Daily*. Retrieved from http://view.asiae.co.kr/news/view.htm?idxno=2018110910472848909 (Korean)

Noland, M. (2009). Telecommunications in North Korea: Has Orascom made the connection? *North Korean Review*, *5*(1), 62–74.

Noland, M., Robinson, S., & Wang, T. (2001). Famine in North Korea: causes and cures. *Economic Development and Cultural Change*, *49*(4), 741–767.

Non-state Actor. (n.d.). Retrieved June 1, 2019, from Oxford Dictionaries website: https://en.oxforddictionaries.com/definition/non-state_actor

North Korea Today. (n.d.). [Video file]. Retrieved April 22, 2019, from YouTube website: https://www.youtube.com/channel/UCNaH2TGwop7CHZvnj0t3yjA

North Korea's gifted school, "the Number One Secondary School." (2001, September 20). *NK Chosun*. Retrieved from http://nk.chosun.com/news/articleView.html?idxno=10940 (Korean)

Northam, J. (2014, December 22). Obama considers listing North Korea a "sponsor of terrorism" after Sony hack. Retrieved from https://www.npr.org/2014/12/22/372526834/obama-considers-listing-north-korea-a-sponsor-of-terrorism-after-sony-hack

Novetta Threat Research Group. (2016). *Operations Blockbuster: Unraveling the long thread of the Sony attack*. McLean, VA: Novetta.

Nye, J. S. (2004). *Soft power: The means to success in world politics* (1st ed.). New York, NY: Public Affairs.

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly*, 18–38.

Obama, B. (2010). *National security strategy of the United States*. Washington, D.C.: The White House.

Obama, B. (2014, December 19). *Remarks by the President in year-end press conference* [Press Release]. Retrieved November 7, 2018, from The White House website: https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference

Office of Foreign Assets Control. (2018, September 13). Treasury Targets North Korea-Controlled Information Technology Companies in China and Russia. Retrieved February 25, 2019, from U.S. Department of the Treasury website: https://home.treasury.gov/news/press-releases/sm481

Office of the Press Secretary. (2012, March 27). *Nuclear security summit, Seoul, March 2012: Multinational statement on nuclear information security* [Press Release]. Retrieved January 24, 2019, from The White House website: https://obamawhitehouse.archives.gov/the-press-office/2012/03/27/nuclear-security-summit-seoul-march-2012-multinational-statement-nuclear

Office of the Press Secretary. (2013, May 7). *Joint declaration in commemoration of the 60th anniversary of the alliance between the Republic of Korea and the United States of America* [Press Release]. Retrieved January 22, 2019, from The White House website: https://obamawhitehouse.archives.gov/the-press-office/2013/05/07/joint-declaration-commemoration-60th-anniversary-alliance-between-republ

Office of the Press Secretary. (2015a, April 28). *Remarks by President Obama and Prime Minister Abe of Japan in joint press conference* [Press Release]. Retrieved January 23, 2019, from The White House website: https://obamawhitehouse.archives.gov/the-press-

office/2015/04/28/remarks-president-obama-and-prime-minister-abe-japan-joint-press-confere

Office of the Press Secretary. (2015b, October 16). *Joint fact sheet: The United States-Republic of Korea alliance: Shared values, new frontiers* [Press Release]. Retrieved January 22, 2019, from The White House website: https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new

Office of the Press Secretary. (2016, February 9*). FACT SHEET: Cybersecurity National Action Plan* [Press Release]. Retrieved January 23, 2019, from The White House website: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Office of Public Affairs, U.S. Department of Justice. (2018, September 6). North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber attacks and intrusions. Retrieved November 7, 2018, from The U.S. Department of Justice website: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Office of the Secretary of Defense. (2015). *Military and security developments involving the Democratic People's Republic of Korea*. Washington, D.C.: Department of Defense.

Office of the Spokesperson. (2018a, June 21). The 5th U.S.-Republic of Korea bilateral cyber consultations [Press release]. Retrieved February 20, 2019, from U.S. Department of State website: http://www.state.gov/r/pa/prs/ps/2018/06/283418.htm

Office of the Spokesperson. (2018b, July 26). The sixth U.S.-Japan cyber dialogue [Press release]. Retrieved February 22, 2019, from U.S. Department of State website: http://www.state.gov/r/pa/prs/ps/2018/07/284573.htm

Office of the Spokesperson. (2018c, July 27). US-Japan-ROK experts meeting on cybersecurity [Press release]. Retrieved February 22, 2019, from U.S. Department of State website: http://www.state.gov/r/pa/prs/ps/2018/07/284670.htm

Office of the Spokesperson of U.S. State Department. (2017, January 5). Key outcomes of the U.S.-Japan-ROK trilateral vice foreign ministerial meetings [Press release]. Retrieved January 28, 2019, from U.S. Embassy & Consulate in Korea website: https://kr.usembassy.gov/010517-key-outcomes-u-s-japan-rok-trilateral-vice-foreign-ministerial-meetings/

Oh, Byung-Min. (2010, July 7). What were the July 2009 DDoS attacks? *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=21860 (Korean)

Oh, Da-In. (2018a, April 29). NATO won the world biggest cyber defense exercise, Locked Shields, in this year. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=68931 (Korean)

Oh, Da-In. (2018b, July 5). All cyber offense and defense contests across the world. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=71000 (Korean)

Oh, Da-In. (2018c, August 30). FY 2019 Budget for Information security increased 39% year on year. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=72549 (Korean)

Oh, Jong-Tack. (2018, June 11). ROK MND holds white hat contest, one of the top four hacking competitions in Korea. *Newsis*. Retrieved from http://www.newsis.com/view/?id=NISX20180611_0000332572&cID=10301&pID=10300 (Korean)

On, Gi-Hong. (2014, December 25). China may cooperate with the South Korean government for the investigation on KHNP hack. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=44868 (Korean)

Orascom Telecom, Media & Technology. (2012). *Final prospectus*. Retrieved from Orascom Telecom Media and Technology Holding S.A.E. website: https://www.financeuncovered.org/wp-content/uploads/2016/02/192__OTMT-Prospectus.pdf

Orascom Telecom, Media & Technology. (2013, May 28). Koryolink reaches two million subscribers. *Orascom Telecom Media and Technology*. Retrieved from http://otmt.com/en-us/pressreleases.aspx?id=205

Pak, J. H. (2018, February 6). The education of Kim Jong-un. Retrieved July 10, 2018, from Brookings website: https://www.brookings.edu/essay/the-education-of-kim-jong-un/

Pallin, C. V. (2017). Internet control through ownership: The case of Russia. *Post-Soviet Affairs*, *33*(1), 16–33.

Park, Chan-Mo. (1994). *A comparative study on computer science between South and North Korea*. Seoul, Korea: The Korean Federation of Science and Technology Societies. (Korean)

Park, Chan-Mo. (1999). Current status of software research and development. *International Journal of Korean Studies*, *3*(1), 148–162.

Park, Chun-Sik. (2018, November 21). A lack of attention to cyber national security [Forum]. *The Digital Times*. Retrieved from http://www.dt.co.kr/contents.html?article_no=2018112202102269640002&ref=naver (Korean)

Park, D., & Beyer, J. L. (2017, December 21). Making sense of North Korea's hacking strategy. *Reuters*. Retrieved from https://www.reuters.com/article/beyer-cyber/column-commentary-making-sense-of-north-koreas-hacking-strategy-idUSL1N1OL289

Park, D., & Newton, M. (2017, December 1). Russia is now providing North Korea with internet: What that could mean for cyber warfare. *Forbes*. Retrieved from https://www.forbes.com/sites/outofasia/2017/12/01/russia-is-now-providing-north-korea-with-internet-what-that-could-mean-for-cyber-warfare/

Park, J., & Pearson, J. (2017, May 22). Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-northkorea-exclusive/exclusive-north-koreas-unit-180-the-cyber-warfare-cell-that-worries-the-west-idUSKCN18H020

Park, M. (2018, September 14). ROK MND holds the 2018 Cyber Working Group, Seoul Defense Dialogue. *Boannews*. Retrieved from https://www.boannews.com/media/view.asp?idx=72995&kind=2 (Korean)

Park, Sangjoo. (2008). North Korean internet. *Information & Communications Policy*, *20*(15), 69–72. (Korean)

Park, Seong-Uk. (2016, March 24). ROK Army hacking defense competition. *KTV*. Retrieved from http://www.ktv.go.kr/content/view?content_id=520132&unit=151 (Korean)

Park, Tae-Hee. (2017, March 22). North Korea's fourth industrial revolution is to CNC (Computer Numerical Control)-lized all over the country. *The JoongAng Ilbo*. Retrieved from http://news.joins.com/article/21396168 (Korean)

Park, Young-Tae. (2004, July 15). Around 20 countries, including the U.S., started to develop hacking troops 10 years ago. *The Korea Economic Daily*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&oid=015&aid=0000726354&sid1=001 (Korean)

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Services Research*, *34*(5), 1189–1208.

Paul, P. K., Bhuimali, A., & Shivraj, K. S. (2016). Internet infrastructure and governing bodies: an international perspectives. *Indian Journal of Information Sources and Services*, *6*(2), 9–12.

Perlroth, N., & Corkery, M. (2016, May 26). North Korea linked to digital attacks on global banks. *The New York Times*. Retrieved from https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html

Perlroth, N., & Sanger, D. E. (2014, December 22). North Korea loses its link to the internet. *The New York Times*. Retrieved from https://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html

Personnel Operating Budget Division. (2018, December). *Fiscal Year 2019 ROK MND budget proposal*. ROK MND. (Korean)

Personnel Operating Budget Division. (2019, January). The change in ROK military expenditure. Retrieved February 19, 2019, from ROK MND website: http://www.mnd.go.kr/mbshome/mbs/mnd/subview.jsp?id=mnd_010401020000 (Korean)

Pinkston, D. A. (2016). Inter-Korean rivalry in the cyber domain: The North Korean cyber threat in the Sŏn'gun Era. *Georgetown Journal of International Affairs*, *17*(3), 60–76.

Powell, R. (1994). Anarchy in international relations theory: The neorealist-neoliberal debate. *International Organization*, *48*(2), 313–344.

PRC Ministry of Foreign Affairs. (2016, February 13). Wang Yi talks about US's plan to deploy THAAD missile defense system in ROK. Retrieved January 28, 2019, from Ministry of Foreign Affairs of the People's Republic of China website: https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1340525.shtml

Prendergast, C. (1999). The provision of incentives in firms. *Journal of Economic Literature*, *37*(1), 7–63.

Qin, J., Zhou, Y., Reid, E., Lai, G., & Chen, H. (2007). Analyzing terror campaigns on the internet: Technical sophistication, content richness, and web interactivity. *International Journal of Human-Computer Studies*, *65*(1), 71–84.

Ranger, S. (2018, April 27). This giant cyber defence exercise has teams defending power grids, 4g networks, drones from hacker attack. *ZDNet*. Retrieved from https://www.zdnet.com/article/this-giant-cyber-defence-exercise-has-teams-defending-power-grids-4g-networks-and-drones-from-hacker/

Raud, M. (2016). *China and cyber: Attitudes, strategies, organisation*. Tallinn, Estonia: NATO CCD COE.

Rid, T. (2013a). *Cyber war will not take place*. London, UK: Hurst & Company.

Rid, T. (2013b). Cyberwar and Peace: Hacking Can Reduce Real-World Violence. *Foreign Affairs*, *92*(6), 77–87.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *The Journal of Strategic Studies*, *38*(1–2), 4–37.

RiskBased Security. (2014, December 5). A breakdown and analysis of the December 2014 Sony hack. Retrieved December 10, 2017, from RiskBased Security website: https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/#thebeginning

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

Rodong Sinmun, Joson Inmingun, & Chongnyon Jonwi. (1999, January 1). The 1999 new year common editorial. *Korean Central News Agency*. (Korean)

Rodong Sinmun, Joson Inmingun, & Chongnyon Jonwi. (2000, January 1). The 2000 new year common editorial. *Korean Central News Agency*. (Korean)

Rodong Sinmun, & Rodongja Sinmun. (1998, September 17). Keep our self-reliant national economy stance to the end. *Korean Central News Agency*. (Korean)

ROK Military Reform Committee. (2005). *Summary of military reform plan 2020*. Seoul: Korea: ROK Ministry of Defense.

ROK Ministry of Foreign Affairs. (2013, October 16). The 2013 Global Conference on Cyberspace. Retrieved February 22, 2019, from ROK Ministry of Foreign Affairs website: http://www.mofa.go.kr/www/brd/m_4080/view.do?seq=347551&srchFr=&amp%3BsrchTo=&amp%3BsrchWord=&amp%3BsrchTp=&amp%3Bmulti_itm_seq=0&amp%3Bitm_seq_1=0&amp%3Bitm_seq_2=0&amp%3Bcompany_cd=&amp%3Bcompany_nm=&page=527 (Korean)

ROK Ministry of Foreign Affairs. (2018, June 21). The 5th U.S.-Republic of Korea Bilateral Cyber Consultations. Retrieved February 20, 2019, from ROK Government 24 website: https://www.gov.kr/portal/ntnadmNews/1501654 (Korean)

ROK Ministry of Unification. (2004, March 23). *The weekly North Korea, Vol. 686*. Retrieved from http://nkinfo.unikorea.go.kr/nkp/trend/viewTrend.do?diaryId=8754&trendMenuId=ECNMYISS (Korean)

ROK Ministry of Unification. (2009, April). Monthly report on North Korea. *ROK Ministry of Unification*. (Korean)

ROK Ministry of Unification. (n.d.-a). Kim Jong Un's public events. Retrieved from The Portal about the Information on North Korea website: http://nkinfo.unikorea.go.kr/nkp/trend/publicEvent.do (Korean)

ROK Ministry of Unification. (n.d.-b). North Korea: Education systems. Retrieved April 3, 2018, from The Information Portal on North Korea website: http://nkinfo.unikorea.go.kr/nkp/overview/nkOverview.do?sumryMenuId=CL400 (Korean)

ROK Ministry of Unification. (n.d.-c). North Korea: Juche ideology. Retrieved February 18, 2019, from The Information Portal on North Korea website: http://nkinfo.unikorea.go.kr/nkp/overview/nkOverview.do?sumryMenuId=PO001 (Korean)

ROK Ministry of Unification. (n.d.-d). North Korea: Military policy. Retrieved February 18, 2019, from The Information Portal on North Korea website: http://nkinfo.unikorea.go.kr/nkp/overview/nkOverview.do?sumryMenuId=MENU_17 (Korean)

ROK Ministry of Unification. (n.d.-e). North Korea: Residential control. Retrieved November 6, 2018, from The Information Portal on North Korea website: http://nkinfo.unikorea.go.kr/nkp/overview/nkOverview.do?sumryMenuId=SO304 (Korean)

ROK Unification IT Forum. (2015). *A Study on the long-term policy for South and North Korea's IT cooperation* (No. 2015–05; pp. 1–268). Naju, Korea: Korea Communications Agency. (Korean)

ROK MND (Ministry of National Defense). (2008). *The 2008 defense white paper*. Seoul, Korea: The ROK Ministry of National Defense.

ROK MND. (2009, June). *The defense reform 2020*. ROK Ministry of National Defense. (Korean)

ROK MND. (2010). *The 2010 defense white paper*. Seoul, Korea: ROK Ministry of National Defense.

ROK MND. (2011, October 18). In 2012, defense informatization budget will be increased. Retrieved February 25, 2019, from ROK Policy Briefings website: http://www.korea.kr/briefing/pressReleaseView.do?newsId=155789263&pageIndex=3487&repCodeType=&repCode=&startDate=2008-02-29&2018-11-19&srchWord= (Korean)

ROK MND. (2012). *The 2012 defense white paper*. Seoul, Korea: ROK Ministry of National Defense.

ROK MND. (2014a). *The 2014 defense white paper*. Seoul, Korea: ROK Ministry of National Defense.

ROK MND. (2014b, February 7). The 1st U.S.- ROK Cyber Cooperation Working Group. Retrieved February 21, 2019, from ROK Government 24 website: https://www.gov.kr/portal/ntnadmNews/61089 (Korean)

ROK MND. (2014c, September 18). The outcome of the 6th Korea-U.S. Integrated Defense Dialogue. Retrieved April 27, 2019, from ROK Policy Briefings website: http://www.korea.kr/policy/pressReleaseView.do?newsId=155993718 (Korean)

ROK MND. (2015, October 29). The 3rd U.S.- ROK Cyber Cooperation Working Group. Retrieved February 21, 2019, from ROK Policy Briefings website: http://www.korea.kr/briefing/pressReleaseView.do?newsId=156082384 (Korean)

ROK MND. (2016). *The 2016 defense white paper*. Seoul, Korea: ROK Ministry of National Defense.

ROK MND. (2017, September 5). Enforcement Decree of Cyber Command Act. Retrieved December 20, 2018, from ROK National Law Information Center website: http://www.law.go.kr/LSW/lsEfInfoP.do?lsiSeq=197233# (Korean)

ROK MND. (2018a). *The 2018 defense white paper*. Seoul, Korea: ROK Ministry of National Defense. (Korean)

ROK MND. (2018b, September 4). The 7th Seoul Defense Dialogue (SDD) to be held from September 12th to 14th. Retrieved January 24, 2019, from Government 24 website: https://www.gov.kr/portal/ntnadmNews/1587852

ROK MND. (2018c, September 13). The 2018 Cyber Working Group, Seoul Defense Dialogue 2018, was held. Retrieved February 22, 2019, from Government 24 website: https://www.gov.kr/portal/ntnadmNews/1597272 (Korean)

ROK MND. (2018d, December 13). FY 2019 Military Expenditure based on Military reform 2.0. Retrieved June 2, 2019, from ROK Policy Briefings website: http://www.korea.kr/news/policyNewsView.do?newsId=148856341&pWise=mMain&pWiseMain=G1 (Korean)

ROK NDC (National Defense Committee). (2008, November 21). *Fiscal Year 2009 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2009, November 23). *Fiscal Year 2010 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2010, December). *Fiscal Year 2011 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2011, November). *Fiscal Year 2012 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2012, November). *Fiscal Year 2013 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2013, December). *Fiscal Year 2014 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2014, November). *Fiscal Year 2015 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2015, October). *Fiscal Year 2016 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2016, November). *Fiscal Year 2017 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2017, November). *Fiscal Year 2018 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NDC. (2018, November). *Fiscal Year 2019 ROK National Defense Committee Budget Report*. ROK National Assembly. (Korean)

ROK NIS. (2013, September 2). The national cyber security management regulation. Retrieved February 20, 2019, from ROK National Law Information Center website:

http://www.law.go.kr/%ED%96%89%EC%A0%95%EA%B7%9C%EC%B9%99/%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EC%A0%84%EA%B4%80%EB%A6%AC%EA%B7%9C%EC%A0%95 (Korean)

Ross, S. A. (1973). The economic theory of agency: The principal's problem. *The American Economic Review*, *63*(2), 134–139.

Roth, A. (2015, May 8). Russia and China sign cooperation pacts. *The New York Times*. Retrieved from https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html

Salehyan, I. (2010). The delegation of war to rebel organizations. *Journal of Conflict Resolution*, *54*(3), 493–515.

Sanger, D. E., Kirkpatrick, D. D., & Perlroth, N. (2017, October 15). The world once laughed at North Korean cyberpower. No More. *The New York Times*. Retrieved from https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

Sanger, D. E., & Schmidt, M. S. (2015, January 2). More sanctions on North Korea after Sony case. *The New York Times*. Retrieved from https://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html

Sarkees, M. R., & Schafer, P. (2000). The correlates of war data on war: An update to 1997. *Conflict Management and Peace Science*, *18*(1), 123–144.

Schmitt, B. E. (1924). Triple alliance and triple entente, 1902–1914. *The American Historical Review*, *29*(3), 449–473.

Schmitt, M. N., & Vihul, L. (2014). Proxy wars in cyberspace: The evolving international law of attribution. *Fletcher Security Review*, *I*(II), 54–73.

Scobell, A., & Sanford, J. M. (2007). *North Korea's military threat: Pyongyang's conventional forces, weapons of mass destruction, and ballistic missiles*. Carlisle, PA: Strategic Studies Institute (U.S. Army War College).

Scott Williams's teaching experience at Pyongyang University of Science and Technology (D. Park & S. Williams, Interviewer) [Personal Interview]. (2017, March 6).

Seo, S.-Y. (2016). North Korea's mobile communications market: Mobile phones and tablet PCs. *ICT & Media Policy*, *28*(11), 16-26. (Korean)

Shalal, A. (2016, June 16). Massive cyber attack could trigger NATO response: Stoltenberg. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-nato-idUSKCN0Z12NE

Shanghai Cooperation Organisation. (n.d.). Retrieved February 22, 2019, from Shanghai Cooperation Organisation website: http://eng.sectsco.org/

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, *40*(7), 1–29.

Sherstobitoff, R., Itai Liba, M., & Walter, J. (2013). *Dissecting operation troy: Cyberespionage in South Korea*. Retrieved from McAfee website: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf

Shields, N. P. Criminal complaint against Park Jin Hyok., Nathan P. Shields, Special Agent, FBI (United States District Court for the Central District of California 2018).

Shim, E. (2015, October 20). Spy agency: North Korea hackers stole sensitive South Korean data. *UPI*. Retrieved from https://www.upi.com/Top_News/World-News/2015/10/20/Spy-agency-North-Korea-hackers-stole-sensitive-South-Korean-data/9041445353950/

Shin, C. G., & Lee, S. (2013). A study of countermeasure and strategy analysis on North Korean cyber terror. *The Journal of Police Science*, *13*(4), 201–226. (Korean)

Shin, Gi-Lim. (2015, June 1). The U.S. provides cyber umbrella for Japan. *News1*. Retrieved from http://news1.kr/articles/?2258629 (Korean)

Shin, Hyo-Sook. (2015). North Korea's education system. *Forum for Korean Contemporary History*, *6*, 10–29. (Korean)

Shin, Hye-Kwon. (2013, September 26). The budget for informatization will be 515.4 billion won for the next year. *The Electronic Times*. Retrieved from http://ciobiz.etnews.com/news/article.html?id=20130926120017 (Korean)

Shin, Hye-Kwon. (2015, June 21). The budget for informatization in 2016 will be increased to 551.3 billion won. *The Electronic Times*. Retrieved from http://ciobiz.etnews.com/news/article.html?id=20150619120019 (Korean)

Shin, Hyonhee. (2018, August 20). As food crisis threatens, humanitarian aid for North Korea grinds to a halt. *Reuters*. Retrieved from https://www.reuters.com/article/us-northkorea-usa-aid-insight/as-food-crisis-threatens-humanitarian-aid-for-north-korea-grinds-to-a-halt-idUSKCN1L529H

Shin, J. (2016). International responses against North Korea`s cyber attacks. *The Korean Journal of Unification Affairs*, *28*(2), 61–90. (Korean)

Shin, Jong-Hwan. (2013, September). Major internet incidents in South Korea. *Internet & Security Focus*, 36–53. (Korean)

Shinkman, P. D. (2016, September 29). America is losing the cyber war. *US News & World Report*. Retrieved from https://www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries

Siboni, G., & Siman-Tov, D. (2014). *Cyberspace extortion: North Korea versus the United States* (No. 646; pp. 1–3). The Institute for National Security Studies.

Sigholm, J. (2013). Non-state Actors in Cyberspace Operations. *Journal of Military Studies*, *4*(1), 1–36.

SIPRI. (n.d.). SIPRI military expenditure database. Retrieved February 18, 2019, from Stockholm International Peace Research Institute website: https://www.sipri.org/databases/milex

Small, M., & Singer, J. D. (1969). Formal alliances, 1816–1965: An extension of the basic data. *Journal of Peace Research*, *6*(3), 257–282.

Snyder, G. H. (1984). The security dilemma in alliance politics. *World Politics*, *36*(4), 461–495.

Snyder, G. H. (1997). *Alliance Politics*. Ithaca, NY: Cornell University Press.

Song, K.-J. (2005). *IT education in North Korea* (MA Thesis). Retrieved from Korean Research Information Sharing Service. (Chonbuk National University). (Korean)

Song, U., & Lee, Y. (2014, December 27). "John" who attacked banks last year is back to the KHNP Hack. *JTBC News*. Retrieved from http://news.jtbc.joins.com/article/article.aspx?news_id=NB10698657 (Korean)

Sparkes, M. (2014, February 5). *North Korean computers get "Apple" makeover*. Retrieved from https://www.telegraph.co.uk/technology/apple/10619703/North-Korean-computers-get-Apple-makeover.html

StatCounter. (2018a, May). Desktop vs mobile vs tablet market share worldwide. Retrieved July 10, 2018, from StatCounter: Global Stats website: http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide

StatCounter. (2018b, May). Operating system market share Democratic People's Republic of Korea: May 2017 - May 2018. Retrieved June 27, 2018, from StatCounter: GlobalStats website: http://gs.statcounter.com/os-market-share/all/north-korea

Stimmekoreas. (2013). *Kim Jong Un goes around newly built Unha Scientists Street* [Video file]. Retrieved from https://www.youtube.com/watch?v=-M7O-R0b1Mc (Korean)

Stinissen, J. (2015). A legal framework for cyber operations in Ukraine. In K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine*. Tallinn, Estonia: NATO CCD COE.

Strom, D. (2018, September 25). The Sony hacker indictment: 5 lessons for IT security. Retrieved January 8, 2019, from CSO Online website: https://www.csoonline.com/article/3305144/hacking/the-sony-hacker-indictment-5-lessons-for-it-security.html

Sung, Ho-Cheol. (2015, July 24). South Korea-the U.S. do not have cyber alliance. *The Chosun Ilbo*. Retrieved from http://premium.chosun.com/site/data/html_dir/2015/07/24/2015072400368.html (Korean)

Sung, Ki-Noh. (2017, February 16). The north spreads groundless rumors. *Boannews*. Retrieved from https://www.boannews.com/media/view.asp?idx=53481 (Korean)

Support the training program for computer gifted students: In a program development class of the Guemseong Number One Secondary School. (2008, May 8). *The Kyoyuk Sinmun*. (Korean)

Swaine, M. D. (2017). Chinese views on South Korea's deployment of THAAD. *China Leadership Monitor*, 52, 1–15.

Symantec. (2013). *Symantec intelligence report (June 2013)*. Retrieved from Symantec website: https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_06-2013.en-us.pdf

Symantec. (2016, September 30). What is the difference between viruses, worms, and Trojans? Retrieved April 8, 2018, from Technical Support website: https://support.symantec.com/en_US/article.TECH98539.html

Symantec Security Response. (2009, July 9). Born on the 4th of July. Retrieved May 7, 2018, from Symantec Security Response website: http://www.symantec.com/connect/blogs/born-4th-july

Symantec Security Response. (2013, June 26). Four years of DarkSeoul cyberattacks against South Korea continue on anniversary of Korean War. Retrieved March 28, 2018, from

Symantec Security Response website: http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war

Symantec Security Response. (2016a, February 24). Collaborative operation blockbuster aims to send Lazarus back to the dead. Retrieved April 3, 2018, from Symantec Security Response website: http://www.symantec.com/connect/blogs/collaborative-operation-blockbuster-aims-send-lazarus-back-dead

Symantec Security Response. (2016b, May 26). SWIFT attackers' malware linked to more financial attacks. Retrieved April 3, 2018, from Symantec Security Response website: http://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

Symantec Security Response. (2017a, February 12). Attackers target dozens of global banks with new malware. Retrieved April 3, 2018, from Symantec Security Response website: http://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware

Symantec Security Response. (2017b, May 22). WannaCry: Ransomware attacks show strong links to Lazarus Group. Retrieved from Symantec Security Response website: https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group

Talmadge, E. (2017, June 12). North Korea, cyberattacks and "Lazarus": What we really know. Retrieved December 12, 2017, from Novetta website: http://www.novetta.com/2017/06/north-korea-cyberattacks-and-lazarus-what-we-really-know/

Tang, S. (2009). The security dilemma: A conceptual analysis. *Security Studies*, *18*(3), 587–623.

Tarakanov, D. (2013, September 11). The "Kimsuky" operation: A North Korean APT? Retrieved April 2, 2018, from Securelist - Kaspersky Lab's cyberthreat research and reports website: https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/

Taylor, A. (2017, October 2). North Korea appears to have a new internet connection — thanks to the help of a state-owned Russian firm. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2017/10/02/north-korea-appears-to-have-a-new-internet-connection-thanks-to-the-help-of-a-state-owned-russian-firm/

Taylor, A. (2018, March 24). Russia wants to build a bridge to North Korea. Literally. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/worldviews/wp/2018/03/24/russia-wants-to-build-a-bridge-to-north-korea-literally/?noredirect=on&utm_term=.ff010067581d

Taylor, P. (2013). *The Thirty-Six Stratagems: A modern-day interpretation of a strategy classic*. Oxford, UK: Infinite Ideas.

Thachuk, K. (2005). Corruption and international security. *SAIS Review*, *25*(1), 143–152.

The 2012 Seoul Nuclear Security Summit. (2012, March). *The Seoul Communique of the 2012 Seoul Nuclear Security Summit*. Retrieved from http://overseas.mofa.go.kr/ch-geneva-ko/brd/m_8850/view.do?seq=916144&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=7

The Economist Intelligence Unit. (2006). *Country report: North Korea*. London, UK.

The Internet Assigned Numbers Authority. (n.d.). *IANA report on the relegation of the .KP top-level domain.* Retrieved July 12, 2018, from The Internet Assigned Numbers Authority (IANA) website: https://www.iana.org/reports/2007/kp-report-11sep2007.html

The Office for Government Policy Coordination. (2016a, December 12). ROK government, the national cybersecurity policy coordination meeting. Retrieved February 20, 2019, from ROK Policy Briefings website: http://www.korea.kr/news/policyNewsView.do?newsId=148825995 (Korean)

The Office for Government Policy Coordination. (2016b, December 12). The national cybersecurity policy coordination meeting. Retrieved February 20, 2019, from ROK Policy Briefings website: http://www.korea.kr/policy/pressReleaseView.do?newsId=156172812 (Korean)

The Red Star TV. (n.d.). [Video file]. Retrieved April 22, 2019, from YouTube website: https://www.youtube.com/channel/UCJ7i-yFvuzn9FbUdU77WKcA

The Russian Government. (2015, April 30). *Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in ensuring international information security*. The Russian Government.

The Statistics on North Korea's GDP. (n.d.). Retrieved June 15, 2018, from The Bank of Korea website: /portal/main/contents.do?menuNo=200091 (Korean)

The U.S. National Intelligence Council. (2007). *Nonstate actors: Impact on international relations and implications for the United States* (No. DR-2007-16D). Office of the Director of National Intelligence.

The White House. (2015, January 2). Executive Order: Imposing additional sanctions with respect to North Korea. Retrieved April 2, 2018, from Office of the Press Secretary website: https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/executive-order-imposing-additional-sanctions-respect-north-korea

The White House. (2017a). *Briefing on the attribution of the WannaCry malware attack to North Korea* [Video file]. Retrieved from https://www.youtube.com/watch?v=pfqing4mbVI

The White House. (2017b, June 30). Joint statement between the United States and the Republic of Korea [Press release]. Retrieved January 22, 2019, from The White House website: https://www.whitehouse.gov/briefings-statements/joint-statement-united-states-republic-korea/

The World Bank. (n.d.-a). Military expenditure (% of GDP). Retrieved December 19, 2018, from The World Bank website: https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=KR

The World Bank. (n.d.-b). Population, total. Retrieved June 1, 2019, from The World Bank website: https://data.worldbank.org/indicator/SP.POP.TOTL?locations=KP

Tian, N., Fleurant, A., Kuimova, A., Wezeman, P. D., & Wezeman, S. T. (2018). *Trends in world military expenditure, 2017* (p. 8). Solna, Sweden: Stockholm International Peace Research Institute (SIPRI).

Towle, P. (1981). The strategy of war by proxy. *RUSI Journal*, *126*(1), 21–26.

Trend Micro Forward-Looking Threat Research Team. (2017, October 17). A closer look at North Korea's internet - TrendLabs security intelligence blog. Retrieved April 26, 2018, from TrendLabs Security Intelligence website: https://blog.trendmicro.com/trendlabs-security-intelligence/a-closer-look-at-north-koreas-internet/

Tzu, S. (2000). *The Art of War* (Vol. 14; L. Giles, Trans.).

Ugly person Kim Heung-Kwang in an academic scholar's skin. (2016). Retrieved from https://www.youtube.com/watch?v=74okdqX5D9k (Korean)

U.K. Foreign & Commonwealth Office. (2017, December 19). Foreign office minister condemns North Korean actor for WannaCry attacks. Retrieved April 3, 2018, from The U.K.

Government website: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

Ullah, Z. (2012). Early computer vs modern computer: A comparative study and an approach to advance computer. *Global Journal of Computer Science and Technology Interdisciplinary*, *12*(11), 1–15.

U.N. Documents for DPRK (North Korea). (n.d.). Retrieved January 15, 2019, from https://www.securitycouncilreport.org/un-documents/dprk-north-korea/

U.N. G.G.E. (n.d.). Retrieved January 23, 2019, from GIP Digital Watch website: https://public.tableau.com/shared/864K279C5?:embed=y&:showVizHome=no&:host_url=https%3A%2F%2Fpublic.tableau.com%2F&:embed_code_version=3&:toolbar=yes&:animate_transition=yes&:display_static_image=no&:display_spinner=no&:display_overlay=yes&:display_count=yes&:loadOrderID=0

United Nations International Telecommunication Union (ITU). (n.d.). Country ICT data (until 2016). Retrieved April 2, 2018, from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

United States Forces Korea. (2018, October 31). Joint communique of 50th U.S.-ROK Security Consultative Meeting. Retrieved January 22, 2019, from United States Forces Korea website: http://www.usfk.mil/Media/News/tabid/12660/Article/1679753/joint-communique-of-50th-us-rok-security-consultative-meeting.aspx

UNODA. (n.d.). Developments in the field of information and telecommunications in the context of international security. Retrieved December 27, 2018, from United Nations Office for Disarmament Affairs website: https://www.un.org/disarmament/topics/informationsecurity/

U.S. DHS. (2016). *Joint statement from the Department of Homeland Security and Office of the Director of National Intelligence on election security*. Retrieved from U.S. Department of Homeland Security website: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

U.S. DoD. (2011). *Cyberspace policy report*. Washington, D.C.: U.S. Department of Defense.

U.S. DoD. (2015a). *The DoD cyber strategy*. Washington, D.C.: The Department of Defense.

U.S. DoD. (2015b, April 15). The 7th Korea-U.S. Integrated Defense Dialogue (KIDD), Washington, D.C. Retrieved February 21, 2019, from U.S. Department of Defense website:

https://dod.defense.gov/News/News-Releases/News-Release-View/Article/605461/the-7th-korea-us-integrated-defense-dialogue-kidd-washington-dc/

U.S. DoD. (2018a, March 20). *13th Korea-U.S. integrated defense dialogue joint press statement* [Press release]. Retrieved February 21, 2019, from U.S. Department of Defense website: https://media.defense.gov/2018/Mar/20/2001892577/-1/-1/1/13th-Korea-U.S.-Integrated-Defense-Dialogue.PDF

U.S. DoD. (2018b, July 26*). Joint press statement for the 14th Korea-U.S. integrated defense dialogu*e [Press release]. Retrieved February 21, 2019, from U.S. Department of Defense website: https://media.defense.gov/2018/Jul/26/2001947071/-1/-1/1/JOINT%20PRESS%20STATEMENT%20FOR%20THE%2014TH%20KIDD.PDF

U.S. DoD. (2018c, July 26). U.S., South Korea conclude 14th integrated defense dialogue. Retrieved February 21, 2019, from U.S. Department of Defense website: https://dod.defense.gov/News/Article/Article/1585273/us-south-korea-conclude-14th-integrated-defense-dialogue/

U.S. Embassy in Korea. (2016, December 19). U.S.-ROK-Japan experts meeting on cybersecurity of critical infrastructure. Retrieved December 26, 2018, from U.S. Embassy in Korea website: https://kr.usembassy.gov/121916-u-s-rok-japan-experts-meeting-cybersecurity-critical-infrastructure/

US-CERT. (n.d.). HIDDEN COBRA - North Korean malicious cyber activity [US-CERT]. Retrieved from https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity

USCYBERCOM Public Affairs. (2018, May 17). Cyber mission force achieves full operational capability. Retrieved February 4, 2019, from U.S. Cyber Command website: https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.

von Clausewitz, C. (2007). *On war* (M. Howard & P. Paret, Trans.). New York, NY: Oxford University Press.

Wagstaff, J., Auchard, E., & Kiselyova, M. (2017, October 2). Russian firm provides new internet connection to North Korea. *Reuters*. Retrieved from

https://www.reuters.com/article/us-nkorea-internet/russian-firm-appears-to-be-offering-internet-connection-to-north-korea-38-north-idUSKCN1C70D2

Walt, S. M. (1987). *The origins of alliances*. Ithaca, NY: Cornell University Press.

Waltz, K. N. (1979). *Theory of international politics*. Reading, MA: Addison-Wesley Publishing Company.

Walzer, M. (2006). *Just and unjust wars: A moral argument with historical illustrations* (4th ed). New York, NY: Basic Books.

Warf, B. (2015). The hermit kingdom in cyberspace: Unveiling the North Korean internet. *Information, Communication & Society*, *18*(1), 109–120.

Wawro, G. (2014). *A mad catastrophe: The outbreak of World War I and the collapse of the Habsburg Empire*. New York, NY: Basic Books.

We aim to train world best students: computer gifted students studying with kid's artists. (2001, May 7). *The Choson Sinbo*. (Korean)

Weber, M. (1919). *Politics as a vocation* [Lecture script].

Weedon, J. (2015). Beyond "cyber war": Russia's use of strategic cyber espionage and information operations in Ukraine. In K. Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (pp. 123–134). Tallinn, Estonia: NATO CCD COE.

Wellman, D. A. (1989). *A chip in the curtain: computer technology in the Soviet Union*. Washington, D.C.: National Defense University.

Wesley, J. J. (2010, April). *Qualitative document analysis in political science*. 1–15. Retrieved from https://www.poltext.org/sites/poltext.org/files/p2wesley._09102010_131253.pdf

Westad, O. A. (2005). *The global cold war: Third world interventions and the making of our times*. New York, NY: Cambridge University Press.

While the 20th century is the age of the machine industry, the 21st century is the age of the information and communication industry. (2001, April 22). *Rodong Sinmun*. (Korean)

Wilford, G. (2017, May 21). North Korea hackers have been linked to NHS cyber attack. *The Independent*. Retrieved from http://www.independent.co.uk/news/world/asia/nhs-ransomware-wannacry-north-korea-hackers-cyber-attack-us-south-korea-a7747826.html

Williams, M. (2010, June 10). North Korea moves quietly onto the internet. *Computerworld*. Retrieved from https://www.computerworld.com/article/2518914/enterprise-applications/north-korea-moves-quietly-onto-the-internet.html

Williams, M. (2011, May 3). Dot KP domain assigned to Star. Retrieved April 25, 2018, from North Korea Tech website: https://www.northkoreatech.org/2011/05/03/dot-kp-domain-assigned-to-star/

Williams, M. (2013, August 12). Kim Jong Un visits "cell phone factory." *North Korea Tech*. Retrieved from https://www.northkoreatech.org/2013/08/12/kim-jong-un-visits-cell-phone-factory/

Williams, M. (2014, January 31). North Korea's red star OS goes Mac. *North Korea Tech*. Retrieved from https://www.northkoreatech.org/2014/01/31/north-koreas-red-star-os-goes-mac/

Williams, M. (2017, October 1). Russia provides new internet connection to North Korea. Retrieved from 38North website: http://www.38north.org/2017/10/mwilliams100117/

Wirtz, J. J. (2017). The Cyber Pearl Harbor. *Intelligence and National Security*, *32*(6), 758–767.

Won, Byung-Chul. (2018, July 27). The Blue House eliminates the Cybersecurity Secretary. *Boannews*. Retrieved from http://www.boannews.com/media/view.asp?idx=71783 (Korean)

Yang, Sae-Rom. (2016, December 6). North Korea breached the intranet of the South Korean military, why? *News1*. Retrieved from http://news1.kr/articles/?2850456 (Korean)

Yi, S.-K., Sin, H.-Y., & Heo, E. (2011). Selecting sustainable renewable energy source for energy assistance to North Korea. *Renewable and Sustainable Energy Reviews*, *15*(1), 554–563.

Yonhap News Agency. (2016, March 18). Kim Jong-un orders construction of another scientists' street in Pyongyang. *Yonhap News Agency*. Retrieved from http://english.yonhapnews.co.kr/news/2016/03/18/0200000000AEN20160318003700315.html

Yoo, Ji-hye. (2014, December 27). Whether cyberattacks violate UN Charter or not will be discussed. *The JoongAng Ilbo*. Retrieved from https://news.joins.com/article/16794023 (Korean)

Yoo, Ji-yong, & Lee, K. (2013, July 15). Cybersecurity international cooperation and South Korea's policy orientation. *KIDA Defense Weekly*, *1471*, 1–8. (Korean)

Yoo, S., & Ko, J. (2004). *A study on the digital divide between Two Koreas: A better way to reduce the gap to prepare for reunification* (No. 04–05; pp. 1–128). Seoul, Korea: Korea Agency for Digital Opportunity and Promotion. (Korean)

Yoon, H., & Ko, K. (2011). The cooperative situation and prospects on mobile service in North-South Korea. *Journal of Global Politics*, *4*(2), 7–41. (Korean)

Yoon, K. (2011). North Korea's cyber warfare: The capability and threat. *Military Forum*, *68*, 64–95. (Korean)

Yoon, Sangwon. (2011, June 20). North Korea recruits hackers at school. *AlJazeera*. Retrieved from https://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html

Yoon, Seoyeon. (2015). South Korea's wartime operational control transfer debate: From an organizational perspective. *Journal of International and Area Studies*, *22*(2), 89–108.

Young heroes for the information age are growing: Visiting the Pyongyang Students and Children's Palace. (2001, May 10). *The Kyowon Sinmun*. (Korean)

YTN News. (2013). *North Korea showed its first smartphone, "Arirang"* [Video file]. Retrieved from https://www.youtube.com/watch?v=neCeEk_LYzM (Korean)

Yu, Suk Ryul. (1987). Soviet-North Korean relations and security on the Korean Peninsula. *Asian Perspective*, *11*(1), 74–101.

Zaidi, W. (2018). Liberal internationalism and the search for international peace. In C. P. Peterson, W. M. Knoblauch, & M. Loadenthal (Eds.), *The Routledge History of World Peace Since 1750* (1st ed., pp. 59–69).

Zeller Jr., T. (2006, October 23). The internet black hole that is North Korea. *The New York Times*. Retrieved from https://www.nytimes.com/2006/10/23/technology/23link.html

Zhang, W., Johnson, T. J., Seltzer, T., & Bichard, S. L. (2010). The revolution will be networked: The influence of social networking sites on political attitudes and behavior. *Social Science Computer Review*, *28*(1), 75–92.

Zhebin, A. (1995). Russia and North Korea: An emerging, uneasy partnership. *Asian Survey*, *35*(8), 726–739.

Zúñiga, H. G. de, Jung, N., & Valenzuela, S. (2012). Social media use for news and individuals' social capital, civic engagement and political participation. *Journal of Computer-Mediated Communication*, *17*(3), 319–336.

APPENDIX: YEARLY DEFENSE BUDGET COMPARISON OF ROK MILITARY

Year	Defense Budget (billion won)	Defense Budget-GDP Ratio (%)	Defense Budget-Government Finance Ratio (%)	Defense Budget Increase Rate (%)
1980	2,246.5	5.69	34.7	46.2
1981	2,697.9	5.47	33.6	20.1
1982	3,120.7	5.49	33.5	15.7
1983	3,274.1	4.85	31.4	4.9
1984	3,306.1	4.25	29.6	1.0
1985	3,689.2	4.23	29.4	11.6
1986	4,158.0	4.08	30.1	12.7
1987	4,745.4	3.95	29.6	14.1
1988	5,520.2	3.83	30.0	16.3
1989	6,014.8	3.68	27.3	9.0
1990	6,637.8	3.36	24.2	10.4
1991	7,476.4	3.13	23.8	12.6
1992	8,410.0	3.08	25.1	12.5
1993	9,215.4	2.97	24.2	9.6
1994	10,075.3	2.75	23.3	9.3
1995	11,074.3	2.58	21.4	9.9
1996	12,243.4	2.54	20.8	10.6
1997	13,786.5	2.60	20.7	12.6
1998	13,800.0	2.63	18.3	0.1
1999	13,749.0	2.38	16.4	-0.4
2000	14,477.4	2.28	16.3	5.3
2001	15,388.4	2.24	15.5	6.3
2002	16,364.0	2.15	14.9	6.3
2003	17,514.8	2.16	14.8	7.0
2004	18,941.2	2.16	15.8	8.1
2005	21,102.6	2.29	15.6	11.4
2006	22,512.9	2.33	15.3	6.7
2007	24,497.2	2.35	15.7	8.8
2008	26,649.0	2.41	14.8	8.8
2009	28,980.3	2.52	14.2	8.7
2010	29,562.7	2.34	14.7	2.0
2011	31,403.1	2.36	15.0	6.2
2012	32,957.6	2.39	14.8	5.0
2013	34,497.0	2.41	14.3	4.7
2014	35.705.6	2.40	14.4	3.5
2015	37,555.0	2.40	14.3	5.2
2016	38,842.1	2.37	13.9	3.4
2017	40,334.7	2.33	14.2	3.8
2018	43,158.1	2.38	14.3	7.0