2022-12

A STUDY ON EFFECTIVE COUNTERMEASURES AGAINST CYBER ATTACKS IN SOUTH KOREA

Do, Geunhyoung

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A STUDY ON EFFECTIVE COUNTERMEASURES AGAINST CYBER ATTACKS IN SOUTH KOREA

by

Geunhyoung Do

December 2022

Thesis Advisor:	Wade L. Huntley
Second Reader:	Robert J. Weiner

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
A STUDY ON EFFECTIVE COUNTERMEASURES AGAINST CYBER ATTACKS IN SOUTH KOREA

5. FUNDING NUMBERS

6. AUTHOR(S) Geunhyoung Do

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Based on U.S. cybersecurity policy, this thesis proposes effective countermeasures for the Republic of Korea (ROK) to prepare for, deter, and recover from cyber threats posed by North Korea. This study identifies the most dangerous North Korean cyber strikes facing South Korea by reviewing several cases of North Korean cyberattacks, the ROK's countermeasures, and the severity of the damage caused by the attacks. The study builds on the writings of academics and subject matter experts as well as publicly available government policy documents, although specifics on policy are limited due to national security concerns.

In addition, the study acknowledges how the cybersecurity paradigm has shifted as a result of U.S. planning, reaction to, and establishment of follow-up measures for an attack of a similar type by a cyber superpower. The strategy of deterring an opponent's operations based on the past has evolved into a strategy of preparing for enemy attacks through information sharing and preemptive defense measures, and counterattack by rapid recovery and identification of the enemy through resilience and with tracking technologies. Although the ROK is a country with well-developed information technology, its cybersecurity knowledge, systems, and technology remain weak in comparison to North Korea's abilities. Consequently, it is conceivable that the ROK can respond effectively to North Korea's cyber threats by applying the lessons learned from the United States.

14. SUBJECT TERMS cyber space, cybersecurity, cybersecurity capabilities of South Korea, cyber attack of North Korea, policy of United States cybersecurity, Republic of Korea, ROK	**15. NUMBER OF PAGES** 127
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A STUDY ON EFFECTIVE COUNTERMEASURES AGAINST CYBER ATTACKS IN SOUTH KOREA

Geunhyoung Do
Major, Republic of Korea Air Force
BA, Korea Airforce Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(EAST ASIA AND THE INDO-PACIFIC)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2022**

Approved by: Wade L. Huntley
Advisor

Robert J. Weiner
Second Reader

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Based on U.S. cybersecurity policy, this thesis proposes effective countermeasures for the Republic of Korea (ROK) to prepare for, deter, and recover from cyber threats posed by North Korea. This study identifies the most dangerous North Korean cyber strikes facing South Korea by reviewing several cases of North Korean cyberattacks, the ROK's countermeasures, and the severity of the damage caused by the attacks. The study builds on the writings of academics and subject matter experts as well as publicly available government policy documents, although specifics on policy are limited due to national security concerns.

In addition, the study acknowledges how the cybersecurity paradigm has shifted as a result of U.S. planning, reaction to, and establishment of follow-up measures for an attack of a similar type by a cyber superpower. The strategy of deterring an opponent's operations based on the past has evolved into a strategy of preparing for enemy attacks through information sharing and preemptive defense measures, and counterattack by rapid recovery and identification of the enemy through resilience and with tracking technologies. Although the ROK is a country with well-developed information technology, its cybersecurity knowledge, systems, and technology remain weak in comparison to North Korea's abilities. Consequently, it is conceivable that the ROK can respond effectively to North Korea's cyber threats by applying the lessons learned from the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AML	Anti-Money Laundering
APT	Advanced Persistent Threats
ASEC	AhnLab Security Emergency-response Center
CCDCOE	Cooperative Cyber Defense Center of Excellence
CFT	Countering the Financing of Terrorism
CRI	International Counter Ransomware Initiative
CSA	Cybersecurity Act
CS&C	Office of Cybersecurity and Communications
C-TAS	Cyber Threat Analysis and Sharing
DCI	Defense Critical Infrastructure
DDoS	Distributed Denial of Service
DIB	Defense Industrial Base
DHS	Department of Homeland Security
DNC	Democratic National Committee
DNI	Director of National Intelligence
DOD	Department of Defense
ESG	Election Security Group
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FT	Free Trade Agreement
GCI	National Global Cybersecurity Index
GEC	Global Engagement Center
IC	Intelligence Community
ICBM	Intercontinental Ballistic Missile
ICT	Information and Communication Technology
IRA	Russian Internet Research Agency
ISA	Infrastructure Security Agency
ITU	International Telecommunications Union
JAR	Joint Analysis Report
KAERI	Korea Atomic Energy Research Institute

KAI	Korea Aerospace Industries
KCC	Korea Communications Commission
KCTI	Korea Cyber Threat Intelligence
KF-X	Korean fighter eXperimental
KISA	Korea Internet & Security Agency
KIST	Korea Institute of Science and Technology
KnCERT/CC	Korean Computer Emergency Response Team/Coordination Center
KYC	Know Your Customer
NATO	North Atlantic Treaty Organization
NCCIC	National Cybersecurity and Communications Integration Center
NCET	National Cryptocurrency Enforcement Team
NCSC	National Cyber Security Center
NCTI	National Cyber Threat Intelligence
NIC	National Intelligence Council
NIS	National Intelligence Service
OECD	Organization for Economic Co-operation and Development
OSINT	Open-Source Intelligence
PIMS	Personal Information Management System
PPD	Presidential Policy Directive
RIS	Russian Intelligence Services
SEC	Securities and Exchange Commission
SWIFT	Worldwide Interbank Financial Telecommunications
TSA	Transportation Security Administration
UN GGE	UN Group of Government Experts
VPN	Virtual Private Network
USCYBERCOM	United States Cyber Command

ACKNOWLEDGMENTS

I would want to thank my beloved family first. My wife, Hye-min, assisted me in concentrating on my studies at NPS, as did my daughter, Yeon-woo (Elly), who did not weep and adapted well despite attending her first elementary school in the United States, and my son, Eun-woo, who was always cheerful. In addition, I respect my mother, In-sook, who nurtured me with all her heart and soul, and my father, who must be somewhere in the heavens looking over me. I am also grateful to my childhood pals, NCM, who have been a constant source of emotional support.

I would like to express my sincere gratitude to the Ministry of National Defense and the Korean Air Force for providing me with the opportunity to receive a quality education at the Naval Postgraduate School in the United States. Based on this experience, I will endeavor to contribute to the development of the Korean military.

Lastly, my thesis advisor, Wade Huntley, second reader, Robert Weiner, the GWC, the TPO, and the IGPO. I am grateful to everyone who assisted me in adjusting to life in the United States and assisted me greatly academically.

I genuinely hope that my thesis is not the end, but rather the beginning of something new.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MAJOR RESEARCH QUESTION

South Korea's information and communication technology (ICT) environment is the most well developed among the 40 Organization for Economic Co-operation and Development (OECD) countries, consolidating its status as an Internet powerhouse, but also making it a major target for cyberattacks.[1] In particular, South Korea is being subjected to various types of cyberattacks conducted by North Korea but is unable to respond effectively. North Korea's cyber threat has become a reality that risks South Korea's national security, and the cyber threats that North Korea is presenting confirm that they perceive cyberspace as a strategically important battlefield.[2] Due to the diversification of attack methods and changes in the cyber environment, the form of cyberattacks against South Korea is also gradually changing.

On the other hand, because the United States judged cybersecurity in the same context as the concept of national security early on, it quickly analyzed its adversaries' cyberattacks to identify U.S. vulnerabilities and supplemented them in various ways. As a result, the United States is leading the development of cybersecurity from the position of a superpower in the cyberspace as well as in the military and economic realms.[3]

Therefore, this thesis analyzes the cybersecurity policy developed by the United States to draw lessons for how the Republic of Korea (ROK) can adopt this policy to respond effectively to the cyber threat environment the ROK is facing. The research is

---

[1] Won-sun Cho, "Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues," *Defense Policy Research* 33, no. 2 (summer 2017): 146, https://www.kida.re.kr/frt/board/frtPolicyStudyBoardDetail.do?sidx=363&idx=903&depth=4&searchCondition=ITMVAL3&searchKeyword=117&groupbox=12&pageIndex=1.

[2] Eun-ju Park, "Increasing North Korean Cyber Security Threats and South Korea's Response," *Veteran's Journal* 19, no. 4 (2020): 19, https://doi.org/10.24004/tkafp.2020.19.4.001.

[3] Damien Van Puyvelde and Aaron Brantly, eds., U.S. *National Cybersecurity: International Politics, Concepts and Organization*, Routledge Studies in Conflict, Security and Technology (London ; New York: Routledge, Taylor & Francis Group, 2017), 3, https://doi.org/10.4324/9781315225623.

guided by three questions. Questions 1 and 2 are derived through analysis of the existing literature, and finally, the answer to question 3 is found through the results of that analysis.

1. What are the most dangerous North Korean cyberattack threats that South Korea faces right now? How has South Korea so far dealt with these threats?

2. How do current cyber threats aimed at South Korea compare to those that the United States has encountered? How did U.S. policies address these threats? How successful were these policies?

3. What effective countermeasures against cyberattacks can Korea derive from comparison with U.S. cybersecurity policy?

B. SIGNIFICANCE OF THE RESEARCH QUESTION

The term cybersecurity is difficult to define in one word because it is used so widely and its definitions vary widely, depend on the context, and are often subjective.[4] However, no one can deny the importance of cyber security, and the fact that it is directly related to national security is supported by various examples. In the 21st century, as many governments, businesses, and daily activities around the world go online, cybersecurity has become more important.[5] Vulnerability to cyberattacks paralyzes governments, businesses and day-to-day activities, and ultimately affects national security.

The U.S. cyber security policy started as a simple information security problem in the 1980s, and then developed into the concept of cyber security in the 1990s. In the 2000s, cybersecurity was ultimately elevated as a national security issue due to the development of national and social networks following the spread of the high-speed Internet and the aftermath of the 9/11 terrorist attacks. Since then, cybersecurity targets, approaches, and strategies have been steadily expanded and developed, and recently, a comprehensive and aggressive national cybersecurity strategy inspired by the Cold War strategy has been

[4] Dan Craigen, Nadia Diakun-Thibault, and Randy Purse, "Defining Cybersecurity," *Technology Innovation Management Review* 4, no. 10 (October 2014): 13, https://doi.org/10.22215/timreview/835.

[5] Michael Veale and Ian Brown, "Cybersecurity," *Internet Policy Review* 9, no. 4 (December 17, 2020): 2, https://doi.org/10.14763/2020.4.1533.

adopted and implemented.[6] This preemptive policy has deterred cyberattack actors and has had positive results in reducing distributed denial of service (DDoS) cyberattacks on the United States.[7]

South Korea's response is markedly different from that of the United States. North Korea recognized cyberspace as a space where wars take place and has established a policy in the direction of gaining an asymmetrical military advantage over South Korea through control over cyberspace.[8] In spite of this situation, the South Korean government is repeatedly victimized by North Korean cyberattacks of the same or similar form. North Korea has conducted attacks target not only government agencies, but also on private companies, critical infrastructure, and individuals, but there is no law that can comprehensively protect them. Efforts are being made to respond effectively with a lead agency as the center, but it has not been decided who will oversee the center and in what way.

Many Korean scholars are also stressing the importance of improving South Korea's cybersecurity capabilities. In the past, North Korea conducted cyberattacks for the purpose of extracting military information, but now the means and targets of cyberattacks from North Korea are gradually expanding to include the financial sector as a way to find alternative financial resources for nuclear development amid increasing international

[6] Jin-suk Byun, "The Development of the U.S. Cybersecurity Strategy: Historical Overview and Cyberspace Solarium Commission Report," *Peace Studies* 30, no. 1 (April 30, 2022): 43, https://doi.org/10.21051/PS.2022.04.30.1.41. In the introduction, the author referred to the development of cybersecurity in the United States during severe cyber threats for the past 20 years. In the 1980s, although rudimentary policy responses were started, the term cybersecurity began to appear in the 1990s with the development of the Internet. After the 9/11 terrorist attacks, cyber security was upgraded to the national security level, and now, comprehensive policies and strategies are presented for cyber security.

[7] Sumeet Kumar, Matthew Benigni, and Kathleen M. Carley, "The Impact of U.S. Cyber Policies on Cyber-Attacks Trend," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, 186, https://doi.org/10.1109/ISI.2016.7745464.

[8] Jae-hun Shin and Yong-hun Kim, "The Plan to Strengthen Cyber Security," *Korean Police Research* 15, no. 3 (2016): 86, https://doi.org/G704-001889.2016.15.3.005.

sanctions on North Korea.[9] With the development of South Korea's technological environment, the informatization of politics, the economy, and military affairs is spreading across the country, and all entities such as individuals, companies, organizations, and governments are expanding their activities into cyberspace beyond the real space.

Paradoxically, however, the ROK has become a major target for cyberattacks due to the development of informatization and the expansion of the scope of activity.[10] South Korea's exposure to cyberattack threats is never lower than that of other advanced countries, including the United States, and the main factor is that North Korea recognizes that hacking and cyber terrorism are effective means of attacking the ROK, which has a well-established information and communication infrastructure.[11]

In the rapidly changing world situation, South Korea is surrounded by many military powers and countries with excellent cyberattack capabilities. For the sake of national security, it is now a higher priority to strengthen the ROK's capacity to keep the cyberattack threat to the country at a controllable level. Since the cybersecurity field is a key element among non-military fields, a lot of time, money, and effort needs to be invested to develop the ability to control it.

To inform these needs, this thesis compares the policies of the United States, a powerful cyber security power, to South Korea's existing policies and capabilities. Drawing lessons from this comparison, the thesis aims to develop insights to help South Korea achieve cyber security capacity enhancement efficiently within a short period through the development and implementation of effective policies.

---

[9] Yung-do Kim, Jin-sung Kim, and Kyung-ho Lee, "Major Issues of the National Cyber Security System in South Korea, and Its Future Direction," *The Korean Journal of Defense Analysis* 25, no. 4 (2013): 436, https://doi.org/10.22883/kjda.2013.25.4.001.

[10] Park, "Increasing North Korean Cyber Security Threats and South Korea's Response," 16.

[11] Cho, "Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues," 132.

C. LITERATURE REVIEW

This literature review focuses on the cybersecurity situation in the ROK. Many scholars have different opinions about the cybersecurity situation and capabilities facing South Korea. Hence, it is easier to understand the capabilities of South Korea by classifying them according to several categories and listing the evaluations. Moreover, since each scholar has a different opinion on the same area, this review can find the areas where research needs to proceed. The first part is the evaluation of what scholars have written about Korea's cybersecurity capabilities and the second part lists the lessons scholars argue can be learned from the United States.

1. South Korea's Cybersecurity Capabilities

This section is broadly classified into six categories: Awareness of cyber security, laws and institutions, integration and control agencies, limitations of technology and resources, international cooperation system, and political situation. Various opinions of scholars on this topic were synthesized.

a. Awareness of Cybersecurity

Jung-mi Cha analyzed that although cybersecurity issues are being raised as major national security issues, analysis and perspectives on the cybersecurity situation surrounding the Korean Peninsula are not being made. She insisted that there is still a lack of concrete discussions and alternatives about what kind of cyber threats South Korea faces and in what direction cyber security needs to be strengthened.[12] Kwan Choi and Min-ji Kim mentioned that, although the level of awareness of cyber terrorism in the ROK is similar to that of other major powers, it has not established a national response strategy to support it. The South Korean government maintains a passive attitude in the cybersecurity

[12] Jung-mi Cha, "Cyber Arms Race between U.S. and China and the Rise of North Korean Threat in Cyber Space: Implications for South Korea's Cyber Security," *Unification Research* 23, no. 1 (2019): 81–82.

field and does not have the ability to respond promptly and quickly.[13] Tae-jin Chung and Guang-meen Rhee pointed out that there is no law that can impose sanctions on North Korea, leaving South Korea helpless to respond to an attack on virtual currency. This shows that the South Korean government's awareness of cyber security is still a bit slow.[14]

On the other hand, there is an opinion that it is starting to be recognized as a security issue due to the continuous cyberattacks. Ho-geun Yoo and Gyoo-sang Seol argued that DDoS attacks in 2009 and 2011, cyber terrorism in 2013 and hacking incidents at Korea Hydro & Nuclear Power in 2014 became big social issues and raised awareness. As a result, the ROK government began to give importance to protecting systems from external attacks and further strengthening cybersecurity capabilities.[15] Also, there are opinions that policymakers are aware of the latest cybersecurity issues in situational awareness. According to Tom Leithauser's article, John Kerry, then-U.S. Secretary of State, said "Korea and the United States both recognize the Internet and cyber issues as part of a new frontier for government and people, and South Korea recognizes the importance of cybersecurity." [16] In addition, the U.S. Department of State emphasized in a statement that ROK and U.S. officials conducted cyber consultations, discussing key infrastructure, capacity building, information sharing, research and development, military-to-military cyber cooperation, cybercrime, international security issues in cyberspace, and current trends in the international cyber environment.[17]

---

[13] Kwan Choi and Min-ji Kim, "A Comparative Analysis of the National Defensive System Against Cyber Terrorism for National Security and Public Safety: Focus on the South Korea, America, and France," *The Journal of Police Policies* 29, no. 2 (October 2015): 28–29, https://doi.org/10.35147/KNPSI.2015.29.2.1.

[14] Tae-jin Chung and Guang-meen Rhee, "Legal response to foreign cyber attackers," *Korean Police Studies Review* 19, no. 1 (2020): 291, https://doi.org/10.16961/polips.2019.14.2.65.

[15] Ho-geun Yoo and Gyoo-sang Seol, "Cyber Security System: Issues of Governance Formation and Korea," *Journal of Korean Political And Diplomatic History* 38, no. 2 (2017): 253, https://doi.org/10.18206/kapdh.38.2.201703.237.

[16] Tom Leithauser, "KERRY SEEKS SOUTH KOREA's HELP IN PUSHING CYBERSPACE NORMS," *Cybersecurity Policy Report*, May 25, 2015, http://www.proquest.com/docview/1684453381/abstract/DD6A7BF8BFB64BDCPQ/1.

[17] "U.S., South Korea to Collaborate on Promoting Cyberspace Norms," *Cybersecurity Policy Report*, October 26, 2015, http://www.proquest.com/docview/1729336594/abstract/E1309A5AE6134335PQ/1.

b. Laws and Institutions

There were various opinions of many scholars regarding laws and institutions. Won-sun Cho asserted that South Korea does not even have the most basic legal system in place despite its excellent IT technology. She argued that a lack of law means a lack of agreement on who will have management and responsibility and traditional powers in the way the United States and China are establishing legal systems for systematic responses, but South Korea, one of the countries most frequently victimized by cyberattacks, has yet to come up with a law.[18] Jae-hun Shin and Yong-hun Kim said that, although South Korea has laws related to cyber security, laws such as the "National Cyber Security Management Regulation," "Information and Communications Network Act," and "Information and Communication Infrastructure Protection Act" are inconsistent and the duties of each department are scattered. They claimed that these laws make it difficult for South Korea to respond quickly.[19]

In addition, because the basis of laws related to the cyber terrorism response system is stipulated only by presidential decree, responsibility is unclear and binding is weak. In other words, it was judged that it would be difficult to effectively respond to laws dealing with cybersecurity due to lack of evidence. Seong-yeob Lee argued that in the case of South Korea, it is necessary to establish an integrated basic legal system that encompasses the public and private sectors. He claimed that the current cybersecurity legal system has problems in that related laws and regulations are diverse and scattered, and there is no unified organization in relation to their enforcement. So, he suggested that for the government and the private sector to work together to carry out systematic and unified cyberattack prevention and response tasks at the national level, enactment of an integrated law should be considered.[20]

---

[18] Cho, "Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues," 147–48.

[19] Shin and Kim, "The Plan to Strengthen Cyber Security," 88.

[20] Seong-yeob Lee, "Desirable direction for national cybersecurity legislation and governance: Focusing on the case of the United States and the implications of Korea," *Administrative Law Journal*, no. 67 (March 2022): 258, https://doi.org/10.35979/ALJ.2022.03.67.239.

On the other hand, Benjamin Gosnell Bartlett evaluated that the ROK government had established a robust cyber security system through active intervention and investment. In particular, he thought that the Korea Internet & Security Agency (KISA), established to promote network infrastructure and improve Korea's private sector cybersecurity, is taking a variety of measures to strengthen the public's cybersecurity. In addition to taking direct action to strengthen the cybersecurity of the public, they are also monitoring South Korean websites for malicious code. He argued that The Korea Communications Commission (KCC) also has a clear interest in promoting cybersecurity in the private sector. Specific technical, managerial, and physical measures are being implemented to ensure the protection of personal information online using the Personal Information Management System (PIMS) scheme.[21]

Also, Noh-Soon Chang gave a positive evaluation of the establishment of major strategic tasks and detailed action plans for each ministry through the "National Cyber Security Strategy" established for the first time in Korea in April 2019 and the "National Cyber Security Basic Plan" established in September.[22] In addition, Eun-ju Park evaluated that the "National Cyber Security Strategy" is a synthesis of the policy directions of related ministries to cope with security threats in cyberspace. South Korea's national cybersecurity strategy officially specified the adoption of a deterrent strategy, and it was believed that tactics and means were presented to ensure its effectiveness.[23] Do-kyung Kim and Soon-yang Kim argued that, starting with the "Information Promotion Act" of 1995, which was created to lay the foundation for South Korea's cyber security law, the "Cyber Security Act" was strengthened, and the "Electronic Financial Transactions Act" has been continuously revised in the changing cyber environment. Therefore, they suggested that

[21] Benjamin Gosnell Bartlett, "Institutional Determinants of Cyber Security Promotion Policies: Lessons from Japan, the U.S., and South Korea" (UC Berkeley, 2018), 31, https://escholarship.org/uc/item/02f4879m.

[22] Noh-Soon Chang, "Cybersecurity Threats, Response Strategies, and Korean Implications," *National Security and Strategy* 19, no. 2 (2019): 24, https://doi.org/10.23111/nsas.2019.19.2.001.

[23] Park, "Increasing North Korean Cyber Security Threats and South Korea's Response," 24.

South Korea has made an effort to implement consistent regulations according to changes in the cyber environment.[24]

c. Integration and Control Agencies

Yung-do Kim, Jin-sung Kim, and Kyung-ho Lee mentioned that it is impossible to rationalize the ROK's policies efficiently because Korea's cyber security system is distributed among various departments and its own organizations. In addition, since follow-up management to prevent recurrence is difficult due to such a distributed structure, those authors have insisted that comprehensive and preventive policy establishment is inevitably inefficient. They also pointed out that there is no centralized comprehensive information-sharing center capable of analyzing and distributing information on cyberattacks to the public, as well as the civilian and military sectors, and there is a lead agency to manage, supervise and command it.[25] Similarly, Do-kyung Kim and Soon-yang Kim mentioned the lack of cyber security governance in South Korea. They believed that a well-coordinated national cybersecurity governance was required to overcome South Korea's reliance on cyber infrastructure and the lack of infrastructure for cyber retribution, but they acknowledged that this was not feasible and that each agency was responsible for its own defense.[26]

However, Seong-yeob Lee evaluated South Korea's decentralized system differently. He believed that the centralized type is more likely to be a suitable option than the distributed kind for crisis response, given that cybersecurity work requires overall efficiency and uniformity. Nevertheless, he stated that a decentralized aspect of

[24] Do-kyung Kim and Soon-yang Kim, "Reframing South Korea's National Cybersecurity Governance System in Critical Information Infrastructure," *The Korean Journal of Defense Analysis* 33, no. 4 (December 2021): 696, https://doi.org/10.22883/KJDA.2021.33.4.007.

[25] Kim, Kim, and Lee, "Major Issues of the National Cyber Security System in South Korea, and Its Future Direction," 446.

[26] Kim and Kim, "Reframing South Korea's National Cybersecurity Governance System in Critical Information Infrastructure," 707–8.

cybersecurity may also be required, given that each department is responsible for physical security in its own sector of society.[27]

But James Andrew Lewis argued that cyber security in South Korea works organically well through the National Cyber Security Center (NCSC) under National Intelligence Service (NIS). The national cyber threat response team, comprised of the military and the commercial sector, bolsters the center during times of crisis, and the Korean Computer Emergency Response Team/Coordination Center (KnCERT/CC) administers public and private cyber crises, in his opinion. In addition, he argued that South Korea has its own assessment and certification system that promotes the use of certified and verified IT security products and systems and enhances the security level of national information and communications networks, thereby facilitating the sharing of information and the integration of security systems across departments.[28]

d. Technological and Resource Limitations

Jae-hun Shin and Yong-hun Kim pointed out that South Korea's cyber security infrastructure is insufficient to respond to cyberattacks, which are carried out by North Korea's huge asymmetric forces. In particular, the authors insisted that attacks on individuals due to the increase in the population of SNS users are also a big problem in cyber security, and there is a shortage of manpower to manage and supervise them.[29] Do-kyung Kim and Soon-yang Kim pointed out that despite the fact that the ROK government is continuously raising the national budget for cyber security and distributing more resources to the cultivation of professional cyber security personnel, the government budget

[27] Lee, "Desirable direction for national cybersecurity legislation and governance: Focusing on the case of the United States and the implications of Korea," 256.

[28] James Andrew Lewis, "Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States" (Inter-American Development Bank, 2016), 40–41, https://publications.iadb.org/en/advanced-experiences-cybersecurity-policies-and-practices-overview-estonia-israel-south-korea-and.

[29] Shin and Kim, "The Plan to Strengthen Cyber Security," 88.

for cyber security is, on the whole, a long way behind those of advanced countries that are the leaders in cyber security.[30]

On the other hand, Nir Kshetri gave a positive evaluation of South Korea's technology and manpower training. He noted that South Korea continues to develop defense capabilities against North Korean cyberattacks, and that major domestic antivirus companies such as HAURI and AhnLab have the ability to detect and block cyberattacks. In addition, he said that South Korea's Ministry of National Defense is launching regular joint cyber defense exercises with the United States to improve cyberattack capabilities and is also cultivating cyber-defense expertise.[31]

e. International Cooperation System

Ho-geun Yoo and Gyoo-sang Seol argued that South Korea was making steady efforts for multilateral security. They thought that the ROK has so far been discussing bilateral cyber cooperation with countries such as the United States, Russia, the European Union, India, and Australia, and the government expert group meeting (UN Group of Government Experts, UN GGE), which has been discussing the establishment of a cybersecurity regime. The authors suggested that a cooperative framework including national responsibility activities, core infrastructure protection, and trust-building was developed through this gathering. In addition, they stated that the group conducted the third Cyberspace General Assembly, which was attended by government leaders and international organization representatives and announced their intention to increase international collaboration on critical cyber issues and establish a shared foundation.[32]

However, Jae-hun Shin and Yong-hun Kim pointed out the problems of international cooperation itself. Due to the characteristics of the cyber domain, it is not easy

[30] Kim and Kim, "Reframing South Korea's National Cybersecurity Governance System in Critical Information Infrastructure," 704.

[31] Nir Kshetri, "Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses," *East Asia : An International Quarterly* 31, no. 3 (September 2014): 193–94, https://doi.org/10.1007/s12140-014-9215-1.

[32] Yoo and Seol, "Cyber Security System: Issues of Governance Formation and Korea," 262.

to identify who made an attack routed through the server in another country. The authors claimed that South Korea is boosting cooperative operations on cyber policy with nations such as the United States, Australia, Japan, China, and the European Union in order to address these issues, but cyber space is not being exploited properly owing to its unique nature. [33]

f. The Political Situation

There are also interesting arguments in the existing literature concerning political impacts related to cybersecurity policy development. Because cybersecurity, is directly related to national security, many security factors are restricted due to political factors. Won-sun Cho mentioned that the opposition parties in South Korea, including the Blue House and the NIS, are at odds with each other regarding the establishment of laws and institutions, and there is also competition over who will become the cybersecurity control agency. Also, she mentioned that legislation related to the enactment of the National Cyber Security Act has been continuously proposed since the 17th National Assembly, but the enactment of this security law has been delayed due to concerns of the ruling party and the private sector over the abuse of power by the NIS.[34]

Meanwhile, Hwa-sun Jho and Woong Kwon also mentioned that laws for introducing cyber threat information-sharing system including the private sector were submitted to the 19th National Assembly, but in the end, the law ultimately failed due to resistance from the opposition party and certain civil society organizations. They argued that this was because opponents were concerned about the development of the NIS's control over the business sector, since this legislation centered on the NIS and proposed countermeasures against cybersecurity risks. Consequently, the authors argued that the level of legislative and public-private cooperation in South Korea's cybersecurity governance was relatively low compared to that of the United States, where public-private

[33] Shin and Kim, "The Plan to Strengthen Cyber Security," 91–92.

[34] Cho, "Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues," 148.

cooperation developed through information sharing with the private sector that went beyond infrastructure construction and security technology development.[35]

2. Lessons South Korea Could Learn from the United States

To complement the first section of this literature review, this section focuses on those analysts who have sought to draw from lessons learned by the United States on parallel categories of laws and institutions, integration and control agencies, limitations of technology and resources, the international cooperation system, and the political context. This thesis builds on these existing works.

a. Laws and Institutions

Jae-hun Shin and Yong-hun Kim have argued that it is necessary to enact a "Cyber Security Act" that can integrate and manage various aspects because it is difficult to actively respond to cyberattacks due to the limitations of South Korea's cybersecurity-related laws. In South Korea, the implementation of the law has been postponed because it could lead to the NIS abusing its authority and violating human rights. However, these authors also stated that incorporating only the essence of cybersecurity in the relevant law, as in U.S. law, would be a good method to eliminate content that is unneeded or undesirable.[36] Seong-yeob Lee mentioned that in the case of South Korea, it is necessary to establish an integrated basic law system that encompasses the public and private military, just like the U.S. Cyber Security Act of 2015.[37] According to him, governments worldwide are constructing an integrated legal framework for cybersecurity in terms of national security and national interest, and the United States is establishing governance through cybersecurity laws. As the NIS supervises the public sector and the Ministry of Science and ICT oversees the commercial sector, he stated that South Korea should consider

[35] Hwa-sun Jho and woong Kwon, "Cyber-Security Governance in South Korea and the United States : A Comparison of Securitization of Cyber-Threat," *Information Society & Media* 18, no. 2 (August 2017): 99.

[36] Shin and Kim, "The Plan to Strengthen Cyber Security," 96.

[37] "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance," 2016, https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

introducing an integrated law in order to carry out systematic and unified cyberattack prevention and response responsibilities at the national level.[38]

b. Integration and Control Agencies

Do-kyung Kim and Soon-yang Kim argued that South Korea should also develop an integrated information sharing and analysis center through a department that integrates, analyzes, and shares U.S. information. They asserted that the Office of Cybersecurity and Communications (CS&C) of the U.S. Department of Homeland Security (DHS) continues to conceive and build comprehensive strategies to devise and implement simple and preventative policies regardless of risks. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) analyzes data from public, civilian, and military security management centers in the United States, disseminating the results to various public, business, and military sectors and influencing policy decisions. Therefore, the authors argued that cyber security strategy should be approached from the perspective of national security under strong national leadership, and they emphasized the need for a strong control center that can integrate civil and military information in order to construct an effective cyber security system.[39]

Ki-soo Kang determined that the United States is prepared to respond to cyberattacks from the standpoint of national security. It is true that the ROK government acknowledges the gravity and significance of cyberattacks and is diligently preparing a national strategic level response mechanism. However, he has claimed that a more comprehensive national policy is required to safeguard national security because South Korea's offensive response mechanism to cyberattacks is lacking in comparison to that of the United States. He further argued that the United States' cyber terrorism response task execution system has relatively clear task and agency divisions, whereas South Korea's

[38] Lee, "Desirable direction for national cybersecurity legislation and governance: Focusing on the case of the United States and the implications of Korea," 243.

[39] Kim and Kim, "Reframing South Korea's National Cybersecurity Governance System in Critical Information Infrastructure," 708–9.

government departments and institutions have separate security departments and informatization departments, necessitating a review of the integrated operation.[40]

Kwan Choi and Min-ji Kim evaluated that the United States was fully equipped with a strategic counter-terrorism response posture at the government level, and that South Korea also recognized the seriousness of cyber-terrorism and cyber-war and made every effort to establish a response strategy at the national level to prepare. However, they argued that South Korea had neglected to establish a system for active and defensive countermeasures against cyber terrorism, and it was necessary to devise a strategy in a larger frame to compensate for this. And they suggested that, in the event of a cyber terrorism strike, it is vital to systematically identify the target of the attack and actively respond, as well as to develop a system similar to like the U.S. system that can respond rapidly to the cyber terrorism danger, as proposed by the National Security Council.[41]

c. Limitations of Technology and Resources

Noh-Soon Chang evaluated the cyber deterrence capabilities of the United States and argued that South Korea should also supplement the technical capabilities that could deter North Korea's cyberattacks. Due to the nature of cyber security, it is very important to reveal the country that is the base of a cyberattack and the identity of the attacker. Objectively determining the identity of the attacker, can have the effect of reducing possible threats in the future. Efforts to disclose the identity of attackers and clearly attempt specific punishments and retributions have had long-term strategic effects, as seen in the recent strategic change in the United States. However, the South Korean government's response so far has been to pursue a defensive policy that focuses on securing the network or preparing an effective response system. Chang also expressed that economic sanctions or diplomatic pressure rather than a cyber counterattack would be a more realistic approach

[40] Ki-soo Kang, "National Cyber Security cyber-attack response for Study: South Korea and the United States focused on comparing response system to cyber-attacks," *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, November 2013, 783.

[41] Choi and Kim, "A Comparative Analysis of the National Defensive System Against Cyber Terrorism for National Security and Public Safety," 28.

for stable situation management in South Korea due to the ROK's cyberattack capabilities and legal restrictions. If military tensions rise on the Korean Peninsula in the future, there is a possibility that the level or frequency of cyber threats will also increase and social unrest and confusion will be created. The cyber counter-espionage activity pursued by the United States is not a defensive security activity, but an active defense strategy. Therefore, South Korea also needs to break away from the existing cybersecurity concept and establish an active defense strategy through organizational reorganization, manpower expansion, and budget support.[42]

Tae-hoi Huh, Sangho Lee, and Woo-Young Chang argued that the ROK's current capability and readiness posture for information warfare will not have an immediate effect; however, the strengthening of information warfare and security will eventually have an effect on military power, which will definitely be a major consideration in determining the balance of military capability in neighboring countries, including North Korea. Even while the ROK military has a modernized and advanced information warfare structure, operating system, and procedures, its preparedness for information warfare and cybersecurity lags behind that of the United States, which has a centralized and coherent system, according to those authors. In order to accomplish this, they said that South Korea should concentrate on establishing strategic concepts and doctrines, investing in technology development to implement them, and cultivating talent. The United States recognized the need for an "asymmetric threat strategy" and has actively invested in cyber information warfare despite its overwhelming stockpile of conventional and nuclear weapons, hence it was suggested that the ROK adopt a policy based on the U.S. example.[43]

James Andrew Lewis has pointed out that the South Korean government's investment in private IT and cybersecurity technology development is like the U.S. level, but there is a difference in the way it is done. According to him, the two countries have

[42] Chang, "Cybersecurity Threats, Response Strategies, and Korean Implications," 24–27.

[43] Tae-hoi Huh, Sangho Lee, and Woo-Young Chang, "Contemporary Information Warfare and National Strategy: Korea's Military Cyber Security Issues and Tasks," *International Area Review* 10, no. 1 (March 1, 2007): 231, https://doi.org/10.1177/223386590701000112.

sufficient competitiveness in the IT area on the global market, which was achieved by the state actively investing in the IT industry and offering incentives, while the South Korean government invests directly in the technology development of enterprises. Since U.S. corporations do not get direct government subsidies and incorporate innovative business practices, he believed that South Korea must provide conditions for private enterprises to freely enter the market for the technological development of private companies.[44]

d. International Cooperation System

Tae-jin Chung and Guang-meen Rhee urged that South Korea, like the United States, should sign the Budapest Convention and become a part of the international cooperation system. The Budapest Convention is as follows:

> The Budapest Convention is a criminal justice treaty that provides States with (i) the criminalisation of a list of attacks against and by means of computers; (ii) procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and (iii) international police and judicial cooperation on cybercrime and e-evidence.[45]

The United States is a participant of the Budapest Convention to deal with cyber-crimes according to due process by imposing sanctions on countries responsible for cyber-crimes through international collaboration. Given this new trend in the international community, the authors claimed that it is time for South Korea to join the Budapest Convention and respond cooperatively to cyber-crimes that harm national and international security. In addition, the authors stated that by adhering to international conventions such

[44] Lewis, "Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States," 57.

[45] "The Budapest Convention on Cybercrime: A Framework for Capacity Building – Global Forum on Cyber Expertise," accessed November 6, 2022, https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/.

as the Budapest Convention, South Korea's laws and systems might be enhanced, and cyber attackers could see Korea's active will.[46]

Jung-mi Cha claimed that establishing norms and mechanisms based on multilateral agreements and collaboration is most important for cyberspace deterrence and sustaining peace and stability, as South Korea will be able to secure cyberspace as a result. She emphasized that the United States is extending cyber-military collaboration with its allies, including mutual security treaties with Australia, collaboration on cybersecurity with Japan, and intelligence alliances with the United Kingdom, Canada, Australia, and New Zealand through the Five Eyes. She concluded that the reality that the United States is emphasizing cyber defense with its allies as it expands its bilateral and multilateral alliances in cyberspace should be the focus of significant policy consideration and strategic review in South Korea's cybersecurity strategy and cybersecurity cooperation.[47]

e. Political Situation

Hwa-sun Jho and Woong Kwon stated that disparities in South Korean and American cybersecurity policies influenced the formation of legislation and regulations. The authors argued that while the Obama administration acknowledged cyber threats as a key security issue and strengthened cybersecurity governance, South Korea acknowledged the importance and necessity of cybersecurity, but the security issue had been reduced to a political issue due to the legacy of state-civil society conflict. In addition, they emphasized the need for ongoing efforts to enact laws that exclude political issues in cyber-terrorism, as is the case in the United States, as the disparity in perceptions of cyber threats between the government and the ruling and opposition parties in South Korea results in the absence of a legal system.[48]

---

[46] Tae-jin Chung and Guang-meen Rhee, "A Study on accession by South Korea to the Budapest convention on cybercrime and international cooperation against cybercrime," *The Police Science Journal* 14, no. 2 (May 2019): 66, https://doi.org/10.16961/POLIPS.2019.14.2.65.

[47] Cha, "Cyber Arms Race between U.S. and China and the Rise of North Korean Threat in Cyber Space: Implications for South Korea's Cyber Security," 56–57.

[48] Jho and Kwon, "Cyber-Security Governance in South Korea and the United States : A Comparison of Securitization of Cyber-Threat," 117.

D. POTENTIAL EXPLANATIONS AND HYPOTHESES

In the evaluation of South Korea's cybersecurity capabilities, it was found through literature reviews that various scholars have different opinions on the same facts. They also argued that there are lessons to be learned from the United States to effectively respond to adversary cyberattacks. However, development of lessons from the U.S. experience has not been as comprehensive and systematic as it could be. This thesis aims to address those weaknesses.

The United States is a major power in cybersecurity. It linked cybersecurity early on with national security and actively developed relevant doctrines, norms, and techniques. In addition, it has had an impact on the global cybersecurity environment through the integration of the public-private military cooperation and cooperation with the international community and is now pursuing active security through deterrence rather than defensive security. On the other hand, it was confirmed through the literature review that South Korea is not yet outstanding in terms of cybersecurity capabilities despite its important geopolitical location, political and economic development like that of the United States, and an advanced ICT environment. Therefore, the central hypothesis of this thesis is that the policies implemented by the United States in response to cyberattacks can provide broad lessons applicable to South Korean cybersecurity, enabling a more effective response to North Korean cyberattacks.

This comparison is possible because, due to the nature of the cyber environment, some forms of a cyberattack on the United States are the same as those of attacks on South Korea. Using this point for comparison with the United States, the thesis pinpoints policies and practices that South Korea lacks or needs to supplement. However, since the gap in cybersecurity reality and capabilities between the two countries is considerable and the status and operational environments of each country in the international community are different, these differences must be considered. Strategies and tactics developed by the United States will not automatically be in line with South Korean doctrine, and laws, systems, and structures will not be perfectly applicable. The U.S. experience can offer insights, but the

specific U.S. approach may not work best for South Korea. Therefore, this process will present the added challenge of developing an autonomous security environment with long-term vision and expertise, even if South Korea learns lessons from U.S. cybersecurity.

E. RESEARCH DESIGN

Cyberattacks in South Korea in recent years have been analyzed by many scholars. Research for this thesis builds on this work by finding the characteristics of the biggest cyberattacks and threats that South Korea currently faces, and analyzing the actions taken by the South Korean government, companies, and individuals in response to the threats. The research focuses on identifying cases where the same or similar types of cyberattacks were directed against the United States and analyze how the United States responded to those threats. If the United States defended itself well, the research determines the reason for the success and compare it with South Korea's defense capabilities and policies.

The United States, as a great power, has been the target of many cyberattacks by various actors, and as a result, has developed cybersecurity policies which have greatly influenced the policies and response structures of other countries. In addition, in the cybersecurity area, each country tends not to disclose its policies, whereas the United States provides quite a lot of information unless it is secret data.[49] And since there are many analyses and evaluations of U.S. cybersecurity policies and systems in various countries, it is quite clear how the United States has responded to and resolved several cyberattacks. Therefore, there is extensive body of assessment of the U.S. policies for this thesis to draw on.

Because the U.S. policy cannot be said to be 100% correct, the thesis also considers the success or failure of these policies in determining appropriate lessons to draw from them. Furthermore, since there may be policies that do not match the reality of South Korea, the thesis research considers how to adapt these policies to derive similar measures through localization in the ROK as much as possible.

[49] Van Puyvelde and Brantly, U.S. *National Cybersecurity*, 3.

II. SOUTH KOREA'S CYBER THREAT ENVIRONMENT

North Korea's cyberattacks on South Korea have been going on for decades through a variety of methods. To ascertain the South Korean government's response to these attacks, this research reviewed various reports and other documents to examine the opinions of various scholars on the topic. Since the subject of this thesis analysis is the most threatening cyberattack from North Korea that South Korea currently faces, this chapter analyzes North Korean cyberattack cases since 2013 described in previous studies. The cases were selected based on the latest cases that had a significant economic and social impact. Next, South Korea's response to cyberattacks, follow-up measures, and the purpose of North Korean cyberattacks in the changing international environment are analyzed to identify the cybersecurity threats facing South Korea today.

A. CYBERSECURITY IN SOUTH KOREA

Currently, information resources such as transportation, communication, gas, electricity, water, nuclear power, defense, and finance, which make up South Korea's infrastructure, are interconnected via the Internet, mobile, and cloud, and are closely related to most activities of daily life. According to a survey in 2021, 89% of South Koreans use social media services, nearly double the global average, and second only to the United Arab Emirates.[50] This figure shows that not only South Korea's advanced network infrastructure but also individuals are actively interacting with the cyber world through computers and smartphones.

In addition, South Korea has become a world-class cybersecurity powerhouse by achieving fourth place in the national global cybersecurity index (GCI). The International Telecommunications Union (ITU) under the United Nations measures each member's commitment to cybersecurity through their cyber capabilities and subsequently issues the

[50] Yung-ho Lee, "2nd in the World for Korean SNS Usage Rate," *Korea Economic TV*, June 16, 2021, https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A202106160022.

GCI, which provides a means for alerting and improving cybersecurity.[51] It is raising awareness about cybersecurity, and each country takes measures to improve cybersecurity. In the GCI released in 2021, South Korea ranked fourth in the world with 98.52 points and first in the Asia-Pacific region.[52] Although these figures do not guarantee absolute national cybersecurity capabilities, they show that relatively high levels of technology, awareness, and institutions exist.

Nevertheless, South Korea is suffering attacks on a variety of targets, including individuals, national infrastructure, businesses, and military facilities, and has been continuously damaged by cyberattacks. In South Korea, the amount of economic damage caused by cyber infringement is estimated to be $2.6 billion per year. This is much more than the $1.9 billion in domestic damage from natural disasters.[53] In addition, hacking directed at vulnerable targets such as banks and online shopping malls that results in the illegal collection and leaking of personal information is causing social confusion. Cyberattacks pose a major threat to national security and cause economic and social problems.

An analysis of recent all-out warfare reveals that cyber warfare has frequently occurred before the start of conventional war between countries. During the 2008 invasion of Georgia, Russia launched a cyberattack with the "additional tool" of conventional warfare. And during the 2022 invasion of Ukraine, cyberattacks were carried out several times before the start of the armed conflict, under the name of "hybrid war."[54] Notably, the Korean Peninsula is the only divided country in the world where the relics of the East-West

---

51 International Telecommunication Union, *Global Cybersecurity Index 2020 (*Geneva, Switzerland: International Telecommunication Union, 2021), vi. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

52 International Telecommunication Union, 25, 29

53 Dae-woo Park, "Justification of the National Cyber Security Act," Global Economic, September 7, 2016. https://news.g-enews.com/ko-kr/news/article/news_all/20160907070016615450 8_1/article.html?md=20160907070145

54 Alika Gochua, Thornike Zedelashvili, and Gela Giorgadze, "Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats," *Ukrainian Policymaker* 10 (June 2022): 28–31, https://doi.org/10.29202/up/10/4.

Cold War remain, and local wars and provocations have continued since the division of South and North Korea in 1945. Today, the development of North Korea's cyber capabilities indicate the possibility of a significant cyber dimension to any war on the Korean Peninsula. Therefore, a close analysis of South Korea's cyber threat environment and identification of the greatest threat it faces now are essential not only for minimizing economic and social damage but also for national security.

B. CYBER OPERATIONS OF NORTH KOREA

According to data from the Cyber Operations Command, North Korean DDoS attacks or hacking caused $500 million in damage in 2013. This is only an estimate of the amount of damage collected by the Cyber Operations Command, and experts have judged that the actual amount of damage was much higher.[55] And the NIS announced that the number of cyberattacks that occurred in public institutions between 2015 to 2020 was about 11,700, and 70% to 80% were carried out by North Korea.[56] With North Korea's cyberattacks gaining importance, several scholars have analyzed North Korea's cyber threats. In general, the types of cyberattacks North Korea has leveled against South Korea are largely divided into cyber information collection, cyber terrorism (including psychological warfare), and cyber financial crime.

1. Information Espionage Operations

Through cyberattacks, North Korea steals important information on weapons and technology as well as South Korea's military secrets. In the past, North Korea has obtained South Korean intelligence through traditional espionage, but now it is using hacking as a major means. Hacking is the collection of information such as personal, corporate, and military secrets by taking advantage of vulnerabilities in the network and accessing the network. North Korean cyber agents use network vulnerabilities to access major national

55 "North Korea's Cyber Attacks Damage of $500 million," *YTN*, October 15, 2013, https://www.ytn.co.kr/_ln/0101_201310151027217359.

56 Dang Kim, "11,727 Public Cyber-Attacks," *UPI News*, October 10, 2020, http://www.upinews.kr/newsView/upi202010160030.

government networks, national defense networks, and public networks in South Korea to collect a lot of information easily and illegally.[57]

a. Hacking Attacks

A North Korean hacking incident on the ROK defense network in 2016 became a major social issue. The hack, called Operation Desert Wolf, infiltrated the national defense network and stole a total of 235 GB (15 million pages of A4 paper), including 226 military second-class secrets, 42 third-class secrets, and 27 confidential secrets. At that time, even the "OPLAN 5015," an all-out warfare plan prepared by the ROK-U.S. Combined Forces Command, was leaked. As a result, this incident was recorded as the largest military secret leak since the establishment of the government.[58] The leak also included information on South Korea's special forces, details of the annual South Korea-U.S. military exercises, and information on major military facilities and major power plants.[59]

The hack exploited a temporary vulnerability. Although the military's security intranet is generally considered safe from infringement, a simple mistake by a worker kept a jack connecting the military intranet to the Internet in place for a year after a scheduled maintenance period. To exploit this flaw, North Korean hackers first infiltrated the network of South Korean companies that provided anti-virus software to the South Korean military and then spread malicious code on South Korean military computers connected to the Internet using an anti-virus software server.[60]

In addition to accessing military secrets through the defense network, North Korea obtained technical data through hacking of major national facilities, private companies, and

---

[57] Dong-ryul Yoo, "North Korea's Cyber Threats and Countermeasures," *The Journal of Strategic Studies* 28, no. 3 (November 2021): 16, https://doi.org/10.46226/jss.2021.11.28.3.7.

[58] Yoo, 8–9.

[59] Min-hyung Kim, "North Korea's Cyber Capabilities and Their Implications for International Security," *Sustainability* 14, no. 3 (2022): 6, https://doi.org/10.3390/su14031744.

[60] Kelsey Atherton, "How North Korean Hackers Stole 235 Gigabytes of Classified U.S. and South Korean Military Plans," Vox, October 13, 2017, https://www.vox.com/world/2017/10/13/16465882/north-korea-cyber-attack-capability-us-military.

individuals. Daewoo Shipbuilding & Marine Engineering announced that more than 40,000 items of internal data have been hacked, and the Ministry of National Defense reported to the National Assembly that the stolen data included 60 military secrets, as well as the designs and combat systems of Aegis destroyers and submarines.[61] The leakage of military technology is also directly linked to security issues. In particular, since data on the performance and combat systems of the ships were stolen by North Korea, the South Korean military's operation to precisely strike North Korea's nuclear and missile facilities in case of emergency could be compromised.

In May 2021, traces of hacking by North Korea were found on the computers of the Korea Atomic Energy Research Institute (KAERI), and it was later revealed that defense industries such as Daewoo Shipbuilding & Marine Engineering and Korea Aerospace Industries (KAI) had been hacked by North Korea multiple times. Although the agencies did not know exactly what data or how much data was hacked, they estimated that information about advanced nuclear technology, nuclear submarines and the Korean fighter eXperimental (KF-X) had been stolen.[62] The investigation determined that hackers exploited the vulnerability of a virtual private network (VPN), and traced exploitation to 13 external addresses.[63] One of them included the address of Kimsuky,[64] a North Korean hacker group, so it was judged that North Korea was behind the hacking incident. Kimsuky,[65] an Advanced Persistent Threats (APT) group, was the main attacker.[66]

---

[61] "National core technology is dangerous, and Daewoo Shipbuilding & Marine Engineering is threatening hacking following the Korea Atomic Energy Research Institute," CCTVnews, June 22, 2021, https://m.post.naver.com/viewer/postView.naver?volumeNo=31815687&memberNo=48110825.

[62] Yoo, "North Korea's Cyber Threats and Countermeasures," 8.

[63] Pierluigi Paganini, "North Korean APT Group Kimsuky Allegedly Hacked South Korea's Atomic Research Agency KAERI," Security Affairs, June 19, 2021, https://securityaffairs.co/wordpress/119147/apt/kimsuky-apt-hacked-south-korea-kaeri.html.

[64] Claudia Glover, "North Korea Is Ramping up Cyberattacks on South Korean Targets," *Tech Monitor* (blog), June 22, 2021, https://techmonitor.ai/technology/cybersecurity/north-korean-cyberattacks-on-south-korea-kimsuky. Kimsuky, also known as Velvet Chollima, was first discovered by security firm Kaspersky in 2013 and is a geopolitical-motivated APT group primarily targeting the Korean Peninsula

[65] Chong-woo Kim and Polito Carolina, "The Evolution of North Korean Cyber Threats," *The Asan Institute for Policy Studies*, March 2019, 1–15. Their first attack on South Korea targeted the Sejong Institute, the Korea National Defense Research Institute, and the Ministry of Unification in September 2013

b. Phishing Attacks

In March 2016, South Korea's NIS said in a media report that North Korean hackers sent seductive text messages containing malicious codes to senior South Korean government officials. A significant number of smartphones were infected with malicious codes, resulting in personal text messages and voice communication being stolen.[67] The NIS did not reveal which officials were harmed, but the fact that more than one-fifth of senior officials were infected alone raised problems with their sense of personal security. Despite the ongoing hacking investigation and surveillance of individuals by the NIS, malicious cyber activities against South Korean government personnel and the South Korean military continued. In September 2016, hackers infiltrated the Defense Ministry intranet through the personal computer of the then Defense Minister and attempted to steal military intelligence, including military operations.[68]

In July 2019, North Korea attempted to infiltrate by sending emails containing malicious code to members of South Korean government agencies through Operation Red Salt.[69] These e-mail attack attempts are very simple but effective attack methods, not using new vulnerabilities or advanced attack techniques by attempting to leak information targeting server users rather than directly attacking servers. Malicious code analysis revealed that the attack was not just a one-time attack but was closely related to the defense network hacking incident in 2016. So, researchers at AhnLab, an anti-virus software

---

[66] The U.S. government invented the term APT to refer to entities in the Asia-Pacific area that carried out operations against specified targets at the direction of the State. The U.S. Department of Defense and the intelligence agencies use this word to describe specific threat actors and assaults.

According to McAfee's definition, APTs are a group that steals and attacks a target's valuable data using sophisticated technology, gaining access to trade secrets, intellectual property, national and military secrets, computer source code, and other useful information through ruthless and persistent intrusion. Shem Radzikowski, "CyberSecurity: Origins of the Advanced Persistent Threat (APT)," Dr.Shem, October 8, 2015, https://DrShem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/.

[67] Hancocks Paula, "North Korea Hacked Government Officials' Smartphones, South Korea Says," *CNN*, March 8, 2016, https://www.cnn.com/2016/03/08/asia/south-korea-smartphone-hack/index.html.

[68] "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," U.S. DEPARTMENT OF THE TREASURY, September 13, 2019. https://home.treasury.gov/news/press-releases/sm774

[69] "AhnLab Security Emergency Response Center Report," ASEC REPORT 96 (Sungnam: Ahnlab, 2019), https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.96.pdf.

company, judged that North Korea had been continuously attacking state and major government agencies for years.[70] Although the specific degree of damage is not known, it is judged that the degree of direct damage was not as severe as it might have been due to the rapid detection and response of the AhnLab Security Emergency-Response Center (ASEC).

These incidents demonstrate that North Korea has the capability to successfully penetrate important South Korean government and civilian networks and conduct damaging espionage operations.

2. Cyber Terrorism

According to NATO's definition:

> cyber terrorism is cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal.[71]

Cyber terrorism has the same goals as general terrorism, but because there are no physical restrictions, the means and targets of the attack are diversifying. North Korea has not only caused social confusion and fear among South Korean citizens by attacking South Korean financial institutions, broadcasting companies, and major key facilities through DDoS, but also has generated ideological division in South Korea through online intrusion by hacking units.

a. DDoS Attack

On March 20, 2013, Operation Dark Seoul paralyzed the networks of South Korean broadcasters and banks through a DDoS attack, causing a great shock to South Korean society. This cyberattack shut down KBS, MBC, and YTN public broadcasters simultaneously and temporarily shut down the computers of Shinhan Bank, Nonghyup

70 "AhnLab Security Emergency Response Center Report," 4–5.

71 "What Is Cyberterrorism?," SearchSecurity, accessed October 7, 2022, https://www.techtarget.com/searchsecurity/definition/cyberterrorism.

Bank, and Jeju Bank. The data servers of the broadcasting companies' websites were destroyed, and as the employees' PCs and the banks' servers were infected with malicious code, Internet banking transactions and ATM machines stopped working. A series of attacks took place four times in one week.[72] In the end, it took several weeks for servers and PCs to recover normal operation, and only 10% of attacked websites were up and running within two days.[73] The joint investigation team found that North Korea's Operation Dark Seoul destroyed 48,800 computers and servers, and the damage was about $600 million.[74]

Unlike previous attacks, Operation Dark Seoul was meticulously planned, such as selecting targets in advance and analyzing vulnerabilities by acquiring inside information. As a result of the South Korean government's investigation, it was revealed that the target organizations' internal PCs or servers were intruded for continuous monitoring at least eight months before the attacks, and then the malicious code was distributed internally to destroy data and operating systems.[75] The South Korean government officially determined that this cyber-terrorism was carried out by North Korea for two reasons: first, a well-known North Korean IP address was found on a South Korean server; second, specific strings of malicious codes known to have been used by North Korea in the past were reused. This cyberattack was considered one of the most serious cyberattacks experienced by South Korea and demonstrated North Korea's APT capabilities.[76]

Shortly later, on June 25, 2013, the 63rd anniversary of the outbreak of the Korean War, North Korean hackers attacked the presidential office website and several official

---

[72] Hyuk-chun Kwon, "A Comparative Study on North Korean Cyber Attack Patterns : Focusing on the Three Governments of Roh Moo-Hyun, Lee Myung-Bak and Park Geun-Hye" (Seoul, Konkuk University, 2020), 96, http://www.riss.kr/link?id=T15502639.

[73] Yoo-eun Lee, "Who Was behind South Korean Cyber-Attacks?," aljazeera, accessed October 7, 2022, https://www.aljazeera.com/opinions/2013/3/31/who-was-behind-south-korean-cyber-attacks.

[74] Jae-kwang Kim, "Coping with Legal Issues on Cyber-Security Threat," *KYUNGPOOK NATIONAL UNIVERSITY LAW JOURNAL*, no. 58 (2017): 148, https://doi.org/10.17248/knulaw..58.201705.145.

[75] Kim, 148.

[76] Jonathan A P Marpaung and Hoon-jae Lee, "Dark Seoul Cyber Attack: Could It Be Worse?," *Cryptography & Network Security Lab*, 2013, 4.

media sites, affecting a total of 69 devices.[77] They not only destroyed the server equipment of broadcasting companies, but also tampered with the homepage of the Blue House, the Office of Government Policy Coordination, and launched DDoS attacks on the government integrated computer center, causing access failures to a total of 69 homepages, including the homepages of 43 private institutions. Moreover, South Korea suffered the embarrassment by the display of the slogan "Long live General Kim Jong-un, the unification president," on the website of the Blue House.[78] The hackers deleted the logs and destroyed the hard disk, but the public-private-military joint response team was able to identify the North Korean IP that attacked the website server by examining the digital forensic data. The response team also stated that the June 25 attack was the work of North Korea based on many similarities to the March 20 Dark Seoul operation.[79] And as a result of the investigation, it was revealed that a series of cyber-terrorism attacks in 2013 were carried out by Lazarus, which became the most famous hacking group representing the North Korean regime as the mastermind behind the attacks on Sony and WannaCry in 2014.[80]

b. Psychological Warfare

Psychological warfare has long been considered an important element of warfare. U.S. scholars have applied Clausewitz's doctrine to say that political warfare in peacetime is the use of all means except force to achieve national goals, including white methods such as political alliances and economic measures and black methods such as psychological warfare and support for the insurgents of hostile countries.[81] North Korea has engaged in

---

[77] Sang-Hun Choe, "South Korea Blames North for June Cyberattacks," *The New York Times*, July 16, 2013, sec. World, https://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html.

[78] Yoo, "North Korea's Cyber Threats and Countermeasures," 21.

[79] Won-suk Kim, "South Korea Officially Blames North for June 25 Cyber Attack," *ETNEWS*, July 16, 2013, sec. Internet, https://english.etnews.com/20130716200016?SNS=00002.

[80] Kim and Carolina, "The Evolution of North Korean Cyber Threats," 3.

[81] C. Thomas Thorne and David S. Patterson, eds., *Emergence of the Intelligence Establishment*, Foreign Relations of the United States 1945–1950 (Washington, DC: United States Government Printing Office, 1996), 668.

psychological warfare against South Korea along with military provocations locally since the Korean War, and it has spread false information and disinformation through pro-North Korean sites and social media. According to previous research, North Korea has conducted more than 180 pro-North Korean programs in 20 countries around the world, including "People's Korea," "Pyongyang Times," "Arirang Special Site," and "Between Our People" in order to spread pro-North Korean support in South Korea and promote the superiority of the regime.[82] They beautify and propagate the Juche ideology and military-first politics and spread content that slanders the South Korean leaders, incites anti-American sentiments, and promotes conflict between the government and the private sector.[83] In addition, North Korea's cyber department operates a so-called "comment team" and spreads fabricated information to South Korea, instigating division of public opinion and social disturbance.[84] They are also manipulating public opinion and distributing fake news to create political divisions in society, and they are conducting "cyber-cultural psychology warfare" to spread North Korean culture, including movies, music, and novels.[85]

As such, North Korea's cyber psychological warfare is being conducted in various forms to achieve its purpose. Although high-intensity cyberattacks such as North Korea's information theft and server attacks using DDoS have a large impact on our society, it is possible to respond to subsequent attacks by analyzing the degree of damage and vulnerabilities. However, as cyber psychological warfare consists of low-intensity attacks, the degree of damage and vulnerability and the level of response are not clear and the risks are not clearly visible. As individuals are more likely to be exposed to North Korean cyberattacks due to the recent development of smartphones and the increase in the population of SNS users, cyber psychological warfare poses a great threat to national security. Contents developed by North Korea to show the superiority of the system and

82 Yoo, "North Korea's Cyber Threats and Countermeasures," 14.

83 Dong-sung Kim, "North Korea's Strategic Tactics of United Front and Political-Psychological Warfare," *The Journal of Strategic Studies* 57 (March 2013): 331.

84 Yoo, "North Korea's Cyber Threats and Countermeasures," 15.

85 Jae-hun Park, "A Study on Cybersecurity Strategies against North Korean Cyberattacks" (Incheon, Inha University, 2022), 15, http://www.riss.kr/link?id=T16084674.

materials that distort facts are spreading online indiscriminately through social media, and many people are unwittingly taken in by North Korea's propaganda and attempts to influence public opinion by reproducing distorted data and criticisms of the state and government.[86]

On April 18, 2008, the South Korean government announced the results of a free trade agreement (FTA) with the United States, which included allowing imports of cattle parts at risk of mad cow disease. As it became known that there is a possibility of mad cow disease in American beef and that it is a favorable deal for the United States, public opinion against the Korea-U.S. FTA was formed. In addition, the public's anxiety and concern was amplified when MBC's "PD Notebook," an investigative journalism program, reported on the risk of mad cow disease in American beef. Scientists from the Korea Institute of Science and Technology (KIST) held an emergency press conference regarding the safety of American beef, reporting that there had been no reports of people contracting mad cow disease, and even if cases did emerge, it is a well-controlled disease; and, therefore, it is necessary to calmly address Internet misconceptions and unfounded rumors.[87] Nevertheless, many South Koreans protested against the import of American beef and the Korea-U.S. FTA. Major media and numerous Internet and private broadcasting stations covered the scene of the protests. Because only images that individuals wanted were transmitted in real time without objective review, distortion and prejudice were introduced, which made the situation worse.[88]

The citizens who attended the demonstration participated to protect themselves and their families from the threat of mad cow disease. But the nature of the protest spread to an anti-American movement just because it was American beef. Various social movement groups, including pro-North Korean anti-American groups, participated in the protests and

86 Shin and Kim, "The Plan to Strengthen Cyber Security," 91.

87 Mi-ohk Kim, "Scientists Say The Mad Cow Disease Truth," *Donga*, May 9, 2008, https://www.donga.com/news/article/all/20080509/8576305/1.

88 Sang-ho Lee, "North Korea's Cyber Psychological Warfare and the Options for South Korea's Countermeasure," *Journal of Korean Political And Diplomatic History* 33, no. 1 (2011): 275.

incited them. MBC, which had a progressive tendency at the time, also revealed bias through PD Notebook and a lot of news, causing chaos in society.[89]

While the public sentiments had a genuine basis, North Korea sought to aggravate the situation. A defector from the North Korean Reconnaissance General Bureau revealed that the Reconnaissance General Bureau has the resident numbers and contact information of hundreds of thousands of South Korean citizens and uses this information to join various online communities in South Korea to carry out cyber operations. He also revealed that the mad cow disease incident was an opportunity for North Korea to launch public opinion operations in earnest.[90]

The elements of information warfare and cyber psychology warfare used by the various groups involved in the mad cow disease protests were very similar to the methods of publicity, propaganda, manipulation of public opinion and mobilization used by terrorist groups such as al-Qaeda, and eventually they succeeded in achieving their goals.[91] According to a survey by the Korea Economic Research Institute, 100 rallies were held over a period of three months, the organizers estimated that 700,000 attended, and the social and economic loss amounted to $2 billion.[92] These figures show that cyber psychological warfare not only causes economic damage, but also wastes time and manpower.

---

89 Yang-sup Shim, "The Outcome and Limitation of South Korean Scholars' Studies about the Demonstration against Importing American Beef in 2008," *National Security and Strategy* 16, no. 1 (2016): 105.

90 Kyung-woong Jun, "North Korea joins community with hundreds of thousands of resident numbers... After 'Mad Cow Disease', public opinion work in earnest," *NewDaily*, January 17, 2022, https://www.newdaily.co.kr/site/data/html/2022/01/17/2022011700163.html.

91 Lee, "North Korea's Cyber Psychological Warfare and the Options for South Korea's Countermeasure," 276.

92 On-yoo Park, "Government trust and political failure: Why did the easing of U.S. beef import conditions cause mad cow disease candlelight vigils," *Korean Association of Local Government*, 2021, 904.

c. Cheonan Misinformation

On March 26, 2010, the naval ship Cheonan sank while performing normal missions in the area of Baengnyeong Island, South Korea. The South Korean government conducted an investigation with experts from South Korea, the United States, Sweden, the United Kingdom, and Australia and announced that a North Korean torpedo attacked the Cheonan and killed 46 soldiers.[93]

Despite the results of the experts' investigation, there was a conspiracy theory disseminated through illegal flyers and online communities that the Cheonan sinking was not the work of North Korea, but rather the result of South Korean training or an American torpedo. Ten persons were arrested without imprisonment for distributing unlawful handouts and misleading information, and after analyzing 40 cases, the police concluded that North Korea was responsible for certain Internet postings.[94] North Korea created IDs by stealing the resident registration numbers of South Korean citizens and then posted the comments made by the North Korean National Defense Commission in various South Korean communities. These postings slandered the Cheonan investigation results and disseminated the claim that North Korea did not intervene. North Korea, which was identified as the mastermind, also claimed that the sinking of the Cheonan was the result of a South Korean government conspiracy and appealed to the international community via propaganda websites and numerous media outlets that it had nothing to do with the incident.

North Korea also has dispatched spies to the South or, via underground party organizations, collaborated with pro-North leftist groupings like the Confederation of

93 Lendon Brad, "S. Korea's Final Report Affirms Cheonan Was Sunk by N. Korean Torpedo," *CNN*, September 13, 2010, http://www.cnn.com/2010/WORLD/asiapcf/09/13/south.korea.cheonan.report/index.html.

94 Jun-ki Kwon, "Intensified investigation into Cheonan rumors... Raises rumors behind North Korea," *YTN*, June 1, 2010, sec. 뉴스, https://www.ytn.co.kr/_ln/0103_201006012055527850.

Korean Students' Union.[95] In addition to academies and labor circles, North Korea has also infiltrated religious organizations, politics, and the military to encourage individuals to participate in solidarity actions.[96] This tactic was also applied in the Cheonan episode. According to the findings of a 2013 South Korean investigation into the dissemination of pro-North Korean ideology within the military, an officer who had joined the Confederation of Korean Students' Union before commissioning told his colleagues that the United States was responsible for the sinking of the Cheonan. Another soldier who joined the Confederation of Korean Students' Union prior to enrollment agreed with the North Korean assertion that the sinking of the Cheonan was a South Korean government conspiracy and conveyed false information to his fellow soldiers. The investigators highlighted that it is evident that North Korea's activities influence the creation of public opinion in South Korea, including within the military, although it cannot be proven that all actors followed North Korea's orders.[97]

These diverse North Korean attempts had a significant impact on South Korean public perception regarding the Cheonan tragedy. Although the results of a joint inquiry by experts from each country and South Korean civilian and military personnel confirmed that a North Korean torpedo was responsible for the sinking of the Cheonan, public opinion in South Korea was suspicious of the conclusions. According to the declaration made by the government in June 2010, 75.4% of the population believed that North Korea was responsible for the sinking of the Cheonan, whereas just 32.5% believed the results of the government's inquiry a month later.[98]

---

95 "Confederation of Korean Students' Union," in *Encyclopedia of Korean Culture* (The Academy of Korean Studies), accessed October 17, 2022, http://encykorea.aks.ac.kr/Contents/SearchNavi?keyword=%ED%95%9C%EA%B5%AD%EB%8C%80%ED%95%99%EC%B4%9D%ED%95%99%EC%83%9D%ED%9A%8C%EC%97%B0%ED%95%A9&ridx=0&tot=9288.

96 Kim, "North Korea's Strategic Tactics of United Front and Political-Psychological Warfare," 346.

97 Kim, 343–45.

98 "Distrust Spread over the 'Cheonan Investigation'… Only 32% of the Public Believe the Government Announcement," *Hankyoreh*, September 8, 2010, https://www.hani.co.kr/arti/politics/politics_general/438817.html.

The polarization of public opinion over the Cheonan incident reverberated across South Korean society, as the South Korean government's position of a blatant North Korean provocation had never been directly disputed by the majority of society.[99] At that time, as the government and some civil society groups confronted each other over the truth of the Cheonan incident, South Korean society did not fully accept that the Cheonan was a North Korean act. Despite repeated efforts, the South Korean government was unable to resolve the Cheonan incident.[100] Even with the passage of time, public support for North Korea and mistrust of the South Korean government have mingled with the government's objective of peace on the Korean Peninsula, endangering national security on occasion. And the polarized public opinion on North Korea fostered the seeds of a broader political and ideological position, which eroded the idea that North Korea was South Korea's primary opponent, resulting in numerous social confrontations.[101]

3. Financial Warfare

Recently, North Korea has been subject to sanctions by the United Nations and the international community for its continuous ballistic missile launches and nuclear tests. The UN Security Council's sanctions against North Korea not only freeze North Korea's economic asset, but also the funds, other financial assets, and economic resources of countries that support North Korean programs. Moreover, unlike China and Russia, North Korea is completely isolated from the international community, so sanctions from the international community, led by the United States, are fatal to North Korea and Kim Jong-un. Therefore, many scholars analyzed that North Korea is doing its best to raise funds for Kim Jong-un's rule by mobilizing cyber terrorist organizations to hack banks and

99 Jung-hoon Lee, "The Sinking of Cheonan: Remembering the Tragedy in its 10th Anniversary," *New Asia* 27, no. 1 (2020): 67.

100 Sun-song Park, "The Actor-Network of ROK Ship Cheonan Accident and the Unstability of the Division System in the Korean Peninsula," *Journal of the North Korean Research Society* 17, no. 1 (2013): 319.

101 Lee, "The Sinking of Cheŏnan," 86.

cryptocurrency exchanges around the world, including in South Korea.[102] In fact, the frequency of cyber financial crimes suspected of being committed by North Korea increased immediately after sanctions were taken against North Korea in response to Pyongyang's test-fire of an intercontinental ballistic missile (ICBM)-class Hwasong-15 on November 29, 2017. And it is estimated that North Korea made a lot of money from ransomware, spear phishing, and cryptocurrency theft.[103]

North Korea's cyber financial crimes are broadly classified into three categories.[104] The first is illegal withdrawal through the Society for Worldwide Interbank Financial Telecommunications (SWIFT)[105] inside the bank and ATM terminal hacking. The second is ransomware, a malicious code, to extort ransom money. Last is cryptocurrency stealing through attacks on individuals and cryptocurrency exchange servers. The research here focuses on ransomware and cryptocurrency theft for North Korea's cyber financial threats because in 2017, after it was confirmed that North Korea was using a vulnerability in the SWIFT network, and at the request of the United States, North Korea was expelled from the SWIFT network.[106] And no attacks on South Korea were found after collecting personal information and creating duplicate credit cards through the complementary vulnerability of ATM machines that occurred in 2017.[107]

---

[102] Sang-am Han and Yun-yung Kim, "A Study on Improvement Measures to Protect the Korean Financial Network against Cyber Terrorism by North Kore," *Public Security Policy Research* 34, no. 2 (2020): 320, https://doi.org/10.35147/knpsi.2020.34.2.319.

[103] Myung-hyun Ko, "North Korea's Cyber Force and Financial Crimes," *North Korea Economic Review* 23, no. 10 (October 2021): 55.

[104] Ko, 60.

[105] SWIFT is a vast messaging network banks and other financial institutions use to quickly, accurately, and securely send and receive information, such as money transfer instructions. (https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp)

[106] Han and Kim, "A Study on Improvement Measures to Protect the Korean Financial Network against Cyber Terrorism by North Kore," 334.

[107] Byung-chul Won, "North Korean hackers working with South Korean criminals hack ATMs and steal 230,000 cases of financial information," *security news*, September 6, 2017, http://www.boannews.com/media/view.asp?idx=56864.

a. Ransomware

Ransomware is a program that blocks an authorized user's access to data on a computer through malware and threatens to leak or block access to the victim's data if the ransom is not paid.[108] North Korea's representative ransomware attack was a large-scale cyberattack using WannaCry on May 12, 2017. Targeting vulnerabilities in Microsoft Windows, the ransomware virus infected more than 300,000 computers in 150 countries and cost more than $4 billion.[109] This incident shocked the international community about North Korea's cyberattack capabilities. A subsequent June 10, 2017, attack on South Korean web hosting group Nayana infected 153 Linux servers and more than 3,400 business websites hosted by the company.[110]

Since then, there have been no large-scale ransomware attacks, but domestic corporate ransomware damage continues to increase, and 90% of these attacks are concentrated in small and medium-sized enterprises.[111] According to a Microsoft report published in 2022, North Korea mainly attacks small and midsize businesses through "H0lyGh0st" ransomware,[112] indicating that North Korea is still trying to secure funds through ransomware.

---

[108] Andrew Jenkinson, *Ransomware and Cybercrime* (Boca Raton: CRC Press, 2022), 2, https://doi.org/10.1201/9781003278214.

[109] Selena Larson, "WannaCry: Someone Has Emptied Ransom Accounts Tied to the Cyberattack," *CNN*, August 3, 2017, https://money.cnn.com/2017/08/03/technology/wannacry-bitcoin-ransom-moved/index.html.

[110] Pierluigi Paganini, "South Korean Hosting Provider NAYANA Infected by Erebus Ransomware, It Paid $1 Million to Crooks," Security Affairs, June 21, 2017, https://securityaffairs.co/wordpress/60281/malware/erebus-ransomware-hit-south-korea.html.

[111] Kwang-ha Park, "Ransomware Threatens National Security, and Measures to Prevent Damage Are Urgently Needed," *Information and Communication Newspaper*, January 27, 2022, http://www.koit.co.kr/news/articleView.html?idxno=93254.

[112] Microsoft 365 Defender Threat Intelligence Team, "North Korean Threat Actor Targets Small and Midsize Businesses with H0lyGh0st Ransomware," *Microsoft Security Blog* (blog), July 14, 2022, https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/.

b. Cryptocurrency

North Korean cyber agents achieved significant achievements in 2021 alone, acquiring $400 million worth of digital assets through at least seven attacks (phishing, malware) on cryptocurrency exchanges.[113] According to the report of the North Korea Sanctions Committee under the UN Security Council, North Korea is using hackers to finance the development of nuclear and ballistic missiles, which has been reduced due to the economic sanctions of the United Nations, and is exerting a great deal of effort in stealing cryptocurrencies.[114] The reason is that attacks on cryptocurrency exchanges appeal to North Korea is that they are difficult to identify and the attackers are difficult to track compared to bank attacks, and the government's lack of supervision and regulation on cryptocurrency is used by North Korea as a major means of securing funds.[115] So, in North Korea, profits from attacks on virtual currency exchanges were higher than those from attacks on financial institutions with advanced security technology infrastructure.[116]

Cryptocurrency hacking in South Korea started in February 2017 with an attack on Bithumb, one of the largest cryptocurrency exchanges in South Korea. As can be seen from the Table 1, below, North Korea's attacks on cryptocurrency exchanges are most common in 2017, and this period coincides with the boom in cryptocurrency in South Korea. Through this, it is judged that North Korea's successive attempts to hack cryptocurrency were aimed at the vulnerability of the initial cryptocurrency exchange. These vulnerabilities existed because the South Korean government's understanding of cryptocurrencies was insufficient at the time, and policy was not established, as well as the virtual currency

113 "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High," *Chainalysis* (blog), January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

114 Han and Kim, "A Study on Improvement Measures to Protect the Korean Financial Network against Cyber Terrorism by North Kore," 335.

115 "Sanctions Committee Documents 30 August 2019," UN Documents for DPRK (North Korea), August 30, 2019, 4, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

116 "Sanctions Committee Documents 8 September 2021," UN Documents for DPRK (North Korea) (United Nations, September 8, 2021), 50, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2021_777_E.pdf.

exchanges were created without any preparation, which led to technical weaknesses. From the cases of Bithumb and YouBit, it can be inferred that the hackers' attack skills were superior to the security capabilities of the exchanges as evidenced North Korea's to make repeated attacks rather than just one attack.

Table 1. North Korean Cyberattacks on Cryptocurrency Exchanges in South Korea.[117]

Year	Month	Target	Amount of damage (USD)	Remarks
2017	Feb	Bithumb	7M	First attack
	Apr	Youbit	4.8M	First attack
	May	4 exchanges, 25 people	no damage	-
	Jul	Bithumb	7M	Second attack
	Sep	Monero (cryptocurrency)	25,000	Cryptocurrency hijacking
	Oct	Coinis	2.19M	
	Dec	Youbit	17% of assets	Second attack bankruptcy
2018	Jun	Bithumb	31M	Third attack
2019	Mar	Bithumb	20M	Fourth attack
	May	Upbit	49M	

To summarize the cases from 2017 to 2019, North Korea stole at least $125 million through South Korean cryptocurrency exchange attacks. According to a report by Chainalysis, North Korea stole $170 million through 49 cryptocurrency hacks between

117 Adapted from "Sanctions Committee Documents 30 August 2019," UN Documents for DPRK (North Korea), August 30, 2019, 111–12, and Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," n.d., 51.

2017 and 2021,[118] and due to rising cryptocurrency asset prices, experts have judged that North Korea's virtual dark money will exceed international estimates.[119]

Despite continued sanctions from the United Nations and the international community for North Korea's cryptocurrency theft, that country continue to carry out virtual currency campaigns as a way to raise funds. According to the UN Security Council's Economic Sanctions Report on North Korea, unlike in the past, North Korea seizes virtual currency by identifying potential targets through social media platforms rather than hacking servers and contacting them to spread malicious files through email and news.[120] As foreign currency income drastically decreased due to sanctions against North Korea and the outbreak of Covid-19, North Korea created an additional hacker team in addition to the existing dedicated cyber warfare department.[121] Recent changes in North Korea likely mean various methods will be used to obtain foreign currency through continuous cyber hacking attacks against South Korea and the world.

C. SOUTH KOREA'S RESPONSE TO NORTH KOREAN CYBER OPERATIONS

South Korea responded to North Korea's continued cyberattacks in various ways. To respond to North Korean attacks effectively, government officials established an integrated cybersecurity organization, and they supplemented the insufficient laws and systems through legislation and directives. In addition, to solve technical problems, departments in charge developed their own programs and selected security companies to develop anti-virus software to combat North Korean threats.

---

118 "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High."

119 Joshua Park, "The Lazarus Group: The Cybercrime Syndicate Financing the North Korea State," *Harvard International Review* 42, no. 2 (Spring 2021): 37.

120 "Sanctions Committee Documents 8 September 2021," 50.

121 "Take all the South Korean banks," *Chosun News*, February 11, 2021, https://www.chosun.com/politics/north_korea/2021/02/11/SZSUMEV5DFGEDNZ22SZGJ7NPOY/.

However, as the South Korean response developed, the North Korean attack method also evolved. In the past, it was possible to deter North Korea's cyberattacks with simple technology such as anti-virus software, but now North Korea's attack methods and targets have diversified, and their desired objectives have changed significantly from the past. This section examines how South Korea has responded to cases belonging to the three categories of North Korean cyber threats just discussed.

1. Information Espionage Operations

According to the investigation results of the 2016 defense network hacking incident, a North Korean hacker obtained information from a South Korean Ministry of Defense anti-virus software provider (Hauri) one year before the incident, secured a certificate and anti-virus software source code, and infiltrated through the external Internet network.[122] Originally, the external Internet network and the internal intranet network should have been managed separately, but attackers found a point where the contractor connected the two networks for convenience, and as a result, they were able to penetrate the internal network as well.[123] The security company (Hauri) was in breach of the contract at the time of the business plan signed with the Ministry of National Defense. In addition, according to military security regulations, although soldiers could use PCs for secret work, secret storage was only possible with portable storage devices such as USB. However, some soldiers violated this for convenience, and as a result, North Korean hackers obtained the secrets they had left on internal network PCs.[124]

In relation to this case, the Ministry of National Defense reported to the National Assembly that the anti-virus software management for North Korea's evolving hacking technology was insufficient, and announced that it would push for a full replacement with a

[122] Yoo, "North Korea's Cyber Threats and Countermeasures," 17.

[123] Yoo, 17.

[124] Sung-man Kim, "Countermeasures against hacking of military internal networks," *KONAS*, December 15, 2016, https://www.konas.net/article/article.asp?idx=47494.

new anti-virus software system by the first half of 2017.[125] In addition, they announced a dual strategy of using one type of anti-virus software from the same security company for internal and external networks, but using different products for external and internal networks. As a result, the external network installed the McAfee anti-virus software of a foreign company, but the internal network anti-virus software replacement continued to use the anti-virus software of Hauri, which showed vulnerability to North Korean attacks.[126] From the security company's point of view, the defense ministry's selected anti-virus software business was not profitable because it required high efficiency with a low budget, and the risk was high because the company took all responsibility in case of a hacking incident. Therefore, when the Ministry of National Defense selected an anti-virus software company in 2017, only Hauri supported it and had no choice but to use their weak anti-virus software.[127]

In the 2019 Red Wolf Operation, which targeted public information, the government's investigation revealed that North Korean hackers sent malicious code targeting people working in the security and diplomatic fields, rather than targeting the server. [128] When South Korea was able to respond sufficiently to North Korean cyberattacks with basic server configuration and internal and external network anti-virus software, North Korean hackers began to arm themselves with more complex malicious code.[129] However, the attack did not directly harm national security because the North Korean hackers did not obtain important classified data. Nevertheless, the South Korean government judged that if the defense industry and national core technology companies

[125] Soo-han Kim, "Replacing the Anti-Virus Software after the Defense Network Was Hacked," *Herald Economy*, December 12, 2016, http://news.heraldcorp.com/military/view.php?ud=20161212000777.

[126] In-soon Kim, "Ministry of National Defense Internal Network Anti-Virus Software, Eventually Hauri," *ETNEWS*, January 22, 2018, https://www.etnews.com/20180122000175.

[127] Tae-bum Choi, "Two Years after the National Defense Network Hacking Incident, the Military Internet Security Network Is Still 'Checked,'" *MoneyToday*, 28 2018, https://news.mt.co.kr/mtview.php?no=2018082816237634464.

[128] "2020 National Information Protection White Paper (South Korea)" (South Korea National Intelligence Service, May 2020), 4.

[129] Kyeong-su Shin and Jin Shin, "Scaling cyber threats and responding to national security : A focus on North Korea's cyberattacks," *Strategic Research* 25, no. 3 (November 2018): 71.

were hacked, it would adversely affect national interests and national security. So, under the leadership of the government, a Korea Cyber Threat Intelligence (KCTI) system was set up with the defense industry and the private industry.[130] In the wake of the Korea Hydro & Nuclear Power Plant hacking incident in December 2014, the state-led National Cyber Threat Intelligence (NCTI) was formed to share information among the public and the private and military sectors, but only major cybersecurity-related organizations such as the National Security Office and National Intelligence Service was participating.[131] However, information sharing was started with KCTI as the center, and there were cases in which additional malicious code distribution and hacking attack attempts were blocked through information sharing by companies that actually possess cutting-edge technology. In addition, the amount of cyberattack data shared with the private sector and the government more than doubled compared to the previous year, effectively coping with the North Korean threat.[132]

Due to the COVID-19 pandemic in early 2020, businesses were forced to have their employees work from home and telecommute without being fully prepared for the cybersecurity ramifications of this remote work environment. In the process, corporate networks were exposed to cyberattacks such as unauthorized VPN users, unauthorized connections, and malware propagation through malicious emails.[133] North Korea's hacking in 2021 also attempted to access the server using the VPN vulnerabilities of KAERI and several defense companies. It was a matter of security technology that North Korean hackers aimed at the server's vulnerability, but South Korea minimized the damage through rapid information sharing. NIS recognized the relevant information through reporting to related organizations and blocked the spread of damage by promptly responding. In addition, they identified the cause of the hacking and induced relevant information and

130 "2022 National Information Protection White Paper," National Information Protection White Paper (National Intelligence Service, 2022), 51.

131 "2022 National Information Protection White Paper," 51.

132 Eun-hee Choi, "DPRK's Cyber Threat and Its Implications for ROK's Security : Focusing on the Threat of Cyber Propaganda" (Sungkyunkwan, 2020), 71–72, http://www.riss.kr/link?id=T15520046.

133 Jenkinson, *Ransomware and Cybercrime*. ix

emergency patches to the manufacturer through NCTI.[134] In addition, the government announced the expansion of information sharing to the private sector, including security companies. As of January 1, 2022, 309 national and public institutions and 102 private companies including defense companies are using the information sharing system.[135]

In 2016, when North Korea attacked the network of the South Korean Ministry of National Defense, public opinion denounced the disclosure of military secrets, necessitating the military's rapid development of countermeasures to quell negative public opinion. Because of this, they hurried to discover and punish the hacking incident's perpetrator, and without identifying the issue of changing the anti-virus software supplier, they unsuccessfully attempted to find another provider. Nonetheless, the South Korean government exerted considerable effort in the area of information sharing systems. As North Korea conducts cyberattacks not only via networks but also via individual weaknesses, the South Korean government needed to establish an information sharing system to respond swiftly. Initially, only important national security departments engaged in the information sharing system, but the government has progressively broadened its scope, and now the government, the military, and the private sector actively participate and share information to enhance the degree of security.

2. Cyber Terrorism

North Korean cyber terrorism against South Korea not only uses DDoS attacks on South Korean infrastructure and public facilities, but also penetrates deep into South Korean society via cyber psychological warfare.

a. DDoS Attack

In 2013, the government prepared the "Comprehensive National Cyber Security Measures" to systematically respond to cyber threats that threaten national security, such as

134 "2022 National Information Protection White Paper," 50.

135 "2022 National Information Protection White Paper," 25.

the "3.20 cyber terrorism" and the "6.25 cyber attack" that occurred at short intervals.[136] The main contents included the Blue House taking the lead in strengthening the responsiveness of the cyber threat response system, establishing a smart cooperation system for smooth information sharing between agencies and nurturing information protection experts to create a creative foundation for cyber security. In addition, it was decided to establish detailed implementation plans for each department and to periodically check the implementation performance to continuously supplement and remediate deficiencies.[137] The government announced that the Blue House would act as a "control tower" through the establishment of the "Comprehensive National Cyber Security Measures" and that South Korea would become a world-class cyber security powerhouse worthy of its status as an advanced IT country through mutual cooperation and cooperation among agencies.[138] The media also reported on this measure extensively at the time. However, even after a few years, the South Korean government did not disclose what specific countermeasures it had taken, and the government failed to come up with a solution despite the growing damage caused by North Korea's cyberattacks.[139]

In terms of cyber security technology, efforts were made to minimize damage to the South Korean government. Since 2010, the Korea Internet & Security Agency has been operating a DDoS cyber shelter that bypasses DDoS attack traffic and supports normal users to access the website.[140] Due to the impact of DDoS cyber terrorism, the number of companies using cyber shelters started to increase significantly from 2013 and 2014, and the cyber shelter service addressed a total of 22,800 cases by 2021, which protected 1,350

136 "Comprehensive National Cyber Security Measures" (Department of Science, ICT and Future Planning, 04 2013), https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeqNo=1212488.

137 "Comprehensive National Cyber Security Measures."

138 "2014 National Information Protection White Paper (South Korea)" (South Korea National Intelligence Service, May 2014), 29–30.

139 Park, "Increasing North Korean Cyber Security Threats and South Korea's Response," 24.

140 "2022 National Information Protection White Paper," 109.

DDoS attacks.[141] Table 2 provides a summary of the number of companies using the cyber shelter service and the number of DDoS attacks protected against by the service. .

Table 2. Cyber Shelter Service Status.[142]

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2011	Total
Participating companies	52	101	175	260	413	593	1,012	1,640	2,854	3,839	4,590	7,271	22,800
DDoS defense	25	60	138	116	110	83	96	87	126	167	235	107	1,350

However, although it took more than two weeks for the banking system, servers, and ATM services to be restored to normal after the DDoS attack, the government did not announce any follow-up actions or guidelines for server and PC-related recovery.

b. Cyber Psychological Warfare

In North Korea's cyber psychological warfare discussed earlier, the subject and method of the attack were vague, and it was difficult to determine the exact extent of the damage. These characteristics not only make it hard to judge the scope and capabilities of North Korea's cyber psychological warfare, but also imply that countries with developed information environments are more vulnerable to cyber psychological warfare.[143] Due to this characteristic, the South Korean government also failed to respond to and defend in advance of North Korea's cyber psychological warfare, and it was not able to retaliate or counterattack despite the great damage caused by such methods such as social chaos and economic loss.

In the case of the mad cow disease demonstration in 2008, it started as a demonstration of citizens mobilized by false facts and spread to the anti-American

141 "2022 National Information Protection White Paper," 109.

142 Source: "2014 National Information Protection White Paper (South Korea)" South Korea National Intelligence Service, May 2014, 109.

143 Jae-hyung Lee, Sang-pil Yoon, and Hun-yeong Kwon, "Concept Research and Operation Strategy for Rational Cyber Psychological Warfare Design," *Defense Policy Research* 35, no. 4 (2020): 143.

movement, ultimately causing social and economic losses to the South Korean government. The Ministry of Agriculture, Food and Rural Affairs refuted the PD Notebook claiming that the government did not know, or concealed and minimized, the risk of mad cow disease in American beef during the import negotiations.[144] However, the government did not take any additional measures other than that it requested an investigation into MBC's PD Notebook for defamation.

In response to the Cheonan conspiracy theory in 2010, there was no special countermeasure other than the police investigation into the suspects for spreading false information. The police investigated 40 cases of disseminating false information about the Cheonan on the Internet and posting comments published by the North Korean National Defense Commission on a South Korean Internet site, and they detained ten people.[145] Although the controversy over the grounding of the Cheonan is still used as a tool for political and social disputes more than ten years later, the government has not taken legal measures to prevent such a recurrence.

Although the South Korean government failed to respond to North Korea's large-scale cyber terrorism strikes against social infrastructure and took extensive measures to prevent it, neither the government nor any department made specific efforts. In addition, the government built a system to neutralize North Korea's DDoS attack, but it had little interest in developing a technology to recover quickly if attacked. As a result of the government's inability to devise a countermeasure against the adversary's cyber psychological warfare, social disorder ensued and remains an issue.

3. Financial Warfare

Previously, North Korea crippled the server with malware and demanded a ransom from South Korea in exchange for normal system repair. North Korea, on the other hand, is

144 Hye-ri Lee and Yong-pil Park, "The media 'targeted' of accusations, accusations, and investigations," *Kyunghyang News*, October 5, 2022, https://www.khan.co.kr/article/202210052045005.

145 Jun-ki Kwon, "Strengthening the Investigation of Cheonan's Scaremongering, Raising Rumors of North Korea's Background," *YTN*, June 1, 2010, https://www.ytn.co.kr/_ln/0103_201006012055527850.

currently focusing on stealing cryptocurrency by taking advantage of the advancement of blockchain technology.

a. Ransomware

Due to a ransomware attack in 2017, web hosting company NAYANA paid a significant amount to hackers to repair the damaged server. Since then, the government has made efforts to respond quickly and minimize damage by preparing rules for preventing ransomware damage. As a result, South Korea initially analyzed ransomware WannaCry, which caused simultaneous damage to the world, and came up with countermeasures to minimize domestic damage reports to 21 cases. In addition, the cost of recovering the computer seized by the ransomware was between $200 and $500, which was less than other ransomware, so it did not suffer much economically.[146]

As the world began to respond to ransomware due to the WannaCry incident, the South Korean government announced the "Big Data-based Local Government Integrated Security Control System Construction Project" to respond to cyber threats using new technologies such as ransomware and APT.[147] The government has made efforts to increase the blocking rate of malicious codes and malicious apps by collecting data from cyberattacks, which are becoming more sophisticated and intelligent. Representatively, as a countermeasure against various digital ransomware, the Ministry of Science and ICT has established the "K-Cyber Prevention Promotion Strategy" to share threat information and build a plan for speedy damage recovery in the event of an incursion. Using big data, the Korea Internet & Security Agency created a ransomware prevention system and launched a "Stop Ransomware" website to give response and recovery procedures.[148] As part of these

146 "2018 National Information Protection White Paper (South Korea)" (South Korea National Intelligence Service, May 2018), 47.

147 "2018 National Information Protection White Paper (South Korea)," 77.

148 So-ram Kim, Soo-jin Kang, and Yong-cheol Choi, "Ransomware Status and Response/Prevention Policy Trend in 2021," *REVIEW OF KIISC* 31, no. 6 (December 2021): 7–8.

efforts, the government aims to reduce the amount of damage and protect the public from financial fraud by establishing a pharming blocking system.[149]

b. Cryptocurrency

As cyberattack damage on cryptocurrency exchanges increased rapidly in 2017, the ROK government conducted security checks on ten exchanges, which account for 95% of all transactions. As a result, the government discovered that all the target exchanges were vulnerable to cyberattacks and that personal information protection measures were not implemented properly.[150] Measures to prevent cyberattacks should have been prepared before the establishment of a cryptocurrency exchange, but the basics were not followed due to the rapidly developing cryptocurrency market. In January 2018, according to the government guidelines, to trade on a cryptocurrency exchange, it was necessary to go through Know Your Customer (KYC) rules.[151] The purpose of this procedure was to prevent the increase in speculative demand for cryptocurrencies, as well as to increase the transparency of transactions. As a result, the cryptocurrency that North Korea stole could not be converted into cash, or only a small amount of it could, so that cryptocurrency did not help much in terms of securing foreign currency.[152]

The South Korean government has established regulations for cryptocurrency exchanges but has not yet implemented laws on cryptocurrencies themselves. Currently, there are no consolidated individual laws governing cryptocurrencies; instead, they are governed by individual legislation passed by the appropriate ministries.[153] The South Korean government recently declared that the Framework Act on Digital Assets will be

---

[149] "2018 National Information Protection White Paper (South Korea)," 57.

[150] "2018 National Information Protection White Paper (South Korea)," 2.

[151] Yong-ju Park, "Cryptocurrency Trader Real Name Verification Starts Today," *YTN*, accessed October 17, 2022, https://www.yna.co.kr/view/AKR20180129167500002.

[152] Ko, "North Korea's Cyber Force and Financial Crimes," 64.

[153] Han and Kim, "A Study on Improvement Measures to Protect the Korean Financial Network against Cyber Terrorism by North Kore," 341.

implemented during the first half of 2023.[154] The government stated that the recent Luna crypto incident in South Korea has eroded confidence in cryptocurrency trading, and that it will draft regulations to maintain the market and its players.[155] However, the government has not yet determined whether to institutionalize the cryptocurrency market in order to recognize and protect investors, or whether the special financial regulation will continue to be limited to the prevention of money laundering. This demonstrates that South Korea's cryptocurrency policy is still institutionally deficient.

Seven prominent firms, including KIA and LG, reported ransomware damage in 2021, with employee information, internal contract documents, and financial data being the most affected.[156] It is not difficult to identify whether this is due to South Korea's excellent response or North Korea's lack of incentive to attack with ransomware, but ransomware has not had a direct impact on South Korea's security thus far. The South Korean government began early regulation of cryptocurrency exchanges to avoid North Korean cryptocurrency theft, money laundering, and reckless cryptocurrency speculation. Nevertheless, while this policy has been effective in stopping North Korea from exchanging cryptocurrency within the country, there is still no rule at the national level. In consideration of the cryptocurrency craze that swept South Korea in 2017, it is a major issue since the government has not yet defined cryptocurrency's future direction as of 2022.

D. SOUTH KOREA'S CYBERSECURITY VULNERABILITIES

Section B and C examine North Korean cyberattacks and South Korean responses. There are cases in which damage was minimized in advance by thorough preparation under

154 Jung-woo Kim, "Cryptocurrency Fundamental Act, visible in the second half of the year," *Decenter*, June 2, 2022, https://decenter.kr/NewsView/26739J0GJT.

155 The collapse of the Luna crypto network resulted in a $60 billion loss in value, the greatest crash in the history of cryptocurrencies to date. Despite being aware of the coin's weakness, the coin's creator, Kwon Do-hyung, demanded unreasonable investments. He was eventually jailed for breaking local market regulations and is currently under investigation. "What Really Happened To LUNA Crypto?," Forbes, accessed November 7, 2022, https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/.

156 Kim, Kang, and Choi, "Ransomware Status and Response/Prevention Policy Trend in 2021," 6.

the control of the government or related ministries, or when damage occurred, recovery and effective follow-up measures were prepared. On the other hand, there are cases of insufficient follow-up measures to that did not include preparation of comprehensive countermeasures after a major cyberattack. Drawing on the preceding case analysis, this section discusses why the most serious of North Korea's cyber threats facing South Korea are cyber psychological warfare, cryptocurrency theft, and lack of resilience to damage that can be caused by North Korean cyber terrorism.

The South Korean government is effectively responding to North Korean information espionage activities by establishing an information sharing system. In 2019, the government also formed the Internet-based KCTI that encompasses defense industries and private companies with core technologies. As of January 1, 2022, 309 national and public institutions and 102 private companies, including defense companies, are using the information sharing system. Through this, the companies can share with each other in real time and spread countermeasures and anti-virus software through threat analysis. Ultimately, the cyber threat information-sharing system can effectively defend against North Korea's information theft and hacking, the latest threats such as APT, DDoS attacks, and malicious code inflow.

In 2013, when North Korea's cyber terrorism paralyzed the South Korean network and caused great chaos in society, the Park Geun-hye government prepared a purported comprehensive cyber security plan. However, specific measures were not included in the plan because the government hastily announced comprehensive measures after suffering significant damage. However, on April 3, 2019, the Moon Jae-in government announced the "National Cyber Security Strategy" to ensure the safe and free activities of citizens in cyberspace by responding to increasing cyber threats such as hacking and information theft.[157] This announcement contained a vision and goal to develop South Korea into the world's best leading cybersecurity powerhouse, rather than responding to North Korea's

[157] Park, "A Study on Cybersecurity Strategies against North Korean Cyberattacks," 2.

cyberattacks as in the previous follow-up measures.[158] This national security plan outlined the fundamental approach for cyber security in South Korea. The National Security Office acts as a "control tower" and has prepared a strategy to systematically respond to a cyberattack that may occur at any time and has continued to do so to this day.

The Ministry of National Defense also recognized the burdens of low budget, high efficiency, and full responsibility requirements placed on anti-virus software companies, which were problems with the defense network anti-virus software project in the past and brought many changes to the 2020 military virus prevention system establishment project. The Ministry of National Defense doubled the budget to improve the business structure, which was called the "Holy Grail," and reduced corporate responsibility by placing separate orders for anti-virus software products, installation, and construction.[159] As a result, the Ministry of National Defense uses AhnLab for the internal network and still uses the Hauri anti-virus software for the external network, but the ministry judged that there would be no major problems using two vendors because they were selected through a legal process in relation to the selection of a business operator.

Nevertheless, although North Korea's cyberattacks can be prevented through national cyber security strategies and competitive anti-virus software, the technology and procedures to restore impacted technologies their original state in the shortest time in case of damage are still lacking. After the 2013 North Korean DDoS attack, although it took a lot of time to restore the servers of banks and broadcasters, the government did not take any further action. The KT Internet network failure that occurred in South Korea on October 25, 2021, started with a simple operation mistake by an internal employee and lasted for 89 minutes.[160] From the stock trading system of securities companies to general corporate businesses using KT network, small business owners using POS, and ordinary citizens, all

[158] Ki-jong Lee, "Cybersecurity Control Tower," *Newsfreezone*, March 11, 2022, http://www.newsfreezone.co.kr/news/articleView.html?idxno=367589.

[159] Da-in Oh, "Ministry of National Defense selects AhnLab and Hauri as anti-virus software suppliers," *ETNEWS*, November 23, 2019, https://www.etnews.com/20191123000001?SNS=00002.

[160] Chang-kyu Lee, "KT Communication Failure Is an Expected Result… There Was No Manual or Safety Device.," *News1*, November 9, 2021, https://www.news1.kr/articles/?4487999.

suffered a great deal of inconvenience.[161] On October 15, 2022, the service of Kakao, a South Korean IT company, was stopped due to a data center fire, and it took three days to fully recover. Although Kakao has 134 affiliates, including messengers, transportation, shopping, and finance, experts analyzed that the failure continued so long time because Kakao did not provide backup and server redundancy devices.[162] Service providers, such as Kakao, that affect many parts of South Korea, as well as national infrastructure facilities such as broadcasting stations, KHNP and KT network, must have the ability not only to prevent North Korean cyberattacks, but also to recover from them in the shortest possible time.

In cyber psychological warfare, it is not easy for the government to come up with countermeasures because all the elements of attacker identification, attack means defense, damage size confirmation, and retaliation are not clear. And unlike other North Korean cyberattacks, it is difficult for South Korean citizens to judge the risks and adverse effects of a soft attack. In order to address the problem of cyber psychological warfare, the government and the ruling party have promoted the strengthening of the authority of the National Intelligence Service. However, the opposition party emphasized the issues of individual privacy and human rights and expressed fierce opposition to the enhancement of the function of the National Intelligence Service. As a result, legislation on cyber psychological warfare is also experiencing difficulties.[163]

The government is making efforts through the information sharing system, as described earlier, to prevent and minimize damage from ransomware used by North Korean hackers to secure foreign currency. In addition, through the 2021 South Korea-U.S. summit, the two countries agreed to establish a cyber working group to strengthen cooperation between law enforcement and homeland security agencies to combat ransomware

[161] Do-young Nam, "Event of the Year in 2021," *Tech M*, December 28, 2021, https://www.techm.kr/news/articleView.html?idxno=92561.

[162] Sung-ho Ko, "Kakao Network Failure, Legislative Measures Urgently Needed," *Donga*, October 17, 2022, https://www.donga.com/news/article/all/20221017/115985691/2.

[163] Jho and Kwon, "Cyber-Security Governance in South Korea and the United States: A Comparison of Securitization of Cyber-Threat," 117.

attacks.[164] The government expects effective ransomware response through international cooperation. In order to address the potential North Korean attacks on cryptocurrency exchanges, the government expanded the target of the Internet-based KCTI information sharing system to virtual asset exchanges from 2022.[165] Although this measure provides exchanges with information that can respond to various North Korean cyberattacks, including malicious code, the system and regulations targeting cryptocurrencies are still unclear. And the biggest problem is that North Korea currently needs funds for its nuclear development, but it is suffering from financial difficulties due to economic sanctions. This situation will directly lead to a threat to the relatively weak South Korean cryptocurrency market.

This chapter's evaluation of the most serious North Korean cyber threats facing South Korea, which takes into account South Korea's uneven response to past attacks, provides a more precise framework for seeking lessons from U.S. responses to the cyber threats it has faced, undertaken in the following chapter.

[164] Bo-mi Kim and Il-seok Oh, "North Korea's Cyber Threats and Responses by Major Countries in the Kim Jong-Un Era" (National Security Strategy Institute, November 2021), 23, https://inss.re.kr/upload/bbs/BBSA05/202112/F20211206172938667.pdf.

[165] "2022 National Information Protection White Paper," 51.

III. EVALUATION OF U.S. CYBER POLICIES

A. CYBERSECURITY STATUS IN THE UNITED STATES

The United States has been creating cyber technologies and policies for a long time, seeing the cyber environment as a key component of national security. It has stressed cybersecurity initiatives to boost the U.S. economy and power while also safeguarding its people, territories, and way of life. It has also been preparing for the growing trend in cybercrime around the world by developing a cybercrime monitoring system, establishing an information exchange system, and signing a multilateral treaty. Nonetheless, the United States continues to face cyber security threats from multiple countries. The current threat to the United States is characterized as follows by the Cyber Strategy of the U.S. Department of Defense:

> China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation.[166]

The United States has employed a range of strategies to defend itself against global threats. There are mechanisms that allow for collaboration and exchange of information within the government, including the Department of Defense (DOD), Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI), through cybersecurity initiatives. In addition, the DOD expanded its cybersecurity capabilities

166 "US-DOD-Cyber-Strategy-Summary" (DEPARTMENT OF DEFENSE, September 2018), 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

through cooperation with the private sector and developed international alliances and partnerships to increase the military's cyber operations capabilities.[167]

For some time, the active efforts of the United States on cybersecurity relied on policies and methods based on deterrence theory.[168] According to the 2015 U.S. Department of Defense Cyber Strategy, a number of capabilities are required to deter cyberattacks against U.S. interests by state and non-state actors. If an attacker targets the United States, the likelihood of success should be extremely low, and if the attack is successful, the adversary must be reminded that they will face retaliation. In addition, the United States must proclaim and demonstrate their deterrence capabilities.[169]

The United States began to acknowledge in 2013 that its cyber deterrence methods were ineffective for the large majority of cyberattacks that occur under the limit for U.S. physical reprisal.[170] The enemies were well aware of the United States' comparatively high threshold for armed attack and the limitations of its cyberspace operations. In addition to endangering U.S. cybersecurity without concern for legal or military repercussions, adversaries' actions weakened democratic institutions and sought economic, political, and strategic gains.[171] Adversaries' cyberattack capabilities have subsequently evolved to keep pace with the U.S. defense capabilities, but the United States defenses were still designed for existing forms of cyberattacks; as a result, adversaries' anomalous attacks caused great challenges to government and military cybersecurity strategies.

For this reason, numerous experts began to advocate cyberspace persistence over cyber domain deterrence techniques. They have argued that the United States could use

---

167 "US-DOD-Cyber-Strategy-Summary 2015" (DEPARTMENT OF DEFENSE, April 2015), 3–4.

168 Schneider Jacquelyn, Emily Goldman, and Michael Warner, "Ten Years In: Implementing Strategic Approaches to Cyberspace," *U.S. Naval War College* 45 (2020): 31.

169 "US-DOD-Cyber-Strategy-Summary 2015," 10–11.

170 Jacquelyn, Goldman, and Warner, "Ten Years In: Implementing Strategic Approaches to Cyberspace," 34.

171 "Achieve and Maintain Cyberspace Superiority" (UNITED STATES CYBER COMMAND, April 2018), 3, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

force retaliation in accordance with the theory of deterrence, but that it is essential to continuously project cyber capabilities in order to create and maintain a strategic advantage and effectively counter threats below the level of armed attack.[172]

Therefore, beginning in 2018, the United States announced a major revision of the cyberspace strategy. In April 2018, United States Cyber Command (USCYBERCOM) issued "Achieve and Maintain Cyberspace Superiority," stressing U.S. resilience, forward defense, and continued engagement with the enemy in the cyber domain. Through this posture, the United States aims to limit the adversary's attack range by increasing resilience, identifying the source of hostile operations by defending in advance, and minimizing attack by inflicting a tactical and economic cost on the enemy through persistent engagement below the level of armed conflict.[173]

In September of that year, the DOD published the "U.S. DOD Cyber Strategy," which highlighted a similar approach. For strategic competition in cyberspace, the United States stressed cybersecurity and resilience for DOD and non-DOD Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. The Department of Defense also devised a preemptive neutralization strategy for harmful cyber actions that could block attacks before the danger reached its target, and the strategy aimed to strengthen cyber capabilities by cooperating and sharing information with U.S. allies and partners.[174] Resilience, defense forward, and sustained engagement against adversary efforts are at the core of the United States' paradigm shift in cybersecurity. Supporters contend that the new paradigm is a solution to cyber threats that may handle problems that previous deterrence techniques have not addressed, and that it will no longer be linear.[175]

---

[172] Jacquelyn, Goldman, and Warner, "Ten Years In: Implementing Strategic Approaches to Cyberspace." 38

[173] "Achieve and Maintain Cyberspace Superiority," 6.

[174] "US-DOD-Cyber-Strategy-Summary," 2.

[175] Jacquelyn, Goldman, and Warner, "Ten Years In: Implementing Strategic Approaches to Cyberspace," 39–41.

This chapter describes how, in the context of this strategic transition, the United States has responded to the kinds of significant dangers and vulnerabilities also faced by South Korea, compared to South Korea's response to cyberattacks from North Korea. Although the United States has not been able to entirely protect against cyber threats, its policy paradigm shift is strongly responsive to these threats.

B. COUNTERMEASURES AGAINST CYBER THREATS IN THE UNITED STATES

This section analyzes countermeasures the United States is taking against the kinds of cyber attacks that South Korea is now confronting. These countermeasures include infrastructure facility resilience, avoidance of cyber psychological warfare, and response to cryptocurrency theft. The analysis assesses how the United States. sees each threat today, how it has responded to the most recent cyber attacks, and what preventative steps it has implemented.

1. Resilience

After the 2007 Estonian cyber siege, several technologically advanced governments began to improve national cyber resilience, and public policy thought has undergone a rapid evolution. As a result of the Stuxnet and Saudi Aramco attacks, as well as the escalating use of ransomware against utility firms, a new policy approach for defending essential services has appeared on national agendas.[176] The increased awareness of infrastructure threats has sparked interest in cyber resilience. In the past, people used the term resilience, and the definition made sense in context. The term "cybersecurity resilience" is specifically defined in Presidential Policy Directive-21 (PPD-21). "Security" in the document refers to "reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." And the term "resilience" means "the ability to prepare for and adapt to changing conditions and

[176] Heli Tiirmaa-Klaar, "Building National Cyber Resilience and Protecting Critical Information Infrastructure," Journal of Cyber Policy 1, no. 1 (January 2, 2016): 103, https://doi.org/10.1080/23738871.2016.1165716.

withstand and recover rapidly from disruptions.[177] To put it another way, cybersecurity resilience is the ability to react to changes and recover quickly from damage in order to protect infrastructure facilities from diverse threats.

On August 2, 2012, the Senate blocked a vote on the 2012 Cybersecurity Act (CSA), the most significant legislative action on cybersecurity issues in the United States at the time. Although the laws urged operators of vital infrastructure such as water and electricity providers to upgrade their computer and network systems, policymakers and legislators experienced significant hurdles in their efforts to increase cyber resilience.[178] In a *Wall Street Journal* editorial ahead of the August vote, President Obama pushed the Senate to adopt the bill, claiming that it "would be the height of irresponsibility to leave a digital backdoor wide open to our cyber enemies."[179] And Senator Lieberman, who initiated the bill, underlined the urgency of passing the bill, warning that the president would be forced to issue an executive order if the Senate voted against it.[180] Finally, President Obama stated in Executive Order 13636 (Improving Critical Infrastructure Cybersecurity) on February 12, 2013, that the increase in cyberattacks on critical infrastructure is one of the most dangerous threats to national security facing the United States and must be protected.[181] In PPD-21 (Critical Infrastructure Security and Resilience) issued on February 12, 2013, President Obama underlined that critical infrastructure must be secure, able to endure any hazards, and recover swiftly, and he proposed three strategic challenges:

---

177 "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," whitehouse.gov, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

178 Tiirmaa-Klaar, "Building National Cyber Resilience and Protecting Critical Information Infrastructure," 103.

179 Ramsey Cox and Martinez Jennifer, "Senate Votes down Lieberman, Collins Cybersecurity Act a Second Time," Text, *The Hill* (blog), November 15, 2012, https://thehill.com/policy/technology/268053-senate-rejects-cybersecurity-act-for-second-time/.

180 Cox and Jennifer.

181 "Executive Order -- Improving Critical Infrastructure Cybersecurity," whitehouse.gov, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

- Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;
- Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government;
- Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.[182]

As technology evolves and the cyber environment changes, the reliance on large national facility networks grows, and as adversary cyber assault methods diversify, experts emphasize resilience even more. Philip Quade, former chief of the National Security Agency (NSA) Cyber Task Force, uses influenza as an illustration of the importance of both prevention and resilience. During flu season, he stated that people may lower their risk by getting vaccinated and washing their hands, but just as it is impossible to avoid catching all viruses, it is crucial for critical facilities to restore systems as quickly as possible when hostile cyber threats cannot be avoided.[183] Furthermore, given to the nature of the cyber environment, all dangers must be detected and addressed in all components in order to defend the facility. However, experts underline the necessity of resilience since it is impossible to anticipate and prevent all threats because new functions and components are constantly added to a system with a complex structure that connects multiple systems.[184]

In line with the infrastructure protection strategy of the United States government, DHS has undertaken ongoing efforts to secure infrastructure in numerous ways. In 2017, the department emphasized "Continuity Operation" through Federal Continuity Directive (FCD) 1, highlighting that vital infrastructure must be designed in a four-step procedure to

182 "Presidential Policy Directive -- Critical Infrastructure Security and Resilience."

183 "In Discussion with Philip Quade, Chief of NSA Cyber Task Force," National Security Agency/ Central Security Service, accessed October 19, 2022, https://www.nsa.gov/Press-Room/News-Highlights/ Article/Article/1625859/in-discussion-with-philip-quade-chief-of-nsa-cyber-task-force/ http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FNews-Highlights%2FArticle%2FArticle%2F1625859%2Fin-discussion-with-philip-quade-chief-of-nsa-cyber-task-force%2F.

184 Hyuk Kwon, "A review of power grid cyber & natural disasters and cyber resilience," The Korean Institute of Electrical Engineers 71, no. 2 (February 2022): 26–27.

guarantee that it is robust and continues to operate effectively: Readiness and Preparedness, Activation, Continuity Operations, and Reconstitution.[185] And DHS urged for organizational-level risk assessments and priority to strengthen the FCD-2 infrastructure's resilience. DHS expects that companies will be able to build resilience and adjust more quickly to shifting threats if they recognize emerging hazards to their infrastructure operations and allocate resources to regions with the highest risk.[186]

Despite early emphasis on resilience and several countermeasures, including PPD-21's emphasis on protecting critical infrastructure, the United States was unable to avoid such a cyberattack. Colonial Pipeline, the largest fuel pipeline corporation in the United States, was hacked by ransomware on April 29, 2021. According to cybersecurity experts, hackers exploited compromised passwords to gain access to networks, demanding a ransom in exchange for their recovery.[187] The hack had no effect on the pipeline's ability to function, but the company feared that it would expand to consumers, their financial information, and the operating system. Therefore, the company shut down its oil pipelines, which caused significant disorder in affected parts of the country, such as a gas shortage and soaring gas prices. The corporation operates a pipeline infrastructure that extends from the Houston, Texas region to the New York port. The Colonial Pipeline system has a tank storage capacity of one million barrels and connects more than 270 terminals to refineries on the Gulf Coast and elsewhere for a reliable energy supply. Each day, 100 million gallons of fuel are transported through pipelines and supplied to U.S. airports and the U.S. military.[188] This was the first time the company's pipeline infrastructure had been shut down for an extended period. Colonial was out of operation for six days due to

[185] DHS, "Federal Executive Branch National Continuity Program and Requirements," *Federal Continuity Directive* 1 (January 17, 2017): 45.

[186] DHS, "Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process," *Federal Continuity Directive* 2 (June 13, 2017): 2–3.

[187] William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," *Bloomberg.Com*, June 4, 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[188] "Colonial Pipeline Company," *Hoover's Company Records* (Fort Mill, United States: Mergent, 2022), http://www.proquest.com/docview/1860763829/abstract/C0D5997BC8444D05PQ/1.

ransomware, and it took an additional three days after restarting to achieve full capacity.[189] They also paid the $5 million ransom sought by the hackers in cryptocurrency to restore normalcy, in part because they believed the shutdown of the pipeline would harm public transportation, refineries, and chemical industries.[190]

a. U.S. Response to Improve U.S. Cyber Resilience

At the joint hearing on the Colonial Pipeline incident, experts defined the boundaries of each agency responsible for national cybersecurity and suggested repercussions. Colonial had refused to submit to the Transportation Security Administration (TSA) request to physically examine cyber security 13 times under the excuse of Covid-19, and chose to cooperate with the security evaluation only two weeks after the incident, according to the investigation of the cyber incident. In fact, the TSA had the legal right to examine the enterprise's security competence, but did not do so. In addition, CISA has a program called "CyberSentry" that monitors real-time cyber threats to partner networks of critical infrastructure in which CISA participates, but the program is not legally enforceable. Experts urge that the TSA, CISA, FBI, and other federal agencies that play a role in preventing cyberattacks on critical infrastructure fulfill their respective duties and implement a legislative framework to safeguard critical infrastructure.[191]

Shortly after the Colonial Pipeline incident, President Joe Biden signed the Executive Order on Improving the Nation's Cybersecurity to bolster the United States' cybersecurity defenses against a series of cyberattacks targeting private industry and federal government networks. In this executive order, the government is dismantling information-sharing barriers between the Infrastructure Security Agency (ISA), FBI, and other elements of the Intelligence Community (IC) in an effort to modernize the federal government's

---

189 Stephanie Smith, *Out of Gas: A Deep Dive into the Colonial Pipeline Cyberattack* (London, 2022), https://doi.org/10.4135/9781529605679.

190 Allegra Hobbs, *The Colonial Pipeline Hack: Exposing Vulnerabilities in U.S. Cybersecurity* (London, 2021), https://doi.org/10.4135/9781529789768.

191 CYBER THREATS IN THE PIPELINE: LESSONS FROM THE FEDERAL RESPONSE TO THE COLONIAL PIPELINE RANSOMWARE ATTACK, 117–18 (Washington: U.S. Government Publishing Office, 2021), 2–4.

security net and address software supply chain vulnerabilities. In addition, the document included the consolidation of the federal government's playbook for incident response, as well as the enhancement of its ability to detect and address problems and conduct incident investigations in the shortest time possible for effective follow-up in the event of a security incident.[192]

In addition to executive orders, the Biden administration has released a variety of regulations to defend infrastructure from cyberattacks. Given that the majority of U.S. vital infrastructure is operated by the private sector, the administration has provided cybersecurity performance criteria to encourage the adoption of basic cybersecurity standards, and collaborates extensively with vital industries, such as pipelines, transportation, water, and healthcare, to enhance cyber resilience.[193] In December 2021, the TSA disseminated its criteria for protecting vital infrastructure to private companies: designating a cybersecurity coordinator, reporting damage within 24 hours to CISA, and investigating potential vulnerabilities through cybersecurity vulnerability assessments. In addition, they urged infrastructure companies with little risk to engage freely.[194] In addition, the TSA has changed and reprinted its infrastructure operator cybersecurity standards based on feedback from CISA, industry stakeholders, and federal partners. As threats to critical infrastructure evolve, TSA and CISA announced that they will continue to improve cybersecurity resilience through real-time reactions to changes in the threat

[192] The White House, "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[193] The White House, "FACT SHEET: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity," The White House, October 11, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/.

[194] DHS, "DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators | Homeland Security," Department of Home Security, December 2, 2021, https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.

landscape.[195] And the Cyber Incident Reporting for Critical Infrastructure Act (H.R.5440), signed by President Biden in March 2022 and administered by CISA, provides legal protection and guidance to businesses operating in critical infrastructure sectors, which includes stipulating that businesses reporting cyber incidents within 72 hours and ransom payments within 24 hours.[196] However, this law does not legally enforce the obligations of private companies to protect infrastructure. Instead, Congress is mandating that the Federal Energy Regulatory Commission (FERC) enforce regulations encouraging private companies to invest in advanced cybersecurity technologies and engage in cyber threat intelligence sharing. In doing so, the government promotes autonomous and proactive information exchange regarding cyber threats.

In summary, the U.S. government has prepared numerous laws and systems in anticipation of enemy threats to national critical infrastructure facilities, and various government agencies have developed systems to manage infrastructure facilities and provide private companies with information on cyber threats to prevent enemy attacks. Cyberattacks on infrastructure continue, although in a variety of forms. To prepare as much as possible for infrastructure security, and to adapt after attacks that do happen, the U.S. government often updates policies and practices through executive orders, assigns duties to each department, and ensures private enterprises are fully prepared through regular communication with government agencies and cyber threat sharing.

2. Psychological Warfare

During the November 2016 U.S. presidential election, a server of the Democratic National Committee (DNC) was hacked, information was leaked, and fake information smearing opponents was disseminated, resulting in a sequence of significant incidents that

[195] TSA, "TSA Revises and Reissues Cybersecurity Requirements for Pipeline Owners and Operators | Transportation Security Administration," ransportation Security Administration, July 21, 2022, https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners.

[196] Hunton Andrews Kurth LLP, "Cyber Incident Reporting for Critical Infrastructure Act," Privacy & Information Security Law Blog, September 30, 2022, https://www.huntonprivacyblog.com/2022/09/30/cyber-incident-reporting-for-critical-infrastructure-act/.

may have affected the election. The Director of National Intelligence (DNI) report evaluating the influence of Russia on the 2016 U.S. presidential election campaign asserted that Russia's objectives were to erode public faith in the democratic process in the United States, disparage Secretary Hillary Clinton, and damage her electability for the presidency. The report also analyzed Putin further and concluded the Russian government has established a definite preference for Trump to be elected.[197]

Russia's hacking techniques and strategies for disseminating the hacked information varied. According to the DNI's report, Russian intelligence services gathered information against the major U.S. presidential campaigns, research institutes, and lobbying organizations that they deemed likely to influence future U.S. policies. In July 2015, Russian intelligence gained access to DNC networks and kept this ability until at least June 2016.[198] The Russian Internet Research Agency (IRA) was established in 2013 and acquired server space on U.S.-based computers using IDs obtained from digital payment systems. In addition, they forged identification papers and assumed these accounts on social media networks. The effort included purchasing social media commercials, organizing online rallies, and disseminating hashtags.[199] Russian hackers disclosed secret Democratic Party records on several platforms, including the Democratic Party's role in the primary between Bernie Sanders and Hillary Clinton, fueling divisions inside the Democratic Party.[200] Throughout the U.S. presidential campaign, Russia's criticism of Secretary Clinton was persistently hostile, accusing her of corruption, bad physical and mental health,

[197] Director of National Intelligence, Assessing Russian Activities and Intentions in Recent U.S. Elections., ICA 2017 (Washington, D.C.: Office of the Director of National Intelligence, National Intelligence Council, 2017). ii

[198] Director of National Intelligence, 2.

[199] Stephen McCombie, Allon J. Uhlmann, and Sarah Morrison, "The U.S. 2016 Presidential Election & Russia's Troll Farms," Intelligence and National Security 35, no. 1 (January 2, 2020): 100, https://doi.org/10.1080/02684527.2019.1673940.

[200] Jeong Yoon Yang, Kyudong Kim, and So Jeong Kim, "Implications on National Security Strategies of the Strategic Use of Cyber Capabilities of Foreign Governments: The Case of Alleged Russian Interference in the 2016 U.S. Election," Korean Crisis Management Journal 13, no. 11 (November 2017): 107.

and links to Islamic terrorism.[201] They also revealed that Hillary Clinton used personal emails to process federal documents throughout her term as secretary of state, generating criticism over her qualifications for the presidency.[202]

Instead of the traditional strategy of keeping investigations and findings fully confidential, intelligence agencies have adopted the unorthodox approach of detailing probes and disseminating reports in order to demonstrate Russian involvement. As an example, DHS and the FBI issued the "GRIZZLY STEPPE: Russian Malicious Cyber Activity" Joint Analysis Report (JAR). The report title refers to the RIS's malicious cyber operations known as GRIZZLY STEPPE, related to the 2016 election, and the report demonstrates that RIS was responsible for the U.S. presidential election interference case and details the attack technology used by RIS to penetrate government and private networks.[203] According to the report, the U.S. government has established the involvement of two other RIS actors, APT29 and APT28, in the infiltration of U.S. political parties. APT29 sent spear-phishing emails to around 1,000 individuals in the summer of 2015 to disseminate malicious code and attack political parties. In the Spring of 2016, APT28 launched a second spear-phishing attempt against the same political group, using fake webmail to reset user passwords.[204]

The DNI then released a report titled "Assessing Russian Activities and Intentions in Recent U.S. Elections," which was based on intelligence gathered by the FBI, the Central Intelligence Agency (CIA), and the NSA. In particular, to reinforce its assertion of Russian interference, the report examines the motives and circumstances of Russia's use of cyber

---

[201] Director of National Intelligence, Assessing Russian Activities and Intentions in Recent U.S. Elections., 3.

[202] Gregory F. Treverton et al., Hybrid Threats: Russian Interference in the 2016 U.S. Election (Försvarshögskolan (FHS), 2018), 34, http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574.

[203] Yang, Kim, and Kim, "Implications on National Security Strategies of the Strategic Use of Cyber Capabilities of Foreign Governments: The Case of Alleged Russian Interference in the 2016 U.S. Election," 108.

[204] National Cybersecurity and Communications Integration Center and United States Federal Bureau of Investigation, Grizzly Steppe: Russian Malicious Cyber Activity. (Washington, D.C.: U.S. Department of Homeland Security, NCCIC, 2016), 2–3.

tools and media reports to influence U.S. public opinion.[205] In May 2017, former Director of National Intelligence James Clapper testified before the Judiciary Subcommittee on Crime and Terrorism of the U.S. Senate to discuss Russia's long-time pursuit of influencing efforts to influence public opinion in the 2016 presidential election. He deemed Russia's effort a success that exceeded his expectations.[206]

As a result of the election interference, cyber security experts began to pay more attention to the role of social media, while simultaneously criticizing Facebook and other platforms for propagating incendiary political statements. Democrats and Republicans criticized the social media business for failing to monitor its users. Eventually, Facebook founder Mark Zuckerberg pledged to make changes to prevent the notion that his platform was destructive to democracy.[207]

a. U.S. Response to Russian Election Interference

On April 1, 2015, President Obama signed Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." As cyberattacks from abroad continued to represent a unique threat to national security, foreign policy, and the economy, he stated that the United States requires government intervention.[208] The goal of this Executive Order was to enable the Attorney General, the Secretary of State, and the Treasury Secretary to impose severe financial consequences, including asset freezes, on persons and businesses participating in the conduct of such activities. As a follow-up to EO 13694, to specifically address Russian intervention in the U.S. presidential election, on December 28, 2016, President Obama signed Executive Order

[205] Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent U.S. Elections," January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf

[206] McCombie, Uhlmann, and Morrison, "The U.S. 2016 Presidential Election & Russia's Troll Farms," 97.

[207] Demetri Sevastopulo, Courtney Weaver, and Barney Jopson, "US Charges Russians with 2016 Election Interference," FT.Com, February 16, 2018, http://www.proquest.com/docview/2121959418/citation/1CDA41CB32904BADPQ/1.

[208] "Executive Order -- 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" whitehouse.gov, April 1, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

13757, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities." This directive supplemented the response to cyber risks, including foreign intervention in elections, and its appendix included property freezes and entry controls for five Russian institutions and four individuals.[209]

The United States also responded by passing legislation. The National Defense Authorization Act for Fiscal Year 2017 (S.2943), which was signed into law on December 13, 2016, contains provisions regarding disinformation and other propaganda tactics employed by foreign governments, particularly the Russian Federation and Chinese governments. In this statute, emphasis was placed on the development of an analysis and reaction center since a complete strategy is required to respond to foreign disinformation and propaganda.[210] To prevent operations that harm national security objectives, the U.S. government has established the Global Engagement Center (GEC) and is making worldwide efforts, such as tracking and verifying misinformation activities, with the participation of the United States, its allies, and its partners. The Countering U.S. Adversaries Through Sanctions Act, passed on August 2, 2017, imposes sanctions on enemy nations such as Russia, Iran, and North Korea. Through these legislations, the United States maintains economic sanctions to offset Russia's influence on Europe and Eurasia and to prevent Russia's use of cyber forces to interfere in U.S. politics. It tries to limit Russia's impact on U.S. national security by maintaining sanctions on oil, financial institutions, human rights, and export pipelines.[211] USCYBERCOM also prepared measures to defend against Russian interference in U.S. elections. According to U.S. National Security Director Paul M. Nakasone, USCYBERCOM, in conjunction with the NSA, established the Russia Small Group to ensure transparent 2018 midterm elections,

[209] "Executive Order 13757 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities)," whitehouse.gov, December 28, 2016, https://irp.fas.org/offdocs/eo/eo-13757.htm.

[210] John McCain, "S.2943 - 114th Congress (2015-2016): National Defense Authorization Act for Fiscal Year 2017," legislation, December 23, 2016, 2015/2016, http://www.congress.gov/.

[211] Edward R. Royce, "H.R.3364 - 115th Congress (2017-2018): Countering America's Adversaries Through Sanctions Act," legislation, February 8, 2017, 2017/2018, http://www.congress.gov/.

continuously monitoring adversaries in cyberspace and working to thwart adversary efforts.[212] In 2019, USCYBERCOM and the NSA jointly announced that the Russian Small Group would be operated as a permanent task force for collaborating with comparable organizations against adversary psychological warfare, recognizing Russia as a long-term threat in cyberspace and projecting that Russia would mount a more aggressive threat to American democracy in the 2020 presidential election.[213]

USCYBERCOM later assessed that it was successful in preventing foreign intervention in the 2020 election by working closely with other essential agencies. Accordingly, USCYBERCOM revised the Russian Small Group into the Election Security Group (ESG) and expanded its scope to threats not only from Russia, but also from China, North Korea, Iran, and non-state actors.[214] USCYBERCOM and NSA have chosen a USCYBERCOM general manager and a senior NSA officer to be responsible for the security of the midterm elections in 2022. In doing so, they are once again building a comprehensive defense against outside intervention in the election.[215]

In a March 2021 report, the National Intelligence Council (NIC) assessed Russian cyberattacks on the United States' presidential elections in 2020. As in 2016, the NIC determined that during the election, Russia conducted an operation to undermine public trust and negatively impact politics and society by circulating false material in cyberspace in order to achieve their political goals. However, the United States assessed that this time the Russian effort failed due to physical barriers around the polling locations and meticulous preparations including cyber-monitoring prior to the election. The NIC also

---

[212] C. Todd Lopez, "Cyber Command Expects Lessons From 2018 Midterms to Apply in 2020," U.S. Department of Defense, accessed November 15, 2022, https://www.defense.gov/News/News-Stories/Article/Article/1758488/cyber-command-expects-lessons-from-2018-midterms-to-apply-in-2020/.

[213] Shannon Vavra, "NSA's Russian Cyberthreat Task Force Is Now Permanent," CyberScoop, April 29, 2019, https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/.

[214] Martin Matishak, "NSA, Cyber Command Tap New Election Security Leaders," *The Record by Recorded Future* (blog), May 5, 2022, https://therecord.media/nsa-cyber-command-election-security-leaders/.

[215] Paul Nakasone, "Posture-Statement" (UNITED STATES CYBER COMMAND, April 5, 2022), 5, https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf.

determined that, in the future, it would be challenging for foreign forces to intervene in elections or manipulate the election process.[216] Additionally, according to a 2021 Justice Department press release, the FBI charged two Iranians with participating in a campaign to scare voters and sow dissension during the 2020 U.S. presidential election. Due to the FBI's mitigating efforts, the Iranian suspects' attempt to steal voter information and propagate disinformation via election websites failed.[217]

In summary, the United States has continually attempted to establish comprehensive and strategic countermeasures against Russia, China, and other foreign governments that undermine the interests of the United States and its allies through disinformation and propaganda. These actions have ranged from legislation to executive orders to responsive actions by many different U.S. executive agencies, including USCYBERCOM.

3. Cryptocurrency

Cyberattacks that use cryptocurrencies as a means or purpose provide attackers with numerous benefits. Although cryptocurrency is traceable because all transactions are recorded, it is challenging to identify the owner of the wallets containing the cryptocurrency used in a transaction because wallets can be created anonymously. Also, the decentralized nature of cryptocurrency makes it simpler for criminals to commit crimes without the controls or detection procedures of the conventional banking system.[218] These two significant aspects harm national security by enabling criminals and terrorists to utilize cryptocurrency to finance their operations and profit from illicit acts.[219] The anonymity of

---

216 "Foreign Threats to the 2020 U.S. Federal Elections," INTELLIGENCE COMMUNITY ASSESSMENT (NATIONAL INTELLIGENCE COUNCIL, March 10, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf. i

217 "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," *Department of Justice (DOJ) Documents / FIND* (Washington, United States: Federal Information & News Dispatch, LLC, November 18, 2021), https://www.proquest.com/docview/2599109949/citation/C85B7516205C4375PQ/1.

218 Carolyn Alfieri, "Cryptocurrency and National Security," *International Journal on Criminology* 9, no. 1 (February 25, 2022): 22, https://doi.org/10.18278/ijc.9.1.3.

219 Alfieri, 22.

cryptocurrencies is a major attraction for attackers who fear retaliation from the United States, making cryptocurrencies one of their few viable attack choices.

The United States understood early on that cryptocurrencies would pose a threat to national security and so took precautions. The government was concerned not only about the damage that could be caused by domestic cryptocurrency hacking, but also about the potential for countries subject to economic sanctions to use cryptocurrencies to escape sanctions. Since its launch in 2008, the U.S. government has been concerned that bitcoin could aid money laundering because users can conduct transactions anonymously and without legal repercussions. According to a Wall Street Journal survey, cryptocurrency theft activities produced approximately $90 million in revenue between 2017 and 2018, and the identities and locations of the thieves could not be determined.[220] In 2016, the U.S. Securities and Exchange Commission (SEC) determined that the sequence of token purchases and sales was a security governed by the Securities Act of 1933 and the Securities Exchange Act of 1934. This conclusion was made at a time when the concept and understanding of cryptocurrencies were unclear. [221] In addition, because cryptocurrencies were utilized in a variety of illicit activities, the SEC judged that the commission posed a possible market risk, and they attempted to take the lead in regulating cryptocurrencies.[222]

With the advent of cryptocurrencies, the United States also perceived a threat to the efficacy of the economic sanctions it has employed for national security since the end of the Cold War. The effectiveness of U.S. economic sanctions against countries that pose a danger to national security stems from the view that such sanctions deter the behavior of the target countries and have relatively low costs and political risks compared to the

220 Justin Scheck and Shane Shifflett, "How Dirty Money Disappears Into the Black Hole of Cryptocurrency," *WSJ Pro. Central Banking*, September 28, 2018, n/a.

221 "Is the Party Over? The SEC Investigates Cryptocurrency Offerings," Manatt, accessed October 26, 2022, https://manatt.com/insights/articles/2017/is-the-party-over-the-sec-investigates-cryptocurr.

222 Michael Segal, "Cryptocurrency Regulation under U.S. Securities Laws and Proposed Amendments," *Computer and Internet Lawyer* 36, no. 9 (2019): 13.

deployment of military force.[223] Since the dollar is the world's reserve currency, the United States might employ monetary sanctions as a diplomatic instrument to achieve its economic goals. The U.S. administration was compelled to reconsider the efficacy of economic penalties, however, due to the emergence of cryptocurrencies, which combine anonymity and vulnerability.[224] For that reason, the United States included crypto-currency regulations in the Russian sanction legislation in 2017. The U.S. government acknowledged growing forms of cybercrime and cryptocurrencies as illicit finance trends and emphasized identifying dangers through data analysis and discussion.[225]

The United States has not been immune to cryptocurrency risks despite its initial efforts. Because the Covid-19 outbreak has increased the reliance of businesses and individuals on networks, hackers seeking to steal cryptocurrencies have exploited network vulnerabilities to penetrate the United States. In addition, countries subject to economic sanctions have been using a variety of tactics to circumvent restrictions by evading U.S. surveillance. In early 2020, attackers exploited flaws in VPNs and networks to introduce systems with ransomware and steal money using it. According to The Coveware Quarterly Ransomware Report, between the first and second quarters of 2020, the average ransom grew by 60%, from $111,605 to $178,254, and analysts suspected that this untraceable money moved into the cryptocurrency market.[226]

Several exchanges, including the U.S.-based Bittrex, claim to adhere to regulatory rules, such as validating the source of funds and the wallets used for transactions. However, investigations reveal that Bittrex received $6.3 million in funds from criminal activity in 2018. In addition, after extorting millions of dollars through WannaCry ransomware

223 Deane R Konowicz, "The New Game: Cryptocurrency Challenges U.S. Economic Sanctions" (U.S. Naval War College, 2018), 4, https://apps.dtic.mil/sti/pdfs/AD1062142.pdf.

224 Emily Flitter and David Yaffe-Bellany, "Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions," *The New York Times*, n.d., 1.

225 Royce, "H.R.3364 - 115th Congress (2017-2018)," 51.

226 "Ransomware Attacks Split Between Enterprise & RaaS," Coveware: Ransomware Recovery First Responders, accessed October 26, 2022, https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

attacks, hackers laundered the funds by exchanging them for untraceable Monero coins using ShapeShift, an online exchange owned by a U.S. venture capital firm.[227]

When it ran out of funding for its nuclear test due to UN sanctions and Covid-19, North Korea raised a significant amount of money through cryptocurrency theft. One outstanding example is North Korea's April 2022 theft of $620 million in cryptocurrencies from the online game Axi Infinity.[228] Axi Infinity uses a "bridge" established by the Ronin firm to allow users to transfer payments into and out of the game, and hackers from North Korea attacked the bridge.[229] The "bridge" has recently become a key target for hackers, with the 2022 Binance attack serving as a prime example. According to Changpeng Zhao, CEO of Binance, $570 million worth of cryptocurrencies were stolen via the "cross-chain bridge" hack, a mechanism that enables quick token transfers between platforms.[230] In the midst of the pandemic of 2021, a report by Chanalysis discovered that North Korean hackers stole over $800 million in cryptocurrencies via attacks on platforms such as cryptocurrency exchanges and financial organizations.[231]

a. U.S. Response to Cryptocurrency Problems

As a response to the hacking of cryptocurrencies in the United States, rather than reducing the cryptocurrency market through legislation and regulation, efforts are being undertaken to mitigate damage through post-attack procedures. In truth, both federal and state governments are interested in cryptocurrencies, but there has been no official

---

227 Scheck and Shifflett, "How Dirty Money Disappears Into the Black Hole of Cryptocurrency."

228 "How North Korea Used Crypto to Hack Its Way Through the Pandemic - The New York Times," accessed October 26, 2022, https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

229 Tom Wilson, Elizabeth Howcroft, and Elizabeth Howcroft, "Explainer: Ronin's $615 Million Crypto Heist," *Reuters*, March 30, 2022, sec. Technology, https://www.reuters.com/technology/ronins-615-million-crypto-heist-2022-03-30/.

230 Elizabeth Howcroft and Elizabeth Howcroft, "Binance-Linked Blockchain Hit by $570 Million Crypto Hack," *Reuters*, October 7, 2022, sec. Technology, https://www.reuters.com/technology/hackers-steal-around-100-million-cryptocurrency-binance-linked-blockchain-2022-10-07/.

231 Chainalysis Team, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High," Chainalysis, January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

regulation of cryptocurrencies in place until very recently.[232] This is because some feel that the United States should take the lead in developing blockchain technology, advocating its importance to the future infrastructure of the United States.[233] Through legislation, some states are independently pushing the usage of cryptocurrency. Connecticut has passed laws in 2022 to assist small businesses in adjusting to the post Covid-19 business environment via cryptocurrencies, e-commerce, and social media. Meanwhile, California has authorized private or public enterprises, including government services, to accept cryptocurrencies as payment for the supply of any good or service.[234]

Recently, SEC Chairman Gary Gensler argued that because cryptocurrencies must be classified as securities, there is no need for separate guidelines for regulation, also observing this means formal registration of cryptocurrency companies.[235] This position indicates that the federal government will not enact new legislation directly regulating cryptocurrencies, but there may be restrictions imposed by existing securities regulations. Therefore, the future path of the U.S. government should be closely monitored.

Instead of additional regulation of cryptocurrencies, the United States government concentrates on criminal identification and anti-money laundering by tracking cryptocurrencies that can be used for illegal behavior. The U.S. Department of Justice indicted three North Korean hackers in the Los Angeles District Court in February 2021 following a protracted investigation involving the theft of $1.3 billion via WannaCry ransomware and cryptocurrencies.[236] Jinhyuk Park, who is a suspected member of the Lazarus Group, has been implicated in a number of cyberattacks, including the 2014 Sony

232 "Blockchain & Cryptocurrency Laws and Regulations," Text, GLI - Global Legal Insights - International legal business solutions (Global Legal Group), United Kingdom, accessed October 26, 2022, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa.

233 "Blockchain & Cryptocurrency Laws and Regulations."

234 "Cryptocurrency 2022 Legislation," accessed October 26, 2022, https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2022-legislation.aspx.

235 "Most Cryptocurrencies Are Securities, Says SEC Chair," Investopedia, accessed October 26, 2022, https://www.investopedia.com/gensler-on-crypto-6544288.

236 Alfieri, "Cryptocurrency and National Security," 25.

Pictures hack and the 2016 Bangladesh bank heist.[237] In February 2022, the Justice Department prosecuted a married New York couple for illegally laundering bitcoins stolen in a 2016 hacking of the digital currency exchange Bitfinex and at that time worth over $4.5 billion.[238] The prosecutor stated that this case shows how the government is expediting what it requires: the identification of criminals through the tracking of stolen cryptocurrencies.[239]

The Department of Justice established the National Cryptocurrency Enforcement Team (NCET) on February 17, 2022. This team is comprised of competent prosecutors for cases involving cryptocurrencies and cybercriminals in order to identify the entities that illegally utilize digital assets, as the illicit use of digital assets is on the rise due to the rapid development of technology.[240] With the launch of the Virtual Asset Exploitation Unit in February 2022, the FBI anticipates that it will be able to track down and seize illicit cryptocurrencies through complex investigations centered on international criminal networks, as opposed to simple prosecutions.[241] The Department of Justice anticipates that NCET and the FBI's Virtual Asset Exploitation Unit, as a team of professional cryptocurrency experts, will prepare for future threats by offering technical research, support, and training, in addition to anti-money laundering and asset recovery.[242]

The Treasury Department has for the first time imposed penalties on cryptocurrency exchanges. For instance, "SUEX" paid ransom to criminals in the past owing to

---

237 Park, "The Lazarus Group," 39.

238 Sarah N. Lynch and Chris Prentice, "FBI to Form Digital Currency Unit, Justice Dept Taps New Crypto Czar," *Reuters*, February 17, 2022, sec. Technology, https://www.reuters.com/technology/fbi-form-new-digital-currency-unit-justice-dept-taps-new-crypto-czar-2022-02-17/.

239 Flitter and Yaffe-Bellany, "Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions," 5.

240 "Justice Department Announces First Director of National Cryptocurrency Enforcement Team," February 17, 2022, https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team.

241 James Rundle and Catherine Stupp, "Justice Department Installs New FBI Crypto Crime Unit," *Wall Street Journal*, February 17, 2022, sec. WSJ Pro, https://www.wsj.com/articles/justice-department-installs-new-fbi-crypto-crime-unit-11645129414.

242 "Justice Department Announces First Director of National Cryptocurrency Enforcement Team."

ransomware infections, and the government actively sanctioned this exchange. By doing so, the Treasury Department wanted to increase exchange operators' cybersecurity awareness and diminish the incentives for criminals to profit from exchange assaults.[243] The U.S. government continues to watch the flow of domestic bitcoin and monitors it for theft and money laundering using the previously mentioned methods and to exert pressure on them.

Since a substantial amount of cryptocurrency was recently sent abroad in the form of ransomware, the Biden administration is also making national efforts to combat ransomware and track it. In October 2021, the United States convened a summit with several nations to tackle the proliferation of ransomware worldwide. The attending nations reached a consensus that ransomware is a growing economic and security concern that must be addressed through international cooperation.[244] In addition, they established the International Counter Ransomware Initiative (CRI) to find ways to strengthen collective resilience and remove criminal actors and criminal infrastructure by enlisting the private sector.[245] At the first CRI summit, they focused on building a consensus on ransomware, and at the second CRI summit in October 2022, member countries reaffirmed their mutual cooperation in a joint statement.[246] Partner countries pledged to jointly respond to ransomware and track illegal funds, and also put in place specific measures, including:

- Hold ransomware actors accountable for their crimes and not provide them safe haven;
- Combat ransomware actors' ability to profit from illicit proceeds by implementing and enforcing anti-money laundering and countering the financing of terrorism (AML/CFT) measures, including "know

[243] The White House, "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware," The White House, October 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

[244] The White House, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," The White House, October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

[245] The White House, "FACT SHEET," October 11, 2022.

[246] The White House, "International Counter Ransomware Initiative 2022 Joint Statement," The White House, November 1, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.

your customer" (KYC) rules, for virtual assets and virtual asset service providers;
- Disrupt and bring to justice ransomware actors and their enablers, to the fullest extent permitted under each partner's applicable laws and relevant authorities; and
- Collaborate in disrupting ransomware by sharing information, where appropriate and in line with applicable laws and regulations, about the misuse of infrastructure to launch ransomware attacks to ensure national cyber infrastructure is not being used in ransomware attacks.[247]

In the past, the U.S. government predicted that cryptocurrencies would be used to evade economic sanctions or to finance terrorism. Although it did not actively intervene in cryptocurrencies, blockchain technology, and exchanges, the U.S. government did implement regulations (albeit limited ones) prohibiting cryptocurrencies from being liquidated and laundered. The United States not only led creation of the CRI in its global response, but also established a rapid response mechanism to cyber threats within NATO to prevent cryptocurrency laundering and track attackers. The U.S. government continues to collaborate with allies and partners to build collective responses to cryptocurrency challenges in order to achieve effective cybersecurity.[248]

C. OVERALL ASSESSMENT OF U.S. RESPONSES

The previous section has analyzed countermeasures the United States has taken to obtain infrastructure facility resilience, avoid cyber psychological warfare, and respond to cryptocurrency theft. This assessment provides an overall picture of how well the United States is preparing against cyber threats and how it responds when attacked.

1. Immediate Response

When an adversary's cyberattack is anticipated to pose a threat to national security or inflict real damage, the United States can respond swiftly by issuing an executive order from the president. This executive order not only prepares countermeasures to remedy

247 The White House.

248 The White House, "FACT SHEET," October 11, 2022.

problems as rapidly as possible through threat assessment, but it also provides relevant departments with direct action guidelines and timelines for updating cyber threats as quickly as possible. Since the 9/11 terrorist attacks in 2001, there have been ten executive orders relating to cybersecurity, including E.O. 25547, "Improving the Nation's Cybersecurity," and three executive orders linked to infrastructure protection, including E.O. 22397, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[249] In addition, the executive order for comprehensive national security improvements includes a section on cybersecurity. There are also eight presidential decision directives pertaining to cybersecurity, including the National Security Memorandum X, "Improving Cybersecurity for Critical Infrastructure Control Systems," issued by the Biden administration.[250]

The U.S. executive orders and decision directives on cybersecurity identify the most recent cyber risks confronting the United States, and design and implement effective responses to promote U.S. cyber security regardless of changes in the dominant party or administration.

2. Information Sharing System

To defend critical facilities and operating systems against ATP threats and developing ransomware, the United States government has encouraged information exchange. Threat sharing not only enables companies within the system to effectively respond to the same type of attack that may occur in the future, but it also improves resilience to resume normal operations in the shortest time possible by sharing a certain type of playbook based on the severity of the damage.

However, the federal government cannot compel private enterprises to submit threat information under the United States' information sharing system. Although the

249 "Executive Orders," Federal Register, accessed November 8, 2022, https://www.federalregister.gov/presidential-documents/executive-orders.

250 "Presidential Directives and Executive Orders," Federation of American Scientists, accessed November 8, 2022, https://irp.fas.org/offdocs/direct.htm.

Infrastructure Investment and Jobs Act (H.R.3684) underlined the necessity of sharing information about cyber threats, the federal government cannot force private enterprises to disclose information, and so instead has left private organizations to exchange information autonomously. In fact, the U.S. government learnt from the U.S. pipeline hacking event that private corporations do not proactively and actively respond to cybersecurity competency evaluations, and that when problems develop, private companies may choose to hide rather than tell the government. Therefore, the United States is actively participating in the cyber threat sharing system by providing incentives for companies to self-improve their cyber security capabilities or share threat information voluntarily, thereby enhancing the defense and resilience of infrastructure facilities.

Sharing knowledge about cyber threats does not deter opponent attacks. However, if information about the objective and method of the attack is gathered through threat analysis prior to the enemy's attack, infrastructure companies can prepare for defense and recover quickly even if they are damaged. Accordingly, the evaluation in this chapter judges that the United States government's incentive approach to promote information sharing will be adequately effective.

3. Defend Forward

In cyber psychological warfare, the attacker, the attack method, the degree of harm, and the impact on society are all uncertain, but the U.S. government has embraced the ambiguity by actively investigating and preparing for such attacks. The United States examined the threats to its national security from all directions, identified the perpetrators, and imposed sanctions. By evaluating attack techniques, the U.S. government continued to track and manage the enemy's threats rather than implementing only an immediate reaction to avoid the same type of attack by the same actors on U.S. security in the future. At the front of this proactive effort, the United States employs a "Defend Forward" posture, reflecting the evolving cybersecurity paradigms, to protect itself from harmful cyberattacks. A feature of this posture is to identify and fundamentally obstruct the source of the adversary's cyber actions designed to undermine democracy, such as cyber psychological

warfare. The United States continues to prevent the activities of its enemies by waiting for them to come out in front of their own homes, a shift from its previous posture to defend its own home by waiting at its own door.

Ahead of the 2020 elections, U.S. National Security Director Nakasone stated that by gaining a deeper understanding of the adversary, the United States will know them better than they know themselves. As a result, the United States will be able to bolster its defenses and protect itself more aggressively. Furthermore, he stated that America's adversaries can enhance their capacities and utilize them to launch strikes on the United States, but whenever they try to do so, America is already present and will have a significant influence on those efforts.[251] By successfully defending the 2020 U.S. presidential election from enemy interference demonstrated that these constant and preventative preparations were adequate to counter the enemy's cyber psychological warfare.

4. Track the Enemy

Although the United States acknowledges that cryptocurrencies are difficult to track and are thus exploited by adversaries for ransom payment and a source of money laundering, the United States anticipates that blockchain technology will serve as the foundation for many future innovations. Instead of actively controlling cryptocurrencies and blockchain technology, the government is allowing their widespread adoption in the life sciences and industry. In addition, a CISA investigation reveals that it is sometimes cheaper and more efficient for organizations to donate ransomware to cybercriminals than to repair ransomware-damaged systems and data.[252]

Since the government cannot legally force the decisions of private enterprises, they are putting more effort into forming a team to track and recover cryptocurrencies by forming a team dedicated to that. Even if enemies use ransomware against U.S.

[251] "Why Russia May Have Stepped Up Its Hacking Game," NPR.org, accessed November 9, 2022, https://www.npr.org/2021/01/29/960810672/why-russia-may-have-stepped-up-its-hacking-game.

[252] Alfieri, "Cryptocurrency and National Security," 24.

infrastructure or private companies to steal cryptocurrencies, or hack cryptocurrency exchanges and bridges to steal cryptocurrencies, the tracking team can recover the cryptocurrencies through investigations of multiple sources and identify and prosecute the attackers. In addition, the United States is drafting agreements on the severity and prevention of cyber financial crimes through domestic response teams, supranational organizations, and worldwide initiatives.

When adversaries plan a cyberattack, they compare the effort necessary for the attack to the benefits that may be acquired, and when the benefit is more than the effort, they launch the attack. However, the follow-up procedures that the United States has thus far demonstrated to its enemies through tracking systems are effective at discouraging adversary behavior, since attackers realize they must not only take more trouble to conceal their identities but also are likely to earn significantly less than anticipated even if an attack is successful.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

In 2022, North Korea has not only escalated the situation on the Korean Peninsula through military provocations such as missile launches in the East Sea, the ICBM, and nuclear tests, but also threatens South Korea invisibly through cyberspace. The South Korean government is making attempts to neutralize North Korean cyberattacks using the ROK's superior IT infrastructure and to efficiently respond to cyber threats by enacting laws and establishing rules. Due to the nature of the Internet, South Korea cannot effectively thwart all of North Korea's cyberattack attempts. However, South Korea can predict, prepare for, and actively respond to an assault by North Korea. And even if South Korea suffers harm from a North Korea's cyber assault, the ROK can dissuade North Korea from taking further actions if it recovers to its previous operating condition as quickly as possible, evaluates risks via thorough investigations, and identifies the sources of attacks by successfully tracing them.

In Chapter II, this report assesses the cyber risks which North Korea poses to South Korea based on the severity of damage South Korea would sustain and the government's response. In comparison, Chapter III examined the United States' response to the types of cyber dangers listed in Chapter II. The United States continues to create and reinforce its cyber security policies, adapting to the various cyberattacks it receives from around the globe. This chapter addresses the potential influence of lessons gained from the United States' reaction for the ROK's cyber strategy, building on prior assessments of possible lessons reviewed in Chapter I, and identifies new study directions in the field of cyber security identified via research on South Korean and U.S. cyber strategies.

A. IMPLICATIONS

This research inferred some practical implications for ROK cyber policy through a case study in the United States. And this implication was not based solely on U.S. policy, but on South Korea's present cyber capabilities and cyber environment.

1. Immediate Response

As reviewed in Chapter I, many prior scholars and analysts have focused on challenges of improving South Korea's laws and institutions. South Korea attempted to devise comprehensive procedures and amend the law at the government level to solve the immediate problem in the case of damage caused by a cyberattack from North Korea. However, the government's comprehensive cyber countermeasures are not only vague on the tasks to be completed by each competent department, but they also lack legal compulsion; thus, the relevant ministries either went in a different path or did not move at all. In addition, the government has made efforts to prepare laws to ensure legal binding force and prevent recurrences, but it takes between six months and a year for legislation to be officially promulgated, following consultation and examination by the government, submission to the National Assembly, and passage.[253] Consequently, this strategy is not a prompt reaction to cyberattacks. Furthermore, these laws may be rejected by the National Assembly because of social and political concerns; hence, very little cyber security legislation proposals have received the approval of the National Assembly and been enacted into law.

In order to swiftly respond to North Korea's cyber threat, the South Korean government may consider issuing a presidential decree similar in form and method to the executive order issued by the President of the United States. In accordance with Article 75 of the Constitution of the Republic of Korea, the President may issue presidential decrees pertaining to topics entrusted with specified scope in the Act and matters required for the enforcement of the Act.[254] In addition, the government can utilize the presidential decree to address cyber security concerns at the national level due to the decree's jurisdiction over national security policy and cross-ministry issues. The analysis of prior presidential decrees in South Korea reveals that there are presidential decrees and enforcement decrees in a

253 "Introduction to the Government Legislative System," Government Legislative Support Center, accessed November 18, 2022, https://www.lawmaking.go.kr/lmGde/govLm.

254 "Korean Constitution," National Law Information Center, accessed November 8, 2022, https://www.law.go.kr/LSW/lsInfoP.do?efYd=19880225&lsiSeq=61603#0000.

variety of disciplines, but only three connected to cyber security and none related to infrastructure protection.[255]

Despite acknowledging that cyberattacks pose a direct danger to national security, South Korea's response to these risks is insufficient. Prior scholars and analysts have not paid enough attention to the advantages fast executive actions, rather than slow and inflexible law-making, to improve South Korean cyber security. In order to reply as swiftly as possible to an adversary's cyberattack, one of the most effective tools are a presidential decree with immediate legal effect, as opposed to comprehensive actions that require or lengthy legislation and have no enforcement mechanism.

2. Information Sharing System

Prior analysts have noted the value of integrated U.S. information sharing, and South Korean efforts to follow this lead. Similar to the United States, the South Korean government has built information sharing platforms such as Cyber Threat Analysis and Sharing (C-TAS) administered by KCTI, NCTI, and KISA of the National Intelligence Service to efficiently respond to cyber threats and enhance resilience. In addition, the government is urging government agencies, commercial businesses, cryptocurrency exchanges, and cybersecurity firms to engage and share information.

However, due to private firms' concern about image protection, breaches of trade secrets and proprietary information, and cybersecurity issues, companies may be reluctant to share information about cyberattacks and vulnerabilities, and the South Korean government cannot legally compel private companies to do so. The chief information protection officer of a South Korean private firm said that hackers are upgrading their assault strategies by exchanging information on the dark web, while domestic organizations are unable to exchange information and respond quickly owing to internal confidentiality

255 "Korean Constitution."

rules.[256] So, private businesses are still reluctant to share information regarding cyber threats.

The findings of this thesis build on prior recommendations by showing in more detail how the U.S. government succeeds in generating cooperation among private companies without compelling it. Companies can be urged to actively engage if South Korea creates a way that gives incentives to corporations that share cyber security knowledge and information, as the United States is now doing. If the cyber threat information sharing system now operating in South Korea is maintained and the government legally ensures an incentive structure for firms that submit high-quality information, cooperative reaction to cyber threats will expand, resulting in more effective countermeasures against adversary cyberattacks and speedier reaction when they occur.

3. Defend Forward

South Korea is building preventative capabilities to gather, manage, and eliminate network vulnerabilities in anticipation for North Korean cyberattacks, but it has not yet achieved the preemptive defensive level of the United States. Prior scholars and analysts have only begun to recognize the importance of the newer U.S. active defense strategy as a foundation for all aspects of its cyber security, and the potential of this model for South Korea. The findings of this thesis also show how technology resources are essential to an active defense posture. While perception of the government's cyber defense policy is a factor, South Korea's cyber capabilities are also relevant, because identifying attackers' origins in advance, predicting their behaviors, and continually observing them all requires a high level of technical expertise.

The two countries' situations are not identical. To prevent Russia from interfering in U.S. elections through cyber psychological warfare, the United States deported the guilty parties, applied economic sanctions, forecasted the enemy's intentions in advance, and countered them proactively with superior cyber technology. In contrast to Russia and the

[256] Yoon-hee Kim, "Meeting to Share Hacking Information," *ZDnetKorea*, November 17, 2021, https://zdnet.co.kr/view/?no=20211117173540.

United States, South Korea has few economic and physical ties with North Korea; hence, forced deportation and economic penalties on North Korea have a limited impact. In addition, unlike Russia, North Korea does not overtly interfere in South Korean elections, thus there are little reasons for punishment or retaliation.

However, North Korea continues to promote divisiveness through the manipulation of public opinion in South Korean society and its attempts to influence the political judgment of the government. The South Korean government can effectively respond to North Korea's cyber psychological warfare if it adopts a "Defend Forward" policy similar to that of the United States and abandons the current practice of researching and responding to a situation after it has occurred. However, the government and its cyber-related ministries must thoroughly comprehend the paradigm shifts in cyber security that this requires, and develop the cyber capabilities within each institution to enable this more active posture.

4. Track the Enemy

The findings of this thesis support prior analysts' observations that the U.S. emphasis on cyber collaboration with allies and global institutions should be a model for South Korea's cybersecurity strategy. Some recent actions move in this direction. The South Korean government seeks international collaboration by joining as a member of the CRI, which is led by the United States, in order to identify the objective of cyberattacks and recover stolen cryptocurrency. In addition, through the recent international symposium on "Response to North Korean Cryptocurrency Theft," the ROK pledged to develop a network of cooperation by exchanging information on North Korea's types of cryptocurrency theft and countermeasures.[257] By joining the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) as a regular member in May 2022, for the first time by a non-

[257] Ministry of Foreign Affairs, "Korea-U.S. joint public-private symposium held in response to North Korean cryptocurrency theft," Ministry of Foreign Affairs, November 17, 2022, https://overseas.mofa.go.kr/www/brd/m_4080/view.do?seq=373025.

NATO country, it is anticipated that South Korea's cyberspace security capabilities would be enhanced via the building of a worldwide cyber security network.[258]

In contrast to the government's international cooperation efforts, domestic attempts to track cryptocurrencies and cyberattacks remain weak. In response to the rise in cryptocurrency mishaps, the police have established and run a cryptocurrency-tracking unit, but this is to prevent individuals from causing economic loss through cryptocurrency hacking.[259] The police are not involved in large-scale cryptocurrency thefts or cyberattacks directly connected to national security that are directed by North Korea. In response to a request from the U.S. intelligence agency, South Korean prosecutors are monitoring and tracing leaked cryptocurrencies in Korea,[260] but they lack the capacity to independently examine and track them.

The South Korean government must determine whether to acknowledge cryptocurrencies as a tool of speculation and tighten regulation, or whether to view cryptocurrencies as a future technology and prioritize responsiveness above control. To prevent North Korean cryptocurrency hacking and money laundering, if the South Korean government strengthens laws and systems for cryptocurrency and blockchain technology, the move will make it mandatory to improve the security capabilities of cryptocurrency exchanges, supplement user authentication systems, and reduce the anonymity of cryptocurrency.

However, blockchain may lag behind future-oriented worldwide trends such as applications for business and healthcare systems that use the technology's benefits in this instance. If the South Korean government, like the United States, sees blockchain and

---

258 Byung-chul Won, "Registered as a regular member of 'NATO CCDCOE' in Korea," *security news*, May 9, 2022, http://www.boannews.com/media/view.asp?idx=106621.

259 Bum-soo Park, "The National Police Agency spends 1.9 billion won to purchase a cryptocurrency tracking solution," Coindesk Korea, August 4, 2022, http://www.coindeskkorea.com/news/articleView.html?idxno=80678.

260 Min-ah Lee, "Establishment of a Dedicated Team for the Financial Services Commission to Prevent Cryptocurrency Crimes," *Chosun News*, December 29, 2017, https://biz.chosun.com/site/data/html_dir/2017/12/29/2017122900772.html.

cryptocurrencies as a viable technology and reduces restrictions on the technology, the government will not discourage enemy assaults, but it should establish a team of specialists in each sector to track and reclaim cryptocurrency.

B. FUTURE RESEARCH

This thesis identifies the cyberthreat posed by North Korea by analyzing the level of damage South Korea has experienced from North Korean cyberattacks. Therefore, up until this point, the South Korean government has responded appropriately, but has not found any potential variables that constitute a significant danger to national security. The United States regards a ransomware attack on infrastructure by an adversary as a serious concern and is making significant actions to protect a system for sharing information and ensuring resilience of infrastructure. In South Korea, the damage from ransomware attacks such as WannaCry has been mitigated. Nevertheless, ransomware attacks on small businesses continue to this day, but the scope of the damage they cause is minimal, and thus, they do not constitute a significant danger to national security. Therefore, in this research, this type of attack was not regarded a cyber threat from North Korea to which the government needed to respond adequately. However, if a single act, such as the U.S. colonial pipeline attack, causes catastrophic damage to a nation's critical infrastructure, that type of act poses a significant threat to national security. Therefore, it is worthwhile to conduct more study into how to identify possible cyber threats from adversaries.

This study classifies North Korea's unique attack tactics and examines South Korea's response to such attacks. Recently, attackers have demanded bitcoin as a form of payment of ransom in operations employing malicious code. In such cases, DDoS or ransomware attacks are launched to steal desired confidential information. To date, however, study materials on North Korean cyber threats have only classified North Korea's offensive targets and tactics. As the cyber environment continues to evolve and the adversary's attacks become more complex, it will be effective for the defender, as an active actor, to determine and employ countermeasures for the target and objective of the

adversary's cyberattack, as opposed to passively classifying incidents according to the subject of the attack.

In certain instances, although the cyber environment has continued to expand and evolve in real time, this study has not used the most recent data gleaned from the environment. In the case of the South Korean government's response, it was difficult to find the government's current cyber security policies outside of the defense white paper, whereas the U.S. government's cyber security policies could be understood through numerous press releases and reports from various organizations. Even so, due to the limits of Open-Source Intelligence (OSINT), it was difficult to identify specific policies.

Nonetheless, South Korea and the United States are progressively enhancing their cyber security capabilities. The South Korean government anticipates enhancing its cyber security capabilities by joining NATO's CCDCOE and engaging in training in 2022. South Korea not only engaged as an observer in cyber defense exercises for coordinated countermeasures against cyber threats, but it is also enhancing its cyber security capabilities by taking part in regular cyber assault exercises, strategic research, and policy formulation meetings.

On May 13, 2022, U.S. President Biden signed Executive Order 14028, "Improving the Nation's Cybersecurity," which promotes national cyber security and safeguards federal government networks and infrastructure.[261] The United States is attempting to alter the paradigm to a "zero trust" architecture, which entails no trust without verification, based on the belief that the government's more sophisticated regulation of cyberattacks can be detrimental to businesses.[262] Due to the lack of available data, cybersecurity research is likely to ignore current activities. Therefore, it is vital to choose high-quality OSINT data to study the most recent cyber security regulations and to pay close attention to their real-time evolution.

---

[261] House, "Executive Order on Improving the Nation's Cybersecurity."

[262] Wayne Tang, "Zero Trust Architecture: A Paradigm Shift in Cybersecurity and Privacy" (FINSEC Forum, September 2022), https://cyber.ithome.com.tw/2022/en/session-page/1331.

C. FINAL OBSERVATIONS

Cyberspace is a significant component of national security in the 21st century. South Korea, as an information technology powerhouse, has built a network infrastructure and established a user-friendly cyberspace. However, in comparison to North Korea's and other adjacent countries' cyber capabilities, South Korea's cyber capabilities and cyber security awareness require significant improvement.

The United States, despite already being a cyber power, is constantly evolving its doctrine and capabilities. That does not mean that South Korea should follow the U.S. model in all ways and adopt the U.S. cyber security policy completely. This is due to the fact that the cyber environments of the United States and South Korea are significantly different. This thesis demonstrates that South Korea, like the United States, already has means in place to effectively respond to external cyberattacks, and that improvement measures are not difficult to implement. South Korea's government can effectively thwart North Korean cyberattacks if it alters its concept of cyber security and responds more aggressively than it is presently.

However, South Korea should pay close attention to the recent paradigm shift in mindset that has altered the foundation of U.S. cyber strategy and policy. Based on this newer thinking, the United States is not only improving its cyber capabilities to respond effectively to a changing cyber environment and threats that grow in a variety of ways, but it is also returning to and focusing on the basics. The paradigm shift is a break from the prior cyber deterrence thinking. In the cyber domain, where the notion of attack and defense is ambiguous, the newer concept allows the U.S. to identify the enemy's source with outstanding capabilities and active tactics, continuously observe, and prepare for fast retaliation.

South Korea should not be content with its current cybersecurity capabilities, but should instead keep an eye on the shifting cybersecurity paradigm led by the United States. This shift is a response to fundamental challenges that are similar to those that South Korea also faces, and the flexibility, responsiveness, resilience and adaptability of the current U.S.

approach may lead to a more forward-looking and proactive cyber security for South Korea. By learning from not just U.S. doctrines and policies, but also new U.S. thinking about cyber security, South Korea will be able to respond aggressively and effectively to the fast changing cyber environment and adversary cyberattacks that emerge in real time.

LIST OF REFERENCES

Academy of Korean Studies. "Confederation of Korean Students' Union." In *Encyclopedia of Korean Culture*. The Academy of Korean Studies. Accessed October 17, 2022. http://encykorea.aks.ac.kr/Contents/SearchNavi?keyword=%ED%95%9C%EA%B5%AD%EB%8C%80%ED%95%99%EC%B4%9D%ED%95%99%EC%83%9D%ED%9A%8C%EC%97%B0%ED%95%A9&ridx=0&tot=9288.

AhnLab. *AhnLab Security Emergency Response Center Report*. ASEC Report 96. Sungnam, ROK: Ahnlab, 2019. https://image.ahnlab.com/file_upload/asecissue_files/ASEC%20REPORT_vol.96.pdf.

Alfieri, Carolyn. "Cryptocurrency and National Security." *International Journal on Criminology* 9, no. 1 (February 25, 2022). https://doi.org/10.18278/ijc.9.1.3.

Aspen Publishers. "U.S., South Korea to Collaborate on Promoting Cyberspace Norms." *Cybersecurity Policy Report*, October 26, 2015. http://www.proquest.com/docview/1729336594/abstract/E1309A5AE6134335PQ/1.

Atherton, Kelsey. "How North Korean Hackers Stole 235 Gigabytes of Classified U.S. and South Korean Military Plans." Vox, October 13, 2017. https://www.vox.com/world/2017/10/13/16465882/north-korea-cyber-attack-capability-us-military.

Bartlett, Benjamin Gosnell. "Institutional Determinants of Cyber Security Promotion Policies: Lessons from Japan, the U.S., and South Korea." PhD diss., UC Berkeley, 2018. https://escholarship.org/uc/item/02f4879m.

Byun, Jin-suk. "The Development of the U.S. Cybersecurity Strategy: Historical Overview and Cyberspace Solarium Commission Report." *Peace Studies* 30, no. 1 (April 30, 2022): 41–76. https://doi.org/10.21051/PS.2022.04.30.1.41.

Cha, Jung-mi. "Cyber Arms Race between U.S. and China and the Rise of North Korean Threat in Cyber Space: Implications for South Korea's Cyber Security." *Unification Research* 23, no. 1 (2019): 43–93. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002467724

Chainalysis. "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High," January 13, 2022. https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

CCTV News. "National Core Technology Is Dangerous, and Daewoo Shipbuilding & Marine Engineering Is Threatening Hacking Following the Korea Atomic Energy Research Institute," June 22, 2021. https://m.post.naver.com/viewer/postView.naver?volumeNo=31815687&memberNo=48110825.

Chang, Noh-Soon. "Cybersecurity Threats, Response Strategies, and Korean Implications." *National Security and Strategy* 19, no. 2 (2019): 1–36. https://doi.org/10.23111/nsas.2019.19.2.001.

Cho, Won-sun. "Cyber Security Discourses and Securitization Theory: On the Analysis of Korean Cyber Security Issues." *Defense Policy Research* 33, no. 2 (summer 2017): 146–77. https://www.kida.re.kr/frt/board/frtPolicyStudyBoardDetail.do?sidx=363&idx=903&depth=4&searchCondition=ITMVAL3&searchKeyword=117&groupbox=12&pageIndex=1.

Choe, Sang-Hun. "South Korea Blames North for June Cyberattacks." *The New York Times*, July 16, 2013, sec. World. https://www.nytimes.com/2013/07/17/world/asia/south-korea-blames-north-for-june-cyberattacks.html.

Choi, Eun-hee. "DPRK's Cyber Threat and Its Implications for ROK's Security : Focusing on the Threat of Cyber Propaganda." Master's thesis, Sungkyunkwan University, Seoul, 2020. http://www.riss.kr/link?id=T15520046.

Choi, Kwan, and Min-ji Kim. "A Comparative Analysis of the National Defensive System Against Cyber Terrorism for National Security and Public Safety: Focus on the South Korea, America, and France." *The Journal of Police Policies* 29, no. 2 (October 2015): 1–36. https://doi.org/10.35147/KNPSI.2015.29.2.1.

Choi, Moon-ki. "Comprehensive National Cyber Security Measures." Department of Science, ICT and Future Planning, Republic of Korea. Press Release, April 2013. https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&bbsSeqNo=94&nttSeqNo=1212488.

Choi, Tae-bum. "Two Years after the National Defense Network Hacking Incident, the Military Internet Security Network Is Still 'Checked.'" *MoneyToday*, 28 2018. https://news.mt.co.kr/mtview.php?no=2018082816237634464.

Chosun News. "Take All the South Korean Banks," February 11, 2021. https://www.chosun.com/politics/north_korea/2021/02/11/SZSUMEV5DFGEDNZ22SZGJ7NPOY/.

Chung, Tae-jin, and Guang-meen Rhee. "Legal Response to Foreign Cyber Attackers." *Korean Police Studies Review* 19, no. 1 (2020): 279–96. https://doi.org/10.16961/polips.2019.14.2.65.

———. “A Study on Accession by South Korea to the Budapest Convention on Cybercrime and International Cooperation against Cybercrime.” *The Police Science Journal* 14, no. 2 (May 2019): 65–84. https://doi.org/10.16961/POLIPS.2019.14.2.65.

Coveware. “Ransomware Attacks Split Between Enterprise & RaaS.” Accessed October 26, 2022. https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report.

Cox, Ramsey, and Martinez Jennifer. “Senate Votes down Lieberman, Collins Cybersecurity Act a Second Time.” Text. *The Hill* (blog), November 15, 2012. https://thehill.com/policy/technology/268053-senate-rejects-cybersecurity-act-for-second-time/.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. “Defining Cybersecurity.” *Technology Innovation Management Review* 4, no. 10 (October 2014): 13–21. https://doi.org/10.22215/timreview/835.

Cybersecurity and Infrastructure Security Agency. “Cybersecurity Information Sharing Act of 2015 Procedures and Guidance.” CISA. 2016. https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

D&B Hoovers. *Colonial Pipeline Company Profile*. Fort Mill, SC: Mergent, 2022. http://www.proquest.com/docview/1860763829/abstract/C0D5997BC8444D05PQ/1.

Department of Homeland Security. “DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators | Homeland Security.” Department of Home Security, December 2, 2021. https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.

———. “Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process.” *Federal Continuity Directive* 2 (June 13, 2017): 1–41. https://www.fema.gov/sites/default/files/2020-07/Federal_Continuity_Directive-2_June132017.pdf

———. “Federal Executive Branch National Continuity Program and Requirements.” *Federal Continuity Directive* 1 (January 17, 2017): 1–64. https://www.gpo.gov/docs/default-source/accessibility-privacy-coop-files/January2017FCD1-2.pdf

Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent U.S. Elections.* ICA 2017. Washington, D.C.: Office of the Director of National Intelligence, National Intelligence Council, 2017.

Federal Register. “Executive Orders.” Accessed November 8, 2022. https://www.federalregister.gov/presidential-documents/executive-orders.

Federation of American Scientists. “Presidential Directives and Executive Orders.” Accessed November 8, 2022. https://irp.fas.org/offdocs/direct.htm.

Flitter, Emily, and David Yaffe-Bellany. “Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions.” *The New York Times*, February 23, 2022. https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html

Forbes. “What Really Happened to LUNA Crypto?” Accessed November 7, 2022. https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/

Global Legal Insights. “Blockchain & Cryptocurrency Laws and Regulations.” Text. GLI Global Legal Group. United Kingdom. Accessed October 26, 2022. https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa.

GFCE. “The Budapest Convention on Cybercrime: A Framework for Capacity Building – Global Forum on Cyber Expertise.” Accessed November 6, 2022. https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/.

Glover, Claudia. “North Korea Is Ramping up Cyberattacks on South Korean Targets.” *Tech Monitor* (blog), June 22, 2021. https://techmonitor.ai/technology/cybersecurity/north-korean-cyberattacks-on-south-korea-kimsuky.

Gochua, Alika, Thornike Zedelashvili, and Gela Giorgadze. “Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats.” *Ukrainian Policymaker* 10 (June 2022): 27–36. https://doi.org/10.29202/up/10/4.

Government Legislative Support Center. “Introduction to the Government Legislative System.” Accessed November 18, 2022. https://www.lawmaking.go.kr/lmGde/govLm.

Han, Sang-am, and Yun-yung Kim. “A Study on Improvement Measures to Protect the Korean Financial Network against Cyber Terrorism by North Kore.” *Public Security Policy Research* 34, no. 2 (2020): 319–55. https://doi.org/10.35147/knpsi.2020.34.2.319.

Hancocks, Paula and K.J. Kwon. “North Korea Hacked Government Officials’ Smartphones, South Korea Says.” *CNN*, March 8, 2016. https://www.cnn.com/2016/03/08/asia/south-korea-smartphone-hack/index.html.

Hankyoreh. "Distrust Spread over the 'Cheonan Investigation'… Only 32% of the Public Believe the Government Announcement," September 8, 2010. https://www.hani.co.kr/arti/politics/politics_general/438817.html.

Hobbs, Allegra. "The Colonial Pipeline Hack: Exposing Vulnerabilities in U.S. Cybersecurity." SAGE Business Cases, 2021. https://doi.org/10.4135/9781529789768.

Howcroft, Elizabeth. "Binance-Linked Blockchain Hit by $570 Million Crypto Hack." *Reuters*, October 7, 2022, sec. Technology. https://www.reuters.com/technology/hackers-steal-around-100-million-cryptocurrency-binance-linked-blockchain-2022-10-07/.

Huh, Tae-hoi, Sangho Lee, and Woo-Young Chang. "Contemporary Information Warfare and National Strategy: Korea's Military Cyber Security Issues and Tasks." *International Area Review* 10, no. 1 (March 1, 2007): 215–38. https://doi.org/10.1177/223386590701000112.

Hunton Andrews Kurth, LLP. "Cyber Incident Reporting for Critical Infrastructure Act." *Privacy & Information Security Law* (Blog), September 30, 2022. https://www.huntonprivacyblog.com/2022/09/30/cyber-incident-reporting-for-critical-infrastructure-act/.

Investopedia. "Most Cryptocurrencies Are Securities, Says SEC Chair." Accessed October 26, 2022. https://www.investopedia.com/gensler-on-crypto-6544288.

Jenkinson, Andrew. *Ransomware and Cybercrime*. Boca Raton, FL: CRC Press, 2022. https://doi.org/10.1201/9781003278214.

Jho, Hwa-sun, and Woong Kwon. "Cyber-Security Governance in South Korea and the United States: A Comparison of Securitization of Cyber-Threat." *Information Society & Media* 18, no. 2 (August 2017): 97–120. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002261724

Jun, Kyung-woong. "North Korea Joins Community with Hundreds of Thousands of Resident Numbers... After 'Mad Cow Disease,' Public Opinion Work in Earnest." *NewDaily*, January 17, 2022. https://www.newdaily.co.kr/site/data/html/2022/01/17/2022011700163.html.

Kang, Ki-soo. "National Cyber Security Cyber-attack Response for Study: South Korea and the United States Focused on Comparing Response System to Cyber-attacks." *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, November 2013, 782–83. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE02411150

Kim, Bo-mi, and Il-seok Oh. "North Korea's Cyber Threats and Responses by Major Countries in the Kim Jong-Un Era." National Security Strategy Institute, November 2021. https://inss.re.kr/upload/bbs/BBSA05/202112/F20211206172938667.pdf.

Kim, Chong-woo, and Polito Carolina. "The Evolution of North Korean Cyber Threats." *The Asan Institute for Policy Studies*, March 2019, 1–15. https://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats/

Kim, Dang. "11,727 Public Cyber-Attacks." *UPI News*, October 10, 2020. http://www.upinews.kr/newsView/upi202010160030.

Kim, Do-kyung, and Soon-yang Kim. "Reframing South Korea's National Cybersecurity Governance System in Critical Information Infrastructure." *The Korean Journal of Defense Analysis* 33, no. 4 (December 2021): 689–713. https://doi.org/10.22883/KJDA.2021.33.4.007.

Kim, Dong-sung. "North Korea's Strategic Tactics of United Front and Political-Psychological Warfare." *The Journal of Strategic Studies* 57 (March 2013): 309–51. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001757692

Kim, In-soon. "Ministry of National Defense Internal Network Anti-Virus Software, Eventually Hauri." *ETNEWS*, January 22, 2018. https://www.etnews.com/20180122000175.

Kim, Jae-kwang. "Coping with Legal Issues on Cyber-Security Threat." *Kyungpook National University Law Journal*, no. 58 (2017): 145–77. https://doi.org/10.17248/knulaw.58.201705.145.

Kim, Jung-woo. "Cryptocurrency Fundamental Act, Visible in the Second Half of the Year." *Decenter*, June 2, 2022. https://decenter.kr/NewsView/26739J0GJT.

Kim, Min-hyung. "North Korea's Cyber Capabilities and Their Implications for International Security." *Sustainability* 14, no. 3 (2022): 1–15. https://doi.org/10.3390/su14031744.

Kim, Mi-ohk. "Scientists Say the Mad Cow Disease Truth." *Donga*. May 9, 2008. https://www.donga.com/news/article/all/20080509/8576305/1.

Kim, Soo-han. "Replacing the Anti-Virus Software after the Defense Network Was Hacked." *Herald Economy*, December 12, 2016. http://news.heraldcorp.com/military/view.php?ud=20161212000777.

Kim, So-ram, Soo-jin Kang, and Yong-cheol Choi. "Ransomware Status and Response/ Prevention Policy Trend in 2021." *KIISC Review* 31, no. 6 (December 2021): 5–12. https://koreascience.kr/article/JAKO202102565127226.jsp-k1ff8j=SSMHB4&py=2012&vnc=v27n6&sp=588

Kim, Sung-man. "Countermeasures against Hacking of Military Internal Networks." KONAS, December 15, 2016. https://www.konas.net/article/article.asp?idx=47494.

Kim, Won-suk. "South Korea Officially Blames North for June 25 Cyber Attack." *ETNEWS*, July 16, 2013, sec. Internet. https://english.etnews.com/20130716200016?SNS=00002.

Kim, Yoon-hee. "Meeting to Share Hacking Information." ZDnetKorea, November 17, 2021. https://zdnet.co.kr/view/?no=20211117173540.

Kim, Yung-do, Jin-sung Kim, and Kyung-ho Lee. "Major Issues of the National Cyber Security System in South Korea, and Its Future Direction." *The Korean Journal of Defense Analysis* 25, no. 4 (2013): 435–55. https://doi.org/10.22883/kjda.2013.25.4.001.

Ko, Myung-hyun. "North Korea's Cyber Force and Financial Crimes." *North Korea Economic Review* 23, no. 10 (October 2021): 55–66. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10959524

Ko, Sung-ho. "Kakao Network Failure, Legislative Measures Urgently Needed." *Donga*, October 17, 2022. https://www.donga.com/news/article/all/20221017/115985691/2.

Konowicz, Deane R. "The New Game: Cryptocurrency Challenges U.S. Economic Sanctions." Paper submitted to U.S. Naval War College, Newport, RI. February 2018. https://apps.dtic.mil/sti/pdfs/AD1062142.pdf.Kshetri, Nir. "Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses." *East Asia: An International Quarterly* 31, no. 3 (September 2014): 183–201. https://doi.org/10.1007/s12140-014-9215-1.

Kumar, Sumeet, Matthew Benigni, and Kathleen M. Carley. "The Impact of U.S. Cyber Policies on Cyber-Attacks Trend." In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 181–86, 2016. https://doi.org/10.1109/ISI.2016.7745464.

Kwon, Hyuk. "A Review of Power Grid Cyber & Natural Disasters and Cyber Resilience." *The Korean Institute of Electrical Engineers* 71, no. 2 (February 2022): 24–28. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11028012

Kwon, Hyuk-chun. "A Comparative Study on North Korean Cyber Attack Patterns: Focusing on the Three Governments of Roh Moo-Hyun, Lee Myung-Bak and Park Geun-Hye." Konkuk University, 2020. http://www.riss.kr/link?id=T15502639.

Kwon, Jun-ki. "Intensified Investigation into Cheonan Rumors... Raises Rumors behind North Korea." *YTN*, June 1, 2010. https://www.ytn.co.kr/_ln/0103_201006012055527850.

———. "Strengthening the Investigation of Cheonan's Scaremongering, Raising Rumors of North Korea's Background." *YTN*, June 1, 2010. https://www.ytn.co.kr/_ln/0103_201006012055527850.

Lee, Chang-kyu. "KT Communication Failure Is an Expected Result… There Was No Manual or Safety Device." *News1*, November 9, 2021. https://www.news1.kr/articles/?4487999.

Lee, Hye-ri, and Yong-pil Park. "The Media Became the 'Target' of Complaints, Accusations, and Investigations." *Kyunghyang News*, October 5, 2022. https://www.khan.co.kr/article/202210052045005.

Lee, Jae-hyung, Sang-pil Yoon, and Hun-yeong Kwon. "Concept Research and Operation Strategy for Rational Cyber Psychological Warfare Design." *Defense Policy Research* 35, no. 4 (2020): 137–67. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09404038

Lee, Jung-hoon. "The Sinking of Cheonan: Remembering the Tragedy on Its 10TH Anniversary." *New Asia* 27, no. 1 (2020): 66–92. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10721471

Lee, Ki-jong. "Cybersecurity Control Tower." *Newsfreezone*, March 11, 2022. http://www.newsfreezone.co.kr/news/articleView.html?idxno=367589.

Lee, Min-ah. "Establishment of a Dedicated Team for the Financial Services Commission to Prevent Cryptocurrency Crimes." *Chosun News*, December 29, 2017. https://biz.chosun.com/site/data/html_dir/2017/12/29/2017122900772.html.

Lee, Sang-ho. "North Korea's Cyber Psychological Warfare and the Options for South Korea's Countermeasure." *Journal of Korean Political And Diplomatic History* 33, no. 1 (2011): 263–90. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE08784771

Lee, Seong-yeob. "Desirable Direction for National Cybersecurity Legislation and Governance: Focusing on the Case of the United States and the Implications of Korea." *Administrative Law Journal*, no. 67 (March 2022): 239–62. https://doi.org/10.35979/ALJ.2022.03.67.239.

Lee, Yoo-eun. "Who Was behind South Korean Cyber-Attacks?" Al Jazeera. Accessed October 7, 2022. https://www.aljazeera.com/opinions/2013/3/31/who-was-behind-south-korean-cyber-attacks.

Lee, Yung-ho. "2nd in the World for Korean SNS Usage Rate." *Korea Economic TV*. June 16, 2021. https://www.wowtv.co.kr/NewsCenter/News/Read?articleId=A202106160022.

Leithauser, Tom. "Kerry Seeks South Korea's Help in Pushing Cyberspace Norms." *Cybersecurity Policy Report*, May 25, 2015. http://www.proquest.com/docview/1684453381/abstract/DD6A7BF8BFB64BDCPQ/1.

Lendon, Brad. "S. Korea's Final Report Affirms Cheonan Was Sunk by N. Korean Torpedo." *CNN*, September 13, 2010. http://www.cnn.com/2010/WORLD/asiapcf/09/13/south.korea.cheonan.report/index.html.

Lewis, James Andrew. "Advanced Experiences in Cybersecurity Policies and Practices: An Overview of Estonia, Israel, South Korea, and the United States." Inter-American Development Bank, 2016. https://publications.iadb.org/en/advanced-experiences-cybersecurity-policies-and-practices-overview-estonia-israel-south-korea-and.

Lynch, Sarah N., and Chris Prentice. "FBI to Form Digital Currency Unit, Justice Dept Taps New Crypto Czar." *Reuters*, February 17, 2022, sec. Technology. https://www.reuters.com/technology/fbi-form-new-digital-currency-unit-justice-dept-taps-new-crypto-czar-2022-02-17/.

Manatt. "Is the Party Over? The SEC Investigates Cryptocurrency Offerings." Accessed October 26, 2022. https://manatt.com/insights/articles/2017/is-the-party-over-the-sec-investigates-cryptocurr.

Marpaung, Jonathan A P, and Hoon-jae Lee. "Dark Seoul Cyber Attack: Could It Be Worse?" *Cryptography & Network Security Lab*, 2013, 1–4. https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Dark_Seoul_Cyberattack.pdf

Matishak, Martin. "NSA, Cyber Command Tap New Election Security Leaders." *The Record by Recorded Future* (blog), May 5, 2022. https://therecord.media/nsa-cyber-command-election-security-leaders/.

McCain, John. "S.2943 - 114th Congress (2015–2016): National Defense Authorization Act for Fiscal Year 2017." Legislation, December 23, 2016. 2015/2016. http://www.congress.gov/.

McCombie, Stephen, Allon J. Uhlmann, and Sarah Morrison. "The U.S. 2016 Presidential Election & Russia's Troll Farms." *Intelligence and National Security* 35, no. 1 (January 2, 2020): 95–114. https://doi.org/10.1080/02684527.2019.1673940.

Microsoft 365 Defender Threat Intelligence Team. "North Korean Threat Actor Targets Small and Midsize Businesses with H0lyGh0st Ransomware." *Microsoft Security Blog* (blog), July 14, 2022. https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/.

Ministry of Foreign Affairs. "Korea-U.S. Joint Public-Private Symposium Held in Response to North Korean Cryptocurrency Theft." Ministry of Foreign Affairs, Republic of Korea. November 17, 2022. https://overseas.mofa.go.kr/www/brd/m_4080/view.do?seq=373025.

Nakasone, Paul. "Posture-Statement." United States Cyber Commad, April 5, 2022. https://www.armed-services.senate.gov/imo/media/doc/5%20Apr%20SASC%20CYBERCOM%20Posture%20Statement%20(GEN%20Nakasone)%20-%20FINAL.pdf.

Nam, Do-young. "Event of the Year in 2021." *Tech M*, December 28, 2021. https://www.techm.kr/news/articleView.html?idxno=92561.

National Conference of State Legislatures. "Cryptocurrency 2022 Legislation." Accessed October 26, 2022. https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2022-legislation.aspx.

National Cybersecurity and Communications Integration Center and United States Federal Bureau of Investigation. *Grizzly Steppe: Russian Malicious Cyber Activity.* Washington, DC: U.S. Department of Homeland Security, NCCIC, 2016.

National Intelligence Council. "Foreign Threats to the 2020 U.S. Federal Elections." Intelligence Community Assessment. March 10, 2021. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

National Intelligence Service of South Korea. *2014 National Information Protection White Paper (South Korea)*. Seoul: South Korea National Intelligence Service, May 2014. https://www.kisa.or.kr/20303/form?postSeq=0011984&page=1#fnPostAttachDownload.

———. *2018 National Information Protection White Paper (South Korea)*. Seoul: South Korea National Intelligence Service, May 2018. https://www.kisa.or.kr/20303/form?postSeq=0011988&page=1.

———. *2020 National Information Protection White Paper (South Korea)*. Seoul: South Korea National Intelligence Service, May 2020. https://www.kisa.or.kr/20303/form?postSeq=0240&page=1.

———. *2022 National Information Protection White Paper*. Seoul: National Information Protection White Paper. National Intelligence Service, 2022. https://www.kisa.or.kr/20303/form?postSeq=12002&page=1.

National Law Information Center. "Korean Constitution." Accessed November 8, 2022. https://www.law.go.kr/LSW/lsInfoP.do?efYd=19880225&lsiSeq=61603#0000.

National Security Agency/Central Security Service. "In Discussion with Philip Quade, Chief of NSA Cyber Task Force." Accessed October 19, 2022. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1625859/in-discussion-with-philip-quade-chief-of-nsa-cyber-task-force/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FNews-Highlights%2FArticle%2FArticle%2F1625859%2Fin-discussion-with-philip-quade-chief-of-nsa-cyber-task-force%2F.

NPR. "Why Russia May Have Stepped Up Its Hacking Game." Accessed November 9, 2022. https://www.npr.org/2021/01/29/960810672/why-russia-may-have-stepped-up-its-hacking-game.

Oh, Da-in. "Ministry of National Defense Selects AhnLab and Hauri as Anti-virus Software Suppliers." *ETNEWS*, November 23, 2019. https://www.etnews.com/20191123000001?SNS=00002.

Paganini, Pierluigi. "North Korean APT Group Kimsuky Allegedly Hacked South Korea's Atomic Research Agency KAERI." Security Affairs, June 19, 2021. https://securityaffairs.co/wordpress/119147/apt/kimsuky-apt-hacked-south-korea-kaeri.html.

———. "South Korean Hosting Provider NAYANA Infected by Erebus Ransomware, It Paid $1 Million to Crooks." Security Affairs, June 21, 2017. https://securityaffairs.co/wordpress/60281/malware/erebus-ransomware-hit-south-korea.html.

Park, Bum-soo. "The National Police Agency Spends 1.9 Billion Won to Purchase a Cryptocurrency Tracking Solution." Coindesk Korea, August 4, 2022. http://www.coindeskkorea.com/news/articleView.html?idxno=80678.

Park, Eun-ju. "Increasing North Korean Cyber Security Threats and South Korea's Response." *Veteran's Journal* 19, no. 4 (2020): 9–30. https://doi.org/10.24004/tkafp.2020.19.4.001.

Park, Jae-hun. "A Study on Cybersecurity Strategies against North Korean Cyberattacks." Inha University, 2022. http://www.riss.kr/link?id=T16084674.

Park, Joshua. “The Lazarus Group: The Cybercrime Syndicate Financing the North Korea State.” *Harvard International Review* 42, no. 2 (Spring 2021): 34–39.

Park, Kwang-ha. “Ransomware Threatens National Security, and Measures to Prevent Damage Are Urgently Needed.” *Information and Communication Newspaper*, January 27, 2022. http://www.koit.co.kr/news/articleView.html?idxno=93254.

Park, On-yoo. “Government Trust and Political Failure: Why Did the Easing of U.S. Beef Import Conditions Cause Mad Cow Disease Candlelight Vigils.” *Korean Association of Local Government*, 2021, 903–18. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10594058.

Park, Sun-song. “The Actor-Network of ROK Ship Cheonan Accident and the Unstability of the Division System in the Korean Peninsula.” *Journal of the North Korean Research Society* 17, no. 1 (2013): 317–54. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09053992.

Park, Yong-ju. “Cryptocurrency Trader Real Name Verification Starts Today.” *YTN*. Accessed October 17, 2022. https://www.yna.co.kr/view/AKR20180129167500002.

Radzikowski, Shem. “CyberSecurity: Origins of the Advanced Persistent Threat (APT).” Dr. Shem, October 8, 2015. https://DrShem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/.

Royce, Edward R. “H.R.3364 - 115th Congress (2017–2018): Countering America’s Adversaries Through Sanctions Act.” Legislation, February 8, 2017. 2017/2018. http://www.congress.gov/.

Sang-Hun, Choe, and David Yaffe-Bellany. “How North Korea Used Crypto to Hack Its Way through the Pandemic.” *The New York Times*. Accessed October 26, 2022. https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

Scheck, Justin, and Shane Shifflett. “How Dirty Money Disappears into the Black Hole of Cryptocurrency.” *Wall Street Journal*, September 28, 2018. https://www.wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743.

Schneider, Jacquelyn, Emily Goldman, Michael Warner et al. *Ten Years In: Implementing Strategic Approaches to Cyberspace*. Newport, RI: U.S. Naval War College, 2020. https://digital-commons.usnwc.edu/usnwc-newport-papers/45/.

SearchSecurity. “What Is Cyberterrorism?” Accessed October 7, 2022. https://www.techtarget.com/searchsecurity/definition/cyberterrorism.

Segal, Michael. "Cryptocurrency Regulation under U.S. Securities Laws and Proposed Amendments." *Computer and Internet Lawyer* 36, no. 9 (2019): 13–25. http://www.proquest.com/docview/2281057752/abstract/BFBCF96CB9084D4EPQ/1.

Sevastopulo, Demetri, Courtney Weaver, and Barney Jopson. "US Charges Russians with 2016 Election Interference." *FT.com*, February 16, 2018. http://www.proquest.com/docview/2121959418/citation/1CDA41CB32904BADPQ/1.

Shim, Yang-sup. "The Outcome and Limitation of South Korean Scholars' Studies about the Demonstration against Importing American Beefs in 2008." *National Security and Strategy* 16, no. 1 (2016): 72–113. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10799223.

Shin, Jae-hun, and Yong-hun Kim. "The Plan to Strengthen Cyber Security." *Korean Police Research* 15, no. 3 (2016): 75–104. https://doi.org/G704-001889.2016.15.3.005.

Shin, Kyeong-su, and Jin Shin. "Scaling Cyber Threats and Responding to National Security: A Focus on North Korea's Cyberattacks." *Strategic Research* 25, no. 3 (November 2018): 53–77. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07566884.

Smith, Stephanie. "Out of Gas: A Deep Dive into the Colonial Pipeline Cyberattack." SAGE Business Cases, 2022. https://doi.org/10.4135/9781529605679.

Stupp, James Rundle and Catherine. "Justice Department Installs New FBI Crypto Crime Unit." *Wall Street Journal*, February 17, 2022. https://www.wsj.com/articles/justice-department-installs-new-fbi-crypto-crime-unit-11645129414.

———. "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware." The White House, October 13, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

Tang, Wayne. "Zero Trust Architecture: A Paradigm Shift in Cybersecurity and Privacy." Paper presented at FINSEC Forum, Taipei, September 2022. https://cyber.ithome.com.tw/2022/en/session-page/1331.

Thorne, C. Thomas, and David S. Patterson, eds. *Emergence of the Intelligence Establishment*. *Foreign Relations of the United States 1945–1950*. Washington, DC: United States Government Printing Office, 1996.

Tiirmaa-Klaar, Heli. "Building National Cyber Resilience and Protecting Critical Information Infrastructure." *Journal of Cyber Policy* 1, no. 1 (January 2, 2016): 94–106. https://doi.org/10.1080/23738871.2016.1165716.

Treverton, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue. *Hybrid Threats: Russian Interference in the 2016 U.S. Election*. Sweden: Försvarshögskolan (FHS), 2018. http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-7574.

TSA. "TSA Revises and Reissues Cybersecurity Requirements for Pipeline Owners and Operators." Transportation Security Administration. July 21, 2022. https://www.tsa.gov/news/press/releases/2022/07/21/tsa-revises-and-reissues-cybersecurity-requirements-pipeline-owners.

Turton, William, and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg. June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

United Nations. "Sanctions Committee Documents 30 August 2019." UN Documents for DPRK (North Korea), August 30, 2019. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf.

———. "Sanctions Committee Documents 8 September 2021." UN Documents for DPRK (North Korea). United Nations, September 8, 2021. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2021_777_E.pdf.

United States Cyber Command. "Achieve and Maintain Cyberspace Superiority." USCYBERCOM, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

U.S. Congress. House of Representatives. Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack. 117th Cong., 1st Sess., June 15, 2021.

U.S. Department of Defense. "Cyber Command Expects Lessons From 2018 Midterms to Apply in 2020." Accessed November 15, 2022. https://www.defense.gov/News/News-Stories/Article/Article/1758488/cyber-command-expects-lessons-from-2018-midterms-to-apply-in-2020/https%3A%2F%2Fwww.defense.gov%2FNews%2FNews-Stories%2FArticle%2FArticle%2F1758488%2Fcyber-command-expects-lessons-from-2018-midterms-to-apply-in-2020%2F.

U.S. Department of Justice. "Justice Department Announces First Director of National Cryptocurrency Enforcement Team," February 17, 2022. https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team.

———. "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election." *Department of Justice (DOJ) Documents / FIND*. Washington, DC: Federal Information & News Dispatch, LLC, November 18, 2021. https://www.proquest.com/docview/2599109949/citation/C85B7516205C4375PQ/1.

U.S. Department of Defense. "US-DOD-Cyber-Strategy-Summary 2015." April 2015. https://www.nist.gov/news-events/news/2015/04/dod-cyber-strategy-new-issuance-april-23-2015.

———. "US-DOD-Cyber-Strategy-Summary." September 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Van Puyvelde, Damien, and Aaron Brantly, eds. U.S. *National Cybersecurity: International Politics, Concepts and Organization*. Routledge Studies in Conflict, Security and Technology. London; New York: Routledge, Taylor & Francis Group, 2017. https://doi.org/10.4324/9781315225623.

Vavra, Shannon. "NSA's Russian Cyberthreat Task Force Is Now Permanent." CyberScoop, April 29, 2019. https://www.cyberscoop.com/nsa-russia-small-group-cyber-command/.

Veale, Michael, and Ian Brown. "Cybersecurity." *Internet Policy Review* 9, no. 4 (December 17, 2020). https://doi.org/10.14763/2020.4.1533.

The White House. "Executive Order on 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" April 1, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

———. "Executive Order -- Improving Critical Infrastructure Cybersecurity," February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

———. "Executive Order on Improving the Nation's Cybersecurity." The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

———. “Executive Order 13757 (Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities),” December 28, 2016. https://irp.fas.org/offdocs/eo/eo-13757.htm.

———. “Fact Sheet: Biden-Harris Administration Delivers on Strengthening America’s Cybersecurity.” The White House, October 11, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/.

———. “Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware.” The White House, October 13, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.

———. “International Counter Ransomware Initiative 2022 Joint Statement.” The White House, November 1, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.

———. “Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021.” The White House, October 14, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

———. “Presidential Policy Directive - Critical Infrastructure Security and Resilience,” February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Wilson, Tom, Elizabeth Howcroft, and Elizabeth Howcroft. “Explainer: Ronin’s $615 Million Crypto Heist.” *Reuters*, March 30, 2022, sec. Technology. https://www.reuters.com/technology/ronins-615-million-crypto-heist-2022-03-30/.

Won, Byung-chul. “North Korean Hackers Working with South Korean Criminals Hack ATMs and Steal 230,000 Cases of Financial Information.” *Security News*, September 6, 2017. http://www.boannews.com/media/view.asp?idx=56864.

———. “Registered as a Regular Member of ‘NATO CCDCOE’ in Korea.” *Security News*, May 9, 2022. http://www.boannews.com/media/view.asp?idx=106621.

Yang, Jeong Yoon, Kyudong Kim, and So Jeong Kim. “Implications on National Security Strategies of the Strategic Use of Cyber Capabilities of Foreign Governments: The Case of Alleged Russian Interference in the 2016 U.S. Election.” *Korean Crisis Management Journal* 13, no. 11 (November 2017): 105–18. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE08789064

Yoo, Dong-ryul. "North Korea's Cyber Threats and Countermeasures." *The Journal of Strategic Studies* 28, no. 3 (November 2021): 7–36. https://doi.org/10.46226/jss.2021.11.28.3.7.

Yoo, Ho-geun, and Gyoo-sang Seol. "Cyber Security System: Issues of Governance Formation and Korea." *Journal of Korean Political and Diplomatic History* 38, no. 2 (2017). https://doi.org/10.18206/kapdh.38.2.201703.237.

YTN. "North Korea's Cyber Attacks Damage of $500 Million." October 15, 2013. https://www.ytn.co.kr/_ln/0101_201310151027217359.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California