Fall 2017

An Assessment of North Korean Threats and Vulnerabilities in Cyberspace

Jeremiah van Rossum
Missouri State University, vanRossum123@live.missouristate.edu

As with any intellectual project, the content and views expressed in this thesis may be considered objectionable by some readers. However, this student-scholar's work has been judged to have academic value by the student's thesis committee members trained in the discipline. The content and views expressed in this thesis are those of the student-scholar and are not endorsed by Missouri State University, its Graduate College, or its employees.

AN ASSESSMENT OF NORTH KOREAN THREATS AND VULNERABILITIES IN CYBERSPACE

A Master's Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Defense and Strategic Studies

By

Jeremiah Adam van Rossum

December 2017

AN ASSESSMENT OF NORTH KOREAN THREATS AND VULNERABILITIES IN CYBERSPACE

Defense and Strategic Studies

Missouri State University, December 2017

Master of Science

Jeremiah Adam van Rossum

ABSTRACT

This thesis answers the fundamental questions of what North Korean capabilities and intent in cyberspace are and what North Korean threats and vulnerabilities are associated with these. It argues that although North Korea's cyberspace resources and capabilities have increased and reached a level that represents an advanced persistent threat, its cyberspace operations have remained restrained and regional. It also argues that North Korea's valuable assets include its ability to control cyberspace within North Korea and its ability to engage in cyberspace activities and operations from abroad. The thesis recommends that the United States government exploit these assets by denying and disrupting the use of cyberspace by covert cyber units outside of North Korea, as well as by enabling and ensuring the less monitored and less controlled use of cyberspace by civilians inside of North Korea.

KEYWORDS: North Korea, South Korea, cyberspace, cyber conflict, offensive cyberspace operation, cyberattack, cyber espionage, DarkSeoul Gang, Lazarus Group, advanced persistent threat

This abstract is approved as to form and content

Brian Mazanec, PhD
Chairperson, Advisory Committee
Missouri State University

AN ASSESSMENT OF NORTH KOREAN THREATS AND VULNERABILITIES IN CYBERSPACE

By

Jeremiah Adam van Rossum

A Master's Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Master of Science, Defense and Strategic Studies

December 2017

Approved:

Brian Mazanec, PhD: Professor, Department of Defense and Strategic Studies

David Peck, MA: Professor, Department of Defense and Strategic Studies

Andrei Shoumikhin, PhD: Professor, Department of Defense and Strategic Studies

Julie Masterson, PhD: Dean, Graduate College

In the interest of academic freedom and the principle of free speech, approval of this thesis indicates the format is acceptable and meets the academic criteria for the discipline as determined by the faculty that constitute the thesis committee. The content and views expressed in this thesis are those of the student-scholar and are not endorsed by Missouri State University, its Graduate College, or its employees.

ACKNOWLEDGEMENTS

I would like to thank the faculty and staff in the Department of Defense and Strategic Studies for their immense support during my graduate studies. Although difficult at times, I have gained much through this program, academically, professionally, and personally. In particular, I would also like to thank my first reader, Dr. Brian Mazanec, as well as my second and third readers, Prof. David Peck and Dr. Andrei Shoumikhin, for their guidance and feedback.

I dedicate this thesis to my niece, Lily Poole.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIC	accessibility, integrity, and confidentiality
APT	advanced persistent threat
CISR	cyberspace intelligence, surveillance, and reconnaissance
CNA	computer network attack
CND	computer network defense
CNO	computer network operations
DCO	defensive cyberspace operations
DCIDD	Dyadic Cyber Incident and Dispute Dataset
DDOS	distributed denial of service
DHS	Department of Homeland Security (US)
DOD	Department of Defense (US)
DODIN	Department of Defense information network
DOS	denial of service
DPRK	Democratic People’s Republic of Korea
IP	internet protocol
IT	information technology
KCC	Korea Computer Center (DPRK)
KPAF	Korean People’s Armed Forces (DPRK)
MND	Ministry of National Defense (ROK)
NIS	National Intelligence Service (ROK)
OCO	offensive cyberspace operations

OTA	Operational Threat Assessment
RGB	Reconnaissance General Bureau (DPRK)
ROK	Republic of Korea

CHAPTER I: INTRODUCTION

North Korea has been a constant national security challenge for the United States. For decades, it has pursued nuclear weapon and ballistic missile development in violation of treaties, agreements, and norms, threating peace and stability in East Asia. It has also emerged as a threat in cyberspace. It has been implicated in numerous cyberspace operations against the United States and South Korea. In a statement before the Senate Armed Service Committee, Admiral Michael Rogers, commander of United States Cyber Command, listed North Korea among the nations of greatest concern in cyberspace.[1] However, the threat in cyberspace that North Korea poses is not well understood at worst and not well articulated at best. It is also assumed that because North Korea has no significant reliance on the internet, it possesses no significant vulnerabilities in cyberspace. These misunderstandings and assumptions are due to the difficulties created by the secretive nature of North Korea and the nascent and dynamic nature of cyberspace.

This thesis will answer the fundamental questions of what North Korean capabilities and intent in cyberspace are and what North Korean threats and vulnerabilities are associated with these. The thesis will begin by introducing the research approaches and challenges, as well as the significance of adversary activities and operations in cyberspace in chapter one. Chapter two will provide background on conflict in cyberspace, North Korea's national security environment, and North Korea's conventional capabilities and strategy. Chapter three will discuss the frameworks and

[1] Congress, Senate, Armed Services Committee. *Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, before the Senate Armed Services Committee*, by Michael Rogers. 5 April 2016. Web.

methodologies used for subsequent analysis. Chapter four will analyze the threats and vulnerabilities associated with North Korea as evidenced by its cyber power, which includes its resources and strategy. Chapter five will analyze the threats and vulnerabilities associated with North Korea as evidenced by cyberspace operations both by it and against it. Chapter six will discuss the subsequent conclusions. The thesis will conclude by discussing the United States national security implications of this analysis and providing policy recommendations in chapter six.

Arguments

Valerians and Maness propose a theory of cyber restraint and regionalism, claiming that most state interaction in cyberspace can be characterized as limited to restrained offensive cyberspace operations or cyber espionage and focused between regional actors.[2] To test this theory, the authors compiled the Dyadic Cyber Incident and Dispute Dataset (DCIDD), which covers cyber events from 2001 to 2011. However, there have been numerous events involving North Korea since then. This thesis argues that consistent with the theory, cyberspace operations by North Korea have remained focused primarily on South Korea over the United States and limited to offensive cyberspace operations and cyber espionage with minimal effect on South Korean and United States national security. It also argues that traditional disruption or denial approaches to cyberspace operations against North Korea, which have allegedly targeted strategic programs inside North Korea, focus on the wrong asset. Although North Korea values

[2] Valeriano, Brandon and Ryan Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. Print.

these programs, it also values its ability to control cyberspace within North Korea and its ability to engage in cyberspace activities and operations from abroad. These arguments are formalized as follows:

- Hypothesis 1: North Korea's cyberspace resources and capabilities have increased and have now reached a level that represents an advanced persistent threat.

- Hypothesis 2: Despite this increase, North Korea's cyberspace operations have remained restrained (produced minimal effects on South Korean and United States national security) and regional (targeted South Korea over the United States).

- Hypothesis 3: North Korea's valuable assets include its ability to control cyberspace within North Korea and its ability to engage in cyberspace activities and operations from abroad.

Research Approaches and Challenges

The main challenge for this thesis is finding reliable and/or verifiable information on North Korean cyberspace activities. Attribution in cyberspace is difficult, and entities affected by malicious activity are often reluctant to disclose information for various reasons. North Korea in particular is secretive by nature and reveals little information about itself. However, there are various methods for attribution, and most cyber events that are significant enough to be relevant for analysis often have information released by government authorities and/or network security companies. In fact, because events can affect both military and civilian entities and direct evidence can be left behind on the systems and networks of these victims, analysis can actually be easier. Although North Korea maintains strict control over information, there are also human sources with direct and indirect access to this controlled information.

In addition, there is the challenge of addressing “creeping validity” and “threat inflation.” In the former, “possibly” becomes “likely,” “likely” becomes “certainly,” and a presumption becomes established as a conclusion without any new evidence having been introduced.[3] In the latter, through misunderstanding or misrepresentation, concern for a threat is created that goes beyond the scope and urgency that is justified by informed and impartial analysis.[4] When an attempt at simply probing or phishing is described as a “cyberattack” or a “hack,” and a suspicion or an assumption regarding the identity of the perpetrator is presented as a conclusion, the available information must be carefully analyzed.

Significance

Activities related to cyberspace, such as offensive cyberspace operations, cyber exploitation, cyber espionage, and cybersecurity are a concern not only for the United States, but also for the international community. A review of the United Nations resolutions related to cyberspace provides evidence for the increasing significance of these activities; from simply preventing the misuse of information technologies in 2001, to eventually creating an international culture of cybersecurity and accounting for national efforts to protect critical information infrastructures in 2010.[5] Despite this increasing significance, however, cybersecurity efforts are still lagging. As of 2017, only

[3] Clarke, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do about It*. New York, NY: Harpers Collins Publishers, 2010. Print.
[4] Thrall, Trevor and Jane Cramer. *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11*. New York, NY: Routledge, 2009. Web.
[5] “UN Resolutions Related to Cybersecurity.” *International Telecommunication Union*, N.D. Web.

38 percent of countries have published a cybersecurity strategy and only 50 percent are in the process of developing a strategy.[6]

Cyberspace is especially significant for the United States. According to a statement by the former Director of National Intelligence, James Clapper, "[cyberspace] is both a resource on which our continued security and prosperity depends and a globally contested medium within which threats manifest themselves."[7] Within cyberspace, the United States considers North Korea (in addition to Russia, China, and Iran) to be among the most concerning of these threats. According to the Worldwide Threat Assessment of the US Intelligence Community:[8]

> [North Korea] has previously conducted cyberattacks against US commercial entities—specifically, Sony Pictures Entertainment in 2014—and remains capable of launching disruptive or destructive cyberattacks to support its political objectives. [North Korea] also poses a cyber threat to US allies. South Korean officials have suggested that North Korea was probably responsible for the compromise and disclosure of data in 2014 from a South Korean nuclear plant.

To maintain security and prosperity, understanding and addressing North Korean activities in cyberspace is a concern for both the United States and the international community.

[6] "Half of All Countries Aware but Lacking National Plan on Cybersecurity, UN Agency Reports." *United Nations*, 5 July 2017. Web.

[7] Congress, Senate, Armed Services Committee. *Foreign Cyber Threats to the United States*, by James Clapper. 5 January 2017. Web.

[8] Congress, Senate, Select Committee on Intelligence. *Worldwide Threat Assessment of the US Intelligence Community*, by Daniel Coats. 11 May 2017. Web.

CHAPTER II: BACKGROUND

Cyberspace operations, which refers primarily to government actions that are associated with a specific national goal, do not occur in isolation. All operations, both in cyberspace and traditional domains, occur within the context of an established national security environment. It is the perceived internal and external threats that comprise this environment and that motivate national capabilities and strategy, of which cyberspace is a single aspect. As such, to understand North Korea's cyberspace operations, it is necessary to understand its conventional capabilities and strategy as well.

Conflict in Cyberspace

The actors behind the malicious activity in cyberspace are diverse and include any individual or group with the capability and intent. Although the lines are sometimes blurred, the greatest distinction in regard to capability and intent can be made between state and non-state actors. State actors often have a capability that is more advanced and an intent that is more related to political or military goals.

Because the norms of behavior in cyberspace have not yet been established or codified, the nature of the interaction between state actors is ambiguous. The greatest ambiguity is whether certain malicious activity constitutes a cyberwar or whether it could even be considered an act of (traditional) war. Although there is much debate about whether a cyberwar will occur, there is some agreement that it has not yet occurred and that the malicious activity in cyberspace between state actors constitutes cyber conflict at worst, remaining restricted in scope and intensity.[9, 10]

A distinction in regard to the malicious activity that does occur can be made between exploitative incidents and disruptive incidents, which differ by ultimate effect. In an exploitative incident, sensitive information or data is compromised. This is commonly referred to as cyber espionage. In a disruptive incident, physical or virtual operations are hindered. These are commonly referred to as offensive cyberspace operations. These respective incidents are not mutually exclusive, as cyber espionage is often preparation for an offensive cyberspace operation. A policy brief from the Center for International and Security Studies at Maryland suggests that most incidents are exploitative and even for those that are disruptive, the scope, magnitude, and duration of most incidents constitutes a nuisance at worst.[11]

Among the actors in cyberspace, there are some that are considered an advanced persistent threat (APT), in contrast to a traditional threat. Opinions on the characteristics that constitute an APT are varied. According to the rather extensive definition provided by the National Institute of Standards and Technology, there are four distinguishing characteristics of an APT: (1) specific targets and goals, (2) high degree of organization and high amount of resources, (3) extended operations and repeated attempts, and (4) stealth and evasive techniques.[12]

[9] Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35.1 (2012): 5-32. Web.

[10] Stone, John. “Cyber War Will Take Place.” *Journal of Strategic Studies* 36.1 (2013): 101-108. Web.

[11] Gallagher, Nancy and Charles Harry. “Categorizing and Assessing Disruptive Cyber Incidents.” College Park, MD: *Center for International and Security Studies at Maryland*, April 2017. Web.

[12] Chen, Ping, Lieven Desmet, and Christophe Huygens. “A Study on Advanced Persistent Threats.” *IFIP International Conference on Communications and Multimedia Security 2014*. 25-26 September 2014. Web.

Malware and malicious code are the main weapons of cyberwar and cyber conflict. Although malware and malicious code are often synonymous with each other, the former can be thought of more as a program and the latter more as a script. There are three basic types of malware and malicious code that are classified based on the nature of propagation and execution: (1) trojans, (2) viruses, and (3) worms.[13] A trojan is piece of malware that is disguised as a legitimate program but also performs a function that is not authorized by the user, hence the name. It is unable to self-replicate, requiring that an unsuspecting user execute it. Although viruses and worms are able to self-replicate, a virus is executed by being attached to a host program and a worm is not. From here, further classification becomes complicated. The functions of malware and malicious code are varied and not restricted to a certain type. Individual malware and malicious code can have multiple functions and the various types can be embedded within each other. In general, however, malware and malicious code can be used to provide remote-access (ex: backdoors), monitor, collect and exfiltrate data (ex: packet sniffers, listeners, and keystroke loggers), modify or destroy data (ex: logic bombs and wipers), download or deploy additional malware (ex: downloaders and droppers), or conceal activities (ex: rootkits).

Attribution of malicious activity in cyberspace is notoriously difficult. There are a few reasons for this.[14] First, because of the global nature of cyberspace, an event can occur *from* a connected source anywhere in the world *against* a connected target anywhere in the world. Second, even if the source of an event is determined, the owner of

[13] "Malicious Programs." Blog post. *SecureList*, N.D. Web.
[14] Singer, P.W. and Alan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014. Print.

a system or network is not necessarily aware that it was used for malicious activity. That is, it is possible that the actual perpetrator had remote-access. Third, even if it is determined that the perpetrator had remote-access, it is not necessarily possible to identify the perpetrator.

Despite these difficulties, attribution to some degree is possible. [15] In fact, the greater the scale of an operation, such as that characteristic of a state actor, the greater the chance that crucial evidence is left behind (for example, logs from target systems and networks or direct connections from source internet protocol (IP) addresses). Analysis of this evidence, in addition to the tools, tactics, and procedures (TTPs) of the operation, can be used to determine a source. Many aspects of the TTPs can be revealing. For example, to maximize operational efficiency and reduce logistical cost, threat actors often reuse the same infrastructure for operations, such as the same internet service providers or servers. Because malware can be complex to develop, it is often modular, with threat actors reusing the same or similar modules for multiple operations. As operations often adhere to schedules and routines, the pattern of life of behind an operation provides evidence as to the location and identity of the threat actor; for example, timing that coincides with certain national holidays, local time zones, or institutional habits. Language preferences, conventions, and errors in malware can reveal the native language of the threat actor, as well as even background or experience. All this evidence, most importantly, can be used to connect a series of operations.

[15] Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks” *Journal of Strategic Studies* 38.1-2 (2015): 4-37. Web.

Valeriano and Maness advocate, however, for going beyond simply using a forensic model of attribution and propose that in the context of international relations, attribution can be made to a high degree of confidence.[16] This is especially applicable to North Korea, which has obvious targets and goals. For example, even if there is little forensic evidence directly implicating North Korea in a distributed denial of service (DDOS) operation that targets South Korea and the United States on Independence Day or in an offensive cyberspace operation that wipes the hard drives of media corporations and financial institutions in South Korea days after North Korea promises retribution, the most likely perpetrator is obvious. In fact, through offensive cyberspace operations, a perpetrator is often able to simultaneously gain the benefits of signaling (and thus achieve a political goal) while also avoiding the consequences of such operations by maintaining plausible deniability. In addition, although there is the potential for these to be "false flag" operations in which a perpetrator attempts to falsely implicate North Korea, validation of this suspicion requires that there is a more compelling threat actor than North Korea that also has the means, motive, and opportunity.

North Korean National Security Environment

North Korea remains arguably economically and diplomatically the most isolated nation in the world. This isolation is in part self-imposed and due to the guiding national ideology of *Juche* (self-reliance or self-determination), which advocates the protection of the ruling regime and the idea that because North Korea is under constant threat, to

[16] Valeriano, Brandon and Ryan Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. Print.

survive it must remain economically and militarily reliant on no other nation.[17] Its isolation is also in part due to its development of nuclear weapons and ballistic missiles in violation of or disregard for international treaties, agreements, and norms.[18] This development has brought about harsh economic and diplomatic sanctions from most members of the international community. North Korea is also guided by the national policy of *Songun* (military-first), which prioritizes the military in the conduct of state affairs and the allocation of resources.

North Korea perceives external threats from the expanding gap in national power between itself and South Korea and from an increasing distrust of the regional state actors and former allies of China and Russia.[19] There is also the immediate threat perceived in the presence of South Korean and United States armed forces stationed on the peninsula, as well as the potential threat perceived in the United States nuclear deterrent. North Korea, in particular the ruling regime, perceives internal vulnerabilities in decreasing economic control over the population[20] and increasing flow of information other than state-sanctioned media into and within the nation.[21]

North Korea's overall national goals are to perpetually maintain the rule of the current political regime and to eventually reunify the peninsula.[22] To achieve these goals,

[17] "Venerating the Kims: Just One More Religion?" *The Economist*, 7 April 2013. Web.

[18] North Korea withdrew from the Treaty on the Non-Proliferation of Nuclear Weapons in 2003, has never joined the Comprehensive Nuclear-Test-Ban Treaty or Missile Technology Control Regime, and admitted in 2003 that it had violated the Agreed Framework.

[19] Department of Defense, Office of the Secretary of Defense. *Military and Security Developments Involving the Democratic People's Republic of Korea 2015*. 2015. Web.

[20] Ibid.

[21] Fang, Arnold. "North Korea's Self-Imposed Isolation." *The Diplomat*, 15 March 2016. Web.

[22] Department of Defense, Office of the Secretary of Defense. *Military and Security Developments Involving the Democratic People's Republic of Korea 2015*. 2015. Web.

and in light of a military that is powerful in terms of quantity but not in terms of quality,[23] its capabilities and strategy have focused on asymmetrical and irregular warfare, in particular through the use of special operations forces, as well as nuclear, biological, and chemical weapons.

North Korean Conventional Capabilities and Strategy

North Korea's national security apparatus is coordinated under the authority of the Central Military Committee and the National Defense Commission, both of which are chaired by the Supreme Leader, Kim Jong-un. The military is represented by the Ministry of People's Armed Forces, which exercises control over the Korean People's Armed Forces (KPAF). [24] The KPAF includes the Ground Force, Navy, Air Force, Strategic Missile Force, and Special Operations Force. The KPAF is dominated by the Ground Force, most of which is stationed near the demilitarized zone between North Korea and South Korea. It maintains an active force strength of 1.2 million military personnel and a reserve force strength of 7.6 million, with an additional 200,000 special operations personnel.[25] In comparison, allied forces consist of 655,000 South Korean and 23,500 United States military personnel.[26]

[23] Laurence, Jeremy. "North Korea Military Has an Edge over South, but Wouldn't Win a War, Study Finds." *The Christian Science Monitor*, 4 January 2012. Web.

[24] The KPAF is more traditionally referred to as the Korean People's Army (KPA), with the main constituent branches referred to as the KPA-Ground Force, KPA-Navy, and KPA-Air Force. The alternative translation proposed here is more accurate and is used to avoid confusion.

[25] McCafferty, Georgia. "Anniversary Parade Provides Rare Glimpse into North Korea's Military Might." *CNN*, 10 October 2015. Web.

[26] Price, Greg. "U.S. Military Presence in Asia: Troops Stationed in Japan, South Korea, and Beyond." *Newsweek*, 26 April 2017. Web.

Despite these numbers, North Korea's military relies on personnel that are undertrained and undernourished and on equipment that is obsolete.[27] Most of the military systems are overburdened and outdated, being produced in or based on designs from China and the Soviet Union from the 1950s, 1960s, and 1970s. However, Kim Jong-un has placed an emphasis on the development of modern systems.

According to the Center for Strategic and International Studies, North Korea has focused its efforts on developing and expanding asymmetric warfare capabilities, including weapons of mass destruction, ballistic missiles, and special operations and cyberwarfare capabilities.[28] As evidence for this, it has conducted five nuclear tests, with the most recent in September 2016.[29] It has continued and even intensified tests of ballistic missiles, in particular the submarine-launched KN-11 and the mobile-launched KN-15 (a variant of the KN-11), with the initial test for the KN-11 in December 2014 and for the KN-15 in February 2017.[30] Its special operations units are among the best-trained and best-equipped in the military.

North Korea's military strategy is derived from guidance provided by the Soviet Union and experience gained during the guerrilla resistance against Japan. It is offensive in nature and focused on the use of overwhelming surprise, speed, and force with asymmetrical and irregular capabilities to counter the conventional strength of the armed

[27] Blair, David. "North Korea v. South Korea: How the Countries' Armed Forces Compare." *The Telegraph*, 15 September 2015. Web.
[28] Cordesman, Anthony. "Korean Peninsula Military Modernization Trends." Washington, DC: *Center for Strategic and International Studies*, 20 September 2016. Web.
[29] "Missiles of North Korea." Washington, DC: *Center for Strategic and International Studies*, N.D. Web.
[30] Ibid.

forces of South Korea and the United States.[31] This is embodied in the doctrine of "Fast War, Fast End" and demonstrated in the structuring and stationing of the military.

Its military strategy is also characterized by belligerence and provocation, consisting of rhetoric and confrontation that is sometimes violent yet below the threshold for an act of war, which is used to gain concession from regional adversaries.[32]

[31] Hodge, Home. "North Korea's Military Strategy." *Parameters* 33 (2013): 68-81. Web.

[32] Sullivan, Tim. "North Korea and its Provocations: Belligerence as Strategy." *The Washington Times*, 9 February 2016. Web.

CHAPTER III: FRAMEWORKS AND METHODOLOGIES

There are four background topics that must be understood before answering the research questions presented in this thesis: (1) how threat and vulnerability are conceptualized in relation to risk, (2) how the cyber threat is assessed, (3) how cyberspace and cyberspace operations are defined, and (4) how the target is analyzed.

Topic one is addressed through the Department of Homeland Security (DHS) Risk Lexicon. Topic two is addressed through two sets of frameworks and methodologies. The first, from the Sandia National Laboratories Operational Threat Assessment (OTA), is used to analyze cyber threat actors and considers the factors of commitment attributes and resource attributes. The second, from the Valeriano and Maness DCIDD, is used to analyze cyber events and considers the factors of method, severity, interaction, target, and goal. Topic three is addressed through two Department of Defense (DOD) joint publications, 3-13 on information operations and 3-12 (R) on cyberspace operations, as well as Army Field Manual 3-38 on cyber electromagnetic activities. Topic four is addressed through a target-centric approach.

Conceptualizing Risk

The DHS conceptualizes risk as being comprised of a scenario, a threat, a vulnerability, and a consequence as depicted in Figure 1.[33] Within a scenario, a threat exploits a vulnerability, which then has a consequence. The scenario includes a target, an adversary, an attack method, and an attack path. The attack method refers to the tools and

[33] Department of Homeland Security. *DHS Risk Lexicon*, September 2008. Web.

tactics, and the attack path refers to the phases of planning, developing, and executing. The threat is comprised of the capability and intent of the adversary. Because of this inherent relationship, the term ‘threat’ often refers to the adversary as an actor itself and not necessarily a combination of its capability and intent. To avoid confusion, the term ‘threat actor’ is used to maintain a distinction. The vulnerability is an attribute of an entity that renders it vulnerable to exploitation and thus exposes an asset that has value to the adversary. A consequence includes effects that are operational, psychological, physical, and/or economic.

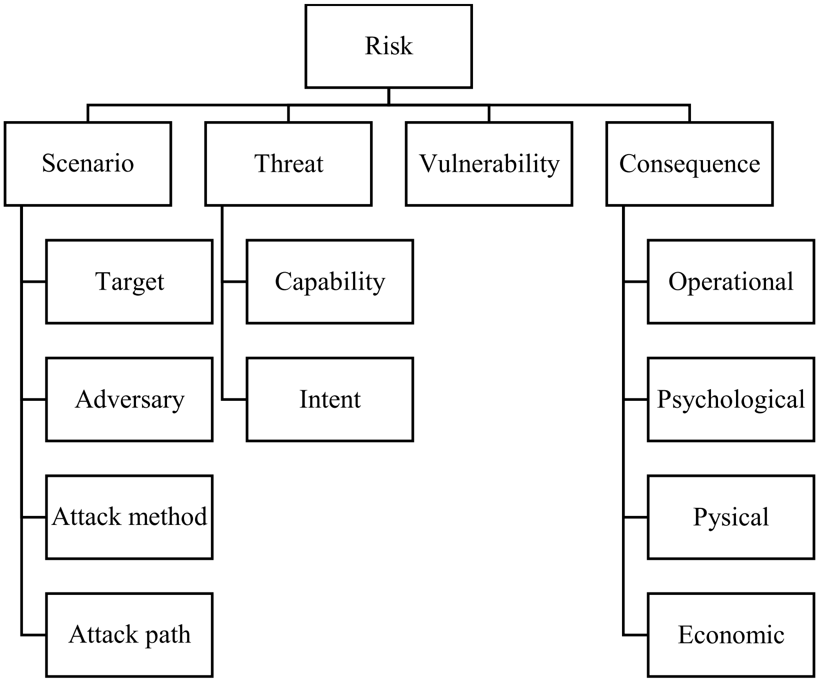

Figure 1. Department of Homeland Security Elements of Risk.

To put these elements of risk in context, an unsecured system or network can be a vulnerability, but only if there is an asset on that system or network worth protecting by an owner or worth acquiring by an adversary. The adversary can be a threat to this unsecured network, but only if it has the means and motives (the capability and intent) to exploit the vulnerability. It is this framework that is used to establish the fundamental elements that must be considered in discussing the issue of North Korean in cyberspace.

Defining Cyberspace and Cyberspace Operations

Cyberspace and cyberspace operations are notoriously difficult to define due to the nascent and dynamic nature of these concepts. Approaches to defining concepts can be either normative or descriptive. DOD joint publications represent a more normative approach. Joint Publication 3-13, the DOD guidance on information operations, states that "cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers".[34] Within this definition, there is an implication that cyberspace has both a physical aspect ("the interdependent network of information technology infrastructures") and a virtual aspect ("[the] resident data").

Joint Publication 3-12 (R), the DOD guidance on cyberspace operations, categorizes cyberspace operations based on intent into offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DOD information network (DODIN) operations.[35] It defines OCO as "the application of force in or through cyberspace" and DCO as "passive and active cyberspace defense operations to preserve the ability to use [cyberspace] capabilities and protect data, networks, network-centric

[34] Department of Defense. *Joint Publication 3-13: Information Operations*, 2014. Web.

[35] Department of Defense. *Joint Publication 3-12 (R): Cyberspace Operations*, 2013. Web.

capabilities, and other designated systems".[36] Previous versions of the guidance referred to OCO more narrowly as computer network attack (CNA) and DCO more narrowly as computer network defense (CND), and included computer network exploitation (CNE). CNE, which was considered an aspect of intelligence, is now referred to more broadly as cyberspace intelligence, surveillance, and reconnaissance (CISR) and is conceptualized as supporting both OCO and DCO. In addition to intent, Joint Publication 3-12 (R) also categorizes cyberspace operations based on capability as follows:

- Cyberspace attack: Actions in cyberspace to deny access to or use of, as well as manipulate the information, information systems, and/or information networks of an adversary. Denial involves efforts to degrade (a function of amount), disrupt (a function of time), and destroy (a function of both amount and time). Manipulation involves efforts to control or alter.

- Cyberspace defense: Actions in cyberspace to secure and defend the information, information systems, and/or information networks of an owner against an adversary. Activities include the actions of protecting, detecting, characterizing, countering, and mitigating.

- Cyberspace intelligence, surveillance, and reconnaissance: Actions in cyberspace to collect intelligence that is required to support current and future operations, including OCO and DCO.

Guidance from the Army, Field Manual 3-12, integrates the concept of cyberspace operations with the concept of electronic warfare operations.[37] It refers to this as cyber electromagnetic activities. This can be understood as a shifting of focus from the virtual aspect of cyberspace in Joint Publication 3-12 (R) to the physical aspect. Through cyber electromagnetic activities, the Army can plan, integrate, and synchronize the

[36] Ibid.

[37] Department of Defense, United States Army. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations*, April 2017. Web.

missions of OCO, DCO, and DODIN with electronic attack, electronic protection, electronic warfare support, and spectrum management operations.

Singer and Friedman represent a more descriptive approach to defining cyberspace and cyberspace operations. Although the authors state that "cyberspace is the realm of computer networks and [users] in which information is stored, shared, and communicated online", the focus is on describing the essential and unique features of cyberspace.[38] Cyberspace, as also defined in Joint Publication 3-13, is foremost an information environment and is characterized by the creation, manipulation, transfer, and storage of data. However, it is also the information systems, networks, and infrastructures that allow these activities to occur. As such, to emphasize, the most important feature of cyberspace is that it has both a physical aspect and a virtual aspect.

There are additional features of cyberspace that distinguish it from the traditional domains of air, land, and sea. Cyberspace obscures conventional geopolitical boundaries, it is artificial and therefore easily and quickly changes (at least relative to the other domains), and activities within it can occur both in an instant and from a distance. Regarding obscuring conventional geopolitical boundaries, it is a common misconception that this means that cyberspace is a global commons, such as sea or space. However, as emphasized earlier, cyberspace does have a physical aspect. This means that even if it is global by virtue of being expansive and interconnected, elements of the infrastructure still reside within sovereign territories that can exercise control over it. The tendency by those in national security to forget the importance of this was even noted by Michael Hayden,

[38] Singer, P.W. and Alan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014. Print.

the former Director of the NSA and former Director of the CIA, who stated that "DOD's construct of a separate domain tended to mute the traditional principles and responsibilities of sovereignty."[39] Although this discussion of attributes is not exhaustive, it does paint a picture of the nature of cyberspace adequate for this thesis.

Singer and Friedman use the availability, integrity, and confidentiality (AIC) triad[40] from the concept of information security to categorize cyberspace operations according to the element of the triad that is threatened.[41] Availability operations are those that deny access to a system or network. These are equivalent to the denial activities of DOD cyberspace attack. Integrity operations are those that penetrate systems or networks to manipulate information. These are equivalent to the manipulation activities of DOD cyberspace attack. Confidentiality operations are those that penetrate systems or networks to monitor activities and exfiltrate information. This is equivalent to DOD cyberspace intelligence, surveillance, and reconnaissance.

With all these operations, it is important to consider the consequence in the context of national security. Although both are confidentiality operations, the theft of credit card information from a retail business is much different than the theft of background investigation information from a government organization or weapon system designs from a defense contractor. An availability operation against a government

[39] Hayden, Michael. "Life in The Cyber Domain." *Playing to the Edge: American Intelligence in the Age of Terror*. New York, NY: Penguin Books, 2016. Print.
[40] This is more traditionally referred to as the CIA triad, but also as the AIC triad to avoid confusion with the Central Intelligence Agency.
[41] Singer, P.W. and Alan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014. Print.

website that denies access to services is also much different than an availability operation against critical infrastructure that denies access to energy or water.

Because inconsistent or exaggerated use of key terms can lead to misunderstanding or inflation of a situation, for the purposes of this thesis, these terms are defined and maintained as follows:

- Cyberspace: An information environment comprised of interconnected systems and networks, including supporting infrastructure, and characterized by the creation, manipulation, storage, and transfer of information and data.

- Offensive cyberspace operations: Deliberate actions to disrupt or deny access to information systems and networks by the adversary or to alter the integrity of information and data on these systems and networks through modification or deletion. This is popularly referred to as cyberattack.

- Defense cyberspace operations: Deliberate actions to protect information systems and networks and ensure the availability, integrity, and confidentiality of the information and data on these systems and networks. This is popularly referred to as cybersecurity.

- Cyber exploitation/Cyber espionage:[42] Deliberate actions to compromise the confidentiality of information systems and networks used by the adversary through the gaining of unauthorized access to monitor activity or exfiltrate information and data.

In addition, 'cyberspace activity' will refer primarily to government and civilian actions in cyberspace that are not associated with a specific national goal, and 'cyberspace operation' will refer primarily to government actions that are associated with a specific national goal. The actions of a cyberspace operation will be categorized as either 'offensive cyberspace operations', 'defensive cyberspace operations', or 'cyber exploitation/cyber espionage' as appropriate. Other actions that are not associated with

[42] Although used as synonymous, cyber exploitation will be used when it is unclear whether any monitoring or exfiltration was successful.

traditional political or military goals yet still represent malicious activity will be referred to as cybercrime.

Characterizing the Cyber Threat

There are numerous methods for characterizing the cyber threat. These range from taxonomies, which classify information about the threat, to frameworks and methodologies, which provide a structure for understanding the threat and an approach to assessing it.

Under the DHS Risk and Vulnerability Assessment program, which was established to assist federal civilian government entities with assessing respective cyber risks and vulnerabilities, Sandia National Laboratories developed the OTA methodology.[43] OTA was designed to assess cyber threats using consistent metrics and models. A generic threat matrix, which is depicted in Table 1, is used in OTA to describe cyber threat actors based on various attributes and then to categorize these along a spectrum from most capable of achieving a goal (threat level 1) to least capable of achieving a goal (threat level 8). That is, each level is an assessment of the threat actor based on its capabilities. OTA was selected for this thesis because, in addition to addressing capabilities in particular, it is intended to be used based on unclassified information.

[43] Sandia National Laboratories. *Categorizing Threat: Building and Using a Generic Threat Matrix*, by David Duggan, Sherry Thomas, Cynthia Veitch, and Laura Woodard, September 2007. Web.

Table 1. Operational Threat Assessment Generic Threat Matrix.

THREAT LEVEL	THREAT PROFILE						
	Commitment Attributes			Resource Attributes			
	Intensity	Stealth	Time	Technical Personnel	Cyber Knowledge	Kinetic Knowledge	Access
1	H	H	Years/Decades	Hundreds	H	H	H
2	H	H	Years/Decades	Tens/Tens	M	H	M
3	H	H	Months/Years	Tens/Tens	H	M	M
4	M	H	Weeks/Months	Tens	H	M	M
5	H	M	Weeks/Months	Tens	M	M	M
6	M	M	Weeks/Months	Ones	M	M	L
7	M	M	Months/Years	Tens	L	L	L
8	L	L	Days/Weeks	Ones	L	L	L

In the generic threat matrix, a threat profile is comprised of both commitment attributes and resource attributes, which together represent the capability element of a threat from the concept of risk. Although the measures for some attributes are quantitative, such as time and technical personnel, others are necessarily qualitative, such as intensity and stealth. These attributes and measures are defined as follows:

- Intensity: The amount of determination and diligence that a threat actor has in pursuit of its goals, as well the amount of associated risk that it is willing to accept. (Low, Medium, or High)
- Stealth: The ability of the threat actor to obscure or conceal the details about itself, including its goals, operations, and structures. (Low, Medium, or High)
- Time: The amount of time that a threat actor is willing to dedicate to planning, developing, and executing operations in pursuit of its goals. (Days to Weeks, Weeks to Months, Months to Years, or Years to Decades)

- Technical personnel: The number of personnel with specialized expertise that the threat actor is able to use in its operations. (Ones, Tens, Tens of Tens, or Hundreds)

- Cyber knowledge: The amount of internal theoretical and practical expertise related to the cyber domain that a threat actor has and its ability to use this expertise in pursuit of its goals. Expertise includes the ability of the threat to share information internally, acquire additional expertise, and conduct research and development. (Low, Medium, or High)

- Kinetic knowledge: The amount of internal theoretical and practical expertise related to the kinetic domain that a threat actor has and its ability to use this expertise in pursuit of its goals. Expertise includes the ability of the threat to share information internally, acquire additional expertise, and conduct research and development. (Low, Medium, or High)

- Access: The ability of the threat actor to penetrate a secured system or network through either cyber or kinetic means. (Low, Medium, or High)

It is important to emphasize that the generic threat matrix is intended to simply provide a best possible match. It is likely that a threat actor will not have an exact fit to a level, but rather will share more attributes with a certain level over another.

In addition to this, Valeriano and Maness provide a framework and methodology for assessing cyberspace incidents in the context of international relations.[44] As such, the focus is on interactions between state actors in cyberspace, although non-state entities as targets are considered. This framework and methodology was used to compile the DCIDD. The factors identified are the method, severity, interaction, target, and goal. From the framework of risk, roughly, the method corresponds to attack method and attack path, the severity corresponds to consequence, the target corresponds to target, and the goal corresponds to intent. The types for each of these factors is depicted in Figure 2.

[44] Valeriano, Brandon and Ryan Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. Print.

It is important to note that for the authors the term ‘cyber incident’ refers to an individual operation and the term ‘cyber dispute’ refers to a series of operations. For the factor of interaction, types 4 through 6 are applicable only to cyber dispute and for the factor of target, types 4 through 7.

FACTOR	TYPES
Method	1. Vandalism 2. Denial of service 3. Intrusion 4. Infiltration 4.1 Logic bomb (any type) 4.2 Virus 4.3 Worm 4.4 Packet sniffer (any type) 4.5 Keystroke logger (any type) 5. Advanced persistent threat 6. Vandalism and denial of service 7. Intrusion and infiltration
Severity	1. Minimal effect 2. Effect on critical national infrastructure or military 3. Dramatic effect on national security strategy 4. Dramatic effect on nation 5. Catastrophic effect on nation
Interaction	1. Nuisance 2. Defensive 3. Offensive 4. Nuisance and defensive 5. Nuisance and offensive 6. Nuisance, defense, and offensive
Target	1. Private 2. Government non-military 3. Government military 4. Private and government non-military 5. Private and government military 6. Government (non-military and military) 7. Private and government (non-military and military)
Goal	1. Disruption of target activity 2. Acquisition of target information and data 3. Modification of target behavior

Figure 2. Factors and Types for Dyadic Cyber Incident and Dispute Dataset.

It is also important to discuss the factor of method, the types for which are described in Table 2 with slight modifications to phrasing. Vandalism includes activities such as website defacements, and common tools include the insertion of malicious code. Denial of service includes activities such as DDOS attacks, and common tools include botnets. Intrusion includes activities such as compromising systems to allow unauthorized access, and common tools include trojans or backdoors. Infiltration includes activities such as forcing systems to conduct unauthorized activity, and common tools include logic bombs, viruses, worms, packet sniffers, and keystroke loggers. According to the authors, intrusions and infiltrations are distinguished from each other in that intrusions are more exploitative and general, and infiltrations are more disruptive and precise. Although the authors also claim that only infiltrations are the methods that states can claim as an act of war, the DOD document that the authors cited did not state this explicitly.[45] From these descriptions, the method used for in operation is understood to be a combination of tools and tactics.

However, because the tools of cyberspace operations (malware or malicious code) represent overlapping tactics, the types as proposed encounter difficulties. The descriptions from Valeriano and Maness for the tools and tactics of the method used in an operation are also different from the classifications for the types and functions of malware presented earlier. For example, the authors categorize malware as infiltration, even though malware can have functions unrelated to infiltration. Although trojans can function as backdoors, backdoors are described as being different in not needing an operator to be installed and executed.

[45] Department of Defense. *Strategy for Operating in Cyberspace*, 1 July 2011. Web.

Table 2. Valeriano and Maness Methods of Cyberspace Operations.

CODE/EVENT	EXAMPLE	EXPLANATION
1. Vandalism	Website defacements	SQL injection or cross-scripting
2. DOS	DDOS attacks	Botnets used to shut down websites with high traffic
3. Intrusion	Trapdoors or trojans, backdoors	Software injected remotely for intrusions and thefts
4. Infiltration	Logic bombs, worms, viruses, packet sniffers, keystroke loggers	Different methods that are used to penetrate target networks; software can be installed remotely or physically
5. APT	Advanced persistent threats	Precise and sophisticated methods that have specific targets; methods can include vandalism, DOS, intrusion or APT
6. Vandalism and DOS	Cyber disputes	Combined incidents of vandalism and DOS
7. Intrusion and Infiltration	Cyber disputes	Combined incidents of intrusion and infiltration

This is the difference between a trojan and a worm or virus, and remote-access is not a function exclusive to any of these types. Infiltration is said to include worms, viruses, packet sniffers, keystroke loggers, and logic bombs, even though worms and viruses can have functions unrelated to infiltration, and trojans can also function as packet sniffers or keystroke loggers. Although logic bombs are described as modifying or deleting data, the reason for categorizing these under intrusion instead of vandalism or denial of service is not clarified. In addition, although the authors note that the types for the methods used in cyberspace operations do not indicate a scale of severity, which is addressed in the severity of the operation, there does seem to be some overlap with the goal of an operation.

However, despite these discrepancies, this methodology is the most practical for assessing the capability and intent (among other aspects) of interactions in cyberspace. In addition to the threat level from OTA that corresponds to capability, all the elements required for a comprehensive assessment are now present.

Analyzing the Target

For the purposes of this thesis, it is helpful to approach the topic as a target of intelligence analysis. Clark advocates a target-centric approach and presents the target as both a system and a network (in the abstract sense not the technological sense). A system is comprised of three elements: (1) the structure or relationships between the entities within the system, (2) the function or the results or effects produced by the system, and (3) the processes or the activities within the system that produce the results or effects. On the topic of North Korean cyberspace operations, the organizations that conduct the operations are a system. There are managers, engineers, operators, and other entities in hierarchical, lateral, and other relationships that plan, develop, and execute cyberspace operations to achieve national goals.

A network is comprised of nodes and links. There are networks *within* systems, as suggested by the presence of entities (nodes) and relationships (links). However, there are also networks *of* systems. North Korean cyberspace operations do not occur in isolation. The organizations that conduct the activities are nodes linked to other supporting or opposing organizations both inside and outside of North Korea. For example, in addition to cyber organizations, the KPAF Air Force and KPAF Navy also support national goals but in traditional domains, and Chinese internet service providers facilitate North Korean cyberspace operations. The United States, as well as its allies and partners, however, attempt to hinder North Korean cyberspace activities both offensively and defensively.

CHAPTER IV: ANALYSIS OF CYBER POWER

Although there is no single definition that is agreed upon, state power can be understood generally as the capacity to conduct certain activities *by* the state and specifically as the ability to use these activities to produce desirable results *for* the state.[46] This implies the existence of resources (that provide the capacity) and strategy (that guides the ability). It is the resources and strategy of a state that establish the context for understanding the threats it poses and the vulnerabilities it possesses. Cyberpower in particular is the capacity and ability to affect desirable outcomes on or in cyberspace. According to Nye, cyberpower is based on resources that relate to the creation, control, and communication of information in cyberspace, such as infrastructure and personnel.[47] The author also recognizes, however, that strategy includes instruments of cyberpower that are both physical and virtual, reflecting the nature of cyberspace itself. For example, a state can destroy systems and networks in the physical world or it can deny access to or manipulate the integrity of information in the virtual world. The following sections will discuss the cyber resources and strategy of North Korea, as well as the assessments of its cyberpower in comparison to other nations.

[46] Tellis, Ashley, Alison Szalwinski, and Michael Wills. "Strategic Asia 2015–16: Foundations of National Power in the Asia-Pacific." Washington, DC: *National Bureau of Asian Research*, 2015. Web.

[47] Nye, Joseph. "Cyber Power." Cambridge, MA: *Belfer Center for Science and International Affairs*, May 2010. Web.

Civilian Cyber Resources and Activities

Although the civilian cyber infrastructure of North Korea lags far behind that of other nations, its development has been cautious yet consistent. Its initial internet connection was established by the Korea Computer Center (KCC) in 2003 via satellite with a German company called KCC Europe, which then for several years operated the '.kp' domain name and hosted North Korean websites.[48] In 2010, after the websites disappeared from the internet, the KCC inquired for several months about reinstating service with no response from KCC Europe. It then terminated its service agreement and transferred its service to a company called Star Joint Venture, a joint venture between North Korea's Post and Telecommunications Corporation and Thailand's Loxley Pacific, which offered internet connection via landline with the Chinese state-owned enterprise China Unicom. Star Joint Venture started hosting North Korean websites on the internet in October 2010. However, the websites were accessible only by using the direct IP addresses until Star Joint Venture acquired official control of the '.kp' domain name in January of 2011. Star Joint Venture remains the single internet service provider for North Korea. It is estimated that there are only a few thousand internet users restricted to elites and to foreigners, with access available only after obtaining an IP address from the Ministry of Post and Telecommunications and computers required to be registered with local authorities.[49] For even these users, the government monitors activities and restricts access to certain websites, such as Facebook, Twitter, and YouTube.[50] It has also

[48] Williams, Martin. "North Korea's Internet Domain Is in New Hands." *PC World*, 19 May 2011. Web.
[49] Boynton, Robert. "North Korea's Digital Underground." *The Atlantic*, April 2011. Web.
[50] Talmadge, Eric. "North Korea Announces Blocks on Facebook, Twitter and YouTube." *The Guardian*, 1 April 2016. Web.

requested that foreign embassies in North Korea that have Wi-Fi require passwords or decrease signal strength to prevent unauthorized access by locals.[51]

In addition to the internet, there is a domestic intranet called *Kwangmyong* (Bright Star) that was established in 2000 and is free to access by the population. Although a misconfiguration in a domain name server exposed 28 websites under the '.kp' domain name to the internet in September 2016, it is estimated that there are from 1,000 to 5,000 websites accessible only through *Kwangmyong*, which is operated under a different domain name system.[52] *Kwangmyong* includes search and email functionality and offers a variety of content, including news and entertainment media and shopping. Actual usage statistics, unsurprisingly, are not available.

All computers, including those used to access both the internet and *Kwangmyong*, are installed with domestic software that is often based on open-source software. For example, the official operating system, *Pulgunbyol* (Red Star), is based off Linux and the official web browser, *Naenara* (My Country), is based off Firefox. Red Star was developed by the KCC in 1998, with the most recent version released in 2013.[53] Other software that has been developed by the government includes a firewall called *Nungna*, an antivirus program called *Kullaksae*, and an access control solution called *Pogom*.[54] According to German researchers, a unique feature of Red Star is that it tags each media

[51] Kang, Tae-jun. "Wi-Fi Access Sparks Housing Boom in Pyongyang." *The Diplomat*, 14 August 2014. Web.

[52] Russon, Mary-Ann. "No, North Korea's Internet Doesn't Only Have 28 Websites, but Reddit Did Manage to Crash Them." *International Business Times*, 22 September 2016. Web.

[53] Not to be confused with the government's Naenara internet portal.

[54] Yang, Jeong-yoon, So-jeong Kim, and Il-seok Oh. "Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities." *International Workshop on Information Security Applications 2016*. 30 March 2017. Web.

file with a unique identifier for the computer once it is accessed.[55] It also prevents users from modifying basic functions of the core operating system or disabling the firewall or antivirus program.[56]

Analysis of a recent tablet produce around 2015 or 2016 by North Korea reveals an increasing sophistication in the degree of surveillance and control incorporated into devices.[57] A program called Red Flag runs as a background process, capturing a screenshot every time the user opens an application, recording the browser history and unique identifier for the tablet, and ensuring that the core operating system is not modified. A tagging feature for media similar to similar to Red Star is also present. In addition, the installation of applications is limited to an approved whitelist. Even more restrictive than this, the tablet is able to access media only if it has the digital certificate either NATISIGN (authorized by the North Korean government) or SELFSIGN (created on the tablet itself). This prevents the sharing of unauthorized media between users.

Much of North Korea's information technology (IT) research and development is done at the state-owned KCC, which was established in 1990. Despite claims of being for research and development, it was reported in 2001 that the KCC had actually been established under the initiative of Kim Jong-nam, the eldest son of Kim Jong-il, for foreign intelligence.[58] Information from the National Intelligence Service (NIS) from 2005 confirmed that Kim Jong-nam, who at the time was involved with security and

[55] "North Korea's 'Paranoid' Computer Operating System Revealed." *The Guardian*, 27 December 2015. Web.

[56] Ibid.

[57] Williams, Martyn. "All That Glitters Is Not Gold: A Closer Look at North Korea's Ullim Tablet." *38 North*, 3 March 2017. Web.

[58] 이교관. "조선컴퓨터센터의 비밀." *NK Chosun*, 11 May 2001. Web.

counterintelligence operations at the Ministry of State Security, used the KCC to control communications into and out of North Korea and to monitor and collect foreign intelligence.[59] There are/were around 1,000 personnel at the KCC, although it has recently been reported that most have been sent abroad to earn money for the regime.[60] Despite possible ulterior functions and in addition to research and development, the KCC is also responsible for the management of computer networks and websites within the nation, education and training, and hardware and software distribution, with offices in China, Japan, and Europe. There are nine centers subordinate to the KCC:[61]

1. Red Star Information Center (internet applications and multimedia)
2. Samilpo Information Center (applications)
3. Osandok Information Center (systems software and operating systems)
4. Mankyong Information Center (information and communications software)
5. Chongbong Information Center (artificial intelligence)
6. Sobaeksu Information Center (control automation and quality engineering)
7. Miryong Information Center (medical applications)
8. Samjiyon Information Center (multimedia systems)
9. Naenara Information Center (digital content production and services)

Other state-owned IT ventures, each with hundreds of personnel, include the Pyongyang Informatics Center, Daeyang IT Company, and Hi-Tech Development Company, as well as IT firms subordinate to commercial enterprises such as the Unha Corporation or Korea Roksan General Trading Company.[62] Another venture, the Kwangmyong IT Center, specializes in network security, data encryption and recovery, and biometric identification and seems to be a spinoff of the Oun Information Center,

[59] 김소열. “北, 04 년부터 中단둥서 사이버戰 활동.” *Daily NK*, 12 July 2009. Web.

[60] 김도형. “北, IT 인력 1500 명 해외 보내 年 4000 만달러 벌어.” DongA Ilbo, 25 August 2016. Web.

[61] There was a significant increase in 2004 when the number of centers expanded from 6 to 9: “북한의 정보화(H/W·S/W 부문) 강화 동향.” *Tongil News*, 24 March 2004. Web.

[62] Tjia, Paul. “North Korea: An Up-and-Coming IT-Outsourcing Destination.” *38 North*, 26 October 2011. Web.

which had been subordinate to the KCC and specialized in information security. North Korea has even pursued joint ventures with foreign entities; for example, the Nosotek (between the North Korean General Federation of Science and Technology and entrepreneurs from Germany) and Hana Electronics (between the North Korean Ministry of Culture and investors from the United Kingdom).[63]

Initial service for North Korea's mobile network was established in November 2002 under Loxley Pacific, the same company that later formed Star Joint Venture.[64] Before this, mobile communications had been limited to senior military and party officials. The 2G network provided service to around 20,000 subscribers until all mobile phone use was banned in 2004 following an alleged assassination against Kim Jong-il that used a remote-detonated explosive device. Service resumed in December 2008 under a company called Koryolink, a joint venture between North Korea's Post and Telecommunications Corporation and Egypt's Orascom Telecom Media and Technology.[65] Although initially limited to voice service and short messaging service (SMS) and around 6,000 subscribers, the 3G network currently supports multimedia messaging service (MMS) and around 3 million subscribers, with the capacity to support up to 6 million.

The network is divided into two tiers, with local subscribers able to connect only to domestic numbers (tier one) and foreign subscribers able to connect only to

[63] The Hana Electronics joint venture was terminated due to irreconcilable differences: O'Carroll, Chad. "Well-Known Electronics Joint Venture Terminated in Pyongyang." *NK News*, 9 September 2015. Web.

[64] Kim, Yonho. "Cell Phones in North Korea: Has North Korea Entered the Telecommunications Revolution?" Washington, DC: *US-Korea Institute*, 2014. Web.

[65] Williams, Martyn. "How a Telecom Investment in North Korea Went Horribly Wrong." *PC World*, 17 November 2015. Web.

international numbers (tier two).[66] Subscribers can contact numbers within the same tier but not those outside of it. As of February 2013, foreign subscribers have also been able to connect to the internet. In 2014, Koryolink provided access to a limited number of websites on *Kwangmyong*.[67] In addition to the regular mobile network, there is a separate network that is reserved for the elites and that uses unique hardware and software to secure communications. This separate network (isolated from both local and foreign subscribers) was required because export restrictions prevented the incorporation of modern encryption technology.

For locals wanting to communicate with the outside world (for example, smugglers or those with defector family members in China or South Korea), Chinese mobile networks can be accessed along some of the border areas between North Korea and China.[68] It has been reported, however, that the North Korean government has been jamming mobile signals to prevent this.[69]

In addition to the conventional networks, such as the internet, *Kwangmyong*, and mobile, there is a human network of illicit storage mediums that are smuggled into and out of North Korea. These storage mediums include CDs/DVDs, USB flash drives, and SD cards that are carried in person, dropped by balloon, or transported via drone. The content is usually news and entertainment media from South Korea that offers a rare glimpse of the outside world. Because personal computers are expensive and difficult to

[66] O'Carroll, Chad. "Inside North Korea's Cell Network: Ex-Koryolink Technical Director Reveals All." *NK News*, 20 August 2015. Web.
[67] Talmadge, Eric. "Online Shopping Has Arrived in North Korea." *Business Insider*, 6 May 2015. Web.
[68] Kim, Yonho. "Cell Phones in North Korea: Has North Korea Entered the Telecommunications Revolution?" Washington, DC: *US-Korea Institute*, 2014. Web.
[69] Ibid.

acquire for many in North Korea, the content is accessed using a smartphone with a USB port or a device called a *notel*, a portable CD/DVD player that also includes a USB port and SD slot, as well as television and radio tuners. These low-cost and low-power devices, which are manufactured in China, were initially smuggled in and distributed illegally.[70] However, demand and usage became so pervasive that the North Korean government capitulated and legalized the devices in 2015, although it did require all to be purchased at state-owned stores and registered with local government authorities. Television and radio tuners on the devices were also fixed to government stations.

Military Cyber Resources and Operations

North Korea has made consistent and dramatic efforts to enhance its military cyber infrastructure. In 2014, it completed the installation of a dedicated high-speed fiber-optic military intranet referred to as *Kumpyol* (Gold Star) that allows for integrated command and control between strategic, operational, and tactical units.[71] According to the most recent white paper from the Ministry of National Defense, North Korea has also doubled its cyberwarfare personnel over four years from an estimated 3,000 in 2012 to 6,800 in 2016[72] and has conducted operations against South Korea to disrupt civilian and military activities and to target critical infrastructure.[73] It is alleged that 1,100 of these personnel conduct covert cyberspace operations from locations abroad, which offer

[70] Gallagher, Sean. "A $50 Device Is Breaking North Korean Government's Grip on Media." *Ars Technica*, 27 March 2015. Web.

[71] "'북한군 인트라넷에 광케이블망 설치'<RFA>." *Yonhap News*, 23 April 2011. Web.

[72] Ministry of National Defense. *2016 Defense White Paper*, 2016. Web.

[73] Park, Donghui. "North Korea Cyber Attacks: A New Asymmetrical Military Strategy." *University of Washington*, 28 June 2016. Web.

increased internet capacity and increased operational anonymity.[74] The personnel operate under the cover of legitimate North Korean IT firms abroad or joint ventures in China and Southeast Asia.

The Reconnaissance General Bureau (RGB) of the KPAF is responsible for intelligence and covert operations. It is comprised of six bureaus with compartmentalized functions, including operations, reconnaissance, cyber and technology, intelligence abroad, inter-Korean issues, and service support.[75] Around 2009 and 2010, units associated with cyberspace operations that were scattered among the Korean Worker's Party and the Ministry of People's Armed Forces were consolidated under the RGB. North Korea has one confirmed and two suspected cyber units that are subordinate administratively to the RGB but that report directly to the National Defense Commission.[76] These units are outlined in Figure 3.[77]

Bureau 121, the bureau for cyber and technology, is the most important and most infamous unit. It is responsible for both offensive and defensive cyberspace operations, including CNA, CND, and CNE, and has been implicated in multiple high-profile cyberspace operations against South Korea and the United States.[78]

[74] 김봉기. "'北, 최근 청와대·국회 해킹 시도… 국감 자료 빼내가'." *Chosun Ilbo*, 21 October 2015. Web.

[75] Cordesman, Anthony. "Korean Peninsula Military Modernization Trends." Washington, DC: *Center for Strategic and International Studies*, 20 September 2016. Web.

[76] As in any military, it is possible that the designations for and responsibilities of these units have changed over time. This is further complicated by North Korea's secretive nature and the use of varying translations.

[77] This figure was created based on information in:
Jun, Jenny, Scott LaFoy, and Ethan Sohn. "North Korea's Cyber Operations: Strategy and Responses." Washington, DC: *Center for Strategic and International Studies*, 2015. Web.

[78] Jun, Jenny, Scott LaFoy, and Ethan Sohn. "North Korea's Cyber Operations: Strategy and Responses." Washington, DC: *Center for Strategic and International Studies*, 2015. Web.

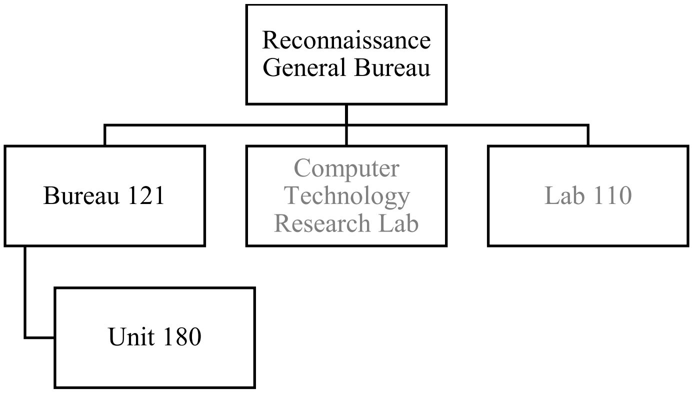
Reconnaissance General Bureau
Bureau 121
Computer Technology Research Lab
Lab 110
Unit 180

Figure 3. Cyber Units under the Reconnaissance General Bureau. Units in grey are unconfirmed or suspected of having been merged or disbanded.

Its alternative designation, the Cyber Warfare Guidance Bureau under the Electronic Reconnaissance Bureau, denotes that it is possibly overseen personally by Kim Jong-un, which is an indication of its strategic significance.[79] According to a defector who studied with eventual operators for Bureau 121 at Kim Il Military University, [80] the unit is comprised of around 1,800 personnel and has teams inside and outside of North Korea.[81]

Mention of Unit 180 emerged in 2017 following a series of ransomware operations around the world. According to a defector, a former professor at Kim Il Military University, Unit 180 is responsible for cyberspace operations aimed at acquiring money for the regime, oftentimes by breaching the computers and networks of financial institutions and transferring money out of accounts.[82] Although its position within the

[79] Ibid.

[80] The official designation of this institution is Unit 144 of the KPAF. However, it has undergone several name changes. It was founded in 1986 as the Command Automation College and later renamed Mirim University and again in 2000 the Kim Il Military University.

[81] Park, Ju-min and James Pearson. "In North Korea, Hackers Are a Handpicked, Pampered Elite." *Reuters*, 5 December 2014. Web.

[82] Park, Ju-min and James Pearson. "North Korea's Unit 180, The Cyber Warfare Cell That Worries the West." *Reuters*, 20 May 2017. Web.

structure of the RGB was not specified, the designation and mission most likely places it subordinate to Bureau 121.

Other suspected units under the RGB include the Computer Technology Research Lab and Lab 110. Although little information is available, it is possible that these units are responsible for the development of exploitation tools and techniques. It is also possible that Computer Technology Research Lab and Lab 110 have been merged with other units or disbanded.[83]

In addition to the RGB, there are two cyber units subordinate to the GSD of the KPA. These units are outlined in Figure 4.[84] Although, again, little information is available, it is possible that the Operations Bureau is responsible for joint cyber mission coordination and integration, as well as the planning and disseminating of cyber strategy. According to a report from the Korean Institute for National Unification, the Command Automation Bureau conducts computer network operations (CNO) and is responsible for developing malware and searching for exploits.[85] It has from 50 to 60 personnel and includes Unit 31 (malware development), Unit 32 (military software development), and Unit 56 (command and control software development).

Although the Enemy Collapse and Sabotage Bureau conducts operations in cyberspace, its mission is characterized as being more information warfare than cyberwarfare (CNA or CNE). It was also reported in 2016 that pursuant to a recent

[83] Murauskaite, Egle. "North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment." *38 North*, 12 September 2014. Web.

[84] This figure was created based on information in:
Jun, Jenny, Scott LaFoy, and Ethan Sohn. "North Korea's Cyber Operations: Strategy and Responses." Washington, DC: *Center for Strategic and International Studies*, 2015. Web.

[85] Jun, Jenny, Scott LaFoy, and Ethan Sohn. "North Korea's Cyber Operations: Strategy and Responses." Washington, DC: *Center for Strategic and International Studies*, 2015. Web.

restructuring, the GSD has added a Command Information Bureau and implemented an integrated tactical command and control system to enhance its command, control, communication, computer, and intelligence capabilities.[86]

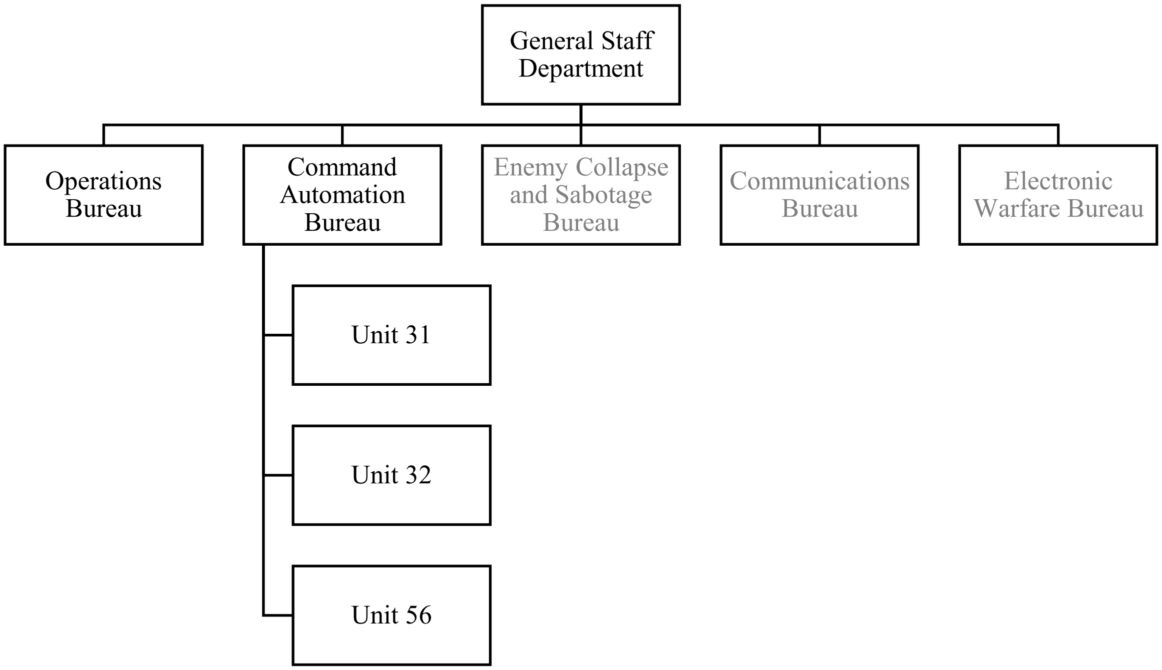
General Staff Department
Operations Bureau
Command Automation Bureau
Enemy Collapse and Sabotage Bureau
Communications Bureau
Electronic Warfare Bureau
Unit 31
Unit 32
Unit 56

Figure 4. Cyber Units under the General Staff Department. Units in grey are assumed to have missions outside the scope of cyberwarfare.

Cyber Strategy

Kim Jong-un once stated that "cyberwarfare is all-purpose sword that can guarantee ruthless strikes of the [Korea People's Armed Forces] along with nuclear weapons and missiles."[87] North Korea's cyberspace strategy reflects its overall offensive

[86] Ministry of National Defense. *2016 Defense White Paper*, 2016. Web.

[87] Yang, Jeong-yoon, So-jeong Kim, and Il-seok Oh. "Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities." *International Workshop on Information Security Applications 2016*. 30 March 2017. Web.

posture and emphasis on asymmetrical and irregular warfare, with cyberspace operations considered “a low-cost, low-risk” means of targeting the vulnerabilities of other states that rely on cyberspace for civilian and military activities.[88] Cyberspace operations offer North Korea the potential to damage or destroy the command, control, and communication networks of South Korea and the United States, neutralizing the benefits that these networks offer without the costs and risks associated with physical operations. North Korea also uses cyberspace to exploit the benefits of the treasure trove of open source scientific and technical intelligence that can be used to support domestic research and development efforts without the risk of defection or influence inherent with sending researchers abroad.[89]

Although the figures are varied, it is estimated that North Korea has spent between $1.1 billion and $3.2 billion overall on nuclear weapons development.[90] This amount is far greater than the cost of training and equipping even 6,800 personnel to conduct cyberspace operations. There are also the high risks of escalation and loss inherent to physical operations. For example, on 23 November 2010, North Korea fired over a hundred artillery shells and rockets at Yeonpyeong Island in South Korea in response to a South Korean naval exercise. South Korea retaliated by shelling North Korean artillery positions. By the end of the conflict, there were 25 South Korean civilian and military casualties and at least 5 North Korean military casualties.

[88] Jun, Jenny, Scott LaFoy, and Ethan Sohn. “North Korea’s Cyber Operations: Strategy and Responses.” Washington, DC: *Center for Strategic and International Studies*, 2015. Web.
[89] Mercado, Stephen. “Hermit Surfers of Pyongyang.” *Studies in Intelligence* 48.1 (2007): N.P. Web.
[90] Park, Ju-min and James Pearson. “North Korea Overcomes Poverty, Sanctions with Cut-Price Nukes.” *Reuters*, 11 January 2016. Web.

Its cyberspace strategy also represents a means of financial income. North Korea has for decades engaged in illicit activities to finance the regime and to overcome economic sanctions. These activities have included the smuggling of goods, the manufacturing of drugs, and the counterfeiting of goods and currency.[91] Often done under the guise of legitimate companies and the protection of diplomatic immunity, countries such as China, Malaysia, and Singapore have been referenced as nodes in the networks of illicit activities by North Korea.[92] Increasing the enforcement of sanctions in these countries also increases the possibility that North Korea will turn to cybercrime to support itself. North Korea has in fact been implicated in the high-profile cybertheft of $81 million from the Bangladesh Bank in February 2016 and cyberextortion of around $55,000 through the ransomware operation WannaCry in May 2017.[93]

Assessment of Cyberpower

Clark approaches cyberpower from a military perspective and defines it as the ability to conduct successful cyberwarfare. [94] Although the author identifies three factors that comprise cyberpower (cyber offense, cyber defense, and cyber dependence), the method for assigning the values is never made explicit. The assessment, which is depicted in Table 3, reveals that North Korea ranks as the highest for cyberpower (despite its low offensive ability) due to its high defensive ability and low dependence.

[91] Greitens, Sheena. "Illicit: North Korea's Evolving Operations to Earn Hard Currency." Washington, DC: *Committee for Human Rights in North Korea*, 2014. Web.

[92] Berger, Andrea. "A Familiar Story: The New UN Report on North Korean Sanctions Implementation." *38 North*, 16 March 2017. Web.

[93] Fung, Brian. "What You Need to Know About Bitcoin after the WannaCry Ransomware Attack." *The Washington Post*, 15 May 2017. Web.

[94] Clarke, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do about It*. New York, NY: Harpers Collins Publishers, 2010. Print.

Table 3. Cyberpower and Ranking According to Clark. Nations are listed from highest to lowest.

NATION	OFFENSE	DEFENSE	DEPENDENCE	TOTAL
North Korea	2	9	7	18
Russia	7	5	4	16
China	5	4	6	15
United States	8	2	1	11

Valeriano and Maness maintain the same approach as Clark but assign different values as depicted in Table 4. [95] In this alternate assessment, there is a notable difference in the value assigned to defensive ability for North Korea, with North Korea also ranking lowest for cyberpower. Although, again, the method for assigning values is not made explicit, these assessments do reveal the complicated nature of cyberspace and some of the factors that are relevant in evaluating cyberpower.

Table 4. Cyberpower and Ranking According to Valeriano and Maness. Nations are listed from highest to lowest.

NATION	OFFENSE	DEFENSE	DEPENDENCE	TOTAL
Russia	7	8	3	18
China	8	5	4	17
United States	10	5	2	17
North Korea	3	2	9	14

[95] Valeriano, Brandon and Ryan Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. Print.

The Australian Strategic Policy Institute approaches cyberpower from a development perspective, which it refers to as cyber maturity.[96] It defines cyber maturity as the presence and operation of effective physical and institutional cyber infrastructure and identifies five categories.

1. Governance: Ability and intent to address cyber issues through legislation and regulation domestically and to engage internationally. Includes the factors of (1a) organizational structure, (1b) legislation/regulation, and (1c) international engagement.

2. Financial cybercrime enforcement: Capacity to address financial cybercrime. Includes the factor of (2) financial cybercrime.

3. Military application: Capability and intent regarding the military use of cyberspace. Includes the factor of (3) military application.

4. Digital economy and business: Understanding of the importance of cyberspace on economy and business. Includes the factors of (4a) engagement between government and business and (4b) digital economy.

5. Social engagement: Public awareness of and engagement on cyber issues. Includes the factors of (5a) public awareness, (5b) fixed broadband penetration, and (5c) mobile broadband penetration.

The cyber maturity rankings for China, North Korea, South Korea, and the United States are depicted in Table 5.

Table 5. Cyberpower and Ranking According to Australian Strategic Policy Institute.

RANK	NATION	SCORE
1	United States	88.1
2	South Korea	83.6
8	China	63
22	North Korea	16.7

[96] Australian Strategic Policy Institute. "North Korea." *Cyber Maturity in the Asia-Pacific Region 2016*, 2016. Web.

Trusting these assessments, although North Korea does not have the same offensive cyber ability as the more powerful nations of the United States, Russia, and China and lags far behind in cyber development, it does have a considerable defensive cyber ability and negligible cyber dependence. This is due to its aforementioned isolation and almost absolute control over all forms of information technologies and communications (including computers, mobile phones, the internet, and all other networks). North Korea is able to easily and effectively sever its connection to cyberspace if threatened, and the operation of its infrastructure has little reliance on cyberspace.

CHAPTER V: ANALYSIS OF CYBERSPACE CAPABILITIES AND INTENT

In the DCIDD, from 2008 to 2011, Valeriano and Maness identified three North Korean cyberspace operations against the United States, ten against South Korea, and one against Japan. Of these, information on eight operations could not be found at the source cited or in any other source. These operations have therefore been excluded from the analysis. The authors also identified one South Korean cyberspace operation against North Korea in 2011. However, again, information was unable to be found, and this operation has been excluded. The resulting timelines cover all other cyberspace operations both by North Korea and against North Korea from July 2009 to February 2017.

There are a few notes regarding the timelines:

- Dates provided indicate the month and year that an operation occurred or a series of operations ended for offensive cyberspace operations and the month and year that either was discovered for cyber exploitation or cyber espionage.

- Events listed are those for which there was an analysis or investigation by credible authorities, such as government organizations or network security companies.

- Technical details are omitted unless pertinent.

- It is expected that sensitive information that possibly reveals sources and methods has been withheld by intelligence organizations.

- In addition to the assessments unique to this thesis, operations from July 2009 to April 2011 include the assessments from the DCIDD for reference only. Because the discrepancies are minor, any discussion is considered beyond the scope the thesis.

- An ‘X’ in a table indicates that there is not enough information to assign a value for that factor.

According to Valeriano and Maness, there is a tendency in the international system for ‘cyber hype’ (otherwise a form of ‘threat inflation’).[97] Media headlines and articles often refer to CNA and CNE operations as a generalized “cyberattack” or “hack,” regardless of nuances in the technical sophistication of the threat actor, the target vulnerabilities, operational goals, and the degree to which any of this can be confirmed.[98] Many events or series of events are characterized as a sophisticated threat actor executing a successful “cyberattack” or “hack” against a vulnerable or fragile target. The danger of this is not only that perceptions of the threat and interactions in the international system will be misguided, but also that nations will waste human, financial, and technical resources in addressing the wrong threat and therefore remain vulnerable.

The threat from North Korea’s cyberspace operations has already been analyzed in regard to its resources and strategy. This can be thought of as its potential threat. The requirement now is a detailed analysis of the actual threat that cuts through the threat inflation. That is, how North Korea’s cyberspace resources and strategy are realized for use in operations and what effect this has on its targets. As noted by the Korea Economic Institute of America:[99]

> In cyberspace, many of the North Korean capabilities and intentions may be revealed only after a real attack takes place in the virtual domain,
> for which they will either claim responsibility or which will be undeniably traced back to the North Korean government or the non-state actors commissioned or controlled by [North Korea].

[97] Jun, Jenny, Scott LaFoy, and Ethan Sohn. “What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?” Washington, DC: *Center for Strategic and International Studies*, 12 December 2014. Web.

[98] In an attempt to remain neutral in characterization, the term ‘threat actor’ is used instead of ‘attacker’ or ‘hacker’.

[99] Mansourov, Alexandre. “North Korea’s Cyber Warfare and Challenges for the US-ROK Alliance.” Washington, DC: *Korea Economic Institute of America*, 2 December 2014. Web.

Cyberspace Operations by North Korea

July 2009. A series of DDOS operations on July 4, July 7, and July 9 disrupted access to the websites of 27 financial institutions, government organizations, and media corporations in South Korea and the United States.[100] According to Symantec, the computers used in the operations were infected with a piece of malware referred to as TROJAN.DOZER and propagated through email using varies worms.[101] On July 10, a time bomb contained in the malware destroyed data in the MBR and partition table of the infected computers and overwrote the hard drive with the string "Memory of Independence Day". Network security experts noted that the malware was relatively unsophisticated and that the operations were unable to generate enough requests for data to cause more than minor disruptions.[102] The NIS reported that the operations were likely planned and executed by a specific group or state and an unconfirmed statement implicated North Korea.[103]

Based on this information, the operation against South Korea used the method of a worm (4.3), had an effect on critical national infrastructure or military (2), was an individual cyber event that was offensive (3), targeted government military entities (3), and had the goal of disrupting target activity (1). The operation against the United States used the method of denial of service (2), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted government non-military entities (2), and

[100] Choe, Sang-hun, and John Markoff "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *The New York Times*, 8 July 2009. Web.

[101] Symantec Security Response. "Are the 2011 and 2013 South Korean Cyberattacks Related? Blog post. *Symantec*, 29 March 2013. Web.

[102] Choe, Sang-hun, and John Markoff "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea." *The New York Times*, 8 July 2009. Web.

[103] Ibid.

had the goal of disrupting target activity (1). This is summarized in Table 6 at the end of the section, with the data from the DCIDD recreated in Table 7 for comparison.

January 2011. A DDOS operation in January 2011 disrupted access to the website of an internet forum in South Korea.[104] The users of this internet forum had claimed responsibility for gaining access to the official Twitter and YouTube accounts of the North Korean government and posting derogatory comments and propaganda videos. This was done on January 8 to coincide with the Kim Jong-un's birthday. It was suspected that the DDOS operation was retaliation by North Korea.

Based on this information, the operation against South Korea used the method of a denial of service (2), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted a private entity (1), and had the goal of disrupting target activity (1). This is summarized in Table 6 at the end of the section, with the data from the DCIDD recreated in Table 7 for comparison.

March 2011. A DDOS operation on March 4 disrupted access to the websites of 40 financial institutions and government organizations in South Korea, as well to the websites of Kunsan Air Base and United States Forces Korea.[105] According to Symantec, the computers used in the operation were infected with a piece of malware referred to as TROJAN.KOREDOS that was used for the DDOS operation and to destroy data in the master boot record, as well as a piece of malware referred to as BACKDOOR.PRIOXER

[104] McCurry, Justin. "Korean Hackers Mount Cyber Skirmishes in Propaganda War." *The Guardian*, 11 January 2011. Web.

[105] "South Korea Government Websites Targeted in Cyber Attack." *The Guardian*, 4 March 2011. Web.

that was used to gain remote-access.[106] BACKDOOR.PRIOXER was considered relatively sophisticated due to its discrete method of infection. However, it was uncertain if this was intentional. A report from McAfee noted that the sophistication for the encryption of the malware and command and control of the operation was excessive in comparison to the limited execution and effect of the attack, which was designed to last no more than ten days. [107] It was suspected that the operation was intended to test and observe the time required for the operation to be discovered, analyzed, and mitigated.

Based on this information, the operation against South Korea used the method of a denial of service (2), had an effect on critical national infrastructure or military (2), was an individual cyber event that was a nuisance (1), targeted government non-military entities (2), and had the goal of disrupting target activity (1). The operation against the United States used the method of denial of service (2), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted government military entities (3), and had the goal of disrupting target activity (1). This is summarized in Table 6 at the end of the section, with the data from the DCIDD recreated in Table 7 for comparison.

April 2011. An offensive cyberspace operation on April 12 destroyed system data and disrupted access to the internal network at Nonghyup Bank in South Korea, lasting three days and affecting 30 million customers.[108] According to the results of an investigation by the Seoul Central District Prosecutor's Office, backdoor malware was

[106] Symantec Security Response. "Are the 2011 and 2013 South Korean Cyberattacks Related? Blog post. *Symantec*, 29 March 2013. Web.
[107] McAfee. *Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea*, July 2011. Web.
[108] Rahn, Kim. "NK Launched Cyber Attack on Nonghyup." *The Korea Times*, 3 May 2011. Web.

introduced to the network in September 2010 via the infected laptop of a network security contractor, which was among 201 computers that had been infected during an undisclosed offensive cyberspace operation against financial institutions and government organizations in July 2009. The malware allowed the perpetrator to exfiltrate information (including internet protocols and system passwords) and install malicious code throughout the network over a period of several months. After the malicious code was installed, a remote deletion command was executed, destroying data on 273 of 587 servers. The perpetrator then confirmed the success of the operation and destroyed evidence from both the laptop and the network. Due to the sophistication of the attack, it was suspected that considerable human, financial, and technical resources were required. The operation used malware that was similar to the July 2009 attack, as well as an IP address that was used for a command and control server from the same operation. Normal operations did not resume for a few weeks.[109]

Based on this information, the operation against South Korea used the method of a virus (4.2), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted private entities (1), and had the goal of disrupting target activity (1). This is summarized in Table 6 at the end of the section, with the data from the DCIDD recreated in Table 7 for comparison.

March 2013 (DarkSeoul/Operation Troy). An offensive cyberspace operation on March 20 destroyed data at three media corporations (MBC, KBS, and YTN) and

[109] Harlan, Chico and Ellen Nakashima. "Suspected North Korean Cyber Attack on a Bank Raises Fears for S. Korea, Allies." *The Washington Post*, 29 August 2011. Web.

three financial institutions (Jeju Bank, Nonghyup Bank, Shinhan Bank) in South Korea.[110] The operation used a piece of malware referred to as TROJAN.JOKRA that was used to gain remote-access and delete the MBR and content of any system or network hard drive.[111] The initial infection occurred through a spearphishing email weeks before the operation and was further propagated via email and patch management.[112] The operation occurred days after North Korea promised retribution for an alleged offensive cyberspace operation against it by the United States and South Korea. Normal operations resumed within a few hours. This operation has sometimes been referred to as DarkSeoul.

According to a report from McAfee, this operation was not an isolated event, but rather the culmination of a cyber espionage operation referred to as Operation Troy.[113] Operation Troy represented an APT that had specific targets only in South Korea. The various operations, which included at least those from July 2009, March 2011, and April 2011, were likely intended to collect intelligence regarding the targets to prepare for future offensive cyberspace operations, such as the March 20 operation. Evidence for the suspected connection included similarities in the targets, as well as the TTPs of the operations. Operation Troy and subsequent operations suspected of being related to it have been attributed to a group later referred to as the DarkSeoul Gang, named after the malware and operation that brought it to light.

[110] Choe, Sang-hun. “Computer Networks in South Korea Are Paralyzed in Cyberattacks.” *The New York Times*, 20 March 2013. Web.

[111] Symantec Security Response. “South Korean Banks and Broadcasting Organizations Suffer Major Damage from Cyberattack.” Blog post. *Symantec*, 20 March 2013. Web.

[112] Spearphishing is a more targeted form phishing.

[113] McAfee. *Dissecting Operation Troy: Cyberespionage in South Korea*, by Ryan Sherstobitoff, Itai Liba, and James Walter, 8 July 2013. Web.

Based on this information, the operation against South Korea used the method of a worm (4.3) and was also an APT (5), had an effect on critical national infrastructure or military (2), was a series of cyber events that were a nuisance and offensive (5), targeted private entities (1), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

June 2013. A series of DDOS operations on June 25 (the anniversary of the start of the Korean War) disrupted access to the websites of government organizations in North Korea and South Korea. [114] The homepage of the Blue House in South Korea was also defaced with a message praising Kim Jong-un as the leader of a unified Korea. It was uncertain if both countries had attacked each other or if another actor had executed the attacks. However, a blog post by Symantec, attributed at least the operation on South Korea to the DarkSeoul Gang, noting several similarities in the targets and TTPs of this operation with those from July 2009, March 2011, and March 2013 as evidence:[115] Eric Chien, a technical director with Symantec, suspected that the group behind the operation was comprised of between 10 and 50 members.[116]

- Use of multistaged and coordinated operations against high-profile targets in South Korea
- Use of destructive payloads, such as malicious code for hard drive wipes and DDOS operations, configured to trigger on significant dates
- Overwriting hard drive sectors with strings that have political themes

[114] Choe, Sang-hun. "Cyberattacks Disrupt Leading Korean Sites." *The New York Times*. 26 June 2013. Web.

[115] Symantec Security Response. "Four Years of DarkSeoul Cyberattacks against South Korea Continue on Anniversary of Korean War." Blog post. *Symantec*, 26 June 2013. Web.

[116] Finkle, Jim. "Four-Year Hacking Spree in South Korea Blamed on 'Dark Seoul Gang'." *Reuters*, 26 June 2013. Web.

- Use of patching mechanisms from legitimate third-parties to propagate across internal networks
- Use of specific encryption and obfuscation methods
- Use of webmail servers from specific third-parties to store files
- Use of similar command and control structures

An official from the Ministry of Science, ICT, and Future Planning also noted that an analysis of the malicious code and affected systems revealed evidence of an IP address from North Korea, as well as similarities in the TTPs.

Based on this information, the operation against South Korea used the method of denial of service (2), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted government non-military entities (2), and had the goal of disrupting target activity (1). This is summarized in Table 6 at the end of the section.

September 2013 (Operation Kimsuky). Kaspersky Lab reported on 11 September that it had uncovered a cyber espionage operation from at least April to monitor activity and exfiltration information from eleven entities in South Korea, including government organizations, private research institutes, and commercial defense firms.[117] Notable targets were the Ministry of Unification, Korean Institute of Defense Analysis, and Hyundai Merchant Marine. The operation used a piece of malware called TROJAN.KIMSUKY that was likely propagated through a spearphishing email.[118] The malware included a payload consisting of a keystroke logger and malicious code

[117] Tarakanov, Dmitry. “The ‘Kimsuky’ Operation: A North Korean APT?” Blog post. *SecureList*, 11 September 2013. Web.

[118] Ibid.

designed to collect directory listings and '.hwp' documents, as well as provide remote access. Along with targets limited to only South Korea, the report noted that there were Korean language characters in the malware and that the IP addresses associated with the operation originated in China near the border with North Korea. This operation has been characterized as an APT and referred to Operation Kimsuky.[119]

Based on this information, the operation against South Korea used the method of a keystroke logger (4.5) and was also an APT (5), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted government non-military entities (2), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

August 2014. According to a statement from a national assembly member from the Land, Infrastructure, and Transportation Committee made on 5 October 2015, citing the results of a report from the NIS, North Korea was suspected of conducting a cyber espionage operation against the Seoul Metro from at least March to August 2014 that exfiltrated information.[120] It was confirmed in the report that two servers in charge of program installation and patch management had been breached, allowing unauthorized access to at least 213 computers, of which 58 had been infected with malicious code.[121] The Seoul Metro discovered the breach in July, after which it shut down the servers and notified government authorities. The operation exfiltrated several documents but did not

[119] Halliday, Josh and Samuel Gibbs. "North Korean Hackers Suspected of Cyber-Espionage Attack on South." *The Guardian*, 11 September 2013. Web.
[120] 최종석. "北, 서울메트로 서버 5 개월 장악했다." *Chosun Ilbo*, 5 October 2015. Web.
[121] Ibid.

gain access to central computers or networks with direct operational control over the metro system. Due to the absence of a log management system, the NIS was able to secure logs from no earlier than March. Although it was unable to determine the date or method of initial infiltration, it was suspected to have been before March. This operation was characterized as an APT.

Based on this information, the operation against South Korea used the method of intrusion (3) and was also an APT (5), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted a private entity (1), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

November 2014. An offensive cyberspace operation on 24 November against Sony Pictures Entertainment in the United States disrupted computer and network access, exfiltrated sensitive information, and destroyed data on 3,262 of its 6,797 computers and 837 of its 1,555 servers.[122] The operation used a worm that functioned as a dropper to deliver a payload of an additional five pieces of malware to include a listener, backdoors, and wipers.[123] The group that claimed to be responsible called itself the Guardians of Peace and stated that it had conducted the operation response to the planned release of *The Interview*, a comedy movie that depicts the assassination of the supreme leader of North Korea. The group released some of the sensitive information, which included embarrassing correspondence and confidential personal information of employees, and

[122] Elkind, Peter. "Sony Pictures: Inside the Hack of the Century." *Fortune*, 25 June 2015. Web.

[123] Goodin,Dan. "Malware Believed to Hit Sony Studio Contained a Cocktail of Badness." *Ars Technica*, 19 December 2014. Web.

also threatened the release of additional information if the movie was released. [124] The Federal Bureau of Investigation (FBI) conducted an investigation and concluded that North Korea was responsible for the attack. This conclusion was based on several pieces of evidence:

- Technical aspects of the malicious code used were similar to malicious code confirmed to have been developed by North Korea.
- The source of the operation was traced to several IP addresses associated with North Korean entities in China.
- The means and methods of the infiltration were similar to those used against South Korea in March 2013.[125]

Some doubted the attribution of the operation to North Korea, noting that Sony Pictures Entertainment was notorious for its poor network security and was the victim of 24 previous documented incidents.[126] However, Director of the FBI James Comey stated that "I have very high confidence about this attribution, as does the entire intelligence community."[127]

Based on this information, the operation against the United States used the method of a worm (4.3), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted a private entity (1), and had the goal of disrupting target activity (1). This is summarized in Table 6 at the end of the section.

[124] Grisham, Lori. "Timeline: North Korea and the Sony Pictures Hack." *USA Today*, 5 January 2015. Web.
[125] Department of Justice, Federal Bureau of Investigation. *Update on Sony Investigation*, 19 December 2014. Web.
[126] Szoldra, Paul. "A Hacker Explains Why You Shouldn't Believe North Korea Was behind The Massive Sony Hack." *Business Insider*, 10 June 2016. Web.
[127] Comey, James. "Addressing the Cyber Security Threat." *International Conference on Cyber Security*. 7 January 2015. Web.

December 2014. Korea Hydro and Nuclear Power, a subsidiary of the state-owned Korea Electric Power Corporation in South Korea, reported on 22 December that a cyber espionage operation exfiltrated sensitive information from the Gori and Wolseong nuclear power plants, including confidential personal information of employees, designs and manuals for at least two reactors, and estimates of radiation exposure among local residents. A user on Twitter who alleged to be from antinuclear group in Hawaii claimed responsibility for the operation and released some of the information. The user also threatened to release additional information if three of the reactors were not shut down by 25 December. After the reactors were not shut down, the user did release additional information and then demanded money, claiming that other countries had offered to purchase the designs and manuals for the reactors. The results of an investigation by the Seoul Central District Prosecutor's Office implicated North Korea in the operation after discovering that the malware used was similar in composition and function to TROJAN.KIMSUKY and tracing the IP addresses associated with the operation to a city in China near the border with North Korea.[128]

Based on this information, the operation against South Korea used the method of intrusion (3), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted a government non-military entity (2), and had the goal of acquiring target information and data (1). This is summarized in Table 6 at the end of the section.

[128] Park, Ju-min and Mee-young Cho. "South Korea Blames North Korea for December Hack on Nuclear Operator." *Reuters*, 17 March 2015. Web.

October 2015. The NIS reported on 20 October that throughout September and October, a cyber espionage operation had exfiltrated government audit information from the National Assembly and had also targeted the Blue House, Ministry of National Defense, and Ministry of Unification.[129] The computers of three national assembly members and eleven aides. The operation was attributed to North Korea, noting similarities in the targets from previous operations.

Based on this information, the operation against South Korea used the method of intrusion (3), had a minimal effect (1), was an individual cyber event that was a nuisance (1), targeted a government non-military entity (2), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

February 2016. The National Police Agency reported that a cyber espionage operation by North Korea had infiltrated 140,000 computers at 160 government organizations.[130] The operation, which started around 20 months earlier in 2014 and was discovered in February 2016, exfiltrated 42,000 documents, including 40,000 defense-related documents regarding research and development and manufacturing.[131] According to the report, the operators breached a software management system used by commercial firms to install, delete, and update software on all devices connected to the network.[132] This allowed malicious code that exfiltrated information to be installed. An IP addressed

[129] 김봉기. "'北, 최근 청와대·국회 해킹 시도... 국감 자료 빼내가'." *Chosun Ilbo*, 21 October 2015. Web.

[130] Byrne, Leo. "Seoul Says North Korea Carried Out Large-Scale Hack." *NK News*, 14 June 2016. Web.

[131] Kim, Jack. "North Korea Mounts Long-Running Hack of South Korea Computers, Says Seoul." *Reuters*, 12 June 2016. Web.

[132] "북한, 대규모 사이버 공격 준비 확인... 대기업 문서 4 만여건 해킹." *Yonhap News*, 13 June 2016. Web.

used in the operation was traced to North Korea and was identical to an address used in the March 2016 offensive cyberspace operation. Authorities suspected that the operation was possibly preparation for a future offensive cyberspace operation.[133]

Based on this information, the operation against South Korea used the method of intrusion (3) and was also an APT (5), had an effect on critical national infrastructure or military (2), was a series of cyber events that were a nuisance (1), targeted government (non-military and military) entities (6), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

March 2016. The NIS reported on 7 March that North Korea was suspected in a series of cyberspace operations in South Korea, including one successful cyber espionage operation, two successful cyber exploitation operations, and one attempted operation.[134] The cyber espionage operation targeted and exfiltrated information from tens of senior government officials at 14 government organizations via phishing text messages that were sent to smartphones from February to March.[135] The text messages directed users to domains that downloaded and installed malicious code that granted remote-access to mobile devices. From those infected, operators were able to exfiltrate voice communications and text messages, as well as contact information. The cyber exploitation operations were both discovered in February.[136] The first breached the

[133] Ibid.

[134] Choe Sang-hun and David Sanger. "South Korea Accuses North of Hacking Senior Officials' Phone." *The New York Times*, 9 March 2016. Web.

[135] "北, 정부 주요인사 스마트폰 해킹…철도기관도 사이버공격." *Yonhap News*, 7 March 2016. Web.

[136] 손덕호. "국정원 '北, 주요인사 수십명 스마트폰 해킹해 문자·통화내용 유출'." *Chosun Ilbo*, 8 March 2016. Web.

internal network of a security software firm that provided protection for internet financial services and card transactions for millions of users. The second digital certificate of a firm that also provided security software for internet financial services.

The NIS also reported that spearphishing emails were sent to the email accounts of railway employees at two regional operators from January to February. [137] The targeted accounts were closed as soon as the phishing emails were reported. It was suspected yet unconfirmed that the operation was an attempt to access the railway transport control system. Although specific evidence was not provided, the NIS claimed that North Korea was behind all the operations, which was possibly preparation for a future offensive cyberspace operation.

Based on this information, the operation against South Korea used the method of intrusion (3), had a minimal effect (1), was a series of cyber events that were a nuisance (1), targeted private and government non-military entities (4), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

September 2016. A national assembly member from the National Defense Committee announced on 1 October that in September, malicious code from a cyber exploitation operation had been found on a server at the Cyber Command of the Ministry of National Defense (MND).[138] A subsequent report from the MND in December confirmed that the operation breached a routing sever and infected 3,200 computers with

[137] "North Korea Tried to Hack South's Railway System: Spy Agency." *Reuters*, 8 March 2016. Web.
[138] "S. Korea's Military Cyber Command Hacked Last Month." *Yonhap News*, 1 October 2016. Web.

malicious code, including 700 computers that were connected to the intranet.[139] Although the server was isolated to prevent further infection, the intranet was breached and sensitive defense-related documents exfiltrated.[140] The source of the operation was traced to several IP addresses in China associated with North Korea.

Based on this information, the operation against South Korea used the method of intrusion (3), had an effect on critical national infrastructure or military (1), was an individual cyber event that was a nuisance (1), targeted a government military entity (3), and had the goal of acquiring target information and data (2). This is summarized in Table 6 at the end of the section.

February 2017 (WannaCry). A cyber ransom operation emerged in February that targeted 104 organizations in 31 countries around the world and used ransomware to extort money from victims.[141] Reports from Kaspersky Lab and Symantec claimed that a group referred to as the Lazarus Group, with which North Korea is suspected of being associated, was behind the operation. The ransomware and the operation are oftentimes referred to as WannaCry. Based on an assessment that was not made public, the NSA had "moderate confidence" that the threat actor behind two versions of WannaCry, the Lazarus Group, were sponsored by the RGB.[142] Both the NSA and FBI also implicated North Korea in a similar operation involving the high-profile cyber theft of over $81

[139] "Suspected N.K. Attackers Hack into S. Korea's Cyber Command through Main Server." *Yonhap News*, 7 December 2016. Web.

[140] "N. Korea Likely Hacked S. Korea Cyber Command." *Yonhap News*, 5 December 2016. Web.

[141] Finkle, Jim. "North Korean Hacking Group Behind Recent Attacks on Banks: Symantec." *Reuters*, 15 March 2017. Web.

[142] Nakashima, Ellen. "The NSA Has Linked the WannaCry Computer Worm to North Korea." *The Washington Post*, 14 June 2017. Web.

million from the account of the Bangladesh Bank at the Federal Reserve Bank of New York in February 2016.[143]

According to Kaspersky Lab, the Lazarus Group started operations from at least 2009 and developed the malicious code used for the cyberspace operations in March 2013 and November 2014.[144] It was also associated with the development of a backdoor referred to as HANGMAN that was discovered in September 2015. HANGMAN used a zero-day exploit in '.hwp' documents[145] and contained code that connected to an IP address for a command and control server used in a variant of a backdoor referred to as MACKTRUCK. The code for HANGMAN was also similar to a backdoor called PEACHPIT. Both MACKTRUCK and PEACHPIT are associated with cyberspace operations by North Korea.[146] In addition, the report identified the possible existence of a unit within the Lazarus Group, referred to as Bluenoroff, that uses backdoors established through operations by the Lazarus Group for financial gain. Bluenoroff has targeted four types of organizations in nine countries. These have included (1) financial institutions, (2) casinos, (3) companies involved in the development of financial trade software, and (4) businesses associated with cryptocurrency.

According to Symantec, an initial variant of the ransomware that included as payload two pieces of malware from previous cyberspace operations appeared on 10

[143] "US May Accuse North Korea in Bangladesh Cyber Heist: WSJ." *Reuters*, 22 March 2017. Web.

[144] Kaspersky. *Lazarus under the Hood*, April 2017. Web.

[145] The '.hwp' file extension is for Hancom Hangul documents. Hancom is a South Korean software company, and Hangul a word processor with specialized Korean language support, which is used almost exclusively in South Korea.

[146] Jiang, Genwei and Josiah Kimble. "Hangul Word Processor (HWP) Zero-Day: Possible Ties to North Korean Threat Actors." *FireEye*, 7 September 2015. Web.

February. [147] BACKDOOR.DESTOVER was used in the offensive cyberspace operation against Sony Pictures Entertainment in November 2014, and TROJAN.VOLGMER was used in the cyber espionage operation against South Korea in June 2013. At least one organization in February and five organizations from March to April were infected with this variant of the ransomware. The malicious code was propagated within networks using stolen credentials. On 12 May, the operation expanded as a new variant of the ransomware appeared that incorporated a zero-day exploit.[148] This exploit allowed the ransomware to propagate at a much faster rate by eliminating the need to steal credentials. Similarities in TTPs, including shared network infrastructure and shared malicious code, were cited as evidence connecting this operation to others by the Lazarus Group.[149]

The reports from Kaspersky Lab and Symantec represented a coordinated industry-wide effort, called Operation Blockbuster and announced on 24 February 2016, to share intelligence and resources and assist commercial and government organizations in protecting against the Lazarus Group.[150] There were several conclusions made based on this effort:[151]

- The scale and sophistication of the operations is beyond that of criminal organizations and even beyond that of other APT groups.

[147] Symantec Security Response. "Attackers Target Dozens of Global Banks with New Malware." Blog post. *Symantec*, 12 February 2017. Web.
[148] This zero-day exploit, EternalBlue, was ironically an exploit among those allegedly exfiltrated from the NSA and offered for sale by a group called the Shadow Brokers on 14 April 2017.
[149] Symantec Security Response. "WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group." Blog post. *Symantec*, 22 May 2017. Web.
[150] Symantec Security Response. "Collaborative Operation Blockbuster Aims to Send Lazarus back to the Dead." Blog post. *Symantec*, 24 February 2016. Web.
[151] "Lazarus Under the Hood." Blog post. *SecureList*, 3 April 2017. Web.

- The human, financial, and technological resources required for this, as well as the operational errors, indicate that the Lazarus Group is comprised of several units.

- The Lazarus Group has been prolific in the development of malware, avoiding reuse and releasing newer and newer versions.

Based on this information, the operation against South Korea used the method of a worm (4.3) and was also an APT (5), had an effect on critical national infrastructure or military (2), and targeted private and government non-military entities. However, the interaction type and goal type are difficult to assess with this methodology because the series of events were not part of a cyberspace operation but rather part of a cybercrime. The assessment is included here because although the cybercrime is normally outside the scope of activities for a government, North Korea is an exception. This is summarized in Table 6.

Table 6. Assessment of Cyberspace Operations by North Korea.

DATE	NATION	METHOD	SEVERITY	INTERACTION	TARGET	GOAL
07/2009	South Korea	4.3	2	3	3	1
	United States	2	1	1	2	1
01/2011	South Korea	2	1	1	1	1
03/2011	South Korea	2	2	1	2	1
	United States	2	1	1	3	1
04/2011	South Korea	4.2	1	1	1	1
03/2013	South Korea	4.3 (5)	2	5	1	2
06/2013	South Korea	2	1	1	2	1
09/2013	South Korea	4.5 (5)	1	1	2	2
08/2014	South Korea	3 (5)	1	1	1	2

11/2014	United States	4.3	1	1	1	1
12/2014	South Korea	3	1	1	2	1
10/2015	South Korea	3	1	1	2	2
02/2016	South Korea	3 (5)	2	1	6	2
03/2016	South Korea	3	1	1	4	2
09/2016	South Korea	3	2	1	3	2
02/2017	South Korea	4.3 (5)	2	X	4	X

Table 7. Valeriano and Maness Assessment of Cyberspace Operations by North Korea.

DATE	NATION	METHOD	SEVERITY	INTERACTION	TARGET	GOAL
07/2009	South Korea	4.2	2	3	2	0
	United States	2	1	1	2	0
01/2011	South Korea	1	1	1	2	0
03/2011	South Korea	2	1	1	1	0
	United States	2	1	1	2	0
04/2011	South Korea	4.2	1	1	1	0

Cyberspace Operations against North Korea

December 2014. An offensive cyberspace operation against North Korea's internet affected access for several days.[152] Disruption started on 19 December and resulted in complete denial on 22 December, with access restored after ten hours. The operation occurred only hours after President Barak Obama promised a proportional

[152] Perlroth, Nicole and David Sanger. "North Korea Loses Its Link to the Internet." *The New York Times*, 22 December 2014. Web.

response to the offensive cyberspace operation against Sony Pictures Entertainment on 24 November that the FBI attributed to North Korea. The United States government denied any involvement in the operation. North Korea responded by threating its “toughest counteraction […] by far surpassing the ‘symmetric counteraction’ declared by Obama”.[153] There were initial suspicions that the event was benign and due to North Korea itself or even to China, but experts claimed that the event was inconsistent with activities such as maintenance or repair.[154] Because the bandwidth for North Korea is so low, even a small amount of traffic can overload its internet connection. The event was, however, consistent with a DDOS operation.

Based on this information, the operation against North Korea used the method of a denial of service (2), had a minimal effect due to low dependence on the internet (1), was an individual cyberspace operation that was a nuisance (1), and had the goal of disrupting target activity (1). As the distinction between private and government in North Korea is nonexistent and the operation targeted the entire internet, the target is difficult to assess with this methodology. This is summarized in Table 8 at the end of the section.

May 2015. A report from Reuters claimed that the United States had attempted an offensive cyberspace operation against North Korea’s nuclear weapon development program between 2009 and 2010, but was unsuccessful.[155] According to the report, the operation was conducted in tandem with an operation against Iran, referred to as Olympic

[153] Kang, Cecilia, Drew Harwell and Brian Fung. “North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack.” *The Washington Post*, 22 December 2014. Web.

[154] Ibid.

[155] Menn, Joseph. “US Tried Stuxnet-Style Campaign against North Korea but Failed – Sources.” *Reuters*, 29 May 2015. Web.

Games, which also targeted its nuclear weapon development program. Olympic Games used a now infamous piece of malware called Stuxnet that degraded the operation of the centrifuges used by Iran for uranium enrichment. Among other functions, it damaged or destroyed the centrifuges by directing the programmable logic controllers to spin beyond tolerances. Experts speculated that the operation required an unprecedented amount of human, financial, and technical resources to plan, develop, and execute. Stuxnet is considered the only confirmed use of malware by a state actor to cause physical damage against an adversary.

As North Korea and Iran acquired centrifuges from the same source and cooperated on nuclear weapon development activities, it is likely that the programmable logic controllers were similar. Therefore, it is also likely that the operation against North Korea used a variant of Stuxnet. However, there are a few possible reasons that it seems to not have made an impact on the pace of development. First, the malware might not have been able to access the systems and networks, which were not connected to the internet. North Korea has less interaction with foreigners than Iran and thus fewer opportunities to introduce the malware. There is also less intelligence available about its development facilities. Second, even if the malware was introduced, North Korea also uses plutonium, which does not require enrichment.

Based on this information, the operation against North Korea attempted to use the method of a worm, a variant of Stuxnet, (4.3) that was an APT (5), was an individual cyberspace operation that was offensive (3), targeted a government military entity (3), and had the goal of disrupting target activity (1). As the operation was unsuccessful, the severity is not applicable. This is summarized in Table 8 at the end of the section.

March 2017. An article from the New York Times reported that from 2014, the United States had conducted offensive cyberspace operations against North Korea's ballistic missile program as an alternative to reliance on ballistic missile defense systems.[156] According to the article, the high failure rates during flight tests of interceptors indicated that these systems were unable to meet the goal of defending the United States against ballistic missile threats. Statements from officials advocated for the preemptive use of non-kinetic capabilities, such as cyber and electronic capabilities. Then, soon after the test detonation of a nuclear device in February 2013 by North Korea, the United States published Joint Integrated Air and Missile Defense: Vision 2020, which referenced using "cyberwarfare, directed energy, and electronic attack" capabilities and "neutralizing an adversary's offensive air and missile assets prior to use."[157] Throughout 2014 and 2016, the failure rates during flight tests of various ballistic missile systems were noticeably high.[158] All this was cited as evidence for the presence of covert cyberspace operations.

Others, however, argued that even if the United States had the capability, correlation did not equal causation.[159] It was noted that the failures since 2014 were limited to four new missile systems that had never been tested, the BM-25 (five failures), the KN-011 (three failures), an unidentified intercontinental ballistic missile (two

[156] Sanger, David and William Broad. "Trump Inherits a Secret Cyberwar against North Korean Missiles." *The New York Times*, 4 March 2017. Web.
[157] Department of Defense, Joint Chiefs of Staff. *Joint Integrated Air and Missile Defense: Vision 2020*, 5 December 2013. Web.
[158] In particular, the article noted the failure rate of 88 percent for BM-25 compared to 13 percent for the R-27, the missile from the Soviet Union off which it was based.
[159] Lewis, Jeffrey. "Is the United States Really Blowing Up North Korea's Missiles?" *Foreign Policy*, 19 April 2017. Web.

failures), and an unidentified anti-ship missile (two failures).[160] Drawing conclusions from failure rates is difficult because of the numerous factors that must be considered. It is possible that the failures were simply the result of a rushed program and limited resources.

Based on this information and assuming the operation did occur, the operation against North Korea, had an effect on critical national infrastructure of military (2), was an individual cyberspace operation that was offensive (3), targeted a government military entity (3), and had the goal of disrupting target activity (1). There is not enough information to assess the method used in the operation. This is summarized in Table 8.

Table 8. Assessment of Cyberspace Operations against North Korea.

DATE	NATION	METHOD	SEVERITY	INTERACTION	TARGET	GOAL
12/2014	North Korea	2	1	1	X	1
05/2015	North Korea	4.3 (5)	X	3	3	1
03/2017	North Korea	X	2	3	3	1

Assessment of Cyberspace Capabilities

The initial period of North Korean cyberspace operations from July 2009 to April 2011 was characterized primarily by offensive cyberspace operations (almost all of which were DDOS operations) of varying scope and severity. There is evidence that these operations required no more than months by tens of personnel to plan and execute and no more than a medium level of knowledge or access. In fact, DDOS operations often use

[160] Ibid.

botnets of infected computers, which do not necessarily require a high level of commitment or resources to establish. However, by April 2011, the suspected level of resources that were required had increased relative to previous operations. Because targets included up to military government entities in South Korea and the United States, it is assumed that the threat actor was willing accept a high level of associated risk. It was also able to mostly but not entirely obscure the details of its operations. Although attempts were made at wiping hard drives, traces of malware were left behind in all operation Based on these factors, North Korea is assessed at an initial threat level of five according to OTA as of April 2011, which is summarized in Table 9.

Table 9. North Korean Threat Profile as of April 2011

THREAT LEVEL	THREAT PROFILE						
	Commitment Attributes			Resource Attributes			
	Intensity	Stealth	Time	Technical Personnel	Cyber Knowledge	Kinetic Knowledge	Access
5	H	M	Weeks/Months	Tens	M	M	M

The latest period of North Korean cyberspace operations, those from March 2013 to May 2017,[161] has been characterized primarily by cyber espionage. It was from this period that North Korea began to be considered an APT by experts. The operations had specific targets associated with the government and critical national infrastructure, used TTPs that indicated a high degree of organization and high amount of resources, and

[161] This end date represents the final semester during which research for this thesis was conducted, not any significant change in North Korean cyberspace operations.

required extended operations and repeated attempts. Analysis and investigation from almost every subsequent operation has revealed a greater scope and greater intensity of operations, often requiring tens of tens or even hundreds of personnel and months to years to plan, develop, and execute. Although there is indication of a high level of cyber knowledge due to evidence of the internal development and use of sophisticated pieces of malware (two of which each even incorporated a zero-day exploit) there is no indication of more than a medium level of kinetic knowledge or access. Based on these factors, North Korea is assessed at a latest threat level of three according to OTA as of May 2017, which is summarized in Table 10.

Table 10. North Korean Threat Profile as of May 2017

THREAT LEVEL	THREAT PROFILE						
	Commitment Attributes			Resource Attributes			
	Intensity	Stealth	Time	Technical Personnel	Cyber Knowledge	Kinetic Knowledge	Access
3	H	H	Months/Years	Tens/Tens	H	M	M

In addition to the attributes discussed, OTA also considers the multipliers of funding, assets, and technology, which potentially enhance capabilities but do not necessarily increase the threat level. This is because the multipliers can either increase or decrease certain measures. In the case of North Korea, although the increased amount of funding and number of assets evidenced by the analysis of offensive cyberspace operations have provided an increased level of technical personnel and cyber knowledge, these multipliers also have increased the reliance on resources abroad. This has resulted in an increased degree of exposure and therefore a decreased level of stealth. In contrast, the increased sophistication of technology has resulted in an increased level of access.

CHAPTER VI: CONCLUSION

Results

In regard to Hypothesis 1, North Korea's cyberspace resources and capabilities have increased and have now reached a level that represents an advanced persistent threat. Its development of civilian cyberspace resources has been cautious yet consistent. Efforts began in 1990 under the KCC, which has continued and expanded its efforts to include research and development at nine centers and providing IT services abroad from offices in China, Japan, and Europe. North Korea now also operates three state-owned IT ventures and several IT firms.

In 2000, cyberspace in North Korea consisted only of a domestic intranet. By 2002, North Korea had established a mobile network and by 2003, had established an internet connection. Although little information is available on the latter, the former has been ungraded from 2G to 3G and expanded from 20,000 to 3 million subscribers. All this, however, has been accompanied by the development and implementation of domestic software that provides the government with an unprecedented degree of monitoring and control.

In addition, North Korea's development of military capabilities in cyberspace has been consistent and dramatic. In 2014, it completed the installation of a dedicated high-speed fiber-optic military intranet that allows for integrated command and control between strategic, operational, and tactical units. It has one confirmed and two suspected cyber units subordinate to the RGB and two cyber units subordinate to the GSD. North Korea has also doubled its cyberwarfare personnel from an estimated 3,000 in 2012 to

6,800 in 2016.[162] There are reports that it has 1,200 personnel at covert cyber units in China and Southeast Asia.[163] North Korean cyber units have been implicated in several high-profile operations, such as the July 2009 DDOS operation, the November 2014 operation against Sony Pictures Entertainment, and WannaCry. Based on a correlation between the TTPs of North Korean cyberspace operations and these confirmed and suspected cyber units, it is possible that the Lazarus Group (which was previously and/or is alternatively referred to as the DarkSeoul Gang) is actually Bureau 121 and Bluenoroff is actually the subordinate Unit 180.

North Korea possesses a large spectrum of methods used for cyberspace operations, including the tools of botnets, trojans, viruses, and worms. At least 4 out of 15 operations were targeted and sophisticated enough for the threat actor to be considered an APT. Regarding the tools, a recent joint technical alert from the FBI and DHS in fact identified a massive botnet infrastructure that is maintained by North Korea and referred to as DeltaCharlie.[164] The report, which refers to North Korean malicious cyberspace activity as HIDDEN COBRA, confirms that the "tools and capabilities used by HIDDEN COBRA actors include DDOS botnets, keyloggers, remote access tools (RATs), and wiper malware."[165]

In light of its overall operations, North Korea's capabilities can be thought of as representing a high-level threat according to OTA.[166] This places it alongside threats such

[162] By comparison, the United States planned to have 6,000 personnel at its Cyber Command as of 2016

[163] Cordesman, Anthony. "Korean Special, Asymmetric, and Paramilitary Forces." Washington, DC: *Center for Strategic and International Studies*, 9 August 2016. Web.

[164] Department of Homeland Security, US-CERT. *HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure*, 13 June 2017. Web.

[165] Ibid.

[166] A high-level threat corresponds to levels 1-3, medium-level to levels 4-6, and low-level to levels 7-8.

as those represented by the series of offensive cyberspace operations against the Estonian internet in 2007. There is no evidence, however, that it has acquired the resources (the attributes of cyber knowledge, kinetic knowledge, and access) required for an operation such as that against the Iranian uranium enrichment program in 2009 and 2010. Such an operation can be assigned a threat level of one, which represents the greatest form of APT.

In regard to Hypothesis 2, despite the increase in cyberspace resources and capabilities, North Korea's cyberspace operations have remained restrained (produced minimal effects on South Korean and United States national security) and regional (targeted South Korea over the United States). The types of North Korean cyberspace operations are almost equal in occurrence. Out of 15 operations, 7 were offensive cyberspace operations and 8 were cyber espionage. Out of 3 operations against the United States in particular, all were offensive cyberspace operations and none were cyber espionage. It is also interesting to note that no offensive cyberspace operation has been conducted against South Korea since June 2013 or against the United States since November 2014. Although there have been subsequent cyber espionage operations against South Korea, there have no subsequent cyberspace operations against the United States.

There are a few possible explanations for this seeming transition from a period of offensive cyberspace operations to a period of cyber espionage against South Korea. As mentioned earlier, cyber espionage is often preparation for an offensive cyberspace operation. Therefore, it is possible that South Korea has improved at discovering this before the offensive cyberspace operation is executed. This was the suspicion after the operation in February 2016 was uncovered. It is also possible that the period of offensive cyberspace operation was for the testing of capabilities that were to be used for the eventual and current period of cyber espionage. This is similar to the suspicion that the operation in March 2011 was for the testing of capabilities and observing of the time required for the operation to be discovered, analyzed, and mitigated.

The frequency of North Korean cyberspace operations increased in 2011, with two to three operations conducted or discovered each year since then except for 2012. Although any connection is speculation, 2012 was the year that Kim Jong-un assumed the position of supreme leader after his father, Kim Jong-il, died in December 2011. During this transition, the attention of the leadership was on reestablishing legitimacy and refocusing power from the military to the ruling party.[167]

The effects of North Korea's offensive cyberspace operations and cyber espionage operations on South Korea and United States national security have been minimal. The intensity of North Korean cyberspace operations has never exceeded that of an effect on critical national infrastructure or military and most have been below this, with 10 of out 17 operations at the intensity of minimal effect. The intensity of operations against the United States in particular has never exceeded that of a minimal effect.

From the framework of risk, the consequences of these operations can be difficult to determine and measure. There are likely psychological consequences for most operations. However, the research on the psychological consequences in relation to cyber terrorism is limited, and it is unclear whether these cyber incidents can even be

[167] Lee, Hong-yung. "North Korea in 2012: Kim Jong-Un's Succession." *Asian Survey* 53.1 (2013): 176-183. Web.

characterized as cyber terrorism.[168] The operational and resultant economic consequences are easier to measure. During the multiple DDOS operations by North Korea, government and civilian entities were unable to provide services via the internet for hours or sometimes even days. This resulted in operating losses, as well as investigation and remediation costs. The MND estimated that North Korean offensive cyberspace operations between 2009 and 2013 had cost $805 million.[169] Sony Pictures Entertainment reported that the offensive cyberspace operation in September 2014 had cost $15 million. Although these figures seem high, the actual economic consequences are low in comparison to overall national or corporate budgets.[170]

The focus of North Korean cyberspace operations is overwhelmingly on South Korea. 12 out of 17 operations have focused on South Korea exclusively, and only 1 out of 17 operations has focused on the United States exclusively. However, this single event in November 2014 was instigated by the planned release of a comedy movie by the United States that offended North Korea. Dissimilar from previous operations against both South Korea the United States, there was a single target that was unassociated with the government or military, an articulated personal motive, and a demand to cancel the release of the movie. This operation was uncharacteristic of most operations by state actors.

In regard to Hypothesis 3, North Korea's valuable assets include its ability to control cyberspace within North Korea and its ability to engage in cyberspace activities

[168] Gross, Michael, Daphna Canetti, and Dana Vashdi. "The Psychological Effects of Cyber Terrorism." *The Bulletin of the Atomic Scientists* 72.5 (2016): 284-291. Web.

[169] "정희수 '북한 사이버 공격으로 8 천 600 억원 피해'." *Yonhap News*, 15 October 2013. Web.

[170] Hackett, Robert. "How Much Do Data Breaches Cost Big Companies? Shockingly Little." *Fortune*, 27 March 2015. Web.

and operations from abroad. The North Korean government has implemented extreme measures to ensure control over the flow of information into and within the nation. It has developed intrusive software (or malware in any context other than the North Korean government) that monitors and controls activities on almost all devices, systems, and networks used by its citizens. Although access to these has been increasing, it is still restricted.

Although cyberspace infrastructure in North Korea has been developing, greater capacity and greater anonymity is offered by locations abroad. A reported 1,100 out of 6,800 cyberwarfare personnel conduct operations from covert locations abroad. [171] It has also been reported that 1,000 personnel from the KCC have been sent abroad to earn money for the regime. [172] As these KCC personnel represent a broad range of IT experience and expertise and the North Korean government has been implicated in illicit activities before, it is likely that this earning of money is not entirely benign. As with its military cyberspace operations existing within an overall national security strategy, this emphasis on moving activities abroad exists within an economic strategy to circumvent debilitating sanctions. It is possible that this was the motivation behind the alleged high-profile cybertheft of $81 million from the Bangladesh Bank in February 2016 and cyberextortion of around $55,000 through the ransomware operation WannaCry in May 2017.

[171] 김봉기. "'北, 최근 청와대·국회 해킹 시도… 국감 자료 빼내가'." *Chosun Ilbo*, 21 October 2015. Web.

[172] 김도형. "北, IT 인력 1500 명 해외 보내 年 4000 만달러 벌어." DongA Ilbo, 25 August 2016. Web.

The incident involving WannaCry in particular highlights another danger posed by North Korean cyberspace activities in general. There was some speculation that because this operation was so uncharacteristic of a state actor or even other operations attributed to North Korea, it was possibly the act of a non-state actor that was simply associated with or supported by North Korea.[173] This introduces the potential for the proliferation of cyber weapons, either intentionally for financial gain or unintentionally through the traces of malware and malicious code left behind after an operation. In fact, a comprehensive report from Hewlett Packard emphasizes the potential for such proliferation of cyber weapons in light of the past proliferation of kinetic weapon expertise by North Korea and the current relationships with Russia, China, Iran, and Syria that involve cyberspace.[174] For example, North Korea has relied on China for IT resources and Russia for cyber training and concluded agreement with Iran in 2012 to combat "common enemies" in cyberspace and a similar agreement with Syria in 2002.[175]

On another note, as revealed through the analysis, the characterization of operations as being "sophisticated" or even a "cyberattack" or a "hack" is often misleading. At least one of the targets, Sony Pictures Entertainment, had notoriously poor network security.[176] Two of the incidents simply involved attempts at phishing text messages or emails, most of which were unsuccessful. It is also important to remember

[173] Elias, Groll. "Security Firms Tie WannaCry Ransomware to North Korea." *Foreign Policy*, 23 May 2017. Web.
[174] Hewlett Packard Security Research. *Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape*, August 2014. Web.
[175] Ibid.
[176] Steinberg, Joseph. "Massive Security Breach at Sony – Here's What You Need to Know." *Forbes*, 11 December 2014. Web.

that sophistication is relative to a particular time. Something that was sophisticated several years ago is not necessarily sophisticated now.

Counterarguments

There are two main competing arguments regarding the implications of malicious cyberspace activity. The first argument claims that it represents a nuisance that will unlikely escalate to an existential threat to national security (cyber threat inflation theory). The second argument claims that it represents a threat to national security that will possibly result in serious damage or destruction (cyber threat theory). This thesis generally supports the former.

That is, although there is little indication of any counterargument by experts that North Korean cyberspace capabilities have not increased, there is a counterargument that North Korean cyberspace operations will possibly result in serious damage or destruction for South Korea and United States. However, this counterargument is unsubstantiated. As demonstrated by the analysis, North Korean cyberspace operations have been restrained, never having effects on national security strategy and never having physical consequences. Even if North Korea does have the capabilities for such escalated cyberspace operations (and there is no evidence of this), these operations are inconsistent with its overall military strategy.

In addition to a misunderstanding of North Korean cyberspace capabilities and intent, some experts have noticed a trend of characterizing all offensive cyberspace operations as sophisticated and suspect that it is an attempt to shift the blame for lapses in cybersecurity practices.[177]

[177] Winkler, Ira. “The ‘Sophisticated Attack’ Myth.” *Computer World*, 10 February 2015. Web.

CHAPTER VII: DISCUSSION

National Security Implications

The greatest threat from North Korea in cyberspace currently is its capability not its intent. As mentioned, threat is a combination of capability and intent. North Korea has demonstrated the capability to conduct offensive cyberspace operations and cyber espionage against both government and civilian targets. It has also dedicated resources toward developing and enhancing this capability. However, the operations have been consistent with an overall military strategy that consists of rhetoric and confrontation that is below the threshold for an act of war. Cyberwarfare is simply another form of asymmetric warfare. Even in the most alarmist scenario, if North Korea wanted to cause damage or destruction to critical infrastructure in South Korea, there is no reason it could not have done this already through traditional covert means, even despite the benefit of anonymity offered by cyberspace operations.

North Korea is not the greatest threat to the United States in cyberspace. North Korea is often referenced along with Russia and China as being among the most serious threats to the United States in cyberspace. In the assessment of cyberpower, Clark listed it first among the three nations and Valeriano and Maness listed it third among the three nations. According to the Worldwide Threat Assessment of the US Intelligence Community, "[North Korea] probably remains capable and willing to launch disruptive or destructive offensive cyberspace operations to support its political goals."[178] However, as

[178] Congress, Senate, Armed Services Committee. *Worldwide Threat Assessment of the US Intelligence Community*, by James Clapper. 9 February 2016. Web.

revealed in this thesis, the focus of the operations is South Korea, not the United States, and the effect of the operations has been limited. In contrast, however, Russia has demonstrated a willingness to target critical infrastructure in and conduct cyber espionage operations against the United States, and China as well has been successful in cyber espionage operations against the United States.[179]

North Korea's cyberspace operations (or cyber weapons) are a complement to its nuclear weapons. The greatest North Korean activities of concern for the United States are cyberspace operations and nuclear weapon/ballistic missile development. Placing the threats that the respective weapons represent within an impact/probability chart or matrix, nuclear weapons exemplify a threat that is high-impact but low-probability, and cyber weapons exemplify a threat that is low-impact but high-probability. Nuclear weapons have an enormous destructive force that is kinetic and therefore high impact. However, because of this and the numerous uncertainties associated with the potential consequences for the actual use of nuclear weapons (the "threat that leaves something to chance" in theories of deterrence), they have a low probability of being used.

In contrast, almost all cyber weapons have a damaging or disrupting effect that is only virtual and therefore low-impact.[180] However, because cyber weapons can be used to effect relatively quickly and anonymously, they have a high probability of being used. It is therefore reasonable to assume that absent some sort of existential threat, North Korea will maintain its use of cyberspace operations for OCO and CISR in the virtual world and its use of nuclear weapons for deterrence in the physical world.

[179] Ibid.

[180] The obvious exception is Stuxnet, which did have an effect that was kinetic.

Because North Korea values its ability to control cyberspace within North Korea and its ability to engage in cyberspace activities and operations from abroad, these assets are also valuable targets for the United States. According to an expert on North Korea, Jieun Baek, "[The erosion of control over information] is probably the biggest weakness that the government has. And that's evident because of the way they react to foreign information coming in, versus other threats like economic sanctions or verbal condemnations by other countries."[181] Because of its expansive and interconnected nature, which allows for the greater flow of information, the inability to control cyberspace represents a serious threat to the North Korean regime. The implications for even limited (yet legal) means of information flow between North Korean citizens via even domestic cyberspace, such as mobile phone, are significant. Such means allow for greater interpersonal communication and the formation of constituencies that are able to bring pressure on the regime.[182] This forces the regime to reconsider its approach of control through individual isolation and creates the protentional for positive change.[183]

In addition, there has often been a disconnect between the goals for United States national security policy regarding North Korea and the instruments of state power that can be used to achieve these goals. That is, the United States wants North Korea to abandon its nuclear weapon and ballistic missile development but has relied only on diplomatic and/or economic instruments, such as negotiations and sanctions. Due to the physical risks of retaliation and escalation, the traditional military threat cannot be

[181] Baek, Jieun. "How Media Smuggling Took Hold in North Korea." Interview. *PBS*, 18 December 2016. Web.

[182] Kretchun, Nat. "The Regime Strikes Back: A New Era of North Korean Information Controls." *38 North*, 9 June 2017. Web.

[183] Ibid.

addressed with a traditional military response. In contrast, a cyberspace threat has no such physical risks, and can therefore be addressed with a cyberspace response, as well as diplomatic and economic responses. Because the locations abroad from which North Korea engages in cyberspace activities and operations also likely have dual purposes (economic and military), eliminating the ability to use these locations denies North Korea the resources and capabilities required to leverage multiple instruments of state power. For these reasons, the aforementioned assets related to North Korea in cyberspace are valuable to the United States as potential targets for leveraging its own instruments of state power to advance its national security and foreign policy goals.

Policy Recommendations

Before offering policy recommendations, it is necessary to review the current United States strategies related to cyberspace. These can be broadly divided into diplomatic strategy and military strategy. For the former, according the International Strategy for Cyberspace released by the White House in 2011:[184]

> The United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide state actions, sustain partnerships, and support the rule of law in cyberspace.

For the latter, the DOD has declared five strategic goals:[185]

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;

[184] Office of the President of the United States. *International Strategy for Cyberspace*, May 2011. Web.
[185] Department of Defense. *The DOD Cyber Strategy*, April 2015. Web.

2. Defend the DOD information network, secure DOD data, and mitigate risks to DOD missions;
3. Be prepared to defend the US homeland and US vital interests from disruptive or destructive cyberattacks of significant consequence;
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

The United States government should focus on denying and disrupting the use of cyberspace by covert cyber units outside of North Korea. Because the systems and networks outside of North Korea are dependent on the use of host nation infrastructure and compliance with host nation regulation, they are more vulnerable. Because these locations provide greater capacity and anonymity, they also are likely more valuable to the North Korea regime. There are two options suggested for this denial and disruption. The first is directly through offensive cyberspace operations, which would neutralize a node from the network of units that support the system of cyberspace operations. The second is indirectly through the conclusion of an agreement or a treaty that codifies international norms prohibiting the conduct of certain types of operations against certain types of targets, which would neutralize the node by obligating the host nation to address cyber harm emanating from within its territory. Even if the node is not neutralized due to the inability or unwillingness of the host nation, an agreement or a treaty at least alters the properties of the system of regulations and creates a difficult operating environment for the unit. These two options are potentially mutually exclusive.

A response has already been made against North Korean cyberspace assets, albeit in the context of counterproliferation. In June 2017, the Office of Foreign Assets Control at the Department of the Treasury added the KCC to the list of designation entities for sanctions due its role in earning foreign money for the regime and the Munitions Industry Department in particular, which is involved in key aspects of the ballistic missile development program.[186] As such, expanding sanctions to include any North Korean entity associated with malicious cyberspace activities or operations represents a third option.

The United States government should focus on enabling and ensuring the less monitored and less controlled use of cyberspace by civilians inside of North Korea. Cyberspace operations against strategic programs have been unsuccessful at noticeably deterring or even delaying the progression of these programs. This does not mean, however, that North Korea is invulnerable to such operations. It means only that those specific programs are. The aforementioned vulnerability to information other than state-sanctioned media has already been exploited for use by the human network of illicit storage mediums that are smuggled into and out of North Korea. Assuming that a greater flow of information equates to a greater chance for change in regime behavior, the asset of monitoring and control is worth targeting. Providing access to information could be accomplished by supporting the efforts of non-governmental organizations to get CDs/DVDs, USB flash drives, and SD cards into North Korea. This access could then be assured by initiating efforts to defeat or circumvent the software placed on the devices, systems, and networks by the North Korean government.

[186] Department of the Treasury, Office of Foreign Assets Control. *Treasury Sanctions Suppliers of North Korea's Nuclear and Weapons Proliferation Programs*, June 2017. Web.

Such cyberspace operations could even occur within a more comprehensive and more active information operation campaign. After the flow of and access to information has been increased in North Korea, the United States could release public information that is truthful yet damaging to the legitimacy and credibility of the regime. The duration and intensity of this campaign could be tailored to act either as a means of deterrence in cyberspace, signaling the capability of the United States to disrupt regime control, or as a means of destabilization.

The United States government should enhance information and intelligence sharing with allies and partners, as well as with civilian entities. As revealed in the analysis of cyberspace operations by North Korea, the threat is comprised of multiple pieces of a puzzle. Different pieces of evidence can be left behind on different private and government systems and networks. Different series of operations against private and government targets in the United States and other countries can be connected to reveal a greater scope and intensity that is otherwise not obvious from an individual operation. It is all this evidence that completes the puzzle of the actual cyberspace capabilities and intent of an adversary.

Some executive efforts to enhance information and intelligence sharing have been made. For example, The DHS established the United States Computer Emergency Readiness Team (US-CERT) in 2003 to collect, analyze, and disseminate cybersecurity information shared among private and government entities. However, legislative efforts have lagged. The Cyber Intelligence Sharing and Protection Act (CISPA) passed the

House of Representatives but not the Senate in 2013.[187] Despite concerns over liability and anonymity, the alternate Cybersecurity Information Sharing Act (CISA) was signed into law in 2015. However, although CISA facilitates information sharing, it does not require information sharing. There are also no provisions in executive agreements or treaties or in legislative acts that establish means of or obligation for information and intelligence sharing between allies and partners. These are significant missing pieces of the puzzle that need to be addressed.

Directions for Future Research

There are three directions for future research that are best captured in the following questions: (1) What are the nuanced differences in effects or consequences between exploitative cyber incidents and disruptive cyber incidents? (2) How does the analysis of cyber events in this thesis compare to the analysis in the updated DCIDD expected to be released soon after the thesis is completed? What are the implications for national security if North Korea is engaged in cybercrime?

As mentioned earlier, exploitative incidents and disruptive incidents differ in regard to ultimate effect. However, this is not reflected in the factor of severity in the DCIDD. If the ultimate consequence is different, then is it reasonable to assume that the implication for national security will be different. Recognizing the importance of this distinction, the Center for International and Security Studies at Maryland has published a framework for categorizing and assessing the severity of disruptive cyber incidents and is

[187] Greenemeier, Larry. "A Quick Guide to the Senate's Newly Passed Cybersecurity Bill." *Scientific American*, 28 October 2015. Web.

finalizing a separate framework for exploitative cyber incidents.[188] It is also worth considering consequences that are not only operational or economic (as was done in this thesis), but also psychological. That is, do North Korean cyberspace operations have consequences that are psychological and what are the implications for national security?

Of the fourteen dyadic cyber events in the DCIDD that identified North Korea as the perpetrator, seven were unable to be found and one was omitted because although the indicated event did occur, no confirmation was found for one of the three targets. In addition to these discrepancies, for the remaining six dyadic cyber events that overlapped between the DCIDD and this thesis, there were minor discrepancies for the coding of some of the factors. Because of this, it possible that there will be similar discrepancies in comparison to the updated DCIDD that are worth addressing.

[188] Gallagher, Nancy and Charles Harry. "Categorizing and Assessing Disruptive Cyber Incidents." College Park, MD: *Center for International and Security Studies at Maryland*, April 2017. Web.

WORKS CITED

Australian Strategic Policy Institute. “North Korea.” *Cyber Maturity in the Asia-Pacific Region 2016*, 2016. Web.

Baek, Jieun. "How Media Smuggling Took Hold in North Korea." Interview. *PBS*, 18 December 2016. Web.

Berger, Andrea. “A Familiar Story: The New UN Report on North Korean Sanctions Implementation.” *38 North*, 16 March 2017. Web.

Blair, David. “North Korea v. South Korea: How the Countries' Armed Forces Compare.” *The Telegraph*, 15 September 2015. Web.

Boynton, Robert. “North Korea’s Digital Underground.” *The Atlantic*, April 2011. Web.

Byrne, Leo. “Seoul Says North Korea Carried Out Large-Scale Hack.” *NK News*, 14 June 2016. Web.

Chen, Ping, Lieven Desmet, and Christophe Huygens. “A Study on Advanced Persistent Threats.” *IFIP International Conference on Communications and Multimedia Security 2014*. 25-26 September 2014. Web.

Choe, Sang-hun. “Computer Networks in South Korea Are Paralyzed in Cyberattacks.” *The New York Times*, 20 March 2013. Web.

Choe, Sang-hun. “Cyberattacks Disrupt Leading Korean Sites.” *The New York Times*. 26 June 2013. Web.

Choe Sang-hun and David Sanger. “South Korea Accuses North of Hacking Senior Officials’ Phone.” *The New York Times*, 9 March 2016. Web.

Choe, Sang-hun, and John Markoff “Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea.” *The New York Times*, 8 July 2009. Web.

Clarke, Richard and Robert Knake. *Cyber War: The Next Threat to National Security and What To Do about It*. New York, NY: Harpers Collins Publishers, 2010. Print.

Comey, James. “Addressing the Cyber Security Threat.” *International Conference on Cyber Security*. 7 January 2015. Web.

Congress, Senate, Armed Services Committee. *Foreign Cyber Threats to the United States*, by James Clapper. 5 January 2017. Web.

Congress, Senate, Armed Services Committee. *Statement of Admiral Michael S. Rogers, Commander, United States Cyber Command, before the Senate Armed Services Committee*, by Michael Rogers. 5 April 2016. Web.

Congress, Senate, Armed Services Committee. *Worldwide Threat Assessment of the US Intelligence Community*, by James Clapper. 9 February 2016. Web.

Congress, Senate, Select Committee on Intelligence. *Worldwide Threat Assessment of the US Intelligence Community*, by Daniel Coats. 11 May 2017. Web.

Cordesman, Anthony. "Korean Peninsula Military Modernization Trends." Washington, DC: *Center for Strategic and International Studies*, 20 September 2016. Web.

Cordesman, Anthony. "Korean Special, Asymmetric, and Paramilitary Forces." Washington, DC: *Center for Strategic and International Studies*, 9 August 2016. Web.

Department of Defense, Joint Chiefs of Staff. *Joint Integrated Air and Missile Defense: Vision 2020*, 5 December 2013. Web.

Department of Defense. *Joint Publication 3-12 (R): Cyberspace Operations*, 2013. Web.

Department of Defense. *Joint Publication 3-13: Information Operations*, 2014. Web.

Department of Defense. *The DOD Cyber Strategy*, April 2015. Web.

Department of Defense. *Strategy for Operating in Cyberspace*, 1 July 2011. Web.

Department of Defense, Office of the Secretary of Defense. *Military and Security Developments Involving the Democratic People's Republic of Korea 2015*. 2015. Web.

Department of Defense, United States Army. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations*, April 2017. Web.

Department of Homeland Security. *DHS Risk Lexicon*, September 2008. Web.

Department of Homeland Security, US-CERT. *HIDDEN COBRA – North Korea's DDOS Botnet Infrastructure*, 13 June 2017. Web.

Department of Justice, Federal Bureau of Investigation. *Update on Sony Investigation*, 19 December 2014. Web.

Department of the Treasury, Office of Foreign Assets Control. *Treasury Sanctions Suppliers of North Korea's Nuclear and Weapons Proliferation Programs*, June 2017. Web.

Elias, Groll. “Security Firms Tie WannaCry Ransomware to North Korea.” *Foreign Policy*, 23 May 2017. Web.

Elkind, Peter. “Sony Pictures: Inside the Hack of the Century.” *Fortune*, 25 June 2015. Web.

Fang, Arnold. “North Korea’s Self-Imposed Isolation.” *The Diplomat*, 15 March 2016. Web.

Finkle, Jim. “Four-Year Hacking Spree in South Korea Blamed on ‘Dark Seoul Gang’.” *Reuters*, 26 June 2013. Web.

Finkle, Jim. “North Korean Hacking Group Behind Recent Attacks on Banks: Symantec.” *Reuters*, 15 March 2017. Web.

Fung, Brian. “What You Need to Know About Bitcoin after the WannaCry Ransomware Attack.” *The Washington Post*, 15 May 2017. Web.

Gallagher, Nancy and Charles Harry. “Categorizing and Assessing Disruptive Cyber Incidents.” College Park, MD: *Center for International and Security Studies at Maryland*, April 2017. Web.

Gallagher, Sean. “A $50 Device Is Breaking North Korean Government’s Grip on Media.” *Ars Technica*, 27 March 2015. Web.

Goodin,Dan. “Malware Believed to Hit Sony Studio Contained a Cocktail of Badness.” *Ars Technica*, 19 December 2014. Web.

Greenemeier, Larry. “A Quick Guide to the Senate's Newly Passed Cybersecurity Bill.” *Scientific American*, 28 October 2015. Web.

Greitens, Sheena. “Illicit: North Korea’s Evolving Operations to Earn Hard Currency.” Washington, DC: *Committee for Human Rights in North Korea*, 2014. Web.

Grisham, Lori. “Timeline: North Korea and the Sony Pictures Hack.” *USA Today*, 5 January 2015. Web.

Gross, Michael, Daphna Canetti, and Dana Vashdi. “The Psychological Effects of Cyber Terrorism.” *The Bulletin of the Atomic Scientists* 72.5 (2016): 284-291. Web.

Hackett, Robert. “How Much Do Data Breaches Cost Big Companies? Shockingly Little.” *Fortune*, 27 March 2015. Web.

“Half of All Countries Aware but Lacking National Plan on Cybersecurity, UN Agency Reports.” *United Nations*, 5 July 2017. Web.

Halliday, Josh and Samuel Gibbs. “North Korean Hackers Suspected of Cyber-Espionage Attack on South.” *The Guardian*, 11 September 2013. Web.

Harlan, Chico and Ellen Nakashima. “Suspected North Korean Cyber Attack on a Bank Raises Fears for S. Korea, Allies.” *The Washington Post*, 29 August 2011. Web.

Hayden, Michael. “Life in The Cyber Domain.” *Playing to the Edge: American Intelligence in the Age of Terror*. New York, NY: Penguin Books, 2016. Print.

Hewlett Packard Security Research. *Profiling an Enigma: The Mystery of North Korea’s Cyber Threat Landscape*, August 2014. Web.

Hodge, Home. “North Korea’s Military Strategy.” *Parameters* 33 (2013): 68-81. Web.

Jiang, Genwei and Josiah Kimble. “Hangul Word Processor (HWP) Zero-Day: Possible Ties to North Korean Threat Actors.” *FireEye*, 7 September 2015. Web.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. “North Korea’s Cyber Operations: Strategy and Responses.” Washington, DC: *Center for Strategic and International Studies*, 2015. Web.

Jun, Jenny, Scott LaFoy, and Ethan Sohn. “What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?” Washington, DC: *Center for Strategic and International Studies*, 12 December 2014. Web.

Kaspersky. *Lazarus under the Hood*, April 2017. Web.

Kang, Tae-jun. “Wi-Fi Access Sparks Housing Boom in Pyongyang.” *The Diplomat*, 14 August 2014. Web.

Kim, Jack. “North Korea Mounts Long-Running Hack of South Korea Computers, Says Seoul.” *Reuters*, 12 June 2016. Web.

Kim, Yonho. “Cell Phones in North Korea: Has North Korea Entered the Telecommunications Revolution?” Washington, DC: *US-Korea Institute*, 2014. Web.

Kretchun, Nat. “The Regime Strikes Back: A New Era of North Korean Information Controls.” *38 North*, 9 June 2017. Web.

Laurence, Jeremy. “North Korea Military Has an Edge over South, but Wouldn't Win a War, Study Finds.” *The Christian Science Monitor*, 4 January 2012. Web.

“Lazarus Under the Hood.” Blog post. *SecureList*, 3 April 2017. Web.

Lee, Hong-yung. “North Korea in 2012: Kim Jong-Un’s Succession.” *Asian Survey* 53.1 (2013): 176-183. Web.

Lewis, Jeffrey. “Is the United States Really Blowing Up North Korea’s Missiles?” *Foreign Policy*, 19 April 2017. Web.

“Malicious Programs.” Blog post. *SecureList*, N.D. Web.

Mansourov, Alexandre. “North Korea’s Cyber Warfare and Challenges for the US-ROK Alliance.” Washington, DC: *Korea Economic Institute of America*, 2 December 2014. Web.

McAfee. *Dissecting Operation Troy: Cyberespionage in South Korea*, by Ryan Sherstobitoff, Itai Liba, and James Walter, 8 July 2013. Web.

McAfee. *Ten Days of Rain: Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea*, July 2011. Web.

McCafferty, Georgia. “Anniversary Parade Provides Rare Glimpse into North Korea's Military Might.” *CNN*, 10 October 2015. Web.

McCurry, Justin. “Korean Hackers Mount Cyber Skirmishes in Propaganda War.” *The Guardian*, 11 January 2011. Web.

Menn, Joseph. “US Tried Stuxnet-Style Campaign against North Korea but Failed – Sources.” *Reuters*, 29 May 2015. Web.

Mercado, Stephen. “Hermit Surfers of Pyongyang.” *Studies in Intelligence* 48.1 (2007): N.P. Web.

Ministry of National Defense. *2016 Defense White Paper*, 2016. Web.

“Missiles of North Korea.” Washington, DC: *Center for Strategic and International Studies*, N.D. Web.

Murauskaite, Egle. “North Korea’s Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment.” *38 North*, 12 September 2014. Web.

“N. Korea Likely Hacked S. Korea Cyber Command.” *Yonhap News*, 5 December 2016. Web.

Nakashima, Ellen. “The NSA Has Linked the WannaCry Computer Worm to North Korea.” *The Washington Post*, 14 June 2017. Web.

“North Korea Tried to Hack South's Railway System: Spy Agency.” *Reuters*, 8 March 2016. Web.

"North Korea's 'Paranoid' Computer Operating System Revealed." *The Guardian*, 27 December 2015. Web.

Nye, Joseph. "Cyber Power." Cambridge, MA: *Belfer Center for Science and International Affairs*, May 2010. Web.

O'Carroll, Chad. "Inside North Korea's Cell Network: Ex-Koryolink Technical Director Reveals All." *NK News*, 20 August 2015. Web.

O'Carroll, Chad. "Well-Known Electronics Joint Venture Terminated in Pyongyang." *NK News*, 9 September 2015. Web.

Office of the President of the United States. *International Strategy for Cyberspace*, May 2011. Web.

Park, Donghui. "North Korea Cyber Attacks: A New Asymmetrical Military Strategy." *University of Washington*, 28 June 2016. Web.

Park, Ju-min and James Pearson. "In North Korea, Hackers Are a Handpicked, Pampered Elite." *Reuters*, 5 December 2014. Web.

Park, Ju-min and James Pearson. "North Korea Overcomes Poverty, Sanctions with Cut-Price Nukes." *Reuters*, 11 January 2016. Web.

Park, Ju-min and James Pearson. "North Korea's Unit 180, The Cyber Warfare Cell That Worries the West." *Reuters*, 20 May 2017. Web.

Park, Ju-min and Mee-young Cho. "South Korea Blames North Korea for December Hack on Nuclear Operator." *Reuters*, 17 March 2015. Web.

Perlroth, Nicole and David Sanger. "North Korea Loses Its Link to the Internet." *The New York Times*, 22 December 2014. Web.

Price, Greg. "U.S. Military Presence in Asia: Troops Stationed in Japan, South Korea, and Beyond." *Newsweek*, 26 April 2017. Web.

Rahn, Kim. "NK Launched Cyber Attack on Nonghyup." *The Korea Times*, 3 May 2011. Web.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35.1 (2012): 5-32. Web.

Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks" *Journal of Strategic Studies* 38.1-2 (2015): 4-37. Web.

Russon, Mary-Ann. “No, North Korea's Internet Doesn't Only Have 28 Websites, but Reddit Did Manage to Crash Them.” *International Business Times*, 22 September 2016. Web.

“S. Korea's Military Cyber Command Hacked Last Month.” *Yonhap News*, 1 October 2016. Web.

Sandia National Laboratories. *Categorizing Threat: Building and Using a Generic Threat Matrix*, by David Duggan, Sherry Thomas, Cynthia Veitch, and Laura Woodard, September 2007. Web.

Sanger, David and William Broad. “Trump Inherits a Secret Cyberwar against North Korean Missiles.” *The New York Times*, 4 March 2017. Web.

Singer, P.W. and Alan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014. Print.

“South Korea Government Websites Targeted in Cyber Attack.” *The Guardian*, 4 March 2011. Web.

Steinberg, Joseph. “Massive Security Breach at Sony – Here's What You Need to Know.” *Forbes*, 11 December 2014. Web.

Stone, John. “Cyber War Will Take Place.” *Journal of Strategic Studies* 36.1 (2013): 101-108. Web.

Sullivan, Tim. “North Korea and its Provocations: Belligerence as Strategy.” *The Washington Times*, 9 February 2016. Web.

“Suspected N.K. Attackers Hack into S. Korea's Cyber Command through Main Server.” *Yonhap News*, 7 December 2016. Web.

Symantec Security Response. “Are the 2011 and 2013 South Korean Cyberattacks Related? Blog post. *Symantec*, 29 March 2013. Web.

Symantec Security Response. “Attackers Target Dozens of Global Banks with New Malware.” Blog post. *Symantec*, 12 February 2017. Web.

Symantec Security Response. “Collaborative Operation Blockbuster Aims to Send Lazarus back to the Dead.” Blog post. *Symantec*, 24 February 2016. Web.

Symantec Security Response. “Four Years of DarkSeoul Cyberattacks against South Korea Continue on Anniversary of Korean War.” Blog post. *Symantec*, 26 June 2013. Web.

Symantec Security Response. “South Korean Banks and Broadcasting Organizations Suffer Major Damage from Cyberattack.” Blog post. *Symantec*, 20 March 2013. Web.

Symantec Security Response. “WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group.” Blog post. *Symantec*, 22 May 2017. Web.

Szoldra, Paul. “A Hacker Explains Why You Shouldn't Believe North Korea Was behind The Massive Sony Hack.” *Business Insider*, 10 June 2016. Web.

Talmadge, Eric. “North Korea Announces Blocks on Facebook, Twitter and YouTube.” *The Guardian*, 1 April 2016. Web.

Talmadge, Eric. “Online Shopping Has Arrived in North Korea.” *Business Insider*, 6 May 2015. Web.

Tarakanov, Dmitry. “The ‘Kimsuky’ Operation: A North Korean APT?” Blog post. *SecureList*, 11 September 2013. Web.

Thrall, Trevor and Jane Cramer. *American Foreign Policy and the Politics of Fear: Threat Inflation since 9/11*. New York, NY: Routledge, 2009. Web.

Tjia, Paul. “North Korea: An Up-and-Coming IT-Outsourcing Destination.” *38 North*, 26 October 2011. Web.

“UN Resolutions Related to Cybersecurity.” *International Telecommunication Union*, N.D. Web.

“US May Accuse North Korea in Bangladesh Cyber Heist: WSJ.” *Reuters*, 22 March 2017. Web.

Valeriano, Brandon and Ryan Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York, NY: Oxford University Press, 2015. Print.

“Venerating the Kims: Just One More Religion?” *The Economist*, 7 April 2013. Web.

Williams, Martin. “North Korea's Internet Domain Is in New Hands.” *PC World*, 19 May 2011. Web.

Williams, Martyn. “All That Glitters Is Not Gold: A Closer Look at North Korea’s Ullim Tablet.” *38 North*, 3 March 2017. Web.

Williams, Martyn. “How a Telecom Investment in North Korea Went Horribly Wrong.” *PC World*, 17 November 2015. Web.

Winkler, Ira. “The ‘Sophisticated Attack’ Myth.” *Computer World*, 10 February 2015. Web.

Yang, Jeong-yoon, So-jeong Kim, and Il-seok Oh. “Analysis on South Korean Cybersecurity Readiness Regarding North Korean Cyber Capabilities.” *International Workshop on Information Security Applications 2016*. 30 March 2017. Web.

김도형. “北, IT 인력 1500 명 해외 보내 年 4000 만달러 벌어 [15,000 North Korean IT Personnel Sent Abroad and Earning 40 Million Dollars Per Year].” DongA Ilbo, 25 August 2016. Web.

김봉기. “‘北, 최근 청와대·국회 해킹 시도… 국감 자료 빼내가’ [Recent North Korean Hacking Attempt against Blue House… Data from Government Audits Stolen].” *Chosun Ilbo*, 21 October 2015. Web.

김소열. “北, 04 년부터 中단둥서 사이버戰 활동 [North Korean Cyberwarfare Activities since 2004 in Dandong, China].” *Daily NK*, 12 July 2009. Web.

“북한, 대규모 사이버 공격 준비 확인… 대기업 문서 4 만여건 해킹 [Preparations by North Korea for Large-Scale Cyberattack Confirmed… over 40,000 Documents Hacked from Large Corporations].” *Yonhap News*, 13 June 2016. Web.

“‘북한군 인트라넷에 광케이블망 설치’<RFA> [RFA: North Korean Military Installs Fiberoptic Intranet].” *Yonhap News*, 23 April 2011. Web.

“북한의 정보화(H/W·S/W 부문) 강화 동향 [North Korea’s Trend of Intensifying Informationization (in Fields of Hardware and Software)].” *Tongil News*, 24 March 2004. Web.

“북한의 IT 센터들, 해외시장 진출에 적극적 [North Korea’s IT Centers Actively Advancing into Foreign Markets].” *Yonhap News*, 12 July 2009. Web.

“정희수 ‘북한 사이버 공격으로 8 천 600 억원 피해’ [860 Billion Won in Damages from North Korean Cyberattacks].” *Yonhap News*, 15 October 2013. Web.

손덕호. “국정원 ‘北, 주요인사 수십명 스마트폰 해킹해 문자·통화내용 유출’ [NIS: Smartphones of Several Key Government Personnel Hacked and Text and Voice Content Leaked].” *Chosun Ilbo*, 8 March 2016. Web.

이교관. “조선컴퓨터센터의 비밀 [Secrets of the Korea Computer Center].” *NK Chosun*, 11 May 2001. Web.

최종석. “北, 서울메트로 서버 5 개월 장악했다 [North Korea Infiltrated Servers of Seoul Metro over Period of 5 Months].” *Chosun Ilbo*, 5 October 2015. Web.

“北, 정부 주요인사 스마트폰 해킹…철도기관도 사이버공격 [North Korea Hacks Smartphones of Key Government Personnel… Also Conducts Cyberattack against Subway Corporation].” *Yonhap News*, 7 March 2016. Web.