International Journal of Cybersecurity Intelligence & Cybercrime

Volume 4 | Issue 2 Article 2

8-2021

North Korean Cyber Attacks and Policy Responses: An Interdisciplinary Theoretical Framework

North Korean cyber-attacks, cyberterrorism, criminological theoretical frameworks, the network theory of world politics, expert interview

Recommended Citation

Hwang, J., & Choi, K.-S. (2021). North Korean cyber attacks and policy responses: An interdisciplinary theoretical framework. International Journal of Cybersecurity Intelligence and Cybercrime, 4(2), 4-24. https://www.doi.org/10.52306/04020221NHPZ9033

IJCIC Center for Cybercrime Investigation & Cybersecurity

North Korean Cyber Attacks and Policy Responses: An Interdisciplinary Theoretical Framework

Jeeseon Hwang*, Seoul National University, South Korea
Kyung-Shick Choi, Boston University, U.S.A.

Keywords: North Korean cyber-attacks, cyberterrorism, criminological theoretical frameworks, the network theory of world politics, expert interview

Abstract:
This study conducts a qualitative analysis of the objectives, forms, current trends, and characteristics of North Korean cyber terror attacks and suggests a way to ensure further progress towards a successful international policy response. Despite the capricious changes that have recently occurred within the international political atmosphere, North Korea continues to constitute a threat to international stability through its ongoing advancement of nuclear weapons and long-range ballistic missiles. The difficulty of attribution and the relatively low costs associated with launching cyber offensives make cyber terrorism an attractive option for North Korea. In an effort to direct attention to these circumstances, this study aims to share explicit experts' perspectives in the field of cyberterrorism in South Korea. Consequently, the study purports to contribute to existing academic discussion and practices on cyber terror and cybercrime. Furthermore, this study adopts perspectives from criminological theoretical frameworks and the network theory of world politics to substantiate a more comprehensive view of North Korea's cyberterrorism which considers the multifaceted and asymmetrical nature of cyberterrorism within the context of postmodern international politics.

Introduction

Within the 21st century, cyberspace has become an area of importance in international security. Cyber offensives such as cybercrime, cyber-espionage, cyber-war, and "hacktivism" have become standard procedures for adversarial states and non-state actors to establish their calculated and contentious objectives. While cyber-attacks were originally deemed to have been perpetrated by individuals or unaffiliated organizations, state endorsed cyber offensives have also become widespread. The relatively low costs of launching offensives work in tandem with the difficulty of targeted actors to attribute the attacks to a particular actor and retaliate with a commensurate level of force in order to make cyber-attack an attractive option for pariah states that have limited military and economic resources. North Korea has reportedly developed advanced cyber warfare capabilities and its substantial workforce is allegedly involved in "the Internet's dark side activities" with the explicit support of the state (Kshetri, 2014). Despite the increase in threats to cybersecurity, the fact that there is no single definition of cyberterrorism in international society as well as in academia and in relevant international cases remains a prominent problem in terrorism studies (Kim, 2017). However, it is possible to extract certain characteristics from past attacks widely regarded as examples of cyberterrorism to reach a definition suitable for the purposes of this research.

*Corresponding author
Jeeseon Hwang, Department of Political Science, 1 Gwanak-ro, Gwanak-gu, Seoul, South Korea.

Email: k8hwang@snu.ac.kr

Choi et al. (2018) indicate that terrorism in cyberspace would be considered a criminal activity with organized actions and those who have a shared group identity to achieve their ideological goals. From this viewpoint, cases of North Korean cyber-attacks against institutions in other states involving highly trained North Korean citizens and an organized system can be defined as a form of cyberterrorism in addition to cyber-attack.

While the general North Korean population has restricted access to advanced Internet infrastructure, the country has a highly trained cyber army as well as a long history of launching cyber offensives upon other states. In 2009, North Korean assaults that derived from servers in Georgia, Austria, Germany, and the U.S., shut down computers in the presidential palace in Seoul for several days. On July 4 2009, hackers attacked servers in the U.S. Treasury Department and the Secret Service (Mauro, 2009; Warf, 2015). Similar Distributed Denial of Service (DDoS) attacks that occurred in 2011 afflicted the South Korean government and bank sites, and in 2012, South Korea's conservative JoongAng Daily was hacked. Following this sequence of cyber-attacks, on March 20, 2013, North Korea initiated waves of cyber assaults using malware against South Korean banks and broadcast stations. It was confirmed that North Korea incapacitated 48,000 computers and paralyzed networks. However, they tenaciously sought to conceal their digital trail and firmly denied involvement (Cho, 2013; Choe, 2013; Warf, 2015). In March 2013, North Korean hackers disabled numerous ATMs in Seoul, unleashing a malware known as Dark Seoul, which was designed to evade antiviral software. Similar onslaughts were reported against South Korea's presidential palace, military websites, the U.S. Treasury Department, and the Federal Trade Commission (Sang-Hun, 2013a, 2013b; Warf, 2015). These high-profile cyber-attacks have been accompanied by other attacks widely regarded as being perpetrated by North Korea. In many cases, the target of North Korea's cyber offensives has been South Korea. According to the Korean Ministry of Defense, hacking attempts against South Korean forces increased from 4,000 cases in 2017 to approximately 5,000 cases in 2018, and then ascended to 9,533 cases in 2019 (VoaKorea, 2020).

Although South Korea has often borne the brunt of North Korean cyber terror attacks, North Korean cyber-attacks also pose a threat to international security, with the United States also a main target of attack. The United States Department of Homeland Security (DHS) proclaimed that the North Korean government has been perpetrating cyber terror attacks on news agencies as well as on key infrastructure facilities, and the form of these acts of cyberterrorism have included destruction of data and data theft (Kim, 2017).

The rationale for North Korea's use of cyber war power as a strategic weapon is that it is cost-effective, easy to utilize, it spreads quickly, and it can cause huge repercussions. Moreover, there is no need for physical infiltration, anonymity allows for secrecy, and sanctions and retribution are difficult (Lee, 2009b; Lim et al., 2014). Considering these advantages, North Korea's use of the asymmetrical characteristics of cyberspace to further its economic and political agenda is only to be expected. Erlendson (2013) asserted as North Korea is integrating its cyber strategies into the whole military and national security strategy, cyber war power in North Korea is a strategic weapon and key resource for the state to reach its objectives (Lim et al., 2014). This makes it possible to conclude that the motivation and purpose behind the North Korean cyber terror attacks are within the parameters of the state's long-term policy objectives, and that the perpetrated cyber-attacks will multiply in number as well as in form in the future.

Consequently, a thorough analysis of North Korean cyber-attacks, along with a systematized policy response are necessary in order to mitigate the effects of further cyber-attacks. Unfortunately, there remains a general lack of academic discussion on North Korea's cyber-attacks. In an effort to direct attention to these circumstances, the current study utilizes criminological theoretical frameworks to conduct an analysis of the objectives, forms, current trends, and characteristics of North Korean cyber terror attacks, and suggests a way to ensure further progress towards formulating an international policy response. Assessing a nation's ability to project power through cyber means is problematic, primarily because it is largely attributed to the secrecy of those capabilities within government departments and the diffusion of responsibilities through those bureaucracies (Warf, 2015). Moreover, information related to North Korea's cyber policies is severely limited due to the country's reclusiveness, making reliance on the allegations of a select few defectors inevitable. It is also difficult to determine the validity of much of the information that has been disclosed thus far (Lee et al., 2016).

Recognizing that obtaining first-hand evidence can be quite difficult, this study utilizes a problem-centered expert interview approach to conduct a qualitative analysis of the North Korean cyber-attacks. It then moves on to suggest a path forward in international policy response. The study purports to contribute to existing academic discussions on cyber terror and cybercrime. In addition, it also adopts perspectives from the network theory of world politics to substantiate a more comprehensive view of North Korea's cyber-attacks which considers the multifaceted and asymmetrical nature of cyber-attacks within the context of postmodern international politics.

Theoretical Frameworks: Theoretical Applications

The development of the Internet has enabled private and non-state actors to perpetrate cyber-attacks against actors much more powerful than themselves. The North Korean government remains a top actor in the orchestration of cyber-attacks upon other states. This section applies the network theory of world politics to offer a more contemporary political context of North Korea's cyber-attacks. The findings will be used in the next section to analyze experts' individual views about policy response and to suggest a way of action that is currently not being addressed by states.

In light of the potential ramifications of cyber-attacks on international society, a closer examination of the motivations behind North Korea's cyber-attacks is necessary. Thus, analysis using the network theory of world politics is followed by elements of differential opportunity theory to describe the nature of North Korean foreign policy, North Korean subculture and ideology, and social learning mechanisms.

Network Theory of World Politics

The network theory of world politics provides perspectives about the concept of power that is crucial to the understanding of North Korea's cyber-attacks in an international setting and in the formulation of policy response. Political network analyses contribute to a shift of focus from a traditional institutional approach of the state to multi-sectoral policy arenas, which can refer to the emerging formation of a new kind of polity, a network state (Anttiroiko, 2015; Laumann & Knoke, 1987). When it comes to world politics, networks have been regarded as a mode of organization that facilitates collective action and cooperation, exercises influence, or serves as a form of international governance (Halfner-Burton et.al, 2009).

The theoretical aim of Castells (1996) was to present an analysis of the transformation of contemporary society as a grand theory, which adopted network logic as its explanatory scheme alongside informationalism and challenges the traditions of network analysis to reconsider the ways in which the network concept can be used in macro-level theorization (Anttiroiko, 2015). Analyzing power from the perspective of network theory, Rosenau (2005) used the term "Fragmegration" to describe the interaction of integration and fragmentation on the migration of authority as networked people versus public official who serve as nodes of authority. In addition, Kim's (2008a) analysis of network power, network state, and networkarchy suggests that the mechanism of power politics implemented by new network actors surpassing the meaning of material power, is owned by individual nodes (e.g., military, economic power) and is expanding into the dimension of immaterial power in the context of networks such as culture, norms, and diplomacy.

Approaching terrorism from a network standpoint can be an effective strategy to counter terrorism because it may reveal connections that were unrecognized such as identifying key actors and links (adversarial and cooperative), disentangling spatial proximity from organizational structures, and identifying how informational, human, and material resources may be leveraged (Stohl & Stohl, 2007). While physical terrorism only affects the specific place or area where the act took place, cyber terrorism has no spatial limits and the possibility that 'infrastructure,' social 'structure' and 'system', and 'operating principles' will become compromised continues to increase as cyber terror networks are comprised of multiple layers of networks (Kim, 2017). While the application of network analysis to terrorist networks allows for new policy proposals to dissolve those networks, it also highlights that blanket assumptions in regard to their form and function are too simplistic (Halfner-Burton et.al, 2009).

In an effort to lay out a comprehensive international cooperation framework in response to North Korea's cyber terror attacks, the current study adopts perspectives from Kim's (2008a) categorization of network power, in which power derives not from the attributes of individual nodes, but from the ties between nodes as well as from the network as a whole. Kim's framework categorizes network power into collective power, positional power and programming power. Collective power rests on the ability of larger networks to exert influence over smaller ones. Positional power derives from a particular position that a node occupies in a network. Programming power comes from the ability to set the rules of the game itself. These three concepts will be applied in the analysis of expert interviews.

Viewed from the network theory, North Korea can be regarded as a node from an international perspective, while simultaneously being a network in itself, albeit a highly centralized one. It operates on an isolated and controlled scale with a hierarchy similar to that which can be observed in Cloward and Ohlin's description of delinquent gangs. These gangs are organized hierarchically and members exhibit hostility and distrust towards representatives of the larger society (Cloward & Ohlin, 1960).

Differential Opportunity Structure in North Korea

Differential opportunity theory integrates the theoretical perspectives of the sources of pressure that may cause deviance and the way in which the social structure may regulate deviant solutions. In *Delinquency and Opportunity: A Study of Delinquent Gangs*, Cloward and Ohlin (1960) explore the reasons behind the development of delinquent norms.

The main argument of the differential opportunity theory is well represented in the quote below:

> *The disparity between what lower-class youth is led to want and what is actually available to them is the source of a major problem of adjustment. Adolescents who form delinquency subcultures, we suggest, have internalized an emphasis upon conventional goals. Faced with limitations on legitimate avenues of access to these goals, and unable to revise their aspirations downward, they experience intense frustrations; the exploration of non-conformist alternatives may be the result* (Cloward & Ohlin 1960, p. 86).

As the theory has originally been applied to individual members of discrete societies, applying these theories to international relations can cause issues with those who do not agree with comparing a state to an individual actor. In fact, in international relations, the notion of the state as an indivisible "billiard ball" has been criticized for its simplicity. However, the network theory of world politics allows for North Korea to be seen as an individual node in addition to being a highly centralized network. North Korea has a unique political system in which the state's goals are largely based on those of Supreme Leader Kim Jong-un. The system allows for criminological analysis in the sense that 1) the Supreme Leader's goals are unlikely to face open opposition and 2) the state's goals shape its cyber terror regime. Moreover, cyber-attacks as perpetrated by individuals differ from those perpetrated by those receiving compensation from a nation, as the latter may be seen as an instance of one nation directly compromising the security of the targeted nation. In this case, war is possible in accordance with the seriousness of the crime (Kim, 2017).

We have thus studied the theoretical applicability of North Korean cyber-attacks to select and draw upon the four factors of anomie, subculture, differential association, and North Korean cyber-attacks in more detail. The trend of cyber-attacks committed by North Korea includes the following three stages: anomie caused by the difference between legitimate purposes and means, the resulting sub-cultural creation, and differential association/learning that leads to the persistent development of more cyber-attacks.

Anomie in North Korea Foreign Policy

Durkheim emphasized the need for society to regulate the social goals of its members, to keep them within the limits of possible achievement, in order to avert tension, frustration, and consequent deviant behavior (Cloward & Ohlin, 1960). Durkheim (1897/1951) described anomie as occurring when human desires are not sufficiently regulated. Durkheim's conceptualization of anomie was built upon and revised by Merton (1938), who observed that anomie occurs when the balance between culture goals and institutional means is upset. Building upon this theoretical argument, Cloward & Ohlin (1960) asserted the pervasive feeling of position discontent leads individuals to compete for higher status and so contributes to the survival of the industrial order, but it also produces acute pressure for deviant behavior.

Terrorist organizations have traditionally rejected culturally recognized means to achieve socially accepted goals and have provided organizations in certain countries with different interpretations of these goals (cf. Schmidt, 2012) (Choi et al, 2018). When applying the concept of anomie in international relations, national power is not readily coordinated with a competent organization of legitimate, i.e., internationally defined and accepted, means. This results in the tendency to lean toward illegitimate state action that is not condoned by other members of the international society.

Historically, North Korea's foreign policy has not appeared to be overly influenced by international norms and regulations. Largely isolated from the international society and facing increasing sanctions, the legitimate means available for North Korea to reach its political or financial objectives are severely limited. This, in turn, leads North Korea to use illegitimate means (e.g., nuclear threats, money laundering) to achieve these goals. A dictatorship equipped with a lethal arsenal, unbounded by international norms, is especially dangerous (Cronin, 2014) with the development of IT. This continues to provide an easier channel for North Korea to make use of illegitimate avenues to pursue its goals.

Subculutre and Ideology of North Korea

The theory of differential opportunity indicates that the deviant individual who is unable to gather social support will have greater difficulty in establishing firm grounds for the defiance of the official system, due to needing the justification of their beliefs and social validation of the appropriateness of deviant acts (Cloward & Ohlin, 1960). Once the individual realizes insuperable discrepancies between goals and legitimate means, a subculture must form within in order for delinquency to develop. This subculture will begin to acquire a set of beliefs and values that rationalize the shift in norms as a natural response to a trying situation (Cloward & Ohlin, 1960). Therefore, this subculture becomes the basis upon which social values and norms shift to provide support for deviant behavior to develop.

North Korea's isolation has provided ample opportunity for a unique subculture to develop that preceded the development of IT and cyberspace. The most crucial elements of the delinquent subculture are the prescriptions, norms, or rules of conduct that define the activities required of a full-fledged member (Cloward & Ohlin, 1960). North Korea's foreign policy has focused largely on patterns of offensive realism, aggressive revisionism and hyper-nationalism, and these patterns are retained by strict party-centered recruitment, education, and promotion of diplomatic elites (Kim et al., 2019). These patterns of foreign policy have been upheld by the Juche ideology, a "man-centered ideology" which focuses on self-reliance. This type of ideology compels people to struggle against a hostile environment in order to turn it into a favorable one (Kim, 2011). North Korea's personal dictatorship is supported by this ideology in which the nation, the system, and the leader become one (Kim et al., 2019). After the death of Kim Il Sung, military-first politics began to function as the authoritative operating principle of North Korea. Thus, these two elements (Juche ideology and military-first politics) essentially assisted in justifying provocative actions such as ballistic missile and nuclear tests. Moreover, the development of the Internet makes cyber aggravation tactics more attractive. Part of the reason is that, compared with so-called "kinetic energy" actions (such as dropping bombs and firing bullets), cyber-attacks are anonymous, so it is difficult to attribute such attacks to a specific source (Kshetri, 2014).

Social Learning Mechanism in North Korea's Cyber Army

Although the formation of subcultures provides social and cultural justifications for deviant behavior, it is necessary for the behavior to be learned and passed down in order for deviant systems to emerge. The environment is key in order for the individual to acquire the values and skills, and a support system is necessary once the individual has taken on that particular role (Cloward & Ohlin, 1960). Social learning is a cognitive process in which one's character and environment are constantly participating in mutual interactions. The principal view of this theory is centered around group power that endorses criminality (Akers et al., 1979).

While this theory specifies how the rationalizations, norms, rules, and motivations of non-normative behavior are learned, it also defines the roles of positive and negative social mechanisms, all of which work to condition the "learner" toward or away from crime (Akers, 1985, 1992; Bandura, 1977; Winfree et al., 1994). North Korea continues to develop and invest in an elite cyber force under the control of its military, the Korean People's Army, and the Reconnaissance General Bureau — Kim Jong Un's clandestine security apparatus (Ioanes, 2020). In fact, since the mid-1980s, this state established Mirim College, Moranbong College, among others, in which they train people to become professional hackers to enhance their cyber-attacking capabilities (Boo, 2017). Dominant roles within delinquent subcultures often require the performance of deviant behavior (Cloward & Ohlin, 1998). Those who succeed will become cyber-soldiers secretly located in East Asia, the Middle East, and South America, where they will perform cyber missions directed by the state (Kim &Yang, 2020). These cyber-soldiers are identified as threats to international security. For instance, a cyber-soldier named Park Jin Hyok, was charged with executing high profile cyberattacks such as the 2017 WannaCry ransomware attack and the 2014 hack of Sony Pictures ("FBI Charges", 2018). While North Korea denies any connection with this cyber-soldier and the attacks and attribution is difficult due to the nature of cyber-attacks, this example illustrates how the development of a subculture encourages learning by individuals who agree with the norms of that subculture.

As illustrated above, applying the concepts of anomie, subculture, and social learning is conducive to forming a better understanding behind North Korea's motivations for cyber terror activities. North Korea lacks legitimate methods to achieve its national goals, which in turn, leads the state to use illegitimate means to achieve their objectives. The continued isolation of North Korea has created abundant opportunities for subcultures imposed by ideology to develop where their norms differ from those recognized by the international community. In addition, North Korea's social learning mechanism creates more learning opportunities through differential association where members accept and perform these norms. As a result, a well-trained cyber army continues to grow and execute cyber terrorist attacks directed by the elite in North Korea.

Methodology

This research utilizes a semi-structured expert interview approach to examine the ways in which experts in the fields of information security and cybercrime perceive North Korea's cyber-attacks. The responses are then analyzed using the theory of differential opportunity and the network theory of world politics as conceptual frameworks, the former helping to explain motivations and patterns of North Korean cyber terror attacks and the latter providing implications for a way to regulate and counter these attacks.

Qualitative interviews were conducted with eight national and information security experts in South Korea who were selected through a snowballing technique. Initially, four experts were asked and agreed to participate in the study: a professor in the field of cybercrime, an expert from the National Intelligence Service, and two police officers. These four participants were chosen based on a purposive sampling methodology. The selection criteria were based upon the relevance of their work to addressing North Korea's cyber-attacks. All initial experts had at least ten years of experience in their respective fields, which included national security, cyber-terrorism and internet security. The original participants referred to other experts who were then contacted to participate in the study. The final sample consisted of two professors in cyber-crime/information, two experts at the National Intelligence service, and four experts in the police force, all of whom have knowledge and experience with cyber terrorism. This sample was made up of seven males and one female, and there also existed variation in the years of experience, ranging from ten years of service to more than twenty years of service.

The interview guide was structured so as to obtain responses about the trends, motivations and impacts, the strengths and weaknesses of current prevention efforts, effective prevention strategies and suggestions to policy makers. The initial questions were designed to be open-ended. These were followed by more structured questions to guide responses more specific to the study. An interview with an application for permission to use the research with anonymity was sent to each participant by the first author. Interviews were then scheduled according to the availability of the experts, and interviews were conducted during a period of two months. Experts who consented to participate in the research were informed of the purpose of the study and the process. Confidentiality and anonymity of the responses were guaranteed and there were no marks in the interview questions to identify the personal information of the respondents. All interviews were conducted through an online conference platform or email due to COVID-19. All relevant responses were transcribed and used as a part of the analysis process after the interviews.

Policy Analysis via Expert Interviews

This study explores motivations and trends of North Korean cyber terror attacks and analyzes the common stances that experts take in regard to deterrence of these cyber terror attacks. After interviewing a total of eight experts, the data collected was then subjected to a two-level analysis. With regard to motivations and trends, the theory of differential opportunity, and in particular the concepts of anomie, subculture and social learning formed the theoretical framework upon which the responses were analyzed. After the initial analysis, a secondary, more intensive analysis was conducted with regard to policy formulation. The network theory of world politics, and in particular the three concepts of collective power, positional power and programming power formed the basis upon which the responses were analyzed. The results of the analyses are presented below.

Criminological Explanations of North Korean Cyber-Attacks: Motivation

The theory of differential opportunity focuses on situations in which actors internalize conventional goals but are unable to realize them legitimately. Faced with limitations on legitimate avenues of access to these goals, and unable to revise their aspirations downward, they experience intense frustrations; the exploration of non-conformist alternatives may be the result (Cloward & Ohlin, 1960). Viewed from the conception of anomie, North Korean cyber-attacks are not merely statements of belligerence or self-defense tactics. Rather, they reflect the strategic interests of the state when rising sanctions and international isolation provide few avenues to realize them.

Experts recognized that the conventional goals of state power and wealth inspired North Korea to develop its cyber terrorist regime. It is commonly believed that the evolution of the Internet provided a new avenue for illicit activities that North Korea had a long history of being complicit in, and the purpose of obtaining confidential information transitioned to the objective of earning financial benefits. All of the interviewed experts agreed that monetary gain in particular was a strong driving factor of North Korean cyber-attacks. Several quotes illustrate this particular viewpoint:

> After 2011, North Korea has begun to use its hacking abilities to attack the private sector and to gain financial benefit. The targets of attack also spread out from the Korean peninsula, with the Sony Pictures attack of 2014, the Bangladesh Heist of 2016 and WannaCry of 2017 being the main cyber-attacks from North Korea (Expert 2, personal communication, March 13, 2021).
>
> North Korea's cyber-attacks began as methods to obtain confidential information about South Korea's military and security programs but have become more diverse to include gambling, finance and virtual currency, a change which stems from their need for information but also for economic gain (Expert 4, personal communication, March 18, 2021).
>
> Before 2017, North Korea's motivations for cyber-attack were mostly because of need for information but have since expanded to attacks on virtual currency trade centers and financial institutions, and the targets of attack have changed from North Korean related targets such as government officials and defectors to a more general target (Expert 6, personal communication, March 26, 2021).
>
> Based on the characteristics of the malignant codes and the methods of attack, security service centers Lazarus, Kimsuky and APT37- while in the past cyber terror attacks had the goals of theft and destruction of information, current trends see the rise of APT attacks aimed at obtaining foreign currency (Expert 8, personal communication, March 26, 2021).

In addition to confirming that the concept of anomie in the theory of differential opportunity holds in the case of North Korea, the responses formulated by experts show that motivations behind cyber terror can arise from changing state goals. While information was given precedence in the past, current trends illustrate the role of financial opportunity in pushing cyber terror attacks forward, with many experts mentioning bitcoin hacking and ransomware attacks. Cyber-attacks such as Ransomware are executed for the purpose of procuring funds for the North Korean government and for further development of nuclear weapons. Ransomware attacks can inflict even wider destruction when compared to pharming malware. Since 2017, ransomware continues to be on the rise and must now be seen as a major form of North Korean cyber terror. In addition, for victims recovering from ransomware attacks has become increasingly expensive. Moreover, ransomware -related cybercrime costs are expected to exceed $20 billion this year, with a new ransomware attack launched every 11 seconds (Solomon, 2021). Inevitably, monetary loss due to ransomware is only expected to increase in the future.

North Korea's Subculture and Social Learning System

The responses pertaining to understanding of North Korea's subculture and social learning system were less robust compared to the concept of anomie, which could be more easily observed by analyzing trends of cyber-attacks from outside of North Korea. This was largely due to the reclusive nature of the state and the difficulty of knowing with any degree of accuracy the inner workings of North Korea's subculture and social learning apparatus:

> North Korea's cybercrimes are dangerous because of the difficulty of assessing potential damages due to uncertainty about the exact extent of its cyber army and technology (Expert 6, personal communication, March 26, 2021).

> Focus on cyber terrorism is mainly limited to prevention and response to cyber-attacks on national security, thus focusing on the surface of the issue… the activities [related to cyber-attacks] are not well known and thus rather obscure (Expert 6, personal communication, March 26, 2021).

However, the responses in general showed that experts were aware of the social accepted status of cybercrime in North Korea's particular subculture as well as of the social learning system in place to perpetuate the norms of the subculture:

> North Korea, in addition to its State Security Department, United Front Department and the Reconnaissance Bureau has also established a team of hackers in its Ministry of Social Security, which is equivalent to the police force (Expert 1, personal communication, March 1, 2021).

While an extensive amount of accurate information about North Korea's cyber-soldier program is difficult to obtain, it has widely been accepted that North Korea's Ministry of Social Security has established a hacker training center, ostensibly a research center, near the Institute of Natural Science and is training 100 people from Kim Il-Sung University, Kim Chaek University of Technology and selected students from high schools (Kim, 2021). Out of the three forms: criminal, conflict and retreatist subcultures defined in the theory of differential opportunity, the experts' responses showed that North Korea's subculture most closely resembles that of a "criminal subculture", a type of gang devoted to theft, extortion, and other illegal means of securing income (Cloward & Ohlin, 1960).

Moreover, it has been noted that North Korea handpicks teenage computer talents and actively trains and sponsors them, thus creating elite cyber-soldier army. The selection of cyber-soldiers begins at Pyongyang No. 1 Middle School, an elite educational institution whose curriculum is consistent with South Korea's national high school curriculum ("Pyongyang no.1", 2007). Selected talents from the No. 1 senior-middle school continue to receive elite IT education at Geumsung No. 1 and No. 2 senior-middle school's 'specialized computer programs', where those who stand out continue on as cyber-experts at Kim Il-Sung University, Pyongyang University of Computer Science, Pyongyang University of Science and Technology, and Hamhung University of Computer Technology (Kim & Yang, 2020). The most talented are selected for more specialized training and then deployed to hacking units. The competitive selection process of cyber-soldier creation increases the prestige associated with securing a role in the cyber-soldier army and provides strong incentives for North Korean citizens to internalize their new roles through social learning while creating a subculture in which becoming a cyber-soldier is an elite privilege given only to the most talented.

The Network Theory of World Politics: Best Practices in Policies

While there has been an abundant amount of research done on terrorism and network power in international relations, the network perspective has rarely been utilized to provide policy implications in the area of cyber-attacks. Thus, this study utilizes the network theory of world politics as a guide to build effective policies specifically aimed at deterring North Korea's cyber-attacks, which are widely regarded as a form of terrorism.

Inter-Agency and International Cooperation

Kim (2008) viewed network power as a functioning upon three mechanisms: the ‘actor’, the ‘process’, and the ‘system’. The ‘actor’, the first face of network power, may act as a ‘networker’ that gathers nodes together. Power exercised by the ‘actor’ functions much like collective power, in which the scale of the network itself or the number of nodes in the network determines how powerful it is (Kim, 2008). The viewpoint of network power as collective power implies that larger networks with more powerful nodes can exert power over other nodes or networks. However, collective action between nodes in a network is a prerequisite in order for this power to function. Networked collective action, whether transnational networks of activists or illicit combinations of criminals or terrorists, may demonstrate greater capacity than its organizational competitors (Kahler, 2010).

In international relations, it can be difficult to arrive at an agreement where collective action is possible. However, network power of international organizations/treaties is emphasized with regard to international cooperation. Halfner-Burton & Montgomery (2006) found that membership in international organizations partitions states into structurally equivalent clusters and establishes hierarchies of prestige in the international system. In the area of counterterrorist policy regulation, however, there has yet to be a ‘networker’ that has the power to gather many nodes and exert enough collective network power to deter North Korea’s cyber-attacks. This is mainly due to cyber-attacks being relatively new and because there is no single agreement even within single states as to how to legislate against cybercrime. Moreover, attribution of cyber-attacks remains difficult because even when an attacker is identified, it is not always possible to determine whether the motivation behind the act arose from individual motives or an orchestrated attack from a state. Thus, it is difficult for states to justify retaliation against states and not individuals and to reach an international agreement in the area of cybersecurity.

While an international agreement has been difficult to reach, it can be seen from the interview responses that many experts agree that international cooperation is necessary. Indeed, most of the solutions suggested by the experts during the interview rested upon an urgent need for collective power in the international sphere, as shown by the following quotes:

> A continued state of vigilance by global corporations and foreign governments as they upgrade their cybersecurity systems must be kept in conjunction with international consensus about cybersecurity no longer being the problem of a single nation (Expert 2, personal communication, March 13, 2021).
>
> There have been international efforts to jointly deter cyber terror as can be seen in the Convention on Cybercrime. However, the varying legal systems and situations of countries mean that many countries including South Korea have not joined this agreement, which is problematic (Expert 2, personal communication, March 13, 2021).
>
> Cyber-attacks often go through foreign servers, making international cooperation necessary. In order for international cooperation to be facilitated, there needs to be a cooperation mechanism between states (Expert 7, personal communication, March 26, 2021).

States such as North Korea that have internalized a delinquent subculture are not likely to abide by rules even if they are agreed upon. However, international cooperation can facilitate the monitoring and regulation of illicit cyber activities.

Many efforts have been made by international organizations such as the United Nations (UN), International Telecommunication Union (ITU), Organization for Economic Cooperation and Development (OECD) and the North Atlantic Treaty Organization (NATO) to reach a consensus about appropriate rules for cyber behavior. Agreements that have been reached so far have not played pivotal roles in the regulation of cyberspace. Internet Corporation for Assigned Names and Numbers (ICANN) is a global governance model of private-public partnership since it has been governed by an international board of directors drawn from across the Internet's technical, business, academic, and other non-commercial communities (Kim, 2014).

Suspicions of ICANN being a tool of de facto U.S. hegemony among other problems have prevented it from creating a profound change. The discrepancy between the common interest in international cooperation and the mechanisms of actual cooperation between states has been causing difficulty for collective power to be exercised. Furthermore, respecting the acceptable boundaries of privacy conflicts while ensuring a high degree of cybersecurity, makes it difficult for states to act as 'networkers' even within their own boundaries. This second problem will be mentioned more deeply in relation to 'programming power'.

Aligning Response through a Centralized Control Center

The second face of network power is the 'system', in which power derives from the organization and principles of the network itself, with a 'programmer' designing the rules of the game (Kim, 2008). The "Washington Consensus" is a classic example of programming ability in action, and the controversial "Beijing Consensus" is often used to illustrate how China builds its own programming ability in areas traditionally controlled by Western countries. Cybersecurity continues to lack a single 'programmer' and remains unclear whether the current discourse will allow for the rules of the game to be set by a unitary actor.

Unlike traditional power, 'programming power' can also be exercised by less powerful actors. Kim (2014) analyzed middle powers exercising programming power and indicated that their power is concerned with the ability to complement and possibly renovate the whole system, designed by world powers. Due to South Korea's geographical proximity and shared history with North Korea, it has the potential to exercise programming power as a middle power. This would provide system adjustments/adaptations that increase interoperability/compatibility, while reinforcing normative values and legitimation (Kim, 2014). Nevertheless, the lack of unified policy and unstable relations with North Korea continue to prevent South Korea and other states from realizing this potential. Due to the rapid development of technology and mercurial techniques of cyber-attacks, cyber security and cyber terror rules have yet to be established completely in many states. Thus, deciphering which actors are able to exercise programming power to deter cyber terror remains unsolved. As mentioned above in the case of North Korea, the creation of a hierarchical system of cyber warriors and party affiliation means that the rules of the game can also be determined by the party.

In other states, such a high level of centralization is difficult to reach. Nevertheless, experts have proposed several ways in which a certain level of centralization can be reached, thus allowing the state to exercise programming power in determining the rules of the game within their respective jurisdictions.

> National policies to increase investment in related sectors as well as active talent cultivation and improvement of awareness in the public and private sectors are necessary, and most of all there needs to be a central organization that can connect and control these separate areas (Expert 6, personal communication, March 26, 2021).

> Cyber terror response at a national level can be positive in that quicker and systematic response is possible, a national and social safety net can be constructed, and there is possibility of this becoming an advanced industry. However, costs due to administrative factors and certain regulations can also arise (Expert 3, personal communication, March 13, 2021).
>
> Granted, in the area of internet technology a certain amount of decentralization is necessary in order to facilitate innovation and growth. In the field of cybersecurity, there is more need than ever for the state to be able to exercise a certain amount of programming power. This is because the threat to security eventually determines predominance in competition between states in military, economic and social areas (Expert 3, personal communication, March 13, 2021).

Creation of a central oversight organization while ensuring that issues such as privacy are respected requires the rules of the game to be crafted in a way that enhances efficiency while not compromising values upheld by private and public networks.

Mediating Exchanges through Strategic Positioning

Kim (2008) asserted that the 'process,' the third face of network power, focuses on the role of a 'switcher', which controls the level of access between networks. A structural analysis of networks equates the power of a particular node to its position in the network, defined by its persistent relationships with other nodes (Halfner-Burton et al., 2009). A concept central to the idea of positional power presented in the study is the structural idea of centrality. Freeman (1978) substantiated the idea of positional power by defining nine centrality measures based on the three conceptual foundations of degree, closeness, and betweenness.

While degree centrality measures the amount of access a node has to other nodes, closeness centrality relates to the length between nodes. Degree, closeness and betweenness centrality in relation to cyber-attacks are not proportional to the physical positions of the nodes. Rather, betweenness centrality corresponds to the number of shortest paths in the network that pass through a particular node, thus, measuring the dependence of a network on a particular node for maintaining connectedness (Halfner-Burton et.al, 2009).

A node with a high degree of betweenness centrality is at a structurally strategic position which allows it to play the role of broker either between nodes, between networks, or between networks and nodes. By bridging structural holes, brokers occupy central positions in a network structure, acting as nodes through which multiple transactions coalesce (Burt, 1992; Kim, 2014). Though the node itself might not have power in its degree and closeness centrality, brokerage allows the node to translate between different systems and thus gives it positional power in a network. Furthermore, brokerage may alter network structures, leaving actors with a fundamentally different set of network ties, and changing the agenda in a network (Kim, 2014).

The international status of positional power is not conducive to preventing North Korea's cyber terrorist activities. From a geopolitical point of view, China can promote exchanges between North Korea and other countries, thereby occupying a position with highly concentrated betweenness centrality. However, the current tensions between the U.S. and China make it unlikely for China to participate actively in U.S.-led international cooperative efforts to deter cyber-attacks from North Korea. The difficulties in making use of betweenness centrality is not limited to traditional diplomatic relations between countries. The decentralized nature of cyberspace provides an environment in which the state is still the central node, but many other nodes also face high stakes.

In such a decentralized network, it is difficult for hubs to make an appearance. As a result, it is more difficult to see clusters of nodes that appear relative to single nodes or clusters. Thus, occupying a single position no longer necessarily means that a node will have high positional power. Identifying the gaps between nodes or networks and trying to connect these gaps imbue the nodes with a certain amount of power. If this does not oppose the trend of cyber-attacks, it will create waves and can slowly shift the trend.

One way in which a state can exercise positional power is to play a brokerage role between the disparate networks of information and security. As the following quotes show, many experts are aware that it is common for cyber terror attacks as security issues and to respond to these attacks as such. However, many cyber terror attacks rely upon information from the public and private sectors, so a unified response is made difficult.

> As for national security, the National Cyber Security center, the Korean National Police Agency Cyber Bureau, R.O.K. Cyber Command prepare to deter North Korean cyber-attacks, but as for the public, the responsibility of protection falls first to the Korean Internet& Security Agency, making response less effective when the attacking force is North Korea (Expert 2, personal communication, March 13, 2021).

> Although government organizations are being set up, education is being reinforced and the physical defense system of separation between internal and external networks is being strengthened, hacking due to outflow of personal information from emails, and cellphones continues (Expert 4, personal communication, March 18, 2021).

> Active surveillance of cyberspace is necessary, yet the changing political landscape makes this difficult… Surveillance of cyberspace relates to information practices, so it is difficult to arrive at an efficient response just using criminal law (Expert 2, personal communication, March 13, 2021).

These statements illustrate the difficulties that a nation may face when attempting to act as a broker between the two networks of information and security. When these two are viewed as disparate and managed differently, the hybrid nature of cyber terror complicates appropriate response. However, when the two networks of information of security can be connected by governmental policy or organizational reform, a more unified front can be presented, thus equally addressing the issues of national security and individual privacy.

In terms of Internet infrastructure, states must also be able to play the role of broker between internal and external internet networks, thus controlling the flow of information. The following quotes illustrate how a two-pronged approach in which the connection between internal and external networks may be controlled and managed to reach more efficient response.

> In order to strengthen the security of internal computer networks, which are the ultimate goal of the attacker, strengthening the security of the connection point between internal and external networks can prevent or extend the infiltration of internal networks, giving administrators more time to perceive the problem (Expert 5, personal communication, March 26, 2021).
>
> Primarily, a sort of fence in which international and national minimal security measures are realized, and flexibility in which each sector of society has a tailored response in accordance with their situation is needed within this fence (Expert 3, personal communication, March 13, 2021).

Thus, from the perspective of positional power, a state may play the role of broker by mediating exchanges between security and information networks as well as controlling changes between internal and external internet networks.

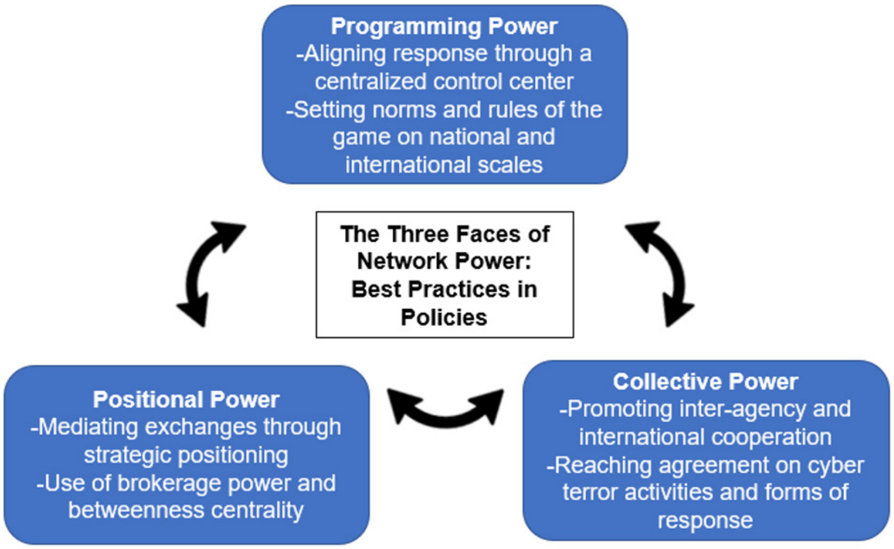

Programming Power
-Aligning response through a centralized control center
-Setting norms and rules of the game on national and international scales
The Three Faces of Network Power: Best Practices in Policies
Positional Power
-Mediating exchanges through strategic positioning
-Use of brokerage power and betweenness centrality
Collective Power
-Promoting inter-agency and international cooperation
-Reaching agreement on cyber terror activities and forms of response

Figure 1. Best Practices in Policies Regarding North Korean Cyber-Attakcs.

Policy Implications and Discussion

Analysis from the perspective of the network theory of world politics as well as insights from experts in cybersecurity showed that policy needs to focus on the ability of governments to exercise positional, programming, and collective power. Collective power suggests policy response in the direction of creating comprehensive legal frameworks and forming stronger international agreement on response to cyber terror. Programming power suggests that governments include the public and private sectors when forming policy to deter cyber-attacks and to set the rules and norms of the game when it comes to cyber terror. Positional power suggests that governmental organizations or officers act as brokers between different networks, for example between the networks of information technology and security in order to more effectively respond to cyber terror attacks. These policy implications can be categorized into legal frameworks and international cooperation, incident response and education.

Legal Framework and International Cooperation

Despite efforts to the contrary, most countries do not have a comprehensive legal framework that stipulates regulations regarding cybercrime. South Korea's legal system regarding cyber-crime is one example. Rather than a comprehensive law that incorporates the entirety of cybersecurity, there are individual public and private laws that have less effect. The Cybersecurity Act, which was signed into law by the South Korean government in 2017, lost effect with the end of the term of the 20th congress. Laws pertaining to the public sector while stipulated in individual laws include the Framework Act on National Informatization and the Act on the Protection of Information and Communications Infrastructure. Legislation pertaining to the private sector of society include the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. as well as the Electronic Financial Transactions Act (Kim & Yang, 2020). The fragmented legislation between public and private sectors as well as the area of national security prevents the government from more effectively responding to cyber-terror attacks. In addition to a comprehensive law that incorporates elements from the whole of cybersecurity, there needs to be a stipulation ensuring continuity of the law despite changes of government and congress.

International cooperation has been similarly difficult to reach. Experts noted that cyber-attacks are becoming more directly related to relations between different countries:

> Hacking, which in the past was done mainly by individuals or small groups with aims of money, glory and technological sense of superiority, has become a form of attack and defense in the dimension of cyber security with larger groups, organizations and states behind the attacks (Expert 3, personal communication, March 13, 2021).

As of now, there is no comprehensive international cyber terror law that has legal effect. Past efforts by international organizations, including the Tallinn Manual which showed international agreement but failed to exercise legal power, have been conducted mainly in terms of normative approaches. However, without the support of more states and efforts to strengthen the power of international agreements, states will continue to be unable to exercise collective power on an international scale. In efforts to ensure that the costs of cyber-attacks outweigh the benefits, governments around the world could benefit from implementation of an arms control policy within cyberspace. Implementing a policy like this can help to establish an agreement between nations in efforts to help diminish criminal acts within the cyberworld (Lee & Choi 2021; Nye 2015).

Public Awareness and Cyber Ethics Education

Another policy objective lies in public awareness and education buttressed by technical support. Experts emphasized the importance of public awareness about cyber-attacks:

> North Korea tends to use phishing mails and phishing sites intended to retrieve information about the target of attack and uses this information to execute APT attacks, overtaking internal systems and stealing confidential information and monetary goods.
>
> Phishing using social engineering tactics is often used, making it harder to detect. Special attention must be paid even to simple tasks like checking emails (Expert 8, personal communication, March 26, 2021).

> In the case of cyber terror, citizens and more widely the public are included in the beginning information collection stages, and when looking at just one section the whole entity becomes harder to perceive… in the case of cyber terror, information collection and damage occurs on a long timescale (Expert 6, personal communication, March 26, 2021).

While public awareness has been recognized as crucial to preventing cyber-attacks more effectively, not enough is being done to raise that awareness. Educating the public about the importance of protecting wireless home networks with secure passwords can potentially minimize the risk of cyber terrorist attacks (Choi, 2015). While the Association of Information Technology Professionals (AITP) and the Association of Computing Machinery (ACM) have codes of ethics containing ethical rules governing the application of computer practice, they have no legal power to improve their execution. Therefore, cybercrime awareness courses should also consider cybercrime laws and regulations to increase awareness and support for laws against cyber-attacks.

Proliferation of cyber ethics norms both nationally and internationally can also aid efforts to deter cyber-attacks. Establishing a mandated ethics program and reinforcement is necessary to insulate and maintain appropriate cyberspace behaviors for the next generation of computer users (Choi, 2015). Although cyber ethics standards are unlikely to become widespread, efforts to establish stricter standards for executing programming power can make states more legitimate to respond to cyber-attacks. In addition, the possibility of integrating elements of cyber ethics into legislation and frameworks for international cooperation should be examined, and teaching ethics must always be accompanied by real-world applications.

Incident Response Policy

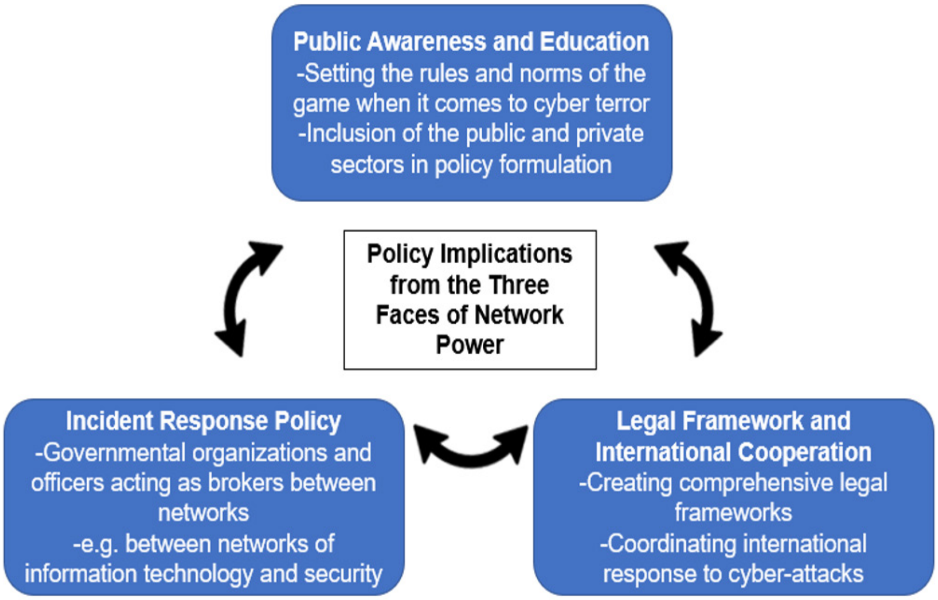
The results of this study have shown that North Korean cyber terror attacks can result in massive damage in a short span of time. While long-term policy goals such as constituting legal frameworks as well as encouraging public awareness about cyber terror are important, immediate measures must be taken to ensure that states can respond to cyber terror attacks that are already taking place. Several quotes from experts show that the capabilities of officers can be necessary to ensure an agile response to cyber terror attacks.

> In addition to constructing hardware and software security technology, we need chief security officers in each institution to make sure that these technologies and policies are being used (Expert 3, personal communication, March 13, 2021).

> Policies regarding the saving of digital forensic evidence and experts to analyze this evidence are necessary in order to provide quick detection of the nature of the attack, the magnitude of devastation and formulation of adequate response after a cyber-attack occurs (Expert 5, personal communication, March 26, 2021).

As described from the quotes above, technical knowledge is necessary to effectively deter and respond to cyber-attacks at any job level in the field of cybersecurity. While recommendations to government agencies provide a method to prevent cyber-attacks, it assumes that employees already have sufficient technical knowledge (e.g., how to patch systems, create back-up files) (Choi et al., 2021).

Unfortunately, most law enforcement officers lack the necessary skills and knowledge to conduct effective cybercrime investigations. Specialized cybercrime investigation training programs are warranted to meet the needs of local/state law enforcement agencies, and technical seminars are needed to ensure regulations can be implemented in advance to respond to cyber terrorist attacks. In addition, collaboration between disciplines and transnational cooperation can help to combat the problem of technology-facilitated crimes in this novel field of cybercrime research. Future studies should be reactive and proactive when investigating, predicting, and examining the effects/origin of cybercrime utilizing information, technology, and global collaboration (Choi, 2021).



Public Awareness and Education
-Setting the rules and norms of the game when it comes to cyber terror
-Inclusion of the public and private sectors in policy formulation

Policy Implications from the Three Faces of Network Power

Incident Response Policy
-Governmental organizations and officers acting as brokers between networks
-e.g. between networks of information technology and security

Legal Framework and International Cooperation
-Creating comprehensive legal frameworks
-Coordinating international response to cyber-attacks

Figure 2. Policy Implications from the Three Faces of Network Power.

Conclusion

This study examined the motivations, current trends, and characteristics of North Korean cyber terror attacks utilizing two different theories. Elements from the theory of differential opportunity included anomie, subculture, and social learning, which were used to analyze the origins and motivations of North Korean cyber-attacks. Insights from the network theory of world politics provided a basis to frame governmental policy response to North Korean cyber terror attacks. The concepts of collective power, positional power, and programming power were used to suggest further policy direction. The two interdisciplinary theoretical perspectives were then used to analyze expert interviews, thus forming a comprehensive understanding of current North Korean cyber-attacks as well as steps forward.

This paper has contributed to prior research by integrating theories from criminology and international relations into one comprehensive framework and analyzing interviews from experts in the area of cyber security to provide validity and specificity to our theoretical approach. This study also has several limitations.

The sample size of experts available for interview was comparatively small at eight experts, and the continued spread of COVID-19 prevented the researchers from conducting face-to-face interviews that could have facilitated closer communication between the interviewer and interviewees. Future studies that incorporate a large sample size of experts can contribute to generalization of the results found by this study.

Conflict of Interest

The authors declare that they have no conflict of interest.

Funding

The authors did not receive support from any organization for the submitted work.

Ethical Approval

All procedures performed in this study involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards.

Informed Consent

All participants provided informed consent.

References

Akers, R. L., Khron, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979). Social learning and deviant behavior: A specific test of a general theory. *American Sociological Review, 44*(4), 636-655.

Anttiroiko, A.V. (2015). Castells' network concept and its connections to social, economic, and political network analyses. *Journal of Social Structure. 16*(11), 18.

Boo, H. (2017). An assessment of North Korean cyber threats. *The Journal of East Asian Affairs, 31*(1), 97-117.

Choi, K. S. (2021). The driving force behind cybercrime: Cyber resilience and cybercriminology. *Journal of Contemporary Criminal Justice,* 1-3.

Choi, K.S. (2015). *Cybercriminology and Digital Investigation.* LFB Scholarly Publishing.

Choi, K.S., Lee, C.S., & Cadigan, R. (2018). Spreading Propaganda in Cyberspace: Comparing Cyber-Resource Usage of Al Qaeda and ISIS. *International Journal of Cybersecurity Intelligence & Cybercrime. 1*(1), 21-39.

Cloward, R. A., & Ohlin, L. E. (1960). Delinquency and Opportunity: *A theory of delinquent gangs.* Free Press.

Cronin, P. M. (2014, December 07). North Korea's Cyber Security Strategy. *The Dong-a Ilbo.* https://www.donga.com/en/article/all/20141207/409646/1/North-Korea%C2%92s-Cyber-Security-Strategy

Durkheim, E. (1897/1951). *Suicide: A study in sociology.* (J.A.Spaulding&G.Simpson, Trans.). New York, NY: The Free Press.

FBI Charges North Korean Park Jin Hyok over Wannacry, Sony Cyber Attacks. (2018, September 7). *AP Reuters*. https://www.abc.net.au/news/2018-09-07/fbi-announces-charges-against-north-korean-sony-hacker/10212078

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks,1*(3),215-239.

Hafner-Burton, E. M. & Montgomery, A. H. (2006). Power positions: International organizations, social networks, and conflict. *The Journal of Conflict Resolution, 50*(1), 3-27.

Hafner-Burton, E. M., Kahler, M., & Montgomery, A. H. (2009). Network analysis for international relations. *International Organization 63*,559-592.

Ioanes, E. (2020, June 17). Kim Jong Un has quietly built a 7,000-man cyber army that gives North Korea an edge nuclear weapons don't. https://www.businessinsider.com/north-korea-kim-jong-un-cyber-army-cyberattacks-nuclear-weapons-2020-6

Kim, H. (2017, June 16). Mi, saibeo gonggyeok judojaro bukan jimok [U.S. Attributes Cyber Attacks to North Korea]. *Daily Security*. https://www.dailysecu.com/news/articleView.html?idxno=20987

Kim, J., Park, H., Oh, K.& Han, K. (2019). Bukan oegyojeongchaek: jeongchaekpaeteongwa bukaegoegyoplsaryebunseok [North Korea's Foreign Policy: Policy Patterns and Analysis of North Korean Nuclear Diomacy]. *Korea Institute for National Unification Report* 19-14.

Kim, M. (2021, February 11). "Namhan eunhaeng mojori teoreora" donjul mareun bukhan, ireon haeking timkkaji [North Korea Establishes a Hacking Team to Solve its Funding Problem]. *Chosun Ilbo*. https://www.chosun.com/politics/north_korea/2021/02/11/SZSUMEV5DFGEDNZ22SZGJ7NPOY/

Kim, S. (2008). The world Politics of network power: Beyond traditional theories of power in international politics. *Korean Political Science Review, 42*(4), 387-408.

Kim, S. (2014). Cyber security and Middle Power diplomacy: A network perspective. *The Korean Journal of International Studies, 12*(2), 323-352.

Kim, S. (2017). Four neighbouring network-states and South Korea in cyber security: Network structure of powers and strategies of a Middle Power. *The Korean Journal of International Studies, 57*(1), 111-154.

Kim, Y. (2011). *North Korean Foreign Policy: Security Dilemma and Succession*. Lexington Books.

Kim, Y. (2012). How to approach the state-sponsored cyber terrorism? Be emphatic about the necessity for Jus ad Bellum and International Security Regime change. *Journal of Global Politics, 5*(2), 117-153.

Kim, Y., & Yang, C. (2020). A Study on the improvement of legal system for cyber terror response in North Korea. *European Constitution Journal*, *33*, 355-384.

Kshetri, N. (2014). Cyberwarfare in the Korean Peninsula: Asymmetries and strategic responses. *East Asia*, 31, 183–201. https://doi.org/10.1007/s12140-014-9215-1

Lee, H & Choi, K.S. (2021). Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. *Victims & Offenders, 16*(3), 363-384.

Lim, J., Kwon, Y., Chang, G., & Baek, S. (2014). North Korea`s cyber war capability and South Korea`s national counterstrategy. *The Quarterly Journal of Defense Policy Studies, 102*, 9-45.

Mathews, L. (2020, Jan 26). Average Cost to Recover from Ransomware Skyrockets To Over $84,000. *Forbes*. https://www.forbes.com/sites/leemathews/2020/01/26/average-cost-to-recover-from-ransomware-skyrockets-to-over-84000/?sh=2502a8d713a2

Mathews, L. (2020, July 29). North Korea-Linked Hackers Are Now Spreading Their Own Ransomware. *Forbes*. https://www.forbes.com/sites/leemathews/2020/07/29/north-korea-hackers-lazarus-vhd-ransomware/?sh=1feb20105b11

Merton, R. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672-682.

Nwalozie, C. J. (2015). Rethinking subculture and subcultural theory in the study of youth crime - A Theoretical Discourse. *Journal of Theoretical & Philosophical Criminology, 7*(1), 1.

Pyongyang No. 1 Senior-middle School, the Most Elite Training Institute in North Korea. (2007, October 22).
Daily NK. https://www.dailynk.com/english/pyongyang-no-1-seniormiddle-school/

Rosenau, J. N. (2005). Illusions of power and empire. *History and Theory, 44(*4), 73-87.

Solomon, Matt. (2021, February 18). North Korean Hackers Charged in WannaCry Ransomware & $1.3 Billion Cybercrime Spree. *Security Bouvelard.* https://securityboulevard.com/2021/02/north-korean-hackers-charged-in-wannacry-ransomware-1-3-billion-cybercrime-spree/#:~:text=Ransomware%2Drelated%20cybercrime%20costs%20expected,email%20that's%20laced%20with%20ransomware.

Stohl, C., & Stohl, M. (2007). Networks of terror: Theoretical assumptions and pragmatic consequences. *Communication Theory, 17*(2), 93-124.

Winfree, L. T., Bäckström, T. V., & Mays, G. L. (1994). Social learning theory, self-reported delinquency, and youth gangs. *Youth & Society, 26*(2), 147-177.