sustainability

MDPI

Article

North Korea's Cyber Capabilities and Their Implications for International Security

Min-hyung Kim

Department of Political Science and International Relations, Kyung Hee University, Seoul 02447, Korea; min-hyung@khu.ac.kr

Abstract: North Korea's economic and technological backwardness does not seem to allow Pyongyang to possess proficient cyberwarfare capabilities. Yet, North Korea's cyber offensive capabilities are a major security threat in a new convergence space called the cyber–physical space (CPS) that connects the real world and the virtual world. How has North Korea become a formidable actor in the CPS, despite economic and technological disadvantages? Put differently, what makes North Korea a global cyber power despite its disconnect from international society? What are North Korea's motivations behind strengthening its cyber capabilities in recent decades and what implications do these hold for international security? The primary objective of this article is to examine North Korea's motivations for strengthening its cyber capabilities and analyze their implications for the sustainability of stability and peace on the Korean peninsula and beyond. By investigating the exemplary cases of North Korea's recent cyberattacks, it seeks to explore the effective ways to manage the risks that North Korea's enhanced cyber proficiencies pose in the current and future CPS.

Keywords: cyberspace; cyber capabilities; international security; North Korea; sustainability of peace

Citation: Kim, M.-h. North Korea's Cyber Capabilities and Their Implications for International Security. *Sustainability* **2022**, *14*, 1744. https://doi.org/10.3390/su14031744

Academic Editor: Hangbae Chang

Received: 13 January 2022
Accepted: 31 January 2022
Published: 2 February 2022

1. Introduction

North Korea currently remains one of the world's most impoverished countries. Its infrastructure of economic and technological development is falling behind. It is also a globally isolated country, as seen from the fact that its current trade volume with China (North Korea's neighboring military ally) accounts for over 90 percent of its total trade [1] (p. 25). In addition, North Korea's lack of electricity has been well reported. Hence, it is not surprising that North Korean society is poorly networked. North Korea controls nearly all inbound and outbound information within its territory. In other words, almost all cyber activities in North Korea are conducted under complete state control and guidance. Indeed, this gloomy picture of North Korea does not seem to allow Pyongyang to possess the cyberwarfare capabilities to pose significant cyber threats to the world. Yet, North Korea's cyber capabilities are a major security threat in a new convergence space called the cyber–physical space (CPS) that connects the real world and the virtual world. They are a destabilizer as well as a disruptor of the stability and peace on the Korean peninsula and beyond.

How has North Korea become a formidable actor in the CPS, despite economic and technological backwardness? In other words, what makes North Korea a global cyber power despite its disconnect from international society? What are North Korea's motivations behind strengthening its cyber capabilities in recent decades and what implications do these hold for international security?

The primary objective of this article is to analyze North Korea's motivations for strengthening its cyber capabilities and examine their implications for the sustainability of stability and peace on the Korean peninsula and beyond. By investigating the exemplary cases of North Korea's recent cyberattacks, it seeks to explore the effective ways to manage the risks that North Korea's enhanced cyber proficiencies pose in the current and future CPS.

The literature on North Korea's cyber capabilities and their implications for international security has not been well-developed yet and remains fragmented. A number of articles on North Korea's cyber capabilities are superficial, technical, and largely policy-oriented (see, for example, [2–7]). While there are some exceptions (see, for instance, [8–13]), they do not specifically examine North Korea's strategic motivations for strengthening its cyber capabilities and their implications for international security in general and the sustainability of stability and peace on the Korean peninsula in particular. By analyzing North Korea's recent cyberattacks based on its motivations of strengthening cyber capabilities, the article seeks to explore their implications for international security and come up with the best security strategies that successfully handle Pyongyang's accelerating cyber threats/attacks. In doing so, the article aims to contribute to the study of North Korea's cyber threats in the current and future CPS particularly and the maintenance of international peace more broadly.

The central thesis of this article is that as a form of asymmetric weaponry, North Korea has strengthened its cyber offensive capabilities in order to achieve three critical strategic goals: counterbalancing the growing gap in traditional military capabilities between North Korea and the US-ROK (Republic of Korea) alliance, causing social disruption in adversaries with little immediate risk of retaliation, and financing the impoverished Pyongyang regime. Hence, the sustainability of stability and peace on the Korean peninsula and beyond depends on how South Korea, along with the US, in particular and international society in general deal with North Korea's cyberattacks and come up with a mechanism for the effective management of Pyongyang's cyber operations. Above all, a high level of international cooperation and inter-agency coordination as well as a public-private partnership is required to effectively handle North Korea's evolving cyber threats.

The structure of this article is as follows. The first section briefly addresses the main features of cyberspace for international security. The second section examines North Korea's motivations behind strengthening its cyber capabilities in recent decades. The third section goes over several examples of North Korea's cyberattacks after a brief introduction of methodology. The fourth section explores effective ways to manage North Korea's cyber threats. The fifth section discusses the implications of North Korea's cyber capabilities for international security. The concluding section deals with the limitations of this research as well as the avenues for future research.

2. Main Features of Cyberspace for International Security

The prevailing definition of cyberspace is all extant computer systems and networks [14] (p. 17). Distinct from physical space, cyberspace has important features. Some of the major features of cyberspace in terms of international security are as follows.

First, attackers in cyberspace enjoy a considerable degree of anonymity. Unlike a missile which normally has a sender's address, a computer code does not have one [8] (p. 8). While some identification features such as IP addresses exist, it is typically very hard to trace the activity's source in cyberspace back to its origin [3] (p. 19). This is the so-called attribution problem. Investigators must handle anonymity whenever a cyberattack (which refers to "the use of code to interfere with the functionality of a computer system for a political or strategic purpose" [14] (p. 19)) takes place to determine who is responsible for the attack [13] (p. 158). Moreover, cyber defense still often counts on "firewalls and intrusion detection systems that fail to filter out attacks using unknown malware or stolen legitimate credentials" [3] (p. 24). As Clark and Landau point out, attribution is a serious problem that is hard to master in finding ways to deter cyberattacks [15]. While some technological improvement on better management of the attribution problem has been made in recent years, finding the origin of the cyber activity is still challenging, costly, time-consuming, and often requires intergovernmental cooperation [3] (p. 19).

Second, as William Lynn III, former U.S. Deputy Secretary of Defense, asserts, "In cyberspace, the offense has the upper hand" [16] (p. 98), (for disagreements, see [17–19]). In other words, the offense generally has an advantage over defense in cyberspace due

to the information asymmetry: "The attacker has great freedom choosing when and how to compromise a system while the defender is forced to continuously defend all possible vectors and assets" [3] (p. 24). Thus, attacking computer systems is much easier and cheaper than detecting cyberattacks and defending against them [8] (p. 9). According to Lieberthal and Singer, this is because "the Internet was designed to share information easily, not prevent its flow" [20] (p. 14). In addition, because of the attribution problem in cyberspace, "Attackers are much more likely to strike if they are unlikely to be targeted in return" [21] (p. 46). Put simply, there are enormous advantages to the offense against the defense in cyberspace.

Third, since cyber operations often blur lines between cyber exploitation, which is the penetration of an enemy's computer system for data exfiltration such as cyber espionage [14] (p. 20), and cyberattack, they have important implications for cybersecurity, which refers to "the measures to protect the operations of a computer system or integrity of its data from hostile action" [14] (p. 18). In particular, they bring about the so-called 'cybersecurity dilemma,' which means that "network intrusions undertaken for defensive purposes are easily misunderstood as preparation for an attack, creating the risk of escalation and use of force" [19] (p. 73). Like the traditional concept of 'the security dilemma' [22], the obvious consequence of the cybersecurity dilemma is a cyber arms race between cyber powers where "Fears of being hacked, optimism about hacking others, or both have spurred massive investments in military cyber operations around the world" [19] (p. 73).

Fourth, deterrence theory has limited applicability in cyberspace. Deterrence refers to states' "efforts to avoid being deliberately attacked by using threats to inflict unacceptable harm on the attacker in response" [23] (p. 55). For deterrence to work, specifically defined enemies and their motivations to do harm should be clear. In cyberspace, however, many attackers are non-state actors (e.g., individuals including criminals) and their motivations greatly vary (e.g., seeking fun, risk-taking, financial gain, prestige among peers, espionage, etc.). Thus, Morgan contends that "With cyberattacks, the fundamental *nature of the threat* to national security remains largely hypothetical" [23] (p. 58). In addition, while "deterrence requires a credible retaliatory response" [24] (p. 7), cyberattacks which usually result in no casualties do not generally trigger automatic retaliation. Moreover, "no feasible act of cyberretaliation is likely to eliminate the offending state, lead to the government's overthrow, or even disarm the state" [25] (p. 31). This means that cyberspace is where traditional deterrence theory has limited applicability. According to Clark and Knake, "of all the nuclear strategy concepts, deterrence theory is probably the least transferrable to cyber war" [26] (p. 189). In a similar vein, Libicki points out that a full-fledged cyberattack, unlike a nuclear attack, may be survivable, although it is oppressive and costly [25] (p. 72). Nye contends that even if deterrence also works in cyberspace, its effectiveness still "depends on who (state or nonstate) one is trying to deter and which of their behaviors" [27] (p. 63).

Fifth, while states remain the strongest players, non-state actors such as individuals and firms are equally as powerful as states in cyberspace. In other words, states and non-state actors have similar capacities to execute cyberattacks; some even argue that "individuals have greater power than the state" [13] (p. 155). Kello contends that non-state players in cyberspace can inflict frightening harm in ways that cause a crisis, which is beyond governments' ability to control [14]. Sanger also points out that cyber weapons empowered non-state actors to credibly threaten states including hegemonic powers with paralyzing strike potential [28]. Additionally, it is important to note with regard to the significance of non-state parties in cyberspace is the fact that in many cases, much of the telecommunication networks and hardware are privately owned and these systems are used by both states and civil society [10] (p. 64). Accordingly, "the challenge of cyber security is essentially one of civil defense: how to equip the private sector to protect its computer systems in the absence of government direction" [14] (p. 29).

Sixth, unlike the physical domain, cyberspace is not only immaterial but also transnational. Unlike in conventional warfare where the enemies are 'out there' beyond national boundaries, the enemies in cyberspace are 'in here' (i.e., inside national boundaries), "par-

ticipating like the rest of us in, as a component of, the interactive and interdependent networks that constitute cyberspace" [23] (p. 58). Simply put, cyber threats nearly disregard national borders as they exploit interconnectivity to target states or organizations directly [29] (p. 78).

Seventh, there are few accepted international laws and norms on proper state responses or countermeasures to cyberattacks. While some international laws and norms for stipulating unacceptable behaviors in cyberspace have emerged (e.g., the Budapest Convention on Cybercrime; also see Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* [30]), they are still largely ambiguous and subject to different interpretations of actors involved. As Jun et al. point out, "Current international law has not come to agreement on fundamental issues such as what actions in cyberspace constitute various degrees of aggressive state behavior (i.e., armed attack or use of force), what would be a legitimate and proportional response in each case, and what the rights and duties of third parties are" [3] (p. 25).

3. North Korea's Motivations for Strengthening Its Cyber Capabilities

Since the mid-1980s, North Korea has made great efforts to strengthen its cyber capabilities. Recognizing its relative inferiority of conventional weapons vis-à-vis those of the US and South Korea, North Korea has invested in asymmetric military capabilities, such as nuclear, ballistic missile, and cyber capabilities. In Pyongyang's strategic thinking, it is asymmetric warfare capabilities that guarantee their national survival [31]. North Korea regards cyber capabilities as 'strategic weapons' [3] (p. 29) as illustrated by Kim Jong-un's remark that "Cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our [North Korea's] military's capability to strike relentlessly" (a 2013 briefing by Nam Jae-joon, former director of South Korea's National Intelligence Service, at the National Assembly, cited in [32]). This goes along with the directive of the late North Korean leader Kim Jong-il, Kim Jong-un's father, for the Korean People's Army General Staff to develop cyber warfare capabilities after the Iraq War in which he emphasized that "In the 20th century, war is with bullets over oil. But in the 21st century, war will be [fought as] information warfare" (cited in [10] (p. 62)). As such, "[w]ar is won and lost by who has greater access to the adversary's military technical information in peace time" (cited in [7] (p. 3)). Accordingly, the strengthening of cyber capabilities is a product of Pyongyang's strategic thinking prepared for a new era. In particular, it serves Pyongyang's three critical strategic goals: offsetting North Korea's inferior conventional military capabilities; causing social disruptions in adversaries' soils with little costs as well as little risk of retaliation; generating revenue under sanction regimes.

First, North Korea's conventional weapons like fighter jets, tanks, and warships are pretty outdated. They cannot compete with modernized and sophisticated military forces of the US and South Korea. Exacerbating this issue, North Korea's economy, which has been lowest-ranked in the world (178th in the world and 40th in the Asia-Pacific region, according to the 2021 Index of Economic Freedom [33]), cannot afford to update its outdated conventional weapon systems. For Pyongyang, therefore, strengthening cyber capabilities is a cost-efficient means to counterbalance the growing gap in traditional military capabilities between North Korea and the US-ROK alliance. As Caesar points out, preparing for conventional warfare requires the development of expensive and onerous weaponry whereas building cyberwarfare capabilities such as a hacking program needs only intelligent people [34]. Since the militaries of the US and South Korea, like those of many advanced countries, are heavily dependent on information and computer networks, they are quite vulnerable to North Korea's cyberattack. North Korea's cyberattack "allows for coercion with minimal operational risk, because there is no hardware or operatives that can be destroyed during the operation" [3] (p. 29). Given the unfavorable conventional weapons balance, North Korea's cyberwarfare capabilities as a form of asymmetric warfare capabilities can marginalize the military strengths of the US and South Korea [35].

In fact, many experts now warn that North Korean hackers are potentially a more significant threat than any other conventional weapons that Pyongyang shows off at military parades every year [36]. Their advanced cyberwarfare skill is world-class and North Korea's cyber capabilities that Pyongyang has improved over decades can shift the balance of power on the Korean peninsula without resorting to war [36]. The danger of North Korea's expanding cyber capabilities is also highlighted in the 2019 report of a UN Panel of Experts on sanctions against Pyongyang, which points out that North Korea had generated about two billion dollars through cybercrime (e.g., stealing from foreign banks, hacking cryptocurrency exchanges) for the recent decades and a great portion of money stolen by North Korean hackers was used to fund making and testing nuclear weapons and inter-continental ballistic missiles (ICBMs) [34,37]. After all, North Korea's cyber capabilities are an effective means for Pyongyang to evade stringent international sanctions imposed against it and direct its resources to nuclear weapons and their delivery systems that it desperately seeks to possess.

Second, North Korea wants to enhance its cyber proficiencies since cyberattack is a cost-efficient as well as risk-minimizing way to cause social disruption in adversaries. By attacking critical infrastructure such as networks of transportation, telecommunication, banking, media, and nuclear power plants that are closely related to people's daily lives, North Korea's cyber operations seek to arouse fear and inconvenience of the public and cause social unrest and disorder. North Korea's cyberattacks against South Korea's broadcasting and media firms such as KBS, MBC, YTN, and *Joongang Ilbo* in 2013, against the Korea Hydro and Nuclear Power (KHNP) Co Ltd. and Wolsong Nuclear Power Plants in 2014, and against Seoul's subway system in 2015 are cases in point. As North Korea is very adept in using diverse hiding techniques to avert cyberattack detection and backtracking [11] (p. 443), it is hard to retaliate timely. North Korea's cyber capabilities therefore allow Pyongyang to disturb the status quo with little immediate risk of retaliation during peacetime [3] (p. 5).

Third, North Korea's cyber operations such as the launching of malicious software (malware) attacks, online bank heists and hacking attacks, phishing attacks, ransomware attacks on cryptocurrency, and stealing funds by fraudulent bank transfers have increased in recent years (see [7] (pp. 22–34) for North Korea's various types of recent cyberattacks). Unlike past cyber operations where Pyongyang sought to cause social disruption or steal critical government and military information, a number of more recent cyberattacks have appeared financially motivated and were related to raise foreign currency and revenue for the Pyongyang regime. As international sanctions tighten in areas such as trade after Pyongyang's series of provocations (i.e., six times of nuclear tests and numerous ballistic missile tests), North Korea seeks to make up for its economic losses and find an alternative means of fundraising for the government. For instance, the Lazarus Group, a North Korean cybercrime organization known for a number of recent disruptive cyber operations, launched a series of cyberattacks against the Society for Worldwide Interbank Financial Telecommunications (SWIFT) banking network in 2015–2016 and made over USD hundreds of million in hard currency. The UN Panel of Experts on North Korea Sanctions Committee reported in 2019 that between 2017 and 2018 North Korea had launched at least five successful cyberattacks against cryptocurrency trades in Asia and had earned 571 million dollars [38] (p. 51). North Korea has bolstered its cyber hacking capabilities as a means of generating resources and revenues under the tightened international sanctions regime. Despite the pandemic of COVID 19, North Korea's 'All Purpose Sword' is working as a vital weapon for Pyongyang's struggle to obtain foreign currencies [39]. In other words, Pyongyang's cyber espionage capabilities have become a major source of financing for the impoverished government of North Korea.

In brief, for North Korea, cyber operations are low-risk as well as cost-effective with usually high yields, considering the low hurdles to entry [6]. Since the mid-1980s, therefore, North Korea has steadily invested in training its brightest students in order to make them the most talented hackers in the world. Kim Chaek University of Technology and Kim

Il Sung University are the two colleges in Pyongyang where the most talented teenagers in math and science at selected middle and high schools are sent to for special training so that they become proficient cyber warriors before they are sent to special overseas institutions (particularly in China and Russia) for further training [34] (p. 7). The Kim Il Military Academy, which was established in 1986, is another key institute where a number of North Korean cyber warriors are trained and produced on a yearly basis. Additionally, in here various programs for computer network defense as well as malware for computer network attacks are developed [10] (p. 67). Seoul assesses that North Korea has approximately 6800 cyberwarfare professionals [40]. The cyber weapon systems that North Korea possesses include electrical (electro-magnetic Pulse or EMP weapons that neutralize or destroy all electronic devices within the influence zone and GPS jammers that disturb the GPS signals), psychological (pro-North Korean applications), and logical (DDos attacks) weapons [11] (p. 440). The Reconnaissance General Bureau (RGB), North Korea's main foreign-intelligence service that directly reports to Kim Jong-un, oversees all of Pyongyang's clandestine cyber operations, and its sub-organizations include Unit 180 and the Lazarus Group, which are accused of a number of recent cyberattacks against Bangladesh Bank, Sony Pictures Entertainment (see [41,42]), and whatnot. According to the analyses of the US government and the Heritage Foundation in 2015, the North Korean cyberattack capability reached a dangerous level, although the level of its threat is relatively lower compared to that of China, Russia, and Iran [11] (p. 440).

4. Methodology and Case Selection

As for methodology in analyzing North Korea's cyber capabilities and their implications for international security, the case study method is employed. The case study method is "the detailed examination of an aspect of a historical episode to develop or test historical explanations that may be generalizable to other events" [43] (p. 5). It is typically related to an in-depth analysis of a single case or several cases. Testing explanations that examine *how*/*why* 'X' causes 'Y' is usually easier with case study than large-*n* methods [44] (p. 116). Hence, the case study method adopted here is likely to allow for an in-depth analysis of the relationship between North Korea's cyber capabilities and the sustainability of stability and peace on the Korean peninsula and beyond.

The three cases that will be examined in detail are North Korea's attack on the South Korean Military Data Center, its attack on the Korea Hydro and Nuclear Power (KHNP) Co Ltd., and its attack on Bangladesh Bank. These cases were selected because they represent North Korea's primary strategic goals of strengthening its cyber capabilities: i.e., counterbalancing North Korea's weaker position in traditional military capabilities, causing social disruption within adversaries, and generating revenues for the Pyongyang regime. In the following section, these cases are analyzed in depth.

5. Recent Examples of North Korea's Cyberattacks

5.1. Attack on the South Korean Military's Data Center, September 2016

North Korean hackers infiltrated South Korea's Defense Integrated Data Center in September 2016 and stole 235 gigabytes of classified military documents. The stolen documents included wartime contingency plans, the so-called 'decapitation' plan' or 'Operation Plan 5015' drawn up by Washington and Seoul, in which in case of war with North Korea on the Korean peninsula procedures for beheading strikes on Kim Jong-un and his top government officials were laid out. Additionally included were intelligence about South Korea's special forces, details about annual US-ROK military drills, and information about key military facilities and major power plants. About 80 percent of compromised data had yet to be identified at the time of report, according to Rhee Cheol-hee, a lawmaker of the ruling Democratic Party [45,46]. In this attack, "North Korean hackers infected 3200 computers, including 700 connected to the South Korean military's internal network, which is normally cut off from the internet" [47]. While the military's secured intranet is generally regarded as being safe from compromise, the hacking was possible due to a

worker's simple mistake. A connector jack that links the military intranet to the internet had not been removed after scheduled maintenance work. Thus, North Korean hackers first infiltrated the network of a South Korean company that provided antivirus vaccine to the South Korean military. They then used the vaccine server to infect internet-connected computers of the South Korean military with malicious codes [45–47].

It is still unknown how critically the North Korean hacking impaired the joint military preparedness of the US and South Korea. What is important to note is that North Korea can easily offset its inferiority of conventional weapons with this kind of cyberattack. Although the South Korean military claimed that the stolen data was not the highest level of classified intelligence, North Korea's cyberattack of stealing the US-ROK military plans was truly a demonstration of the danger of Pyongyang's accelerating cyber capabilities. It was a wake-up call for the US and South Korea that "while we've been (understandably) focused on North Korea's nuclear weapons and ballistic missiles, the country has been quietly developing another powerful tool—a selection of malware and malicious code, a veritable cyber weapons cache" [45]. As Jun et al. point out, North Korea's cyberwarfare capabilities provide Pyongyang with "another means of exploiting US and ROK vulnerabilities at relatively low intensity while minimizing risk of retaliation or escalation" [3] (p. 4).

5.2. Attack on the Korea Hydro and Nuclear Power (KHNP) Co Ltd., December 2014

On 15 December 2014, computer systems of South Korea's nuclear plant operator, Korea Hydro and Nuclear Power Co Ltd., were breached. The hackers used an account called 'president of the anti-nuclear reactor group' and posted the blueprints of nuclear reactors on social media, threatening that more information would be released unless three reactors (i.e., Gori Units 1 and 3, and Wolsong Unit 3) stopped operating by 25 December. As the only nuclear operator in South Korea, KHNP is part of the state-run utility Korea Electric Power Corp and runs South Korea's 24 nuclear reactors that provide about 29 percent of South Korea's energy needs. Although KHNP officials said that only noncritical data had been stolen, the leaked information included "personal details of 10,000 KHNP workers, designs and manuals for at least two reactors, electricity flow charts and estimates of radiation exposure among local residents" [48]. Since the attack against KHNP occurred shortly after North Korea's high-profile cyberattack on Sony Pictures Entertainment as well as on the heels of the Cybersecurity Enhancement Act of 2014, which was passed by the U.S. Congress on 11 December 2014 [49], the US government claimed that Pyongyang was behind the attack. North Korea, as usual, denied its involvement in the attack. After South Korean authorities' probe into the hacking, Seoul concluded that Pyongyang was responsible for the KHNP cyberattack.

Although KHNP's nuclear control systems had not been hacked, North Korea's KHNP attack at the time demonstrated the ease of using the "net connection to leap into the control systems that oversee chemical works, dams, and power plants" [50]. It also heightened the alertness of both the dangers of numerous flaws in the software found on those control systems [50] and the possibility of the safety of the nation's atomic facilities to be compromised. Luckily, no devastating damage has been caused from North Korea's cyberattack on a nuclear facility thus far. However, there is no guarantee that it would be the case in the future. North Korea's KHNP attack again illustrated how vulnerable South Korea's companies (both private and public) and government institutions were against North Korea's cyberattacks. As South Korea's former President Park Geun-hye said at a cabinet meeting after North Korea's KHNP attack, "Nuclear power plants are first-class security installations that directly impact the safety of the people" (cited in [48]). What is worth stressing is that North Korea can easily create social chaos in South Korea with similar kinds of cyberattacks and that Pyongyang's cyber capabilities to cause social disruptions in South Korea are increasing and becoming more sophisticated while the preparations of the South Korean government and society for the cyber defense against the North's attacks lag far behind.

5.3. Attack on Bangladesh Bank, February 2016

On 4 February 2016, North Korea conducted a cyberattack against Bangladesh Central Bank, which was in charge of overseeing the country's currency reserves. Using fake bank accounts, money-laundering casinos, charities, and a variety of accomplices, North Korean hackers who had already penetrated in the bank's SWIFT international transaction system instructed the Federal Reserve Bank (FRB) of New York to make a sequence of transfers totaling USD 951 million, which was almost all amount of Bangladesh Bank's FRB account, to bogus companies around the world [39]. Not all of these requests were successful due to some coincidental details and the mistakes of the hackers—e.g., the address of the bank in Manila included the term 'Jupiter', the name of the sanctioned Iranian ship, which was enough to raise red flags in the Fed's automated computer system [51]; the hackers misspelled some words such as 'foundation'. Nevertheless, USD 81 million of the transfer was approved and wired to their accounts set up in Manila. Surprisingly, the hackers in this theft used the SWIFT global messaging service for the attack. They sent fraudulent SWIFT messages to the FRB in New York as well as Bangladesh Bank and changed the printed confirmation of transactions in order to hide their activity [52] (p. 6).

The Bangladesh Bank heist is particularly important in several aspects. First, it shows that global banking systems are also vulnerable against North Korea's cyberattack. North Korean hackers penetrated in the computer systems of another country's banks and carried out a cyberattack for illicit money transfers, taking advantage of the SWIFT international transaction network, which was regarded as the linchpin of the global financial system. US Congresswoman Carolyn Maloney's response to the report of the heist illustrates this: "it was fascinating, shocking—a terrifying incident, probably one of the most terrifying that I've ever seen for financial markets" [51]. Given that SWIFT sustains billions of USD of international trade on a daily basis, North Korea's hack on Bangladesh Bank using the SWIFT network could critically impair confidence in the global financial system. Second, North Korea's cyberattack on Bangladesh Bank demonstrates that Pyongyang's cyber proficiencies are not only improving but also becoming more sophisticated under the state's careful strategic plan. As the FBI notes, "the audacious Bangladesh Bank hack was the culmination of years of methodical preparation by a shadowy team of hackers and middlemen across Asia, operating with the support of the North Korean regime" [51]. Indeed, North Korea was the first country that hacked and robbed another country's banks [52] (p. 6). It is currently linked to similar attacks on banks in over 20 countries [53] (pp. 109–112) and the money stolen by this kind of cyberattack has been used for funding the development of strategic weapons (i.e., nuclear weapons and ICBMs). Third, North Korea's Bangladesh Bank heist illustrates that Pyongyang increasingly relies on its cyber operations to fund the financially crippled Pyongyang regime under tightened international sanctions. According to a 2018 report, North Korea accounted for 65 percent of total cryptocurrencies that were stolen from online exchanges during 2017–2018 [54]. Sanger et al. also argue that North Korea probably earns USD one billion (which is equal to the value of its export) a year from cyber heists [55]. Hence, North Korea's cyberattack on Bangladesh Bank shows that its cyber hacking on financial institutions is becoming a major means to fund the beleaguered regime.

6. Ways to Manage North Korea's Cyber Threats

In order to effectively handle North Korea's evolving cyber threats and maintain the stability on the Korean peninsula and beyond, the following measures, among others, should be taken.

First, North Korea's Internet infrastructure is largely disconnected from global networks since its Internet traffic is channeled through only two providers—Russia's TransTeleCom (60%) and China's Unicom (40%) [12] (p. 9). Its national intranet called *Kwangmyong* offers websites and email services linking domestic institutions, but is largely unplugged from the World Wide Web [52] (p. 1). This means that North Korea's vulnerabilities to retaliatory actions are relatively low, which generates a kind of bargaining power [56] while

its deniability of attribution is high. In order to heighten the effectiveness of the threats of retaliation against Pyongyang's cyberattacks, therefore, Washington and Seoul should seek to obtain cooperation not only from international society but also from Moscow and Beijing, making it clear that assisting North Korea's illegal cyber operations is an international crime and thus intolerable. In particular, they should be able to impose sanctions against these countries as well as other countries and institutions that host North Korea-sponsored cyber warriors and support their illicit cyber activities. Given that North Korea's proficient cyber agents operate all around the world and most of its cyberattacks are conducted through overseas networks, a high level of international cooperation is necessary for tackling North Korea's various cyberattacks as well as its evolving cyber capabilities. What is most urgently needed is the information-sharing system on the international as well as domestic level that can detect and analyze North Korea's cyber operations, given that most of the North Korean cyberattacks are originated in foreign countries or delivered through foreign servers [11] (p. 451).

Second, the US and South Korea should review NATO's 2014 cyber defense policy revolution in which its leaders concurred that a large-scale cyberattack against its member state could be regarded as an attack against all allies potentially triggering an automatic military response (similar to Article 5 of NATO) and consider the possibility of its application to the 1953 US-ROK mutual defense treaty [8] (p. 9). As NATO's Secretary-General Anders Fogh Rasmussen eloquently said at a news conference, "Today we declare that cyber defense is part of NATO's core task of collective defense" [57]. Additionally, NATO leaders agreed that "A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis" [58]. They reaffirmed the decision at the meeting of the North Atlantic Council in Brussels on 14 June 2021 [59]. In 2019, the US and Japan also agreed that in certain circumstances, a cyberattack constitutes an armed attack triggering Article 5 of US-Japan Security Treaty [60]. The biggest challenge, of course, is to reach a consensus on what constitutes "a large-scale cyberattack" or "certain circumstances" that require(s) an automatic military response. Washington and Seoul should define 'North Korea's extensive or large-scale cyberattack' as well as 'certain circumstances' in order to deter its increasingly drastic cyber operations. Given the high possibility of escalation of a war on the Korean peninsula, the NATO-style cyber defense policy is highly recommended since it is likely to provide the US-ROK alliance with a strong deterrence against North Korea's cyberattacks, which will ensure the sustainability of stability and peace on the Korean peninsula and beyond.

Third, in response to North Korea's growing cyberattacks, Seoul has declared that it would embark on cyber offensive capabilities [9]. More recently, Seoul's cyber capabilities have been integrated in the framework of the US-South Korea alliance with joint programs which aim to develop artificial intelligence-based technologies to fight North Korea's various cyber operations [12] (p. 11). These developments are very encouraging and Washington and Seoul should double their concerted efforts along these lines in order to deal with Pyongyang's increasingly sophisticated cyber capabilities. According to a recent report of South Korea's Ministry of Defense, North Korea now possesses the ability to disrupt the networks of Global Position System (GPS) and has also developed the means to jam precision-guided bombs and high-tech missiles [7]. In addition, Pyongyang has recently integrated cyber capabilities with other conventional weapon systems to achieve its foreign policy goals [61]. If this were true, North Korea's cyber capabilities might disable much of US-ROK strategic weapons deployed in South Korea and as a result create long term political and sociological unrest on the Korean peninsula. Washington and Seoul, therefore, should closely cooperate in cyber defense against North Korea's accelerating cyberwarfare capabilities, particularly in the realm of the enhancement of computer operation, mobile telecommunication, and information systems.

Fourth, South Korea in recent years set up a cyberwarfare command and raised proficient hackers to cope with North Korea's evolving cyberattacks. These efforts are on the right track and Seoul should invest more resources to foster innovative and technologically

sophisticated cyber warriors capable of combating North Korean counterparts. More important than this, however, is the need to implement basic cybersecurity practices such as regular and frequent updates of operation systems and computer software, since failure to do so is likely to lead to significant cybersecurity breaches as North Korea's 2017 WannaCry ransomware attack demonstrates [6]. Given South Korea's ever-growing dependence on Internet service and its vulnerability against North Korea's cyberattacks, strengthening the network security and upgrading cyber defense techniques which can heighten the resilience of crucial infrastructure (military, social, and financial) are essential not just for South Korea's cyber defense but also for the sustainability of peace on the Korean peninsula.

Fifth, because of the close links between the public sector and the private sector in the cyber domain, the public–private partnership is essential to manage North Korea's evolving cyber threats. While military networks have thus far been primary targets of North Korea's cyberattacks, civilian networks such as banking and communication systems are increasingly becoming their main targets. The problem is that a great deal of the advanced technology typically lies with the private firms and they own and operate a bulk of fundamental computer infrastructure that is critical for national security [29] (p. 78) [14] (p. 29), but much of these networks are used not just by governments and militaries but also by private firms and civil society [10] (p. 64). This "dual-use nature of cyberspace often makes it difficult to determine who should be responsible for cybersecurity" and "private firms often underestimate cyber risks and underinvest in cybersecurity or prefer to 'free-ride' while expecting the government to manage the North Korean cyber threat" [10] (p. 64). Additionally, there is a tendency that private firms often do not report about damaging cyberattack incidents due to their consequences of creating a reputational cost [14] (p. 10). This is why the public–private partnership is absolutely necessary to deal with Pyongyang's accelerating cyberattack capabilities. An intimate cooperation and information sharing between governments and private institutions is also important to identify and track North Korea's overseas cyber agents [6].

7. The Implications of North Korea's Cyber Capabilities for International Security

Since North Korea's cyberattacks transcend national borders and inflict damage to a number of countries around the world, they are a major threat to international peace and stability. As cyber weapons are by design not limited in range, they provide North Korea with a low-cost means of developing global military capabilities, unlike huge political and economic costs of technology pursuits of the weapons of mass destruction (WMD) such as nuclear weapons and ICBMs [9]. Mike Pompeo, former US Secretary of State, claims that "North Korea is a bigger threat than Russia when it comes to cyberattacks" [36]. Although his assessment of North Korea's cyberattack capabilities may be exaggerated, senior US intelligence officials in 2017 ranked North Korea as one of the top four cyber threats that can launch devastating cyberattacks against the US [7]. Bruce Klingner, a former CIA Korea deputy division chief at the Heritage Foundation, also contends that "Pyongyang developed advanced cyberwarfare prowess surpassed only a few nations" [36]. North Korea's cyberattack capabilities, along with its capabilities of nuclear weapons, constitute Pyongyang's asymmetric warfare strategies and pose significant threats to international security. As Kello asserts, "The ability of a cyberattack to inflict economic and other damage without resort to traditional violence affords this virtual weapon a special utility: it expands the choice of actions and outcomes available to the strategic offense" [14] (p. 26). Indeed, in the interdependent and increasingly connected world, North Korea's cyber proficiencies allow Pyongyang to exert more power than it actually possesses.

North Korea's evolving cyber capabilities make us rethink the lessons of the theory of stability–instability paradox originally proposed by Glenn Snyder [62]. The stability–instability paradox refers to the phenomenon where the existence of the weapons of mass destruction (in particular, nuclear weapons) increases strategic stability by preventing large-scale wars while at the same time it increases strategic instability due to more frequent

low-intensity conflicts. Jervis explains this as follows: "To the extent that the military balance is stable at the level of all-out nuclear war, it will become less stable at lower levels of violence" [63] (p. 31). Unlike the physical domain where "the costs of high-intensity conflict are so great that all actors have disincentives to escalate and are therefore deterred from taking actions that risk escalation" [10] (p. 68), however, North Korea is difficult to deter in the cyber domain because of many characteristics of cyberspace mentioned earlier (e.g., the advantages of offense over defense, the attribution problem, the absence or ineffectiveness of international laws and norms regulating cyber operations of individuals and states, etc.). Haggard and Lindsay contend that North Korea's cyberattacks extend the stability–instability paradox into global cyberspace [24] (p. 2). Indeed, North Korea's cyberattacks against the South Korean government and private institutions have the potential to create enormous social and political disorder in South Korea with a minimal risk of military retaliation. Likewise, North Korea's cyberattacks on financial institutions such as Bangladesh Bank and SWIFT can cause a turmoil and disruption in the global financial system with little fear of military counteraction. As Kello points out, "The cyber domain is a perfect breeding ground for political disorder and strategic instability" [14] (p. 32).

Moreover, it is noteworthy that although shared norms on cyber operations are slowly emerging in international society, they remain primitive and unenforceable. Currently, international and domestic laws against cyberattacks are largely equivocal and incapable of handling North Korea's evolving cyber threats. Under these circumstances, North Korea's various cyber operations provide Pyongyang with an effective means to evade international sanctions imposed against it. As a result, North Korea's cyber proficiencies undermine international laws and international norms. What is worth emphasizing here with regard to North Korea's expanding cyber operations overseas is strengthened ties between China, Russia, and North Korea in the cyber field. For example, according to the August 2020 UN POE report, a number of North Korean information technology workers entered and illegally stationed in Vladivostok, Russia violating UN Resolution 2397, which prevented North Korean workers from reentering Russia after the mandatory December 2019 repatriation deadline [6]. Similar incidents are found in China as well. These cases demonstrate that China and Russia, North Korea's two traditional allies, continue to provide the Pyongyang regime with technical and training support for critical cyber operations. No matter how risky these developments are for the sustainability of international peace, this trend is likely to continue so far as the Sino-US strategic competition for hegemony intensifies [64,65] and consequently, the Northern allies (i.e., Russia, China, and North Korea) try to pull together to hedge against US hegemony.

Along with nuclear weapons and ballistic missile programs, North Korea has developed cyber capabilities as 'asymmetric warfare capabilities', which provide itself with strategic advantage such as "relatively low-cost but effective means to exert its influence" and an ability "for political, economic, and military coercion without triggering a major armed conflict" [12] (p. 12). Additionally, North Korea's cyberattack capabilities in times of crisis can "increase the propensity of offensive and unrestricted cyber operations given the prevailing perceptions of lesser risks of detection, the lack of accountability, and the resulting low probability of successful deterrence" [12] (p. 11). Moreover, with respect to North Korea's expanding cyberattacks, the absence of agreed degrees of proportionality in cyberspace could result in unreasonable counter-responses whereas the lack of confidence-building measures may prevent attempts to deescalate the crisis [14] (p. 35). After all, what North Korea's accelerating cyber capabilities mean to the students of international security is the following: given the deviation of the current cyber domain from the expected patterns of strategic competition in the international system, scholars and policymakers working on international security should try "to formulate concepts and propose policies that can impose on the chaotic cyber domain the necessary measure of stability to render its contests not just orderly but also 'ordinary'" [14] (p. 39).

8. Conclusions

In addition to becoming a new nuclear-weapon state, North Korea has emerged as a formidable actor in cyberspace. Currently, few states in the world can outperform North Korea's advanced cyberwarfare skills. North Korea's rapidly evolving cyber capabilities, which could paralyze social safety nets and international as well as national infrastructure without resorting to war, not only pose new types of challenges for international security but also threaten the stability and peace on the Korean peninsula.

There are, of course, people who disagree with the above statement (see [52] (pp. 3–4) for a good summary of the debate on North Korea's cyber capabilities). For example, Gartzke contends that "To the degree that powerful states are immune to conventional attack, cyberattacks are at most a nuisance and not a fundamental threat" [21] (p. 63). For him, therefore, North Korea's cyberwarfare capabilities may not be a significant threat to international security. Nevertheless, he admits that if cyberattack is employed jointly with other conventional forms of fighting and if the attacker has a considerable military power, it can affect the long-term balance of power [21] (p. 57). Maness et al. are also skeptical about the effectiveness of North Korea's cyber strategies. They point out that "no North Korea cyber operation has caused a government to back down" [56]. Likewise, Libicki maintains that in general, the ultimate effects of the attack in cyberspace are uncertain [25] (p. 69). Nonetheless, it seems fair to say that Pyongyang has effectively used cyber capabilities to achieve its foreign policy goals [61]. As Chris Inglis, former deputy director of the National Security Agency, contends, North Korea's cyber operations were by and large quite successful because they have "achieved all their aims at a low cost" (cited in [56]).

North Korea will seek to develop more sophisticated hacking skills and continue to conduct cyberattacks on various targets in the world down the road. For North Korea, cyber offensive capabilities are asymmetric and virtual weapons that (unlike nuclear weapons) cost little to make and operate but guarantee high yields when successfully conducted. Due to a high level of deniability, cyberattacks are hard to retaliate in time. Given North Korea's fragile economy, which cannot afford to upgrade its outdated conventional weapons, Pyongyang's cyberwarfare capabilities are a cost-effective means to fill the growing gap in conventional weapons between North Korea and the US-ROK alliance.

Thus far, North Korea's nuclear programs have attracted much attention from the international community. This is understandable, given the significant implications of nuclear weapons (in the wrong hands, in particular) for international security. That said, due attention should also be paid to North Korea's cyber capabilities since by inflicting devastating harm on the global infrastructure such as the international financial system, they pose new types of threats to international security. In order to effectively cope with North Korea's continuously developing cyber capabilities and maintain global stability and peace, a high level of international cooperation and inter-agency coordination as well as a public-private partnership is absolutely necessary.

Needless to say, this research has limitations. Above all, due to space concerns, the three representative cases of North Korea's recent cyberattacks, which reflect Pyongyang's strategic goals of strengthening cyber capabilities, were analyzed in depth. Future research could examine more similar cases and explore their implications for international security in general and the sustainability of stability and peace on the Korean peninsula in particular. Given North Korea's recent efforts to integrate cyber capabilities with traditional military capabilities on the operational level, future research could also analyze this important subject and explore its implications for international security.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. OECD. *North Korea: The Last Transition Economy?* OECD: Paris, France, 2020. Available online: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ECO/WKP%282020%2915&docLanguage=En (accessed on 21 April 2021).
2. Lewis, J.A. Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace. *38 North*, 7 September 2010. Available online: https://www.38north.org/2010/09/speak-loudly-and-carry-a-small-stick-the-north-korean-cyber-menace/ (accessed on 2 May 2021).
3. Jun, J.; LaFoy, S.; Sohn, E. *North Korea's Cyber Operations: Strategy and Responses*; Center for Strategic and International Studies; Rowman & Littlefield: Lanham, MD, USA, 2015.
4. CSS Cyber Defense Project. *Hotspot Analysis: Cyber Disruption and Cybercrime: Democratic People's Republic of Korea*; Center for Security Studies: ETH Zurich, Switzerland, 2018; pp. 1–30.
5. Kim, C.W.; Polito, C. The Evolution of North Korean Cyber Threats. In *Issue Brief*; The Asan Institute for Policy Studies: Seoul, Korea, 2019; pp. 1–12.
6. Bartlett, J. *Exposing the Financial Footprints of North Korea's Hackers*; Center for a New American Security: Washington, DC, USA, 2020. Available online: https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers (accessed on 4 May 2021).
7. Klingner, B. *North Korean Cyberattacks: A Dangerous and Evolving Threat*; The Heritage Foundation: Washington, DC, USA, 2021. Available online: https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat (accessed on 5 May 2021).
8. Mansourov, A. *North Korea's Cyber Warfare and Challenges for the US-ROK Alliance*; Academic Paper Series; Korea Economic Institute of America: Washington, DC, USA, 2014. Available online: http://keia.org/sites/default/files/publications/kei_aps_mansourov_final.pdf (accessed on 7 May 2021).
9. Murauskaite, E. North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment. *38 North*, 12 September 2014. Available online: https://www.38north.org/2014/09/emurauskaite091214/ (accessed on 6 May 2021).
10. Pinkston, D.A. Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the *Songun* Era. *Georget. J. Int. Aff.* **2016**, *17*, 60–76. [CrossRef]
11. Lee, Y.; Kwon, H.; Lee, J.; Shin, D. The Countermeasure Strategy Based on Big Data against North Korean Cyber-attacks. *Korean J. Def. Anal.* **2018**, *30*, 437–454.
12. Raska, M. North Korea's Evolving Cyber Strategies: Continuity and Change. *SIRIUS* **2020**, *4*, 1–13. [CrossRef]
13. Sembodho, K.U.; Trihartono, A.; Hara, A.E. The Limitation of United States Deterrence Strategy towards North Korean Cyber Attacks. *Glob. Strateg.* **2021**, *15*, 149–166. Available online: https://e-journal.unair.ac.id/JGS/article/view/24009 (accessed on 10 May 2021). [CrossRef]
14. Kello, L. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *Int. Secur.* **2013**, *38*, 7–40. [CrossRef]
15. Clark, D.D.; Laudau, S. Untangling Attribution. *Harv. Natl. Secur. J.* **2011**, *2*, 25–40.
16. Lin, W.J., III. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Aff.* **2010**, *89*, 97–108.
17. Lindsay, J.R. Stuxnet and the Limits of CyberWarfare. *Secur. Stud.* **2013**, *22*, 365–404. [CrossRef]
18. Lindsay, J.R. The Impact of China on Cybersecurity: Fiction and Friction. *Int. Secur.* **2015**, *39*, 7–47. [CrossRef]
19. Slayton, R. What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *Int. Secur.* **2017**, *41*, 72–109. [CrossRef]
20. Lieberthal, K.; Singer, P.W. *Cybersecurity and US-China Relations*; Brookings Institution: Washington, DC, USA, 2016.
21. Gartzke, E. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *Int. Secur.* **2013**, *38*, 41–73. [CrossRef]
22. Jervis, R. Cooperation Under the Security Dilemma. *World Politics* **1978**, *30*, 167–214. [CrossRef]
23. Morgan, P.M. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*; The National Academic Press: Washington, DC, USA, 2010. Available online: https://www.nap.edu/read/12997/chapter/7 (accessed on 11 June 2021).
24. Haggard, S.; Lindsay, J.R. North Korea and Sony Hack: Exporting Instability through Cyberspace. In *Asia Pacific Issues*; East-West Center: Honolulu, HI, USA, 2015; pp. 1–8.
25. Libicki, M.C. *Cyberdeterrence and Cyberwar*; RAND Corporation: Arlington, VA, USA, 2009. Available online: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed on 17 January 2022).
26. Clark, R.A.; Knake, R.K. *Cyber War: The Next Threat to National Security and What to Do About It*; HarperCollins: New York, NY, USA, 2010.
27. Nye, J.S., Jr. Deterrence and Dissuasion in Cyberspace. *Int. Secur.* **2017**, *41*, 44–71. [CrossRef]
28. Sanger, D.E. *The War, Sabotage, and Fear in the Cyber Age*; Crown: New York, NY, USA, 2018.
29. Matania, E.; Yoffe, L.; Mashkautsan, M. A Three-Layer Framework for a Comprehensive National Cyber-Security Strategy. *Georget. J. Int. Aff.* **2016**, *17*, 77–84. [CrossRef]
30. Schmitt, M.N. (Ed.) *Tallinn Manual on the International Law Applicable to Cyber Warfare*; Cambridge University Press: Cambridge, UK, 2013.
31. CFR.org Editors. North Korea's Military Capabilities. Council on Foreign Relations. Available online: https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities#chapter-title-0-2 (accessed on 23 December 2021).

32. Bartlett, J. Why Is North Korea So Good at Cybercrime? *The Diplomat*, 3 November 2020. Available online: https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/ (accessed on 11 April 2021).
33. Index of Economic Freedom 2021. Available online: https://www.heritage.org/index/country/northkorea (accessed on 21 October 2021).
34. Caesar, E. The Incredible Rise of North Korea's Hacking Army. *The New Yorker*, 26 April & 3 May 2021 issue. Available online: https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army (accessed on 3 July 2021).
35. The Korea Herald. N. Korea Bolsters Cyberwafare Capabilities. 27 July 2014. Available online: http://www.koreaherald.com/view.php?ud=20140727000135 (accessed on 4 August 2021).
36. Larsen, M.S. While North Korean Missiles Sit in Storage, Their Hackers Go Rampant. *Foreign Policy*, 15 March 2021. Available online: https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/ (accessed on 14 August 2021).
37. Lederer, E.M. UN Experts: North Korea Using Cyber Attacks to Update Nukes. *Associated Press*, 10 February 2021. Available online: https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33 (accessed on 25 August 2021).
38. United Nations. *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*; S/2019/171; United Nations: New York, NY, USA, 5 March 2019.
39. Noone, G. North Korea: The Most Sophisticated Bank Robber around. *TechMonitor*, 11 March 2021. Available online: https://techmonitor.ai/techonology/cybersecurity/north-korea-most-sophisticated-bank-robber-around (accessed on 3 September 2021).
40. Ministry of National Defense of the Republic of Korea. 2020 Defense White Paper. Available online: https://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_202106300300426680.pdf (accessed on 10 September 2021).
41. Valeriano, B. Despite What the Cyber Skeptics Say, North Korea is Behind the Sonly Hack. *Slate*, 23 December 2014. Available online: https://slate.com/technology/2014/12/north-korea-is-behind-the-sony-attack-don-t-listen-to-cyber-skeptics.html (accessed on 16 January 2022).
42. Valeriano, B. Five Questions (and Answers) about North Korea and the Sony Hack. *The Washington Post*, 14 December 2014. Available online: https://www.washingtonpost.com/news/monkey-cage/wp/2014/12/14/five-questions-and-answers-about-north-korea-and-the-sony-hack/ (accessed on 17 January 2022).
43. George, A.L.; Bennett, A. *Case Studies and Theory Development in the Social Sciences*; The MIT Press: Cambridge, MA, USA, 2005.
44. Kim, M. Why Does a Small Power Lead? ASEAN Leadership in Asia-Pacific Regionalism. *Pac. Focus* **2012**, *27*, 111–134. [CrossRef]
45. Atherton, K. How North Korean Hackers Stole 235 Gigabytes of Classified US and South Korean Military Plans. *Vox*, 13 October 2017. Available online: https://www.vox.com/world/2017/10/13/16465882/north-korea-cyber-attack-capability-us-military (accessed on 9 August 2021).
46. Kim, C. North Korean Hackers Stole South Korea-US Military Plans to Wipe Out North Korea Leadership: Lawmaker. *Reuters*, 10 October 2017. Available online: https://www.reuters.com/article/us-northkorea-cybercrime-southkorea-idUSKBN1CF1WT (accessed on 20 August 2021).
47. Choe, S. North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says. *The New York Times*, 10 October 2017. Available online: https://www.nytimes.com/2017/10/10/world/asia/north-korea-hack-war-plans.html (accessed on 10 August 2021).
48. McCurry, J. South Korean Nuclear Operation Hacked amid Cyber-attack Fears. *Guardian*, 23 December 2014. Available online: https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack (accessed on 15 August 2021).
49. Larson, A. Korea Hydro and Nuclear Power Co. Hacked. *Power*, 22 December 2014. Available online: https://www.powermag.com/korea-hydro-and-nuclear-power-co-hacked/ (accessed on 18 August 2021).
50. BBC News. S Korea Nuclear Firm to Hold Cyber-attack Drills after Hack. 22 December 2014. Available online: https://www.bbc.com/news/world-asia-30572575 (accessed on 18 August 2021).
51. BBC News. The Lazarus Heist: How North Korea almost Pulled off a Billion-dollar Hack. 21 June 2021. Available online: https://www.bbc.com/news/stories-57520169 (accessed on 24 August 2021).
52. Chanlett-Avery, E.; Rosen, L.W.; Rollins, J.W.; Theohary, C.A. *North Korean Cyber Capabilities: In Brief*; Congressional Research Service Report; Congressional Research Service: Washington, DC, USA, 3 August 2017; pp. 1–12.
53. United Nations. *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*; S/2019/691; United Nations: New York, NY, USA, 30 August 2019.
54. Huillet, M. Report: North Korea-Sponsored Hacks Comprise 65 Percent of Total Crypto Stolen. *CoinTelegraph*, 19 October 2018. Available online: https://cointelegraph.com/news/report-north-korea-sponsored-hacks-comprise-65-percent-of-total-crypto-stolen (accessed on 11 September 2021).
55. Sanger, D.E.; Kirkpatrick, D.D.; Perlroth, N. The World Once Laughed at North Korean Cyberpower. No More. *The New York Times*, 15 October 2017. Available online: https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html (accessed on 2 October 2021).

56. Maness, R.C.; Valeriano, B.; Jensen, B. North Korea's Offensive Cyber Program Might Be Good, But Is It Effective? *Council on Foreign Relations*, 25 October 2017. Available online: https://www.cfr.org/blog/north-koreas-offensive-cyber-program-might-be-good-it-effective (accessed on 19 January 2022).
57. RTE. Cyber Attacks May Provoke a Military Response—NATO. 5 September 2014. Available online: https://www.rte.ie/news/2014/0905/641671-nato/ (accessed on 17 October 2021).
58. Cheng, J. Raising the Stakes: NATO Says a Cyber Attack on One is an Attack on All. *Defense Systems*, 8 September 2014. Available online: https://defensesystems.com/articles/2014/09/08/nato-cyber-attack-collective-response.aspx (accessed on 30 October 2021).
59. NATO. Brussels Summit Communique. 24 June 2021. Available online: https://www.nato.int/cps/en/natohq/news_185000.htm (accessed on 7 November 2021).
60. Ministry of Foreign Affairs of Japan. Japan-U.S. Security Consultative Committee (Japan-U.S. 2+2). 19 April 2019. Available online: https://www.mofa.go.jp/na/fa/page3e_001008.html (accessed on 18 November 2021).
61. Valeriano, B.; Jensen, B.; Maness, R.C. *Cyber Strategy: The Evolving Character of Power and Coercion*; Oxford University Press: Oxford, UK, 2018.
62. Snyder, G. *Deterrence and Defense*; Princeton University Press: Princeton, NJ, USA, 1961.
63. Jervis, R. *The Illogic of American Nuclear Strategy*; Cornell University Press: Ithaca, NY, USA, 1984.
64. Beeson, M. Hegemonic Transition in East Asia? The Dynamics of Chinese and American Power. *Rev. Int. Stud.* **2009**, *35*, 95–112. [CrossRef]
65. Kim, M. Why Provoke? The Sino-U.S. Competition in East Asia and North Korea's Strategic Choice. *J. Strateg. Stud.* **2016**, *39*, 979–998. [CrossRef]