Hardening the Shield Against North Korea’s “All-Purpose Sword”: An Evolving North Korean Cyber Threat and Its Policy Responses

Jie Gao

North Korea’s cyber warfare is an evolving security threat to the United States, its allies, and the international community. Pyongyang’s advancement in cyber weapons complements its broader strategy of creating an asymmetrical advantage vis-à-vis the U.S.-ROK alliance and is rooted in its guerrilla tradition. Cyber tools are also attractive to the regime because of their cost-effectiveness and low risks of retaliation. Given these motivations and the militarism in North Korean politics, cyber capabilities will continue to receive substantial investments from Pyongyang. This paper proposes four policy recommendations to deter North Korea’s cyber capabilities build-up: 1) establish a cyber defense and cyber deterrence mechanism in the U.S.-ROK alliance, 2) facilitate international cooperation, 3) strengthen public-private partnership, and 4) design a comprehensive government strategy.

Introduction

North Korea often makes news headlines for its use of high-profile nuclear weapons and missile tests. However, the regime also leverages threatening unconventional force through its cyber warriors. The current leader Kim Jong Un himself has acknowledged the significance of cyber warfare by equating it with nuclear weapons and referring to it as an “all-purpose sword” (만능의 보검).1 In recent years, North Korea has demonstrated increasing frequency and improved sophistication of its government-sponsored cyber operations. These capabilities will continue to help North Korea evade sanctions, collect sensitive information, disrupt the global economy, and threaten critical infrastructure if left unchecked.

This paper will provide a tailored overview of the North Korean cyber force and outline a strategy for the United States and South Korea to countermeasure this challenge. An analysis of North Korea’s political culture and security environment that drives it to invest in cyber capabilities will follow. Next, the paper will elaborate on the current state and future trajectory of the North Korean cyber threat by examining its cyber capabilities, objectives, and characteristics. The paper will conclude by offering four policy recommendations suggesting improvements in the U.S.-Republic of Korea (ROK) alliance cyber strategy, increased international cooperation, public-private partnership, and comprehensive U.S. government strategy to build a robust cyber defense and deterrence system against North Korean cyber threats.

Background of the North Korean Cyber Threat

Ruled by a repressive yet insecure regime, Pyongyang applies all instruments of state power to defend its rule. Its insecurity derived from the Korean War when the United States thwarted Kim Il Sung’s plan to unify the Korean Peninsula and almost subverted the newly established government in the 1950s. Thus, regime preservation has become the top priority for Kim and his successors, and developing a strong military force is deemed the most critical means to achieve that.

Against this backdrop, North Korean politics features militarism represented by Kim Jong Il’s Songun, or “military-first policy.” Under Songun, military advancement overrode the prosperity of the civilian economy and
received disproportional resources from the government. The current leader Kim Jong Un has pledged to alleviate the country’s prolonged economic grievance under *byungjin* — a policy that aimed to balance nuclear programs and the civil economy. Nevertheless, North Korea still maintains a high level of military spending, which accounts for around 16% of its total government expenditure since 2012, according to the budget plans announced by its Supreme People’s Assembly (SPA).2

Furthermore, a North Korean defector, previously a computer science professor at North Korea’s Hamheung Computer Technology University, estimated that the regime allocates between 10% and 20% of its military budget on cyber operations.3 These numbers reflect the salience of the military in North Korea’s politics and provide clues to its evolving cyber capabilities despite economic hardship.

The establishment of the Korea Computer Center (KCC) in 1990, the primary agency responsible for information technology strategy, marks the beginning of North Korea’s cyber capabilities. Following the creation of KCC, Kim Jong Il, in 1995 and 1998, issued two directives for the Korean People’s Army (KPA) General Staff to pursue cyber capabilities.4 North Korea’s arms capabilities, fighter traditions, and the incentives cyber operations provide have all served as the foundation for North Korea’s cyber strategy from its inception. First, North Korea’s weak conventional forces dictate its pursuit of asymmetric advantage. Although the KPA manages a troop twice larger than its South Korean counterparts, it lags far behind in equipment, capabilities, and skills.5 Thus, North Korea turned to new weapons, such as nuclear warheads and cyber tools, for asymmetric advantage to make up for its gap in conventional forces.

Second, the decentralized nature of cyber operations is consistent with North Korea’s guerilla tradition. North Korea’s founding leader, Kim Il Sung, established his reputation by fighting against Japanese colonialists as a guerrilla fighter in the 1930s. Kim Il Sung’s guerilla fellows later made up most of the North Korean political elites who led subversion campaigns against South Korea with guerrillas during the Cold War era. North Korean hackers today resemble guerilla fighters, as they sneak in the dark and ambush at the strategic weak points. These cyber guerrillas also seek financial resources through banditry and robbery, similar to their old comrades during the Korean War.6

Third, cyber campaigns are associated with low risks and rarely receive retaliation. Since internet users enjoy a high level of anonymity, investigations to attribute cyber-attacks to a specific party are challenging. Anonymity enables North Korea to deny responsibility for its cyber operations while avoiding the risk of retaliation.7 Furthermore, as the international community primarily focuses on monitoring and sanctioning North Korea’s nuclear and missile programs, Pyongyang takes advantage of the international communities’ diverted attention and a lack of effective deterrents to conduct its cyber operations.8

Fourth, cyber operations are cost-effective, with relatively low barriers to entry and potentially high yield. Although the initial stage of knowledge build-up and personnel training can be laborious, the maintenance and improvement of established cyber capabilities require fewer investments in materials and human resources than other forms of warfare. In addition, North Korean hackers can access technical know-how from open-source resources or illegal domains.9
Despite these incentives, North Korea’s international isolation and economic backwardness have led the international community to underestimate the regime’s determinations and capabilities to develop cyber weapons. A 2009 U.S. National Intelligence Estimate downplayed the possibility of an imminent North Korean cyber threat. However, high-profile incidents such as the 2014 cyber-attack on Sony Pictures and the 2016 cyber theft from the Bangladesh Bank highlight the rapid evolution of North Korea’s cyber capabilities.

In sum, North Korea’s weak conventional force and guerrilla tradition, paired with cyber operations’ cost-effectiveness and low level of risks, suggests North Korea will continue to invest in strengthening its cyber capabilities, regardless of its dire economic situation.

North Korean Cyber Threat Today and Its Future Trends

Kim Jong Un has further strengthened North Korea’s emphasis on cyber warfare. Pyongyang has mainly leveraged cyber tools for disruption, espionage, and financial theft. While North Korean hackers have targeted a broad array of countries, South Korea and the United States are the most frequent targets. This section will introduce the structure of North Korea’s cyber-relevant organizations and analyze its cyber capabilities and future trends based on reported cases.

Organization

Figure 1 illustrates the structure of the North Korean government and military organizations relevant to cyber operations. According to an estimation by the South Korean government, the Reconnaissance General Bureau (RGB) is generally considered the center of North Korean cyber activity, with more than 6,000 full-time cyber experts. RGB directly reports to the State Affairs Commission (SAC), chaired by DPRK leader Kim Jong Un. Subordinated to the RGB, Bureau 121 is North Korea’s most significant cyber unit that conducts various cyberspace missions, including offensive and defensive cyber operations, cyber espionage, network exploitation, and cybercrime. In addition to the RGB, KPA’s General Staff Department (GSD) also engages in North Korea’s cyber operations with missions such as electronic warfare, information warfare, and psychological operations. The five GSD bureaus relevant to cyber operations include the Operations Bureau, Communications Bureau, Electronic Warfare Bureau, Command Automation Bureau, and the Enemy Collapse Sabotage Bureau.
Figure 1: North Korea's Organization of the Cyber-Related Units


Other identified North Korea-tied hacker groups include the Lazarus Group, the Bluenoroff Group, the Andariel Group, TEMP.Firework, and Kimsuky. In addition, Pyongyang’s Mirim College for Electronic Warfare Research reportedly serves as the training camp for future North Korean hackers.

Objectives

North Korea’s cyber operations mainly serve three objectives: causing disruption, conducting espionage, and generating revenue. First, North Korea has carried out cyberattacks on critical infrastructure to disrupt conventional operations and provoke its opponents – two traditions in North Korea’s strategic concepts. For example, in 2008, North Korea conducted large-scale cyberattacks against the South Korean government, which shut down 400 computers at the transition office of South Korea’s President Lee Myung-bak. Even before adopting cyber operations, North Korea’s special forces had attempted to disrupt the South Korean government, for example, with its “Blue House Raid” in 1968. North Korea’s cyber campaigns that jammed airline GPS signals to gain control of the aircraft are also new technology for an old strategy, as one may recall from the bombing of Korean Air Flight 858 in 1987. North Korean common cyberattack targets include media, banking systems, nuclear power plants, transportation networks, and government websites. By focusing on these targets, North Korean cyberattacks try to instill fear and inconvenience in general populations by crippling their infrastructure and services crucial to everyday lives.

Second, North Korea seeks to collect classified and sensitive information through cyber espionage. While South Korean and U.S. military departments and defense industries are the main targets of North
Korean hackers, academic institutions and pharmaceutical companies have also reported information theft tied to North Korea. In September 2016, North Korean hackers infiltrated the South Korea Defense Integrated Data Center and stole 234 gigabytes of classified military documents, including war plans. As previously mentioned, North Korea most likely relies on cyber espionage to overcome its lack of conventional military capability compared to its U.S. and South Korean targets.

Pyongyang has also used cyber operations to collect information for its nuclear programs. In 2019, the North Korea-affiliated hack group Kimsuky broke into the network of a nuclear power plant in Kundakulam, India, for proprietary information on thorium-based reactors.

Third, cyber financial thefts are critical channels for North Korea to generate revenue. As its economy is under heavy sanctions imposed by the international community, particularly the United States, North Korea has been conducting cybercrimes to evade sanctions. One of the most notorious examples is the Bangladesh Bank cyber heist in February 2016. North Korean hackers managed to transfer nearly $81 million from the central bank of Bangladesh after compromising its computer network. A report by the United Nations Security Council (UNSC) estimates that North Korean hackers have stolen a cumulative $2 billion as of 2019. With illicit funds raised from cybercrimes, the Kim regime can continue to develop its nuclear and missile programs as well as provide private benefits to its political elites – both essential to its regime survival.

Capabilities

North Korean hackers have demonstrated increasing sophistication in their tactics. The aforementioned cyber theft of Bangladesh banks in 2016 is a representative case revealing Pyongyang’s cyber proficiencies. During this theft, North Korean hackers took advantage of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’s global network and inserted malware into a SWIFT terminal used by Bangladesh’s central bank. Noted by the FBI, such an operation “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.”

In addition to attacking the weak points of the cyber systems, North Korean hackers are adept at social engineering to exploit human vulnerabilities. For example, North Korean cyber groups have previously sent fake job offers from defense contractors to defense and aerospace experts and retrieved classified information with the data-gathering implants in the emails. North Korean hackers disguised themselves with fictitious social media accounts on WhatsApp, Facebook, and LinkedIn and built their credibility through extensive dialogues via email and phone calls.

However, some observers have also pointed out the limitations of North Korea’s cyber capabilities. Josephine Wolff, an associate professor of cybersecurity policy, noted the WannaCry ransomware policy, noted the WannaCry ransomware launched in 2017 “was surprisingly unprofitable” for a financially-motivated campaign. While the ransomware had attacked around 200,000 computers in 150 countries and requested $300 for each device, estimates by a cybersecurity company showed that North Korea might only have earned $386,905 – though the costs inflicted on affected systems summed up in billions.

Future Trends

In the following years, the international community can expect North Korea to
conduct more frequent cyber operations. Statistics from the South Korean Ministry of Defense showed that “hacking attempts against South Korean forces increased from 4,000 cases in 2017 to approximately 5,000 cases in 2018, and 9,533 cases in 2019.”*33

Through an analysis of data from the UNSC, the Heritage Foundation, and the Council on Foreign Relations, this paper finds that nearly half (43%) of North Korean cyber operations are financially motivated, followed by aims to disrupt (36%) and espionage (21%) (Figure 2). As a result, financial institutions, including banks and cryptocurrency exchanges, are the most common targets of North Korean hackers (Figure 3). Since Pyongyang continues to suffer from economic sanctions, North Korea will likely increase the intensity of its cyber thefts from financial institutions in the near future. In terms of locations, while North Korea has attacked countries worldwide, its cyber operations have

concentrated on targets in South Korea and the United States (Figure 4). This trend will likely continue, given Pyongyang's hostility toward Seoul and Washington. Moreover, there is a notable trend that North Korea’s cyber operations have been expanding in their scope with campaigns against individuals and organizations from multiple countries at one time.

Figure 2: North Korea’s cyber operations by Purpose

Figure 3: North Korea’s cyber operations by Target

Figure 4: North Korea’s cyber operations by Location
Policy Recommendations

North Korea’s cyber-attacks constitute a growing threat to the United States, its allies, and the international system, as Pyongyang uses cyberweapons to cause disruption, conduct espionage, and generate revenue. This paper proposes four policy recommendations to deter Pyongyang’s cyber capabilities build-up:

- Establish a cyber defense and cyber deterrence mechanism in the U.S.-ROK alliance,
- facilitate international cooperation,
- strengthen public-private partnerships,
- and design a comprehensive government strategy.

First, Washington and Seoul should further align their cyber defense and cyber deterrence capabilities through their military alliance.34 South Korea’s recent participation in the cyber defense center for the North Atlantic Treaty Organization (NATO) is a positive development.35 Established in 2008, NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE) provides member nations with “unique interdisciplinary expertise in the field of cyber defense research, training and exercises covering the focus areas of technology, strategy, and law.”36 Seoul’s membership in the CCDCE will improve its understanding of North Korea’s cyber strategy and enhance its cyber defense against Pyongyang’s persistent attacks.

Though it is debatable whether current cyber-attacks from North Korea have strategic effects on South Korea, deterring North Korea’s low-level attacks may be challenging, as deterrence experts assess Pyongyang as “a very determined cyber actor.”37 Therefore, the U.S.-ROK alliance should focus on strategic-level attacks in the cyber domain. Specifically, Washington and Seoul should issue joint statements on cyber deterrence with unambiguous language indicating the incorporation of cyber deterrence in their mutual defense treaty.38 Furthermore, the alliance should formulate a detailed cyber deterrence strategy, identifying the corresponding retaliation against North Korea’s cyber-attacks and properly signaling to Pyongyang.39

Second, Washington and Seoul should reach out to the international community for broader cooperation. While North Korea’s Internet is largely isolated from global networks, its hackers operate around the world and launch cyber-attacks via overseas servers.40 Additionally, considering North Korea’s escalating scope and scale of its cyber operations against multiple countries, combined efforts from the international community to protect critical global infrastructure like the SWIFT are immediately needed to tackle the North Korean cyber threat.

The first step should be expanding the narrow focus on North Korea’s conventional weapons capabilities to incorporate cyberspace into international monitoring and regulation.41 By sharing information with international partners on suspicious cyber activities and tactics North Korean hackers use, U.N. members will be better prepared to defend against North Korea’s cyberattacks and expose their footprints for global warnings. Developing countries in Southeast Asia, Africa, and Latin America should receive special attention in this effort. Based on the historical records, their relatively poor cyber defense systems make them attractive and vulnerable targets of Pyongyang for financial thefts. The United States can assume leadership in facilitating inter-government coordination, establishing the international legal framework and law enforcement agencies, and promoting compliance with cybersecurity standards.42
These efforts also have broader implications for defending and deterring malicious cyber operations by other actors. However, Washington should also be aware of potential pushback from other international actors who may interpret it as Washington’s attempts to dominate cyberspace.

**Third, the United States should strengthen public-private partnerships to countermeasure North Korean cyber-attacks on private corporations and financial institutions.** Private firms tend to “underestimate cyber risks and underinvest in cybersecurity or prefer to ‘free ride’ while expecting the government to manage the North Korean cyber threat.” Moreover, private firms often refrain from reporting cyberattack incidents to protect their reputation. However, the surprising similarity in the cyber tactics used by North Korean hackers suggests the importance of information sharing to alarm the public and private sectors. For example, the malware that attacked Sony Pictures in 2014 had many overlaps with the one used against South Korean banks in 2013. Therefore, it is imperative to encourage information sharing and compliance with cybersecurity rules to improve the resilience of private sector systems.

Washington can achieve this through both formal and informal channels. The government can use legal frameworks such as The Cybersecurity Information Sharing Act to coordinate information sharing among various entities. The Internet Corporation for Assigned Names and Numbers (ICANN) is a model for establishing an informal private-public partnership. Established in 1998 to ensure the network’s stability and security, ICANN has expanded from a U.S. national focus to global governance under the guidance of an international board of directors with diverse backgrounds. In addition, the government should promote education and training programs for individuals to raise public awareness of North Korean cyber tactics.

**Fourth, the United States should establish a comprehensive whole-of-government strategy.** The diversity of Pyongyang’s cyber operations in its targets and effects would require collaborations from at least “the Departments of Treasury, Justice, Defense, Commerce, and Homeland Security as well as the Intelligence Community” directed by the White House. The Department of State International Cyberspace Policy Strategy released in March 2016 is an inspiring attempt. It described a whole-of-government approach to cyber deterrence with diplomacy, law enforcement, economic tools, military force, and intelligence capabilities. The creation of a National Cyber Director that advises the President on cyber policy is another welcomed development. Washington will need to specify the authority and procedures for inter-agency coordination to consolidate these efforts.

**Conclusion**

North Korea’s cyber warfare is an evolving security threat to the United States, its allies, and the international community. Pyongyang’s advancement in cyber weapons complements its broader strategy of creating an asymmetrical advantage vis-à-vis the U.S.-ROK alliance and is rooted in its guerrilla tradition. Cyber tools are also attractive to the regime because of their cost-effectiveness and low risks of retaliation. Given these motivations and the militarism in North Korean politics, cyber capabilities will continue to receive substantial investments from Pyongyang.

To date, North Korean hackers have demonstrated increasing sophistication in their techniques while expanding the scope and scale of their operations. Pyongyang...
mainly applies cyber weapons to cause disruption, conduct espionage, and generate revenue. As such, North Korea poses significant threats to critical infrastructure, classified and sensitive information, and financial institutions around the world.

Defending and deterring North Korean cyberattacks requires extensive inter-government and intra-government cooperation and a public-private partnership. Furthermore, strengthening the U.S.-ROK alliance in cyberspace is critical to preventing North Korea from undermining the stability and security of the Korean Peninsula. Washington and Seoul should send clear messages and take firm actions to counter Pyongyang’s aggression in the cyber domain.

About the Author: Jie Gao is an M.A. candidate in Security Studies at Georgetown University. Her research interests include U.S.-China relations, Chinese domestic politics, security issues in Asia, and artificial intelligence.


8 Kleine-Ahlbrandt, 2020, pp.7-8.


12 The State Affairs Commission replaced the National Defence Commission in 2016 and expanded its scope to include issues aside from defense and security.


14 ROK Ministry of National Defense, 2018


18 Suh, 2022.


22 Kim, Min-hyung, “North Korea’s Cyber Capabilities and Their Implications for International Security,” *Sustainability*, 2022, https://doi.org/10.3390/su14031744

23 Kim, 2022.

24 Thorium is a safer and more efficient alternative to uranium. Klingner, 2021.


29 Kim, 2022, pp.8.
30 Klingner, 2021, pp.7.
39 Ibid.
40 Kim, 2022, pp.9.
43 Pinkston, 2016, pp.64.
44 Kim, 2022, pp.10.
45 Jun, LaFoy, and Sohn, 2015, pp.75.
47 Ibid.
49 Klingner, 2021, pp.11.
51 Klingner, 2021, pp.11.