Michael Raska*

North Korea's Evolving Cyber Strategies: Continuity and Change

https://doi.org/10.1515/sirius-2020-3030

Abstract: Pyongyang sees the Korean Peninsula as entrenched in a geopolitical deadlock among great powers, with the United States continuing to employ what the North Korean regime sees as a "hostile policy" detrimental to its survival, its ability to shape relevant events, and the country's political and economic development. While the core security concerns of South Korea and the United States are North Korea's growing nuclear weapons and ballistic missile capabilities, the alliance must increasingly also prioritize the continuous development of North Korea's cyber capabilities, both offensive and defensive. North Korea aims to gain strategic advantage by pursuing cost-effective, asymmetric military capabilities, including cyber strategies, to gather intelligence, coerce its rivals, financially extort others, and otherwise exert influence in ways that are resistant to traditional deterrence and defense countermeasures. Seoul and Washington need a full-spectrum military readiness posture against the full range of potential North Korean provocations, while European democracies need to strengthen their cyber readiness posture to effectively track and counter North Korea's evolving global cyber operations.

1 Introduction

Since 2009, North Korea's cyber operations, organizational structures, and capabilities have evolved with divergent tactics, techniques, and procedures. These include patterns of cyber espionage and distributed denial of service attacks on select political and socioeconomic targets in South Korea, to cyber-enabled information, economic, and political warfare globally. Indeed, since 2014, the trajectory of North Korea's cyber operations shows an increasing priority on cyber-enabled economic and political warfare, in which North Korean cyber units and state-sponsored hacking groups aim to counter international sanctions, while generating resources for North Korea's economic and technological development.

North Korean hackers, operating largely outside the country, have spearheaded fraudulent cyber operations to circumvent sanctions, gaining access to the international financial system and illegally forcing the transfer of funds from financial institutions, SWIFT banking networks, and cryptocurrency exchanges worldwide.[1] At the same time, North Korea also has been able to protect its critical infrastructure from potential reprisals, limiting its access, dependencies, and vulnerabilities on the internet and communication networks by relying instead primarily on China's internet infrastructure. This has been augmented only recently with a second internet link to Russian networks, and dispersion of its hackers to select countries worldwide, including India, Nepal, Kenya, Mozambique, and Indonesia.[2]

Consequently, North Korea's twenty-first-century cyber operations have essentially become weapons of mass effectiveness working alongside the weapons of mass destruction in its nuclear arsenal, together composing a unified asymmetric political strategy designed to pressure the United States and the wider international community to recognize as legitimate Supreme Leader Kim Jong Un's interpretation of North Korea's sovereignty and security. As Kim reportedly declared in 2013, "cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."[3]

Prior to the analysis, a caveat is in order. Any assessment of North Korea's evolving cyber operations and the strategic rationales underlying them, is a challenging task, not only because attribution is a recurring point of contention but also because of the closed nature of the country's totalitarian government and society. Accord-

***Contact: Dr. Michael Raska**, Assistant Professor at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

1 United Nations 2019, 48–51.

2 Priscilla Moriuchi: North Korea's Ruling Elite Adapt Internet Behavior to Foreign Scrutiny," *Recorded Future Blog,* April 25, 2018; https://www.recordedfuture.com/north-korea-internet-behavior/

3 Hyungsoo Kim: Kim Jong-Un Says 'Cyber Warfare Is an All-Powerful Tool,' Utilizes It as One of Three Major Means of Warfare, *Joongang Ilbo*, November 5, 2013; David Sanger/David Kirkpatrick/Nicole Perlroth: The World Once Laughed at North Korean Cyberpower. No More, *New York Times*, October 15, 2017.

ingly, the available open-source data are limited mainly to threat intelligence reports and investigations by global cybersecurity firms; select statements and publications by the U.S. and ROK governments; select North Korean defectors with partial knowledge of North Korea's cyber activities; secondary literature such as think tank reports and academic articles; and, ultimately, references in North Korean newspapers and other media outlets. Each source carries internal and external validity risks, including government bias and political agendas, outdated data, and intelligence blind spots.

Varying previous assessments over the years have fueled an ongoing debate on the direction, character, capabilities, and strategic impact of North Korea's cyber operations. On the one hand, sceptics argue that there are serious limitations to North Korea's use of cyberspace for political purposes, particularly at the strategic level. According to this view, North Korea's cyber operations alone do not strengthen its capabilities for coercion or deterrence—to date, these capabilities have not caused any government to back down or change course, nor have they enabled Pyongyang to achieve substantial political, military, or financial gains related to North Korea's key strategic objectives. Consequently, this line of thinking goes, North Korea's cyber capabilities do not provide Pyongyang with significant strategic advantages for achieving political aims, nor are they sufficient to degrade U.S. or any other advanced retaliatory capabilities to ensure regime survival.[4]

The opposing perspective, however, is that North Korea's cyber capabilities have gradually evolved in scope and sophistication, driven mainly by strategic necessity, giving the regime power and freedom of action in an adversarial strategic environment. Based on this view, Pyongyang's varying cyber and information operations have provided relatively low-cost asymmetric options for demonstrating power without any visible military commitments, raising hundreds of millions of dollars to support the Kim regime and its nuclear and ballistic missile programs, and, ultimately, enabling Pyongyang to effectively counter stricter economic sanctions under a shroud of plausible deniability.[5]

North Korean hacker groups have indeed been able to develop a wide variety of tools and asymmetric methods for achieving national goals. In particular, North Korea's cyber operations reflect at least three distinct characteristics. First, North Korea's cyber units and hacker groups have shown considerable diversity in terms of their capabilities and experience—from very low-skilled to high-skilled hackers—a range that has made benchmarking their performance solely on such criteria more challenging. At the same time, North Korean hacker groups have been widely dispersed geographically, acting independently or mutually supporting each other based on their specific cyber missions which range from intelligence-driven cyber espionage, information manipulation, and political warfare to offensive and defensive military cyber operations, electronic warfare, and covert financial extortion. Accordingly, the line between low-end and high-end North Korean cyberspace operations frequently has been blurred; North Korea can employ nonstate actors as surrogates, utilize low-cost, off-the-shelf tools that are freely available, and exploit known vulnerabilities and techniques such as denial of service attacks.

At the same time, North Korea may engage in resource- and intelligence-intensive operations that discover vulnerabilities in systems (zero-day exploits) and apply strategies of denial, disruption, destruction, or subversion of information or physical infrastructure. Such operations, whether strategic or tactical, can also range in duration from short to long-term.

North Korea's cyber strategy and tactics continue to reflect "a holistic effort on information warfare that incorporates all aspects of affecting information such as electronic warfare, cyber warfare, and psychological operations."[6] In the long term, North Korea's converging cyber, nuclear, and conventional strategies will pose new challenges to the U.S.-ROK alliance.

2 North Korea's Cyber Units and Organizational Structure

A brief look at the origins of North Korea's cyber operations is a useful starting point. The country's interest in cyber warfare began in the mid-1990s, when the Korean People's Army (KPA) studied the "electronic intelligence warfare" concepts formulated by the People's Liberation Army (PLA) of China, extrapolating the strategic impli-

4 Ryan C. Maness/Brandon Valeriano/Benjamin Jensen: North Korea's Offensive Cyber Program Might Be Good, But Is it Effective? *Blogpost at Council on Foreign Relations, Digital and Cyberspace Policy Program*, October 25, 2017; https://www.cfr.org/blog/north-koreas-offensive-cyber-program-might-be-good-it-effective; James Lewis: North Korea and Cyber Catastrophe—Don't Hold Your Breath, *38 North Blog*, January 12, 2018. Available at: https://www.38north.org/2018/01/jalewis011218/.

5 Sanger/Kirkpatrick/Perlroth: The World Once Laughed at North Korean Cyberpower. No More, op cit.

6 Jun/LaFoy/Sohn 2015, 51.

cations of U.S. electronic warfare and cyber operations during the First Gulf War and the North Atlantic Treaty Organization (NATO) campaign in the Balkans.[7] In 1995, then supreme leader Kim Jong Il issued a directive for the KPA General Staff to develop 'information warfare' capabilities.[8] In September 1998, North Korea established Unit 121 within the Staff Reconnaissance Bureau of the KPA, a unit initially believed to be staffed by between 500 and 1,000 members tasked with research and development of cyberattack techniques, software engineering, cryptography, and networking at top computer science programs in China and Russia, as well as preparing cyber operations from abroad, according to disclosures by two North Korean cybersecurity experts and defectors, Kim Heung Kwang and Jang Se Yul.[9] Most Unit 121 cadres were selected from North Korea's top technology-oriented colleges such as Pyongyang University of Automation (previously called Mirim College), the Amrokgang College of Military Engineering, the National Defense University, and the Pyongyang Computer Technology University.[10] At that time, much of North Korea's computer infrastructure and many of its related facilities were rudimentary, as was the case for much in the early phases of North Korea's cyber warfare programs, which experimented with basic cyberattack techniques and first-generation malware. In 2009, U.S. National Intelligence Estimate dismissed North Korea's cyber capabilities, along with its long-range missile programs, noting that would take years to develop them into a meaningful threat.[11]

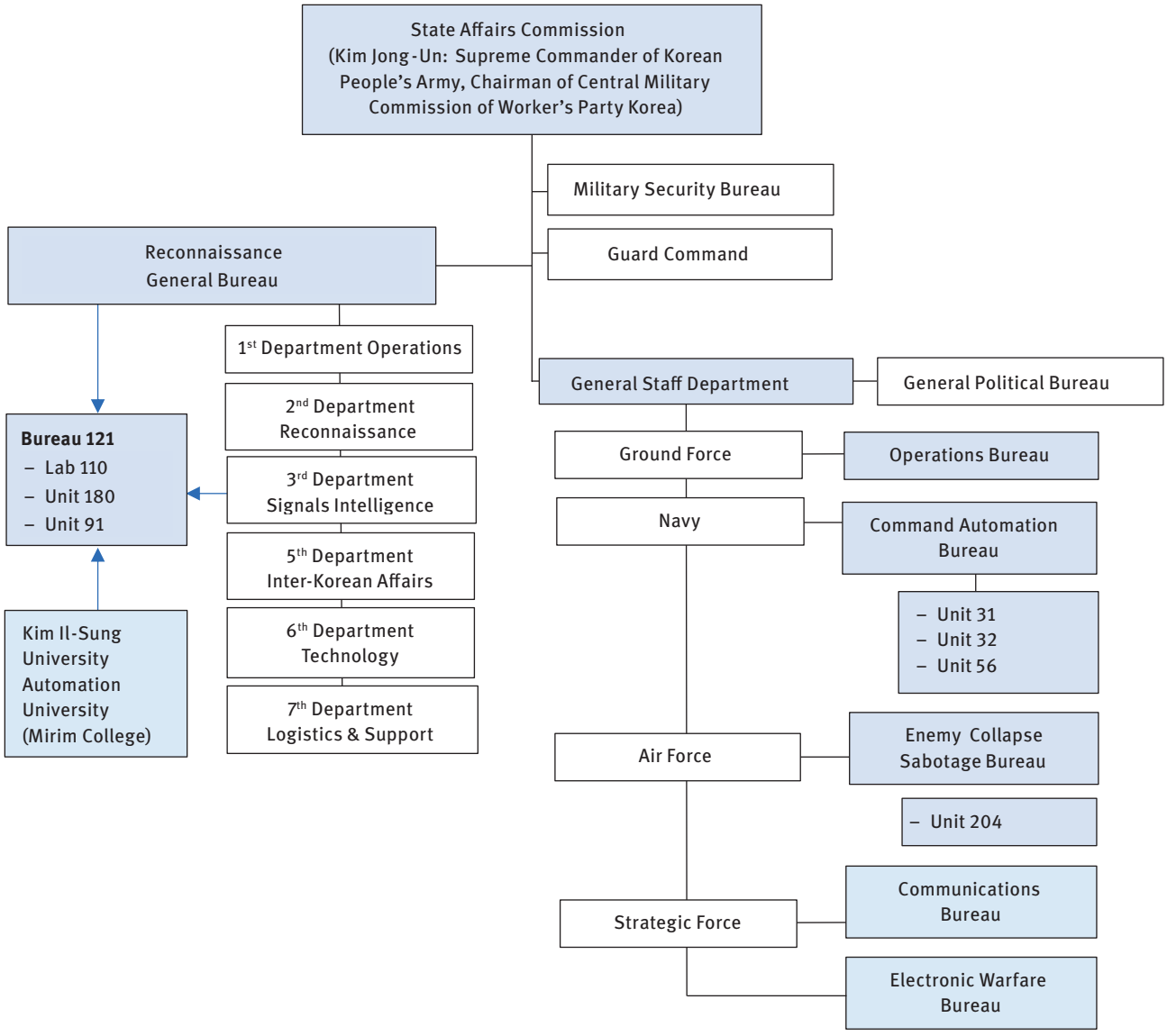
That same year, North Korea unified all of its intelligence and internal security services and initially brought them under the direct control of the National Defense Commission to cement the control of Kim Jong Un as the successor to Kim Jong Il. It merged intelligence organizations and its various cyber departments and bureaus from the Korean Workers' Party, the Operations Department and Office 35 (foreign operations), and the military intelligence Reconnaissance Bureau of the Korean People's Army into one Reconnaissance General Bureau (RGB).[12] The RGB became North Korea's primary foreign intelligence service as well as headquarters for special and cyber operations.[13] The RGB, headed by General Kim Yong Chol (2009–2016), integrated Unit 121, increased its size to 3,000 persons, and upgraded its status to that of a "department" also known as *Bureau 121* – the Cyberwarfare Guidance Bureau.[14]

While the exact structure of the RGB's cyber units has been obscured by secrecy, various cover designations, and internal restructurings over the years, references in open-source literature indicate that *Bureau 121* controls *Unit 91*, *Unit 180*, and *Lab 110*, the core cyber-focused components under the RGB and its six bureaus (which include Operations, Reconnaissance, Foreign Intelligence, Inter-Korean Dialogue, Technical, and Rear Services).[15] In particular, the RGB's largest cyber unit, Bureau 121, likely has been comprised of offensive and defensive cyber intelligence-gathering and attack subunits and teams based on their responsibilities, skills, and mission-tasking – i. e. the stem analysis team, the attack operations team, the code processing team, the development team, the inspection team, the network analysis team, and the battle planning team.[16] Collectively, the primary mission of the unit has likely focused on both offensive and defensive cyber operations, including targeting critical information infrastructure – i. e. communications, transportation networks, electricity grids, and aviation systems in 'unfriendly' nations – primarily the United States and South Korea. At the same time, Bureau 121 conducts cyber espionage against the government, military, defense industry, and media of other target countries.[17]

One of the key enablers to Bureau 121's cyber operations is likely the RGB's Computer Technology Research Lab – Lab 110 – believed to provide software engineering, technical reconnaissance, infiltration of computer networks, intelligence gathering through hacking, and planting viruses on targeted networks.[18] While the exact operational relationship and collaboration between Bureau 121 and Lab 110 is not known, it has been reported that Lab 110 analyzes technological configuration and behavior patterns of targets and then develops tailored software and malware, which is then used by cyber-attacks by the Bureau 121.[19]

7 Pinkston 2016.
8 Pinkston 2016, 60.
9 Sangwon Yoon: North Korea Recruits Hackers at School, *Aljazeera News*, June 21, 2011.
10 Ibid.; s. a. Brian McWilliams: North Korea's School for Hackers, *Wired Magazine*, February 6, 2003; https://www.wired.com/2003/06/north-koreas-school-for-hackers/.
11 Sanger/Kirkpatrick/Perlroth: The World Once Laughed at North Korean Cyberpower, op.cit.
12 Bermudez 2010.
13 Jun/LaFoy/Sohn 2015, 51.
14 Sangwon Yoon: North Korea Recruits Hackers at School, op. cit.
15 Bermudez 2010, Bermudez 2016.
16 Lee 2017, 22.
17 Jiro Yoshino: North Korea's Cybertroops Span the Globe in Quest for Cash, *Nikkei Asian Review*, March 15, 2018; https://asia.nikkei.com/Politics/International-relations/North-Korea-s-cybertroops-span-the-globe-in-quest-for-cash.
18 Tosi 2017, 26.
19 Lee 2017, 22.

Figure 1: North Korea's Cyber Organizations in the Reconnaissance General Bureau and the General Staff Department



Sources: Author; Adapted from ROK Defense White Paper 2012; see also Boo et.al. 2013, 94; Boo 2017; Jun/LaFoy/Sohn 2015; Sang-ho Song: North Korea Bolsters Cyberwarfare Capabilities, Korea Herald, July 27, 2014, http://www.koreaherald.com/view.php?ud=20140727000135

In June 2018, the U.S. Justice Department unsealed charges against an alleged hacker for the North Korean government in connection with a series of major cyberattacks including the 2014 assault on Sony Pictures Entertainment and WannaCry ransomware virus, which infected hundreds of thousands of computers in 150 countries and shut down dozens of emergency rooms in U.K. hospitals.[20] The complaint attributes Park Jin Hyuok as a member of Lab 110 responsible for "a wide-ranging, multi-year conspiracy to conduct computer intrusions and commit wire fraud by co-conspirators working on behalf of the government of the Democratic People's Republic of Korea, while located there and in China... the conspiracy targeted computers belonging to entertainment companies, financial institutions, defense contractors, and others for the purpose of causing damage, extracting information, and stealing money, among other reasons."[21]

20 Hamish Mcdonald: Fog of Cyberwar Spurs Virtual Arms Race On Korean Peninsula, *Nikkei Asian Review*, May 22, 2017.

21 United States District Court for the Central District of California: Criminal Complaint: United States of America v. Park Jin Hyok, Case

In 2013, the RGB under order of Kim Jong-un, reportedly established Unit 180 consisting of around 500 members from the Bureau 121, specifically tasked with hacking international financial institutions to extract foreign currency in support of North Korea's nuclear and ballistic missile programs, as well as install malicious backdoors in the software development business in Japan and China, according to interviews by Kim Heung-kwang.[22] In 2014–15, North Korea reportedly reorganized their cyber divisions – Unit 180 would specialize in targeting cryptocurrency exchanges – for example, in January 2018, South Korea's intelligence agency NIS flagged the Unit 180 as a likely perpetrator of a $530 million theft of the digital cryptocurrency NEM from the Tokyo exchange operator Coincheck.[23] Meanwhile, Bureau 121 expanded their cyber operations beyond South Korea, by attacking foreign nation's infrastructure such as transportation networks, telecommunications, electric and nuclear power grids, and aviation systems.[24] Part of the 2014/15 cyber revamp also included the elite *Unit 91*, initially tasked to conduct cyber espionage operations against government, corporate, and citizen targets of South Korea,[25] but since 2014/15 shifting its focus on "acquiring advanced technologies needed for nuclear development and long-range missiles from developed countries."[26] In 2016, all RGB's cyber units have come under the direct control of the State Affairs Commission (SAC), which replaced the National Defence Commission, as the supreme policy and power organizations of the DPRK Government.[27]

Parallel to the RGB-led cyber units and operations, it is important to note the military-cyber components of the Korean People's Army (KPA) and its General Staff Department (GSD) responsible for integrating cyber capabilities into conventional military operations. At its core, the KPA's conceptions of cyberwarfare seem to have adopted and adapted from China's People's Liberation Army (PLA) electronic intelligence warfare (EIW), computer network warfare (CNW), psychological warfare, military deception, and information warfare (IW).[28] The GSD bureaus such as the Electronic Warfare Bureau and the Enemy Collapse Sabotage Bureau (Unit 204) have been reported to be tasked with varying electronic, information and psychological warfare that leverage cyber operations, primarily to disrupt the ROK – U.S. conventional operations during wartime.[29] Prior and during wartime, KPA's integrated cyber operations would likely be used as asymmetric means supporting varying lines of effort such as drone strikes, special force incursions, and ballistic missile attacks, in order to disrupt U.S.-ROK command and control infrastructure, and overall to offset North Korea's conventional military-technological disadvantages.[30]

In this context, KPA's cyber warfare units are embedded in the GSD's Command Automation Bureau: Unit 31 – responsible for malware development; Unit 32 – responsible for software development for military use; and Unit 56 – responsible for software development for military command and control.[31] These units arguably provide software engineering/development teams, responsible for developing the tools and capabilities, which are likely also used by the operational bureaus within the RGB.

In 2016, the GSD has established a new department for Command, Control, Communication, Computer, and Intelligence (C4I) in the military, which superseded the now defunct Command Information Bureau.[32] The likely purpose of the new C4I department is to accelerate the integration of offensive cyber capabilities into conventional operations – i. e. targeting critical infrastructures, and more importantly, enhancing defensive cyber capabilities of the KPA's command and control systems. These have been reportedly compromised by the U.S. military top secret program to disable North Korea's ballistic missiles before liftoff ("left of launch") by means of cyberwarfare, directed energy, and electronic attacks.[33] To counter such measures, North Korea is reportedly developing a quantum encryption technology in an effort to build a highly secure command and control link between Pyong-

No. MJ18-1479, June 8, 2018, p.3; https://assets.documentcloud.org/documents/4834314/Read-the-DOJ-s-criminal-complaint-against-an.pdf

22 Ju-min Park/James Pearson: Exclusive: North Korea's Unit 180, the Cyber Warfare Cell that Worries the West, *Reuters*, May 21, 2017.

23 Cynthia Kim: South Korean Intelligence says N. Korean Hackers Possibly behind Coincheck Heist – Sources, *Reuters*, February 6, 2018.

24 Steve Miller: Where Did North Korea's Cyber Army Come From? *Voice of America*, November 20, 2018.

25 Charlie Campbell: Why We Shouldn't Be Surprised If North Korea Launched the WannaCry Ransomware Cyberattack, *Time*, May 17, 2017.

26 Steve Miller: Where Did North Korea's Cyber Army Come From, op. cit.

27 National Defense Commission (Defunct); *NK Leadership Watch website*, https://nkleadershipwatch.wordpress.com/dprk-security-apparatus/national-defense-commission

28 Mansourov 2014.

29 Jun/LaFoy/Sohn 2015, 51.

30 TRADOC NK tactics.

31 Jun/LaFoy/Sohn 2015, 47.

32 Lee 2017, 23.

33 David E. Sanger/William J. Broad: Trump Inherits a Secret Cyberwar Against North Korean Missiles, *New York Times*, March 4, 2017.

yang and key missile launching sites such as Wonsan, Tonghae, or Sohae.[34]

3 North Korea's Cyber Activity Clusters

Externally, there has been a significant overlap in classifying North Korean cyber groups based on tactics, techniques, and procedures (TTPs) – some sources may refer to RGB's cyber units as *"Lazarus Group"* and to any activity attributed to North Korea, while other sources track North Korean clusters or groups such as *Bluenoroff, APT37 (Reaper)*, and *APT38* separately. Other sources refer some activity associated with those group names by the RGB's Lazarus Group.[35] The U.S. Government refers to the malicious cyber activity by the North Korean government as *HIDDEN COBRA*.[36] Based on open-source government and private cybersecurity threat-intelligence reports, however, one could argue that there are a number of subgroups associated with the RGB, with distinct TTPs that should not be mistaken to be all under or being subgroups of Lazarus group. (See Table 1).

According to a recent analysis of North Korean-attributed malware by McAfee Labs, for example, "the North Koreans have groups with different skills and tools that execute their focused parts of cyber operations while also working in parallel when large campaigns require a mix of skills and tools."[37] For example, APT 37 (Reaper), Kimsuky and Sun Team have distinct TTPs specializing in political cyber-espionage, when compared to Lazarus-associated Andariel, APT 38 (Bluenoroff) groups focusing on financial extortion and cybercrime. With the increasing scope and levels of sophistication of TTPs, however, North Korea's cyber units have progressively developed their resources, assets, malware arsenals and coding capabilities based on their experience and lessons learned from attacking different targets, and collaborating in various attack campaigns by sharing networking infrastructure and continuously adapting malware code in order to avoid detection.

This has been evident since 2007, when global cybersecurity firms began to publicly identify and track North Korean state-sponsored hacking groups,[38] and major cyber-attacks have been attributed to North Korea. Select North Korean hacker groups are geographically dispersed in China, Russia, Southeast Asia, and even Europe, acting independently or mutually supporting each other based on their specific cyber-missions: from intelligence-driven cyber espionage and information manipulation (APT37, Kimsuky, Sun Team); covert financial extortion (APT38, Andariel); to various disruptive and destructive cyber operations (Lazarus Group).

These begin seriously to emerge in the period from 2007–12 when North Korea developed its first generation of malware – attributed in cyberattacks known as 'Operation Flame' and '1Mission' (2007–2012), 'Operation Troy' (2009–2012), 'Ten Days of Rain' (2011), and 'Dark Seoul' (2013)[39] – principally against military and government targets in South Korea, hacking websites, stealing information, and distributed denial-of-service (DDoS) attacks.[40] For example, in March, 2011, in an operation named 'Ten Days of Rain', a major DDoS attack on 40 South Korean media outlets, critical infrastructures and financial websites, as well as on U.S. military entities in South Korea was attributed to North Korea's Lazarus Group.[41] In March 2013, following the passing of UN Security Council Resolution (UNSCR 2087) and B-52 strategic bomber overflights in South Korea, a cyberattacks dubbed 'Dark Seoul' attributed to North Korea destroyed computer networks of South Korea's three major banks and two largest media broadcasters – the Korea Broadcasting System and Munhwa Broadcasting Corporation, infecting them with viruses, stealing and wiping information.[42] In that year, North Korea intensified its cyber operations against South Korea with cyber espionage campaign (dubbed 'Kimsuky') against South Korean think tanks and industries, and various DDoS attacks on South Korean media outlets, government websites, and financial companies.[43] In 2016, North Korea was attributed with a successful penetration of South Korea's military networks – hacking into the ROK's Cyber Command's Defense Integrated Data Center,

34 Martyn Williams: Catch Me If You Can: North Korea Works to Improve Communications Security, *38North-Website*, April 12, 2017; https://www.38north.org/2017/04/mwilliams041217.

35 *MITRE ATT&CK Database*, "Lazarus Group," Available at: https://attack.mitre.org/groups/G0032/

36 The National Cybersecurity and Communications Integration Center (NCCIC), "HIDDEN COBRA – North Korean Malicious Cyber Activity," https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

37 Rosenberg/Beek 2019.

38 Group-IB 2017.

39 Novetta 2016.

40 Sherstobitoff/Laba/Walter 2018.

41 McAfee Labs 2011.

42 Choe Sang-Hun: Computer Networks in South Korea Are Paralyzed in Cyberattacks, *New York Times*, March 20, 2013; Michael Pearson/K.J. Kwon/Jethro Mullen: Hacking Attack on South Korea traced to China, Officials Say, *CNN*, March 21, 2013.

43 Tarakanov 2013.

Table 1: Identifying North Korea's Cyber Activity Clusters Based on Tactics, Techniques, and Procedures

APT group	Target sectors	Associated malware	Attack vectors
APT 37 *aka:* Reaper, Group 123, Ricochet Chollima, Scarcruft	From 2014 to 2017, APT37 targets concentrated primarily on the South Korean government, military, defense industrial base, and media sector. Since 2017, targets include Japan, Vietnam and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.	APT37 employs a diverse suite of malware for initial intrusion and exfiltration. Their malware is characterized by a focus on stealing information from victims, with many set up to automatically exfiltrate data of interest. Along with custom malware used for espionage purposes, APT37 also has access to destructive malware.	Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyber espionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately.
Kimsuky *aka:* Velvet Chollima	Since 2013, the Kimsuky group has pursued a cyber-espionage campaign against government organizations and defense-related agencies in South Korea as well as institutions and corporations related to South Korea's engagement with North Korea.	Malware able to remote controls the PC, logging keystrokes, stealing documents and collecting directory listings. The name derives from the email account, "Kimsukyang," which was used as drop-point for stolen data in 2013.	Spear phishing methods – targeted cyber scams to lure users to malicious websites or to infect PCs via malicious attached files in order to access systems and sensitive data. Malicious emails disguised as an invitation to a press conference. Recent activity by the Kimsuky group detected in February 2019 during the period ahead of the second U.S.-North Korea summit in Hanoi.
Sun Team	North Korean defectors and journalists in South Korea.	Android malware that contains a backdoor file in the executable and linkable format. The malware poses as a legitimate app. Once the malware is installed, it copies sensitive information including personal photos, contacts, and SMS messages and sends them to the threat actors.	Highly targeted campaign beginning in 2017 used Facebook and KakaoTalk, one of South Korea's most popular chat apps, to spread malware-laced phishing links to targets. Journalists were targeted with fake news stories directing to infected websites.
Andariel – Lazarus subgroup *aka:* Silent Chollima	Initially, cyber espionage targeting ROK military agencies, defense industries, political organizations, security companies, ICT companies, and energy research institutes; Financial targets, such as ATMs, banks, travel agencies, cryptocurrency exchanges, and online gambling users.	Using well-known backdoors, such as Aryan and Gh0st RAT, but also self-developed backdoors such as Andarat, Andaratm, Rifdoor, and Phandoor.	Spear phishing using macros, watering hole attacks exploiting Active-X vulnerabilities, vulnerability exploits on security and IT asset management systems, and supply chain attacks.
APT 38/Bluenoroff Lazarus subgroup *aka:* Stardust Chollima/	Global – exclusively focusing on financial institutions, casinos, financial trade software development companies and cryptocurrency businesses. APT38 has conducted operations in over 16 organizations in at least 11 countries.	This large and prolific group uses a variety of custom malware families, including backdoors, tunnelers, dataminers, and destructive malware to steal millions of dollars from financial institutions and render victim networks inoperable.	This group is careful, calculated, and has demonstrated a desire to maintain access to victim environments for as long as necessary to understand the network layout, required permissions, and system technologies to achieve its goals.

APT group	Target sectors	Associated malware	Attack vectors
Lazarus Group *aka:* Labyrinth Chollima, Whois Hacking Team	Global – Information theft and espionage, disruption, sabotage and financial gain; Lazarus Group activities center on achieving the political goals of the North Korean regime.	The group has deployed multiple malware families across the years depending on targets and objectives. Lazarus uses various code obfuscation techniques, rewriting its own algorithms, applying commercial software protectors, and using its own and underground packers. Most of the tools are designed to be disposable to be replaced with a new generation as soon as they are used.	The Lazarus Group's activity spans multiple years, going back as far as 2009. Its malware has been found in many serious cyberattacks, such as the massive data leak and file wiper attack on Sony Pictures Entertainment in 2014; the cyberespionage campaign in South Korea, dubbed Operation Troy, in 2013; and Operation DarkSeoul, which attacked South Korean media and financial companies in 2013.

Sources: Table compiled by the author based on cyber threat reports FireEye Inc. 2018a and 2018b; Tarakanov 2013; Min 2018, Kaspersky Labs 2017, Ahnlab 2018 and 2019, Crowdstrike 2018, TrendMicro 2018; Novetta 2016.

and extracting 235 gigabytes of classified military documents, including South Korea-U.S. wartime operational plans.[44]

During 2014–15, North Korea reportedly reorganized their cyber divisions – with Unit 180 targeting cryptocurrency exchanges, Unit 91 focusing on cyberespionage for technologies needed for the development of North Korea's nuclear and ballistic missile programs, and Bureau 121 focusing on cyber operations on foreign critical infrastructure – in a transition that expanded the range of cyber targets and operations beyond South Korea. For example, in 2014, North Korean hackers gained global attention in a major cyber-attack on Sony Pictures Entertainment, which destroyed 70 percent of Sony Picture's laptops and computers, in an attempt to coerce the company not to release the movie "The Interview."[45]

In the same year, North Korean hacker groups were attributed with targeting banks connected to SWIFT global financial messaging system, in attempts to transfer $951 million from the Central Bank of Bangladesh to accounts in Sri Lanka and the Philippines; it managed to steal $81 million.[46] Since then, North Korea has been linked to a series of cyber-attacks specifically aimed for illicit financial gain – in February 2017, for example, several Polish banks have been compromised as well as South Korean cryptocurrency exchange Bithumb, where North Korean Hackers were able to steal USD$7 million.[47] In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the WannaCry global ransomware attack, which infected more than 200,000 computers across 150 countries, including computers and devices of the National Health Service hospitals in England and Scotland.[48] According to the report by the United Nations Panel of Experts on North Korean Sanctions Committee issued in March 2019, North Korea "carried out at least five successful [cyber] attacks against cryptocurrency exchanges in Asia between January 2017 and September 2018, resulting in a total loss of $571 million." In doing so, the report states, "cyberattacks by [North Korea] to illegally force the transfer of funds have become an important tool in the evasion of sanctions and have grown in sophistication and scale since 2016."[49]

At the same time, North Korea has been conducting cyber operations to access and eavesdrop on critical infrastructure in the United States and other countries around the world – for example, in 2018, during the North Korea–United States Singapore Summit, North Korea conducted a cyber-exploitation campaign designed to probe military,

44 Kyongae Choi: N. Korea likely Hacked S. Korea Cyber Command: Military, Yonhap News, 6 December 2016, Christine Kim: North Korea Hackers Stole South Korea-U.S. Military Plans to Wipe out North Korea Leadership: Lawmaker, Reuters, October 10, 2017.

45 Andrea Peterson: The Sony Pictures Hack, Explained, The Washington Post, December 18, 2014, Greg Otto: U.S. charges North Korean hacker over Sony, WannaCry incidents, Cyberscoop, September 6.

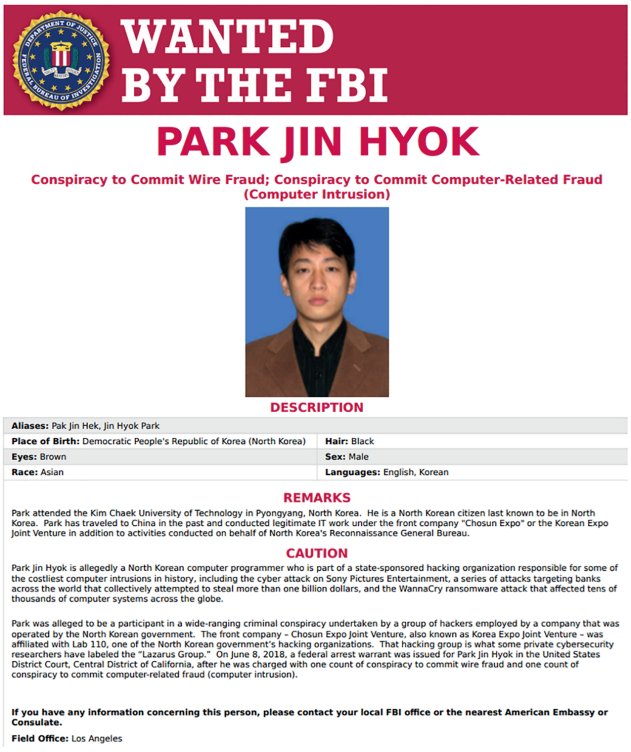
46 Fraser/O'Leary/Cannon/Plan 2018; US Department of Homeland Security 2018.

47 Eduard Kovacs: Malware Attacks On Polish Banks Linked to Lazarus Group, *Security Week*, February 13, 2017.

48 Thomas Bossert: It's Official: North Korea Is Behind WannaCry, *The Wall Street Journal*, December 18, 2017.

49 United Nations 2019, 51.

financial, energy, telecommunications, healthcare and other networks for potential vulnerabilities.[50] While North Korea has rejected all accusations that it has been involved in illicit hacking activities, it has been arguably less concerned with attribution either – i. e. using relatively simple false flags such as the "Guardians of Peace" in the wake of the Sony attack or other names such as the "New romantic Cyber Army Team" and the "WhoIs Team" in previous attacks on South Korean targets.[51] According to the 2014 ROK Defense White Paper, "North Korea currently operates about 6,000 cyber warfare troops and conducts cyber warfare, including the interruption of military operations and attacks against major national infrastructure, to cause psychological and physical paralysis in the South."[52]



WANTED BY THE FBI

PARK JIN HYOK

Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	**Hair:** Black
Eyes: Brown	**Sex:** Male
Race: Asian	**Languages:** English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company - Chosun Expo Joint Venture, also known as Korea Expo Joint Venture - was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

Source: FBI 2018 https://www.fbi.gov/wanted/cyber/park-jin-hyok

4 Assessment of North Korea's Cyber Strategies

The above timeline and empirical evidence suggests that North Korea's cyber units have gradually evolved over the past decade in three distinct phases, parallel with changing political and economic priorities of the regime and available resource allocation. From 2009–11, North Korea's cyber operations targeted primarily South Korean government offices, financial industry, as well as U.S. military and defense targets; characterized by hacktivist political messages and threats. The highly publicized attack on Sony represented the pinnacle of this activity, marking one of the first times a nation-state targeted a corporate entity for political aims. From 2012–15, North Korea focused on cyber espionage activities – such as APT37 and APT38 groups – targeting South Korean and U.S. government offices, defense contractors, universities and think tanks, as well as North Korean defectors abroad. From 2016–18, North Korean hacker groups began to expand the scope and sophistication of their operations, most likely under increasing pressure from financial sanctions, and increasingly conduct financially motivated cyber operations.[53] Second, North Korea has gradually demonstrated a resolve for a cyber-escalation – targeting critical infrastructures of other nation states as well as private corporations and banks for varying political motivations – i. e. retaliation, coercion, or covert intelligence gathering, and increasingly also illicit financial gain to bypass stricter international sanctions and generate foreign currency. In doing so, it has been undeterred by international norms. Third, the essential 'dialectics of North Korea's cyberspace' has reflected asymmetry in terms of its functionality and vulnerability – North Korea's internet infrastructure is isolated from global networks, with the country's entire Internet traffic channeled through only two providers – China's Unicom (40 %) and Russia's TransTeleCom (60 %).[54] Notwithstanding its growing intranet infrastructure, the country is still by and large unplugged from the global internet, and China's "Great Firewall" provides an "additional layer of protection, censorship, and surveillance for North Korea's cyberspace."[55] This has reduced North Korea's dependencies and potential systemic vulnerabilities to retaliatory actions, and more importantly, mitigated risks of attribution.

50 Sherstobitoff/Malhotra 2018.

51 Andy Greenberg: Russian Hacker False Flags Work – Even After They are Exposed, *Wired Security,* February 27, 2018; https://www.wired.com/story/russia-false-flag-hacks/.

52 Republic of Korea, Ministry of National Defense 2014, 27.

53 FireEye Inc. 2019.

54 Peter Georgiev: North Korea Opens Second Internet Connection via Russia, *Transitions Online,* April 16, 2018.

55 Mansourov 2014.

Table 2: Timeline of North Korean Cyber Operations

03/2007	According to cybersecurity experts working on **Operation Blockbuster**, the Lazarus Group starts to develop its **first generation of malware**;
2009	**The Lazarus Group** starts its **Operation Troy** and its wiper malware.
07/2009	Lazarus Group conducts **Distributed Denial of Service (DDoS) attacks** against 17 South Korean and U.S. government websites.
03/2011	Lazarus Group conducts a DDoS attack on 40 South Korean media outlets, critical infrastructures and financial websites, as well as on U.S. military entities in South Korea, in an operation named **Ten Days of Rain.**
03/2013	**Lazarus Group shuts down 32,000 computers** in South Korean broadcast and financial companies.
06/2013	DPRK is attributed with a **DDoS attack against 69 South Korean media outlets** and government websites.
09/2013	Kaspersky Lab discovers **a cyberespionage campaign named the Kimsuky campaign** against South Korean think tanks and industries.
2014	**DPRK is attributed to a cyber-attack on 140,000 South Korean government and business computers** and tries to penetrate the control system for the South Korean transportation network. **APT37**, a cyberactor associated with the DPRK government, targets South Korean media and websites on DPRK refugees with watering hole attacks.
08/2014	**DPRK hackers attack the British TV broadcaster Channel 4**. The channel had planned to release a TV show on a nuclear scientist being kidnapped by the DPRK. The TV show was cancelled after the cyberattack.
11/2014	**Lazarus Group targets Sony Entertainment Pictures** with wiper malware. The group identifies itself as the Guardians of Peace and demands that a comedy movie about a plot to assassinate Kim Jong-un not be released. The group also steals information from Sony and leaks it on the internet.
10/2015	Lazarus Group is linked to **cyberattacks against banks in the Philippines.**
12/2015	Lazarus Group is linked to **cyberattacks against the Tien Phong Bank in Vietnam**.
02/2016	Lazarus Group conducts a **cyberattack on the Bangladesh Central Bank** through the SWIFT messaging system and steals US$81 million.
04/2016	**DPRK hackers penetrates the South Korean Defense Integrated Data Center** and steal classified documents.
11/2016	**APT37** targets South Korean government and financial institutions as part of a cyberespionage campaign.
2017	**Lazarus Group** infiltrates the website of the Polish financial regulator and infects visitors with malware.
02/2017	DPRK hackers steal US$7 million worth of cryptocurrency from the South Korean **cryptocurrency exchange Bithumb.**
04/2017	A series of **spear phishing emails targeting US defense contractors** is attributed to the Lazarus Group.
05/2017	**Ransomware WannaCry infects approximately 200,000 computers in over 150 countries**. Cybersecurity companies Kaspersky Lab and Symantec affirm that the Lazarus Group is behind WannaCry. The NSA attributes the ransomware WannaCry to the DPRK.
09/2017	Lazarus Group **targets users of the cryptocurrency exchange Coinlink** with spear phishing emails.
2018	**Operation Sharpshooter** – cyber operations to access critical infrastructure in the United States and other countries around the world, a cyber-exploitation attack designed to probe military, financial, energy, telecommunications, healthcare and other networks for potential vulnerabilities.

Source: Adapted from Baezner 2018

In the absence of conventional warfare and escalation, future conflicts on the Korean Peninsula will likely increasingly reflect parallel and continuous confrontations in and out of cyber space, and varying cyber-attacks by both state and non-state actors. At the high-end of cyber-enabled information conflict spectrum on the Korean Peninsula might be "existential cyber-attacks" characterized as causing sufficient wide scale damage for a government potentially to lose control of the country, including loss or damage to significant portions of military and critical infrastructure: power generation, communications, fuel and transportation, emergency services, financial services, etc. Such attacks, however, will be proceeded or accompanied by the use of disinformation,

concealment, and deception campaigns – aimed to shape target population's perceptions and beliefs, while gradually pressuring top political leadership to fall into a decision objectively leading to its own defeat – for example by untangling the U.S.-ROK Alliance. Both North and South Korea's online activities and behavior will therefore have increasingly offline consequences, and vice-versa, blurring distinctions between civil and military domains, state and non-state actors, principal targets and weapons used. In times of crisis, the character of asymmetric cyber-attacks may also increase the propensity for 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.

5 Policy Recommendations

There are some steps that South Korea must take domestically to integrate cyber operations more holistically into its military posture and doctrine. In 2011, the ROK's Ministry of Defense published its cyber-defense strategy – the Master Plan for Defense Cyber Policy, which emphasized four key policy directives: adapting South Korea's laws to enable cyber operations; integrating cyber and physical operations in a military doctrine – the Joint Cyber Operations Manual; establishing ROK Cyber Command under the Joint Chiefs of Staff office; and creating early warning and crisis management mechanisms for responding to cyber crises.[56] Since then, South Korea has enhanced civil-military cooperation in the cyber domain, including joint programs with the Ministry of Science, IT, and Future Planning and the National Intelligence Service (NIS) to create a possible cyber reserve force, and closer coordination of intelligence border monitoring, joint response to North Korea's electronic warfare and GPS jamming, and a special warfare-centered combat skills augmentation plan.

Aside from these domestic measures, Seoul should also prioritize joint efforts with the U.S. military to ensure that the alliance leverages cyber operations as effectively as possible. More recently, South Korea's cyber capabilities have evolved in the strategic framework of the U.S.-ROK alliance with joint programs developing artificial intelligence-based technologies to counter a range of cyber threats.[57]

The key challenge for the future of the U.S.-ROK Alliance, however, will be able to adapt to potential changes to the character of warfare. Since the early 1990s, South Korea has been undergoing a comprehensive military modernization drive in order to respond to the widening spectrum of North Korean threats, mitigate technological and interoperability gaps with the U.S. forces, and eventually attain self-reliant defense posture. In the process, South Korea's defense planners have been searching for a new strategic paradigm and operational concepts that would allow greater flexibility, adaptability, and autonomy under conditions of strategic uncertainty. However, with the ambitious scope, required timelines, and relatively high costs, South Korea's defense reforms have propelled perennial policy debates on the feasibility, affordability, pace, direction, character, and implementation of South Korea's defense transformation. These policy debates have reflected five key enduring challenges for South Korea's defense planning: (1) how to balance and prioritize South Korea's current operational requirements vis-à-vis North Korea and future-oriented and relatively uncertain regional threats; (2) how to ensure budgetary support and sustain projected increase in defense resource allocation required for implementing select defense reforms; (3) how to streamline and reduce the ROK force structure without mitigating its operational readiness and capabilities; (4) when to transfer current wartime operational command control (OPCON) from the U.S. forces to South Korea without mitigating deterrence; and ultimately, (5) how to shape the future strategic template of the U.S.-ROK alliance.[58]

In other words, the compelling and relatively ambitious character of South Korea's future-oriented defense reform plans over the past two decades have been in sharp contrast to the prevailing political, strategic, and operational realities such as contrasting calibrations of defense requirements, structural dependence on the U.S.-ROK alliance, static, defensive force posture, and inter-service rivalries in the organizational force structure that have sustained the relevance of traditional security concepts and strategic culture. Arguably, there has not been a major military change within the South Korea's military. Instead, South Korea has experienced progressive shifts from operational and military-technological emulation to selective capability adaptation in the gradual or evolutionary process of military modernization.

56 Republic of Korea, Ministry of National Defense 2014.
57 Lee 2016, 70.
58 Raska 2016a, 32.

Notwithstanding concerted efforts to resolve existing technological and operational gaps in the context of combined interoperability with U.S. forces, particularly in areas of air power, C4ISR, and cyber operations; as well as joint interoperability among the three distinctly separate ROK services, South Korea's defense reforms, including the integration of cyberwarfare capabilities, have not significantly changed the "cognitive-template" nor organizational force structure of the ROK military. The ROK forces have not been fully able to align its military-technological potential in their modernization trajectory with the required organizational, conceptual, and operational innovation to utilize advanced technologies, including cyber capabilities, in new ways.[59] Under these conditions, North Korea has been gradually gaining a strategic advantage by pursuing cyber capabilities in conjunction with nuclear and ballistic missile programs as asymmetric capabilities, which provide relatively low-cost but effective means to exert its influence and provide a capability for political, economic, and military coercion without triggering a major armed conflict.

Literature

AhnLab (2018): *Full Discloser of Andariel: A Subgroup of Lazarus Threat Group*. Gyeonggi-do, South Korea: AhnLab Analysis Report, June 23; https://jp.ahnlab.com/global/upload/download/techreport/[AhnLab]Andariel_a_Subgroup_of_Lazarus%20(3).pdf;

AhnLab (2019): Operation Kabar Cobra: Tenacious Cyber-Espionage Campaign by Kimsuky Group. Gyeonggi-do, South Korea: AhnLab Analysis Report, February 28; https://jp.ahnlab.com/global/upload/download/techreport/[Analysis_Report]Operation%20Kabar%20Cobra%20(1).pdf

Baezner, Marie (2018): *Cyber Disruption and Cybercrime: Democratic People's Republic of Korea*. Zurich: Center for Security Studies (CSS), ETHZ

Bermudez, Joseph (2010): *A New Emphasis on Operations Against South Korea? A Guide to North Korea's Intelligence Reorganization and the General Reconnaissance Bureau*. Washington, D.C.: *38 North Special Report*; https://www.38north.org/wp-content/uploads/2010/06/38north_SR_Bermudez2.pdf

Bermudez, Joseph (2016): *North Korea Reorganizes Security Services*. London: IHS Jane's; https://www.janes.com/images/assets/196/66196/North_Korea_reorganises_security_services.pdf

Boo, Hyeong-wook (2017): An Assessment of North Korean Cyber Threats, *The Journal of East Asian Affairs*, 31 (1), 97–117

Boo, Hyeong-wook et. al. (2013): *A Study on Future Direction of Defense Cyber Policy*. Korean Institute for Defense Analysis report (*in Korean*) p. 94

Crowdstrike (2018): *Global Threat Report 2018*. Sunnyvale, Cal: A Crowdstrike Special Report; https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

FireEye Inc. (2018a): *APT 38 – Un-usual Suspects*. Milpitas, Cal.: FireEye Report, 2018; https://content.fireeye.com/apt/rpt-apt38

FireEye Inc. (2018b): *APT37 (Reaper) The Overlooked North Korean Actor*. Milpitas, Cal.: A FireEye Special Report; https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

FireEye Inc. (2019): *M-Trends 2019*. Milpitas, Cal.: FireEye Mandiant Services Special Report, https://content.fireeye.com/m-trends

Fraser, Nalani/O'Leary, Jacqueline/Cannon, Vincent/Plan, Fred (2018): APT38: *Details on New North Korean Regime-Backed Threat Group*. Milpitas, Cal.: FireEye Threat Research Report, October 3; https://www.fireeye.com/blog/threat-research/2018/10/apt38-details-on-new-north-korean-regime-backed-threat-group.html

Group-IB (2017): *Lazarus Arisen: Architecture, Tools, Attribution*. Singapore/Moscow: Group-IB Investigation Report, May 30; https://www.group-ib.com/blog/lazarus

Jun, Jenny/LaFoy, Scott/Sohn, Ethan (2015): North Korea's Cyber Operations: Strategy and Responses. Washington, D.C.: Center for Strategic and International Studies

Kasperksy Labs (2017): *Lazarus under the Hood*. Moscow: A Kaspersky Forensic Investigation Report; https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

Lee, Chung Min (2016): *Enhancing US Power Projection*, in: Patrick Cronin (ed.): Breakthrough on the Peninsula: Third Offset Strategies and the Future of Defense of Korea. Washington D.C.: Center for New American Security p.70, https://www.cnas.org/publications/reports/breakthrough-on-the-peninsula

Lee, Duri (2017): How to Improve the ROK and U.S. Military Alliance Against North Korea's Threats to Cyberspace: Lessons From NATO's Defense Cooperation. Monterrey, Cal.: Naval Postgraduate School; Master of Science Thesis in Information Strategy and Political Warfare (December)

Mansourov, Alexander (2014): *North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance*. Seoul: Korean Economic Institute, KEI Academic Paper Series

McAfee Labs (2011): *Ten Days of Rain – Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea*. Santa Clara, Cal.: McAffee White Paper, July; https://securingtomorrow.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf

Min, Jaewon (2018): *North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk*, McAfee Labs Blog, January 11; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/north-korean-defectors-journalists-targeted-using-social-networks-kakaotalk/

Novetta (2016): *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack*. McLean, Va.: Novetta Special Report; https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Pinkston, Daniel A. (2016): Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the Son'gun Era, *Georgetown Journal of International Affairs*, 27 (3), 60–76

Raska, Michael (2016a): *South Korea's Military Innovation Trajectories*, in: Patrick Cronin (ed.): *Breakthrough on the*

59 Raska 2016b, 95–130.

Peninsula: Third Offset Strategies and the Future of Defense of Korea. Washington D.C.: Center for New American Security

Raska, Michael (2016b): *Military Innovation in Small States: Creating a Reverse Asymmetry.* New York: Routledge

Republic of Korea, Ministry of National Defense (2012): *2012 Defense White Paper*. Seoul: MoD

Republic of Korea, Ministry of National Defense (2014): *2014 Defense White Paper*. Seoul: MoD

Rosenberg, Jay/Beek, Christiaan (2019): *Examining Code Reuse Reveals Undiscovered Links among North Korea's Malware Families.* Santa Clara, Cal.: McAfee Labs Report, August 9; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families

Sherstobitoff, Ryan/Laba, Itai/Walter, James (2018): *Dissecting Operation Troy: Cyberespionage in South Korea.* Santa Clara, Cal.: McAfee White Paper, May 4; https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf

Sherstobitoff, Ryan/Malhotra, Asheer (2018): *Operation Sharpshooter Targets Global Defense, Critical Infrastructure.* Santa Clara, Cal.: McAfee Labs, December 12; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/

Tarakanov, Dmitri (2013): *The 'Kimsuky' Operation: A North Korean APT?* Moscow: Kaspersky APT Reports, September 11, 2013, https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/

Tosi, Scott (2017): North Korean Cyber Support to Combat Operations, *Military Review*, (4), 43–51

Trend Micro (2018): *A Look Into the Lazarus Group's Operations.* Irving, Texas: Trend Micro Cybercrime and Digital Threats Blog, January 24; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/a-look-into-the-lazarus-groups-operations

United Nations (2019): *Report of the Panel of Experts established pursuant to resolution 1874 (2009*), New York: United Nations, S/2019/171, March 5.

US Department of Homeland Security (2018): *HIDDEN COBRA – FASTCash Campaign*. Washington, D.C.: National Cybersecurity and Communications Integration Center, October 2; https://www.us-cert.gov/ncas/alerts/TA18-275A