해양안보 Maritime Security
제3권 제1호(통권 3호)

Vol. 3, No. 1, 2021
pp. 45-72

The Role of Cyber in Kim Jong Un's Byungjin Line:
North Korea's Political Culture, Hackers, and Maritime Tactics

Benjamin R. Young*

◀ Abstract ▶

North Korea's cyber capabilities represent a relatively new threat to global financial institutions and foreign governments, particularly the U.S and South Korean governments. Based primarily on publicly available sources, such as journalistic accounts and scholarly publications, this qualitative paper analyzes the ways in which North Korean leader Kim Jong Un has bolstered his country's asymmetric power and advanced his line of *byungjin* (dual development in the economy and military). Particularly by merging the cyber and maritime domains, North Korean operatives generate more revenue for the regime and helps keep the heavily sanctioned leadership in power. Despite the increased international attention to North Korean hackers, few analysts have examined the important role of cyber in the DPRK's internal political culture, specifically in advancing Kim Jong Un's *byungjin* line. Cyber fits into the DPRK's longstanding tradition of irregular warfare and guerilla-based armed struggle. Cyber also further advances Kim's personal reputation in the DPRK as an economic innovator and military strategist. This paper pays particular attention to the role of the DPRK's cyber operations in both ideological and maritime contexts. Recently, North Korean hackers have targeted South Korean shipbuilding industries and developed a blockchain scam, known as Marine Chain. North Korean cyber agents have increasingly paid attention to the nexus of cyber and maritime domains in their activities.

Key Worlds : hackers, Kim Jong Un, Byungjin, cyber, North Korea

* Benjamin R. Young is an Assistant Professor of Homeland Security and Emergency Preparedness at the Wilder School of Government and Public Affairs at VCU (Virginia Commonwealth University). He is the author of *Guns, Guerillas, and the Great Leader: North Korea and the Third World* (Stanford University Press, 2021). He received his Ph.D. from The George Washington University in 2018. He has previously taught at the U.S Naval War College and Dakota State University. He has published peer-reviewed articles on North Korean history and politics in a number of scholarly journals and is a regular contributor to NKNews.org. He has also written for *The Washington Post, Nikkei Asia, The Guardian, The Diplomat,* and *The National Interest.*

In late November 2014, North Korean hackers attacked the servers of Sony Pictures Entertainment and released sensitive personal information of several top executives. The hackers leaked Sony employees' social security numbers, confidential emails, and unreleased movies on the web. This widely publicized event captured U.S national attention as Sony was set to release "The Interview," a comedic film that features North Korea's leader Kim Jong Un being assassinated.[1] While many journalists and cyber security analysts have researched the fallout of this cyber attack, few have investigated the connection between North Korea's cyber operations and the regime's unique political culture. As a country with an authoritarian system and one-party dictatorship, North Korea's cyber operatives are intimately connected to their government's political culture that they have been enmeshed in since an early age. Kim Jong Un has referred to his country's cyber capabilities as an "all-purpose sword," which indicates the regime's awareness that the cyber domain is a flexible and maneuverable space for North Korean operatives.[2]

In this paper, I borrow historian Chang-tai Hung's framework that political culture includes "shared values, collective visions, common attitudes, and public expectations created by high politics."[3] North Korea's political culture, with its anti-Americanism and hostile view of the Western liberal international order, shapes and molds the mentality of its citizens. As political elite in North Korean society, North Korea's hackers embrace and conform to the regime's political culture. The regime's paranoia of the outside world and view of the Kim family as god-like figures affects the way North Korean hackers operate in cyberspace. North Korean cyber operatives see themselves as digital guardians of the leadership's dignity and bolster the asymmetric power of

---

1) Emily VanDerWerff and Timothy B. Lee, "The 2014 Sony hacks, explained," *Vox*, June 3, 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

2) Kong Ji-Young, Lim Jong In and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," *2019 11th International Conference on Cyber Conflict* (CyCon), 2019, https://ieeexplore.ieee.org/document/8756954?signout=success.

3) Chang-tai Hung, *Mao's New World: Political Culture in the Early People's Republic* (Ithaca and London: Cornell University Press, 2011), 5-6.

the regime's military. They see themselves at war with an unjust international system and an outside world that aims to destroy their country. For example, Fred Plan, senior analyst of cyber espionage at Mandiant Intelligence, explains:

> One of the things that makes North Korean actors relatively more dangerous than operations from other countries is that the Pyongyang regime is isolated and disconnected from global economic trade and diplomatic engagement. As a result, North Korea isn't as incentivized to 'play by the rules' and the country continues to step over boundaries that define the acceptable behaviors of other nation-states. This is a key factor as to why only North Korean groups carry out state-sponsored cybercrime, such as digital bank heists, and are relatively more likely to deploy destructive wiper malware.[4]

The DPRK's apocalyptic view of the global order should be taken into consideration when analyzing North Korean cyber activities, as the Kim family regime's cyber operations are often a reflection of its political culture.

The 2014 Sony hack was one of the first instances in which the American public realized the extent to which North Korean hackers embodied the cultish leader worship system and paranoid nationalism of their authoritarian government. To the North Korean hackers, "The Interview" was a direct violation of their national sovereignty and a direct affront to their national dignity. The personality cult in North Korea, which represents the Kim family as god-like figures and views the "U.S imperialists" as the forever enemy of the Korean people, influences the everyday lives of people living in the Democratic People's Republic of Korea (the official title of North Korea; hereafter DPRK). North Korean hackers are no exception and see their leadership in an almost god-like perspective. This paper does not investigate the technical nature of North

4) Quoted in John Leyden, "Beyond Lazarus: North Korean cyber-threat groups become top-tier, 'reckless' adversaries," *The Daily Swig,* May 12, 2021, https://portswigger.net/daily-swig/beyond-lazarus-north-korean-cyber-threat-groups-become-top-tier-reckless-adversaries

Korea's cyber campaigns but rather it qualitatively traces the ways in which North Korea's unique political culture and ideology shapes the regime's cyber activity. Given this journal's focus on maritime security, this paper pays particular attention to Pyongyang's fusion of cyber and maritime domains.

During his first speech as leader of the DPRK, Kim Jong Un said in 2012 that his "first, second, and third priorities" were to strengthen the military and pledged that his people "will never have to tighten their belt again."[5] In the DPRK's political culture, Kim Jong Un has staked much of his personal legitimacy on the parallel development (*byungjin* in Korean) of the national economy and military, particularly the country's nuclear program and navy. Kim Jong Un unveiled his *byungjin* line at the 2013 plenary session of the Party's Central Committee. North Korea analyst Er-Win Tan views Kim Jong Un's *byungjin* line "as an effort to introduce two layers of regime security for Pyongyang."[6] Some outside analysts and observers predicted that Kim Jong Un's economic half of the *byungjin* line would be predicated on some type of Chinese-style market reform and attraction of foreign investment. For example, Scott Snyder said, "If we look at the means by which North Korea intends to pursue its economic strategy, it appears that there are focused efforts to enhance effectiveness of economic management, including possible steps toward reform."[7] Few, if any, analysts or observers saw the potentiality of cryptocurrency or the vital role of cyber attacks in North Korea's economic development. However, North Korea has always pursued its own unique path of self-development. Based on the last eight years of Kim Jong Un's actions, it has become fairly apparent that North Korea

---

5) Choe Sang-hun, "North Korean Leader Stresses Need for Strong Military," *The New York Times*, April 15, 2012, https://www.nytimes.com/2012/04/16/world/asia/kim-jong-un-north-korean-leader-talks-of-military-superiority-in-first-public-speech.html

6) Er-Win Tan, "*Byungjin* and the Sources of Pyongyang's Paranoia," *International Journal of Korean Unification Studies* Vol. 28, No. 2 (2019), 99-100.

7) Scott A. Snyder, "The Motivations Behind North Korea's Pursuit of Simultaneous Economic and Nuclear Development," *Council on Foreign Relations Blog*, November 20, 2013, https://www.cfr.org/blog/motivations-behind-north-koreas-pursuit-simultaneous-economic-and-nuclear-development

has not undergone Chinese-style economic reforms but rather used cyber operations as the regime's main economic driver. Thus, the role of cyber in Kim Jong Un's *byungjin* line deserves greater attention in scholarly discourse. As this paper lays out, cyber fits in well with Kim Jong Un's *byungjin* line since it can be effective for both enhancing the DPRK's military capabilities and the Party's economic prowess in the face of international sanctions.

South Korean researchers have primarily focused on improving the ROK government's official cybersecurity policy and defensive posture to North Korea's cyber attacks. In Korean language reports, South Korean analysts and think tank scholars, such as Chang-Hoon Shin and Gu-Yeon Jeong and Ki-Tae Lee, have emphasized South Korea's defensive response to North Korea cyber attacks and the technical capabilities of DPRK hackers.[8] While useful, these Korean language reports do not link the advancement of the DPRK's cyber capabilities with the unique political culture and ideological context of the North Korean system.

While scholars, such as Andrei Lankov and Grażyna Strnad, have framed Kim Jong Un's *byungjin* line in terms of success or failure, this paper goes beyond this dichotomous approach and inserts cyber into the conversation. In 2017, Lankov argued that Kim Jong Un's *byungjin* line "has produced some notable results and delivered a measure of economic growth."[9] Meanwhile, in a June 2021 piece for *The National Interest*, Strnad casts doubt on the successes of Kim's byungjin line amidst the COVID-19 pandemic and asserts that there is "doubt within the North about the regime's ability to fulfill its *byungjin* (parallel development) line."[10] Given Kim Jong Un's relatively young age and his family's

---

8) Chang-Hoon Shin, "Puk'anŭi saibŏ konggyŏkkwa wihyŏbe taehan uriŭi taeŭng 2014nyŏn 11wŏl SONY sagŏnŭi kyohun," Asan Research Institute Research Brief (April 6, 2015); Gu-Yeon Jeong and Ki-Tae Lee, "Kwahakkisulbalchŏn'gwa puk'anŭi saeroun wihyŏp: saibŏ wihyŏpkwa muin'gi ch'imt'u," Korea Institute for National Unification Research Series (April 2016).

9) Andrei Lankov, "Is Byungjin Policy Failing? Kim Jong Un`s Unannounced Reform and its Chances of Success," *Korean Journal of Defense Analysis* Vol. 29, No. 1 (2017), 25-45.

10) Grażyna Strnad, "Is North Korea's Byungjin Policy in Crisis?," *The National Interest*, June 27, 2021, https://nationalinterest.org/blog/korea-watch/north-korea%E2%80%99s-byungjin-policy-crisis-188649

longstanding grip on power within North Korea's political system, I agree with Lankov in viewing *byungjin* as a long-term goal for Kim Jong Un's regime. Thus, the increasing influence of cyber in North Korea's economic and military activities aligns with Kim's *byungjin* line. As cyber security journalist John Leyden explains, "Along with state-sponsored Russian, Chinese, and Iranian threat actors, North Korean advanced persistent threat (APT) groups are considered to be among the world's most sophisticated."[11]

Ⅰ. Marine Chain

In order to evade UN sanctions and bolster the coffers of the Party, the DPRK government may be using blockchain technology in order to fund its maritime trade. Using a digital token, known as Marine Chain, North Korean cyber agents in 2017 and 2018 attempted to market and dupe foreign investors into funding Pyongyang's illegal shipping industry. This token "would allow investors to buy fractional ownership in cargo ships, thereby hiding the fact that the vessels were owned and controlled by North Korea."[12] As part of its investigation into Marine Chain, the U.S Department of Justice in February 2021 indicted three North Korean computer programmers for "conducting a series of cyberattacks to attempt to steal and extort more than $1.3 billion in cash and cryptocurrency from financial institutions and companies."[13] One of these North Korean computer programmers, Park Jin Hyok, was allegedly involved in the 2014 cyber attack on Sony Pictures and also the creation of Marine Chain. The merging of cyber and maritime tactics represents a

11) Leyden, "Beyond Lazarus."

12) Jason Jiang, "North Korean hackers charged in ship cryptocurrency plot," Splash247.com, February 18, 2021, https://splash247.com/north-korean-hackers-charged-in-ship-cryptocurrency-plot/

13) "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," The U.S. Department of Justice, February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

new frontier of Pyongyang's illicit activities. It reveals an increasingly innovative and potentially desperate North Korean economic strategy.

A pro-DPRK Singaporen national, Captain Jonathan Foong Kah Keon, allegedly helped the North Korean government evade sanctions for years by posing as the CEO of Marine Chain. Foong attended business conferences in Hong Kong in an attempt to lure potential investors to the Marine Chain scam.[14] Cybersecurity researchers at *Recorded Future* noted in a report, "The companies Capt. Foong has worked for have been linked to manipulating the national flag registries for three countries, which were frequently used as flags of convenience for North Korean vessels." The report continues, "Capt. Foong is part of a network of enablers throughout the world that assist North Korea in circumventing international sanctions. These connections to Marine Chain Platform mark the first time this vast and illicit network has utilized cryptocurrencies or blockchain technology to raise funds for the Kim regime."[15]

Using its clandestine networks with international criminal syndicates, the DPRK government has increasingly looked to the seas as a way to evade international sanctions. The Kim family regime depends on maritime trade for its illegal import and export of goods and supplies. Using complex global supply chains, Pyongyang has navigated around maritime sanctions and continued to fund the country's nuclear development program. Using false ship names and open sea ship-to-ship transfers, North Korean ships have evaded UN sanctions on its oil imports. In March 2021, a *New York Times* investigation revealed that China allows DPRK tankers "to use its infrastructure and territorial waters to smuggle oil into North Korea, undermining international sanctions."[16]

---

14) Cristina Maza, "North Korea Regime Is Making Money From Cryptocurrency Scam That Offered Users Ownership of Ships: Report," *Newsweek*, October 25, 2018, https://www.newsweek.com/north-korea-cryptocurrency-scam-kim-jong-un-1188020

15) Insikt Group, "Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite," *Recorded Future,* October 25, 2018, https://www.recordedfuture.com/north-korea-internet-usage/

16) Christopher Koettl, "How Illicit Oil Is Smuggled Into North Korea With China's Help," *New York Times,* March 24, 2021, https://www.nytimes.com/2021/03/24/world/asia/tankers-north-korea-china.html

Chinese cooperation with North Korea in oil smuggling and cyber operations should be an area of concern to U.S and South Korean policymakers. The North Korean government deliberately exploits the regulatory vulnerabilities of both cyberspace and the maritime industry.

II. DPRK Cyber Attacks on South Korean Shipbuilding Industry

Recently, North Korean cyber operatives have also infiltrated the networks of South Korea's nautical industry and may have stolen designs for South Korea's nuclear submarine design and building techniques. In 2017, *Reuters* reported that North Korean hackers likely stole blueprints for South Korean warships from Daewoo Shipbuilding and Marine Engineering Company's database. The South Korean newspaper *Dong-A Ilbo* noted, "About 60 classified military documents were among the 40,000 hacked from the world's biggest shipbuilder. The leaked documents contained information on construction technology, blueprints, weapons systems, and evaluations of the ships and submarines."[17] The cyber attack occurred in April 2016 and a cybercrime unit from South Korea's Ministry of Defense later discovered the hack. South Korean opposition lawmaker Kyung Dae-soo said, "We are almost 100 percent certain that North Korean hackers were behind the hacking and stole the company's sensitive documents."[18]

Since 2016, North Korean hackers have repeatedly attempted to infiltrate Daewoo's computer networks. In June 2021, South Korea's National Intelligence Service "announced that Daewoo Shipbuilding & Marine Engineering, a global leader in submarine design and building, has been exposed to North Korean hacking attempts since late last year."[19]

---

17) "North Korea hacked Daewoo Shipbuilding, took warship blueprints: South Korea lawmaker," *CISOMAG*, November 1, 2017, https://cisomag.eccouncil.org/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker/

18) Haejin Choi, "North Korea hacked Daewoo Shipbuilding, took warship blueprints: South Korea lawmaker," *Reuters,* October 31, 2017, https://www.reuters.com/article/us-northkorea-missiles-cybercrime/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker-idUSKBN1D00EX

South Korean government officials recently announced an official investigation into the Daewoo breach.[20] The merging of cyber attacks and maritime strategy is a new development in North Korean behavior.

In addition to targeting Daewoo, North Korean cyber agents have also attacked Hyundai Merchant Marine, a South Korean maritime shipping company that focuses on worldwide container shipping services. In the same September 2013 cyber attack campaign as the one in which they targeted Hyundai Merchant Marine, North Korean hackers also targeted South Korean think tanks, such as The Sejong Institute, Korea Institute For Defense Analyses (KIDA), and the Ministry of Unification.[21] This suggests that North Korean hackers view South Korea's maritime sector as an important strategic area of vulnerability. As evidenced by the cyber attacks on Daewoo, North Korean hackers have continued to target South Korea's maritime infrastructure. This could have massive implications for the global shipping industry and could disrupt global supply chains.

Ⅲ. Historical and Ideological Context

In 1993, the North Korean regime established the first cyber unit under the guidance of Pyongyang's primary foreign intelligence agency, known as the Reconnaissance General Bureau (RGB). North Korean hackers first targeted South Korean financial institutions and government agencies. After becoming more advanced in their cyber capabilities, North Korean hackers have increasingly turned their sights on the international private sector and cryptocurrency exchanges.[22] In a December 2020 radio

19) "Daewoo Shipbuilding & Marine Engineering Exposed to North Korean Hacking Attacks," *Hellenic Shipping News*, June 23, 2021, https://www.hellenicshippingnews.com/daewoo-shipbuilding-marine-engineering-exposed-to-north-korean-hacking-attacks/

20) "South Korea Probes Possible Hack of DSME Computers," *The Maritime Executive,* June 21, 2021, https://www.maritime-executive.com/article/south-korea-probes-possible-hack-of-dsme-computers

21) Dmitry Tarakanov, "Kimsuky APT: Operation's possible North Korean links uncovered," *SecureList By Kaspersky*, September 11, 2013, https://securelist.com/kimsuky-apt-operations-possible-north-korean-links-uncovered/57335/

interview, U.S Secretary of State Mike Pompeo noted that North Korean hackers posed a greater risk than Russia to U.S governmental cyber systems.[23] According to North Korea expert Bruce Klingner of the Heritage Foundation, "Experts were initially dismissive of North Korea's cyber capabilities, as they had been of the regime's nuclear and missile programs. Pyongyang developed advanced cyberwarfare prowess surpassed by only a few nations. The regime improved its cyber programs to create a robust and global array of disruptive military, financial, and espionage capabilities."[24] According to an August 2019 United Nations Panel of Experts report, North Korean hackers have earned up to $2 billion via illicit cyber activities for the regime.[25] These funds help to keep the Kim family regime in power and are used to bolster the coffers of the heavily sanctioned Korean Workers' Party. North Korea's revenue-generation efforts in cyberspace are increasingly a cause of concern for the international community as these funds most likely subsidize the regime's robust nuclear program.

One of the most concerning aspects of North Korea's recent cyber behavior is its investment in blockchain technology and how Pyongyang uses cryptocurrency to fund its illicit maritime shipping industry. In February 2021, the U.S Justice Department unsealed an indictment against three North Korean computer programmers. From 2017 to 2020, these three North Korean cyber agents allegedly stole more than $100 million in cryptocurrency from banks and companies in more than a dozen countries, including the U.S.[26] John Demers, the head of the U.S Justice

---

22) Steve Miller, "Where Did North Korea's Cyber Army Come From?," *VOA*, November 20, 2018, https://www.voanews.com/east-asia-pacific/where-did-north-koreas-cyber-army-come

23) Byun Duk-Kun, "Pompeo says N. Korea a greater threat than Russia in cyber security," *Yonhap*, December 15, 2020, https://en.yna.co.kr/view/AEN20201215000200325

24) Quote found in Morten Soendergaard Larsen, "While North Korean Missiles Sit in Storage, Their Hackers Go Rampant," *Foreign Policy,* March 15, 2021, https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/

25) United Nations Report of the Panel of Experts established pursuant to resolution 1874, August 30, 2019, https://undocs.org/S/2019/691

26) Robert McMillan and Aruna Viswanatha, "North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says," *Wall Street Journal*, February 17, 2021, https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358

Department's national security division, said, "As laid out in today's indictment, North Korea's operatives, using keyboards rather than guns, stealing digital wallets of cryptocurrency instead of sacks of cash, are the world's leading bank robbers."[27]

With sophisticated cyber capabilities, North Korean hackers are merging financial and maritime sectors. Most notably, three North Korean cyber agents created Marine Chain, a digital token, "representing fractional ownership in marine shipping vessels and marketed it to individuals in Singapore."[28] Marine Chain was a blockchain technology used by these North Korean hackers in an attempt to circumvent international maritime sanctions on the Kim family regime. In order to import foreign goods into the country and evade international sanctions, the DPRK government uses an elaborate illicit network of shipping vessels flown under false flags. In a press conference, U.S Justice Department officials said that Marine Chain would allow the DPRK to "secretly obtain funds from investors, control interests in marine shipping vessels, and evade U.S. sanctions."[29] In recent years, North Korean hackers have also targeted South Korea's maritime shipping industry. In the face of international sanctions and economic troubles in the DPRK, the merging of cyber operations and maritime tactics represents a new North Korean economic strategy and military initiative.

The merging of maritime and cyber in North Korean grand strategy is an increasing threat to the U.S and South Korean governments. North Korean hackers have also targeted Daewoo, South Korea's leading submarine builder, and Hyundai Merchant Marine. North Korean hackers may have also acquired designs for South Korean warships. The DPRK's sinking of South Korea's Cheonan in 2010 and shelling of Yeonpyeong

---

27) Quote found in McMillan and Aruna Viswanatha, "North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says."

28) Nikhilesh De, "DOJ Charges 3 North Korean Hackers With Stealing $100M+ From Crypto Firms," *Coindesk.com*, February 17, 2021, https://www.coindesk.com/doj-charges-3-north-korean-hackers-with-stealing-100m-from-crypto-exchanges

29) Dan Mangan, "North Korean hackers charged in massive cryptocurrency theft scheme," CNBC, February 17, 2021, https://www.cnbc.com/2021/02/17/north-korean-hackers-charged-in-massive-cryptocurrency-theft-scheme.html

Island in that same year demonstrate North Korea's recent maritime aggression. In January 2021, Kim Jong Un claimed that his country completed plans for a nuclear-powered submarine.[30] According to North Korea's official state-run news agency, Kim Jong Un "stressed the need to steadily and reliably increase the national defense capability by directing big efforts to the development of the naval weapons and equipment such as submarine."[31] The combining of maritime and cyber strategies represents a new asymmetric threat from Pyongyang. By merging maritime and cyber domains, Pyongyang is also increasing its irregular military power in order to counter conventional U.S and South Korean forces. Since North Korea is weaker in conventional military means, the Kim family regime has had to develop asymmetric forms of boosting its military might. Thus, the DPRK's merging of maritime and cyber activities is both a financial and military-minded maneuver. The creation of a nuclear submarine bolsters Kim Jong Un's status in the DPRK's internal political culture as a military genius and strong-willed naval commander.

Cyber operations allow the DPRK to subvert foreign adversaries and acquire foreign currency without the risk of all-out war. This "gray zone" of cyberspace enables the North Korean government to avoid military retaliation and allows it hackers to secure much-needed currency for the heavily sanctioned Kim family regime. North Korean strategists and policymakers are adept at reaching the line of all-out military confrontation and then pulling back at the last minute. Cyber warfare and espionage allows North Korea to avoid any of these military risks as the international community has yet to form cohesive rules or norms for cyber activities from nation-state actors. Compared to Pyongyang's long history of drug smuggling and illegal arms deals, hacking remains a relatively new aspect of North Korea's revenue-generation efforts.

---

30) "Kim Jong-un calls US 'biggest enemy' and says nuclear submarine plans 'complete'," The Guardian, January 8, 2021, https://www.theguardian.com/world/2021/jan/09/kim-jong-un-calls-us-biggest-enemy-and-says-nuclear-submarine-plans-complete

31) "Kim Jong Un inspects new submarine, wants North Korea's military bolstered," *Associated Press*, July 23, 2019, https://www.nbcnews.com/news/world/kim-jong-un-inspects-new-submarine-wants-north-korea-s-n1032711

However, it presents significant challenges for the international community as Pyongyang has increasingly devoted a substantial amount of its limited financial resources to strengthening its cyber capabilities.

Ⅳ. Guerilla Mentality and Military Traditions in Cyberspace

The asymmetric nature of cyber activities fits North Korea's political culture and military traditions. The North Korean regime traces its revolutionary heritage and ideological origins to the anti-Japanese guerilla struggle of the 1930s. As a guerilla fighter in Manchuria, Kim Il Sung led a band of partisans in armed anti-colonial struggle against Japanese colonialists. Kim Il Sung's closest comrades from his guerilla days later became the political elite of the DPRK government. Historians Wada Haruki and Adrian Buzo have both claimed that these guerilla experiences later influenced the Kim family regime's thinking and behavior.[32] In his book *Guerilla Dynasty,* Buzo explains, "That Kim Il Sung's guerilla experience and the DPRK's extended Soviet tutelage have definitively shaped the nation remains not so much an argument but a common-sense and recurring theme."[33] Due to their fighting backgrounds, the political elite's guerilla mentality deeply influenced North Korean strategy and behavior in the international arena. I contend that this guerilla tradition still informs North Korea's foreign policy and external behavior, including its cyber activities. The North Korean government uses asymmetric engagement tactics and maneuvers typically deployed by a guerilla fighter. For example, it regularly engages in deception, ambush, quick hit-and-run attacks, and sabotage. As a 2015 CSIS report on North Korea's cyber operations explains, "North Korean strategy emphasizes asymmetric and irregular operations in both

32) Wada Haruki, *Kim Il Sung gwa Manju Hangil Chŏnjaeng* (Seoul: Changbi, 1992); Adrian Buzo, 2nd ed., *The Guerilla Dynasty: Politics and Leadership in North Korea* (New York: Routledge, 2018).

33) Buzo, *The Guerilla Dynasty,* viii.

peacetime and wartime to counter the conventional military strength of the United States and ROK."[34]

The North Korean propaganda apparatus still promotes the exploits of the founders' guerilla experiences and implores citizens to emulate the selfless warrior style of the 1930s anti-colonial fighters. For example, in December 2019, the North Korean government distributed educational materials on the guerilla warfare tactics used by Kim Il Sung during the 1930s to its military. According to Daily NK, a Seoul-based website that is run mostly by North Korean refugees, the materials "outline different warfare tactics including, for example, how to turn enemies against each other in a siege, distract enemies and attack them from the opposite direction, or attack hostile support forces while laying siege to their bases."[35] The tactics of traditional guerilla warfare, with its strategy of ambushes and sabotage, blends well with the 21st century technology of cyber warfare. The DPRK's cyber operations allow the regime to punch above its weight against stronger conventional militaries, such as the U.S or South Korea. The grey zone of cyber espionage also allows Pyongyang a degree of plausible deniability. For example, the North Korean government officially denies the existence of its state-backed hackers.

North Korean hackers operate within a political culture that prioritizes an anti-American ideology and deification of the leadership. On July 4, 2009, a series of distributed denial of service (DDoS) attacks struck South Korean and U.S government and commercial websites. Sites targeted included the Korean assembly, the U.S and South Korean presidents' websites, the U.S State Department, and "naver.com" (a popular search engine in South Korea). The timing of these attacks coordinated with a North Korean missile test launch on July 4 and the 15th anniversary of Kim Il Sung's death on July 8. The target of these attacks and the timing suggests that it was politically motivated and based on the DPRK's

34) Jenny Jun, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Responses," CSIS Special Report, December 2015, https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations

35) Jeong Tae Joo, "N. Korean soldiers study Kim Il Sung-style guerrilla warfare," *Daily NK*, January 3, 2020, https://www.dailynk.com/english/n-korean-soldiers-study-kim-il-sung-style-guerrilla-warfare/

internal dynamics.[36] This event indicates that the North Korean regime does not separate its cyber operations from its political culture. Important dates in North Korea, such as the anniversary of the birthday of the "Great Leader" Kim Il Sung, sometimes coincides with missile test launches or coordinated cyber attacks on foreign adversaries. North Korea's cyber operations are often an extension of the regime's domestic politics and strategic priorities.

Hacking of cryptocurrency exchanges, which is a relatively low cost and low risk endeavor, blends nicely with Kim Il Sung's guerilla legacy. The untraceable nature of cryptocurrency promotes sanctions-breaking activities from rogue actors, such as the DPRK government. North Korea's hacking of cryptocurrency exchanges for much-needed foreign currency enables the regime to remain in power and not be completely dependent on China for trade. Prior to the COVID-19 pandemic, more than 80% of North Korea's foreign trade was with China but the regime has completely closed its outside borders during the coronavirus outbreak.[37] Due to these border closures and the lack of foreign tourism to the DPRK, it is widely believed by experts and analysts that North Korea's economy has drastically shrunk during the global pandemic. Due to the unregulated nature of cryptocurrency exchanges and increasing popularity of virtual money, North Korean hackers have increasingly focused their attacks on cryptocurrency exchanges. In 2020, the North Korean state-backed hacker group, Lazarus Group, conducted a cyber attack on the cryptocurrency exchange KuCoin for $275 million worth of virtual money.[38] According to Chainalysis, a cryptocurrency tracker and

---

36) Jose Nazario, "Politically Motivated Denial of Service Attacks," in Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare* (Washington, D.C: IOS Press, 2010), 163-181.

37) Lee Jeong-ho, "North Korean trade with biggest partner China dives 48 per cent amid sanctions," *South China Morning Post*, July 19, 2019, https://www.scmp.com/news/china/diplomacy/article/3019348/north-korean-trade-biggest-partner-china-dives-48-cent-amid

38) Thomas Brewster, "North Korean Hackers Accused Of 'Biggest Cryptocurrency Theft Of 2020'—Their Heists Are Now Worth $1.75 Billion," *Forbes*, Feb. 9, 2021, https://www.forbes.com/sites/thomasbrewster/2021/02/09/north-korean-hackers-accused-of-biggest-cryptocurrency-theft-of-2020-their-heists-are-now-worth-175-billion/?sh=412fa5d75b0b

law enforcement contractor, this was the largest cryptocurrency theft of 2020 and represented half of all cryptocurrency stolen in that year.[39] A confidential United Nations document that was leaked to CNN revealed that North Korean hackers stole virtual assets worth around $316.4 million dollars between 2019 and November 2020 in order to fund the regime's nuclear development program.[40] Due to the opaque nature of blockchain technology, North Korean hackers appear to be targeting cryptocurrency exchanges and thus putting the regime's guerilla tactics into practice.

V. Sino-DPRK Cyber Solidarity

During his time as a guerilla fighter in the 1930s, Kim Il Sung fought alongside Chinese Communists in rough-and-tumble Manchuria. Unified in their anti-Japanese struggle, the Chinese Communists and Kim Il Sung's guerilla band formed a strong ideological bond during this period. Later, during the Korean War, amidst an American advance into the DPRK in October 1950, China's leader Mao Zedong sent troops across the Yalu River to the Korean peninsula in order to assist his North Korean comrades. The Chinese troops pushed the U.S forces south of the 38th parallel and helped Kim Il Sung's nascent regime reclaim the northern half of the peninsula. Despite some frustrations in their historical relationship, Sino-North Korean comradeship has continued to the present day. It was no coincidence that North Korean leader Kim Jong Un met with Chinese Premier Xi Jinping in January 2019 before his first summit with U.S President Trump.[41] Pyongyang and Beijing rely upon

39) "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options," *Chainalysis*, Feb. 9, 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack

40) Richard Roth and Joshua Berlinger, "North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report," *CNN*, Feb. 9, 2021, https://www.cnn.com/2021/02/08/asia/north-korea-united-nations-report-intl-hnk/index.html

41) Alex Ward, "Kim Jong Un made a surprise visit to China. It's mostly about Trump," *Vox,* January 9, 2019, https://www.vox.com/2019/1/8/18173792/north-korea-kim-trump-china-nuclear

each other for national security reasons and ideological camaraderie as both still maintain an official allegiance to revolutionary socialism. In 2019, Kim Jong Un was quoted in North Korea's state-run media as saying the two countries' "invincible friendship will be immortal on the road of accomplishing the cause of socialism."[42] Despite China's economic growth and Beijing's frustrations with North Korea's lack of economic reform, the fraternal solidarity between the two Parties is still strong. Historical ties, revolutionary solidarity, and mutual security benefits will continue to bond the Korean Workers' Party and the Chinese Communist Party. Based on these shared ideological values and mutual security benefits, the Chinese Communist Party unofficially allows North Korean hackers access to China's cyber infrastructure as a way to assist Pyongyang in its efforts to earn foreign currency and carry out cyber attacks against mutual adversaries, such as the United States government and U.S private sector.

Aside from the massive dependence on trade with its communist neighbor, Pyongyang relies upon China for training of its hackers, access to servers and routers, and Internet connections. According to cyber security researcher Donghui Park, "China has provided educational programs as well as hardware, such as servers and routers, for North Korean cyber warriors… It is estimated that from 600 to 1,000 cyber warfare agents are acting in a variety of cells in China."[43] Although data on this is hard to verify and Beijing officially denies any ties to North Korean cyber activity, it is widely acknowledged by senior U.S government officials that the Chinese government permits North Korean hackers to be trained and based in China. For example, North Korea's computer science students have studied at China's elite science and technology universities, such as Harbin Institute of Technology.[44] In

---

42) "China and North Korea hail 'immortal and invincible' friendship," *The Guardian,* October 6, 2019, https://www.theguardian.com/world/2019/oct/06/china-and-north-korea-hail-immortal-and-invincible-friendship

43) Donghui Park, "North Korea Cyber Attacks: A New Asymmetrical Military Strategy," The Henry M. Jackson School of International Studies Blog, University of Washington Report, June 28, 2016, https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/

October 2020 at a think tank event, John Demers, the U.S Assistant Attorney General for National Security, noted, "There is support through Chinese cyber infrastructure, there's likely support in terms of sharing expertise and training from the Chinese side."[45] In a February 2021 press call, Demers said that both Russia and China have assisted North Korean cyber operatives and that due to the autocratic nature of those governments, it is highly likely that the leaderships in Moscow and Beijing knowingly helped North Korean hackers in their revenue-generation efforts.[46] According to a February 18, 2021 article from *The Washington Post*, "North Korean hackers also used Chinese cryptocurrency traders and criminal networks to launder funds."[47]

It is widely believed that two cyber units of North Korea's Enemy Secret Department Cyber Psychological Warfare, Unit 121 and Unit 110, were based in the Chinese cities of Shenyang and Dandong.[48] According to Kim Heung-kwang, a former North Korean computer science professor who defected from the country in 2004, Unit 121 (also known as Bureau 121) began its "large-scale operation in China in 2005." Unit 121 primarily worked out of a North Korean-owned hotel, Chilbosan Hotel, in Shenyang. Kim told CNN in a 2015 interview, "Team members entered China separately -- in smaller groups -- 20 members at a time. When they entered China, they came under different titles. For example an office worker, an official with a trade company or even as a diplomatic staffer."[49] Shenyang's location near the border with the DPRK and the

---

44) Jason Bartlett, "Why Is North Korea So Good at Cybercrime?" *The Diplomat*, November 13, 2020, https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/

45) "Senior U.S. official accuses China of aiding North Korea cyber thefts," *Reuters*, October 22, 2020, https://www.reuters.com/article/us-usa-northkorea-china/senior-u-s-official-accuses-china-of-aiding-north-korea-cyber-thefts-idUSKBN2772RX

46) Eric Geller, "North Korean hackers are 'the world's leading bank robbers,' U.S. charges," *POLITICO*, February 17, 2021, https://www.politico.com/news/2021/02/17/us-charges-north-korean-hackers-wannacry-sony-469406

47) Tonya Riley, "The Cybersecurity 202: Investigations into Russian, North Korean hackers are shaping Biden's foreign policy," *The Washington Post,* February 18, 2021, https://www.washingtonpost.com/politics/2021/02/18/cybersecurity-202-investigations-into-russian-north-korean-hackers-are-shaping-biden-foreign-policy-anne-neuberger-cybersecurity-biden-administration-cybersecurity/

48) Park, "North Korea Cyber Attacks: A New Asymmetrical Military Strategy."

city's cyber infrastructure allowed North Korean hackers secure access to high-speed Internet connections. However, a January 2018 report from *Dong-A Ilbo* stated that the Chilbosan Hotel closed amidst increased international scrutiny and sanctions. North Korean hackers apparently left the hotel a month before it officially closed and returned to the DPRK.[50] Nonetheless, North Korean cyber agents' entry into China allows the regime greater access to computer servers and networks that are not accessible in the DPRK due to international sanctions. North Korean hackers operating within China advances the DPRK's cyber capabilities and allows the Kim family regime a degree of deniability during cyber attacks and cyber espionage. Sino-DPRK cyber partnerships are an increasing threat to global financial institutions, cryptocurrency exchanges, and foreign governments.

Ⅵ. Russia-DPRK Cyber Solidarity

Although the Soviet Union collapsed in the early 1990s, the North Korean government still maintains close political and economic ties to Moscow. Vladimir Putin and Kim Jong Un's mutual distrust of the West has allowed the two countries to continue a beneficial partnership that has extended into cyberspace. According to the August 2020 United Nations Panel of Experts report, Putin's government violated UN sanctions on the DPRK by allowing North Korean workers to re-enter Russia after the December 2019 UN deadline that prohibited North Korean forced labor abroad.[51] Putin's government refusal to follow UN

---

49) Will Ripley, "North Korean defector: 'Bureau 121' hackers operating in China," *CNN,* January 7, 2015, https://edition.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html

50) Wan-Jun Yun and Dong-Yeon Jung, "North Korean hackers withdraw from their hub in Shenyang," *Dong-A Ilbo,* January 11, 2018, https://www.donga.com/en/article/all/20180111/1186969/1/North-Korean-hackers-withdraw-from-their-hub-in-Shenyang

51) Jason Bartlett, "Exposing the Financial Footprints of North Korea's Hackers," *CNAS*, November 18, 2020, https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers; "Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)" (S/2020/840).

sanctions on North Korean forced labor abroad enables the Kim family regime to continue many of its illicit activities, including its cyber operations, in the Russian Federation. In 2019, Putin and Kim Jong Un met for their first ever summit and the Russian President concluded after the meeting in Vladivostok, "Chairman Kim Jong Un is a fairly open person, leading a free discussion on all issues that were on the agenda."[52)]

Although North Korea's economic ties to the Russian Federation pales in comparison to Sino-DPRK trade relations, the Kim family regime uses Russian territory as another base for its cyber operations. Anonymous sources told *The Japan Times* in February 2018 that a group of North Korean IT specialists moved from Hong Kong to Vladivostok in order to evade international sanctions. The group, which consists of five to seven members in their 20s and 30s, likely engaged in generating foreign currency for the Kim family regime.[53)] The August 2020 UN Panel of Experts report on North Korea announced that three groups of North Korean IT specialists were actually based in Vladivostok and earned approximately $230,000 U.S dollars in March 2020.[54)] It is highly likely that more North Korea cyber operatives are illegally stationed in Russia.

In Fall 2017, *38North* reported that a Russian telecommunications company, TransTeleCom, installed fiber optic lines to North Korea. This connection allowed the North Koreans another way to access the worldwide web. In addition to accessing the Internet via a Chinese route, the Russian Internet connection allowed North Koreans a second link to the worldwide web.[55)] This second link allows the North Korean government to primarily base their cyber operations inside the DPRK and limits any potential of cyber agents' defection. More importantly, it increases North

---

52) Nathan Hodge, "Putin 'pleased' with Kim summit, and will inform US on talks," *CNN*, April 25, 2019, https://www.cnn.com/asia/live-news/kim-jong-un-vladimir-putin-summit-intl/index.html

53) "Shadowy North Korean IT group believed hiding out in Russian Far East: sources," *The Japan Times*, February 18, 2018, https://www.japantimes.co.jp/news/2018/02/18/world/politics-diplomacy-world/shadowy-north-korean-group-believed-hiding-russian-far-east-sources/

54) Bartlett, "Exposing the Financial Footprints of North Korea's Hackers," *CNAS*; "Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)" (S/2020/840).

55) Martyn Williams, "Russia Provides New Internet Connection to North Korea," *38North*, October 1, 2017, https://www.38north.org/2017/10/mwilliams100117/

Korea's international bandwidth capacity and the ability to better evade international sanctions. The Russian government and private sector assisted North Korea's cyber capabilities by providing a safe haven for its IT specialists and an additional Internet connection for the DPRK government.

Ⅶ. Conclusion

North Korea's resilience in the post-Cold War world has been based on guerilla-style militarism, leader worship, and social control. With an estimated 6.5 million North Koreans in the military, virtually every citizen in the DPRK has some kind of personal linkage to the vast military-industrial complex. One is much more likely to see a soldier walking on the streets of Pyongyang than a factory worker. Militarism in North Korean culture is ubiquitous, a far cry from an industrial worker-based Communist society, such as the former Soviet Union. Added into this politico-cultural mix of militarism and social regimentation is the newly embraced technology of hacking and cyber war. As this article detailed, cyber is playing an increasing role in both North Korea's economic and military development. Cyber activity boosts Kim Jong Un's long term plan of parallel development in the economy and military. Despite widespread news coverage of North Korean cyber attacks, few outside analysts or observers have linked the DPRK's cyber operations to Kim Jong Un's *byungjin* line. This paper filled this gap and offered a corrective to the framing of Kim Jong Un's *byungjin* line as an immediate success or failure.

References

Associated Press, "Kim Jong Un inspects new submarine, wants North Korea's military bolstered," *Associated Press*, 23 July 2019, https://www.nbcnews.com/news/world/kim-jong-un-inspects-new-submarine-wants-north-korea-s-n1032711.

Bartlett, Jason, "Why Is North Korea So Good at Cybercrime?" *The Diplomat*, 13 November 2020. https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/.

_____, "Exposing the Financial Footprints of North Korea's Hackers," *CNAS*, 18 November 2020, https://www.cnas.org/publications/reports/exposing-the-financial-footprints-of-north-koreas-hackers; "Report of the Panel of Exports Established Pursuant to Resolution 1874 (2009)" (S/2020/840).

Buzo, Adrian, *The Guerilla Dynasty: Politics and Leadership in North Korea*, New York: Routledge, 2018.

Brewster, Thomas, "North Korean Hackers Accused Of 'Biggest Cryptocurrency Theft Of 2020'—Their Heists Are Now Worth $1.75 Billion," *Forbes*, 9 February 2021, https://www.forbes.com/sites/thomasbrewster/2021/02/09/north-korean-hackers-accused-of-biggest-cryptocurrency-theft-of-2020-their-heists-are-now-worth-175-billion/?sh=412fa5d75b0b.

Byun, Duk-Kun, "Pompeo says N. Korea a greater threat than Russia in cyber security," *Yonhap*, 15 December 2020, https://en.yna.co.kr/view/AEN20201215000200325.

Chainanalysis, "Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options," *Chainalysis*, 9 February 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack.

Choi, Haejin, "North Korea hacked Daewoo Shipbuilding, took warship blueprints: South Korea lawmaker," *Reuters*, 13 October 2017, https://www.reuters.com/article/us-northkorea-missiles-cybercrime/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker-idUSKBN1D00EX.

Choe, Sang-hun, "North Korean Leader Stresses Need for Strong Military," *The New York Times*, 15 April 2012, https://www.nytimes.com/2012/04/16/world/asia/kim-jong-un-north-k

orean-leader-talks-of-military-superiority-in-first-public-speech.html.

CISO MAG, "North Korea hacked Daewoo Shipbuilding, took warship blueprints: South Korea lawmaker," *CISO MAG*, 1 November 2017, https://cisomag.eccouncil.org/north-korea-hacked-daewoo-shipbuilding-took-warship-blueprints-south-korea-lawmaker/.

De, Nikhilesh, "DOJ Charges 3 North Korean Hackers With Stealing $100M+ From Crypto Firms," *Coindesk.com*, February 17, 2021, https://www.coindesk.com/doj-charges-3-north-korean-hackers-with-stealing-100m-from-crypto-exchanges.

Geller, Eric, "North Korean hackers are 'the world's leading bank robbers,' U.S. charges," *POLITICO*, February 17, 2021, https://www.politico.com/news/2021/02/17/us-charges-north-korean-hackers-wannacry-sony-469406.

Hellenic Shipping News, "Daewoo Shipbuilding & Marine Engineering Exposed to North Korean Hacking Attacks," *Hellenic Shipping News*, 23 June 2021, https://www.hellenicshippingnews.com/daewoo-shipbuilding-marine-engineering-exposed-to-north-korean-hacking-attacks/.

Hodge, Nathan, "Putin 'pleased' with Kim summit, and will inform US on talks," *CNN*, 25 April 2019, https://www.cnn.com/asia/ live-news/ kim-jong-un-vladimir-putin-summit-intl/index.html.

Hung, Chang-tai, *Mao's New World: Political Culture in the Early People's Republic*, Ithaca and London: Cornell University Press, 2011.

Insikt Group, "Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite," *Recorded Future*, 25 October 2018, https://www.recordedfuture.com/north-korea-internet-usage/.

Jeong, Gu-Yeon and Ki-Tae Lee, "Kwahakkisulbalchŏn'gwa puk'anŭi saeroun wihyŏp: saibŏ wihyŏpkwa muin'gi ch'imt'u," *Korea Institute for National Unification Research Series* (April 2016).

Joo, Jeong Tae, "N. Korean soldiers study Kim Il Sung-style guerrilla warfare," *Daily NK*, 3 January 2020, https://www.dailynk.com/english/n-korean-soldiers-study-kim-il-sung-style-guerrilla-warfare/.

Jun, Jenny, Scott LaFoy, and Ethan Sohn, "North Korea's Cyber Operations: Strategy and Responses," *CSIS Special Report*, December 2015, https://www.csis.org/analysis/north-korea%E2%80%99s-cyber-operations.

Koettl, Christopher, "How Illicit Oil Is Smuggled Into North Korea With

China's Help," *New York Times*, 24 March 2021, https://www.nytimes.com/2021/03/24/world/asia/tankers-north-korea-china.html.

Kong, Ji-Young, Lim Jong In and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," *11th International Conference on Cyber Conflict (CyCon)*, 2019, https://ieeexplore.ieee.org/document/8756954?signout=success.

Lankov, Andrei, "Is Byungjin Policy Failing? Kim Jong Un`s Unannounced Reform and its Chances of Success," *Korean Journal of Defense Analysis* Vol. 29, No. 1 (2017), 25-45.

Larsen, Morten Soendergaard, "While North Korean Missiles Sit in Storage, Their Hackers Go Rampant," *Foreign Policy*, 15 March 2021, https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/.

Lee, Jeong-ho, "North Korean trade with biggest partner China dives 48 per cent amid sanctions," *South China Morning Post*, 19 July 2019, https://www.scmp.com/news/china/diplomacy/article/3019348/north-korean-trade-biggest-partner-china-dives-48-cent-amid.

Leyden, John, "Beyond Lazarus: North Korean cyber-threat groups become top-tier, 'reckless' adversaries," *The Daily Swig*, 12 May 2021, https://portswigger.net/daily-swig/beyond-lazarus-north-korean-cyber-threat-groups-become-top-tier-reckless-adversaries.

Mangan, Dan. "North Korean hackers charged in massive cryptocurrency theft scheme," *CNBC*, 17 February 2021, https://www.cnbc.com/2021/02/17/north-korean-hackers-charged-in-massive-cryptocurrency-theft-scheme.html.

Maza, Cristina, "North Korea Regime Is Making Money From Cryptocurrency Scam That Offered Users Ownership of Ships: Report," *Newsweek*, October 25, 2018, https://www.newsweek.com/north-korea-cryptocurrency-scam-kim-jong-un-1188020.

McMillan, Robert and Aruna Viswanatha, "North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says," *Wall Street Journal*, 17 February 2021, https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358.

Miller, Steve, "Where Did North Korea's Cyber Army Come From?," *VOA*, 20

November 2018,
https://www.voanews.com/east-asia-pacific/where-did-north-koreas-cyber-army-come.

Nazario, Jose, "Politically Motivated Denial of Service Attacks," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, Washington, D.C: IOS Press, 2010.

Park, Donghui, "North Korea Cyber Attacks: A New Asymmetrical Military Strategy," *The Henry M. Jackson School of International Studies Blog, University of Washington Report*, 28 June 2016,
https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/.

Reuters, "Senior U.S. official accuses China of aiding North Korea cyber thefts," *Reuters*, 22 October 2020,
https://www.reuters.com/article/us-usa-northkorea-china/senior-u-s-official-accuses-china-of-aiding-north-korea-cyber-thefts-idUSKBN2772RX.

Riley, Tonya, "The Cybersecurity 202: Investigations into Russian, North Korean hackers are shaping Biden's foreign policy," *The Washington Post*, 18 February 2021,
https://www.washingtonpost.com/politics/2021/02/18/cybersecurity-202-investigations-into-russian-north-korean-hackers-are-shaping-biden-foreign-policy-anne-neuberger-cybersecurity-biden-administration-cybersecurity/.

Ripley, Will, "North Korean defector: 'Bureau 121' hackers operating in China," *CNN*, 7 January 2015,
https://edition.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html.

Roth, Richard and Joshua Berlinger, "North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report," *CNN*, 9 February 2021,
https://www.cnn.com/2021/02/08/asia/north-korea-united-nations-report-intl-hnk/index.html.

Shin, Chang-Hoon, "Puk'anŭi saibŏ konggyŏkkwa wihyŏbe taehan uriŭi taeŭng 2014nyŏn 11wŏl SONY sagŏnŭi kyohun," *Asan Research Institute Research Brief* (6 April 2015).

Snyder, Scott A., "The Motivations Behind North Korea's Pursuit of Simultaneous Economic and Nuclear Development," *Council on*

Foreign Relations Blog, 20 November 2013, https://www.cfr.org/blog/motivations-behind-north-koreas-pursuit-simultaneous-economic-and-nuclear-development.

Strnad, Grażyna, "Is North Korea's Byungjin Policy in Crisis?," *The National Interest*, 27 June 2021, https://nationalinterest.org/blog/korea-watch/north-korea%E2%80%99s-byungjin-policy-crisis-188649.

Tan, Er-Win, "Byungjin and the Sources of Pyongyang's Paranoia," *International Journal of Korean Unification Studies* Vol. 28, No. 2 (2019), 97-128.

Tarakanov, Dmitry, "Kimsuky APT: Operation's possible North Korean links uncovered," *SecureList By Kaspersky*, September 11, 2013, https://securelist.com/kimsuky-apt-operations-possible-north-korean-links-uncovered/57335/.

The Guardian, "China and North Korea hail 'immortal and invincible' friendship," *The Guardian*, 6 October 2019, https://www.theguardian.com/world/2019/oct/06/china-and-north-korea-hail-immortal-and-invincible-friendship.

_____, "Kim Jong-un calls US 'biggest enemy' and says nuclear submarine plans 'complete'," *The Guardian*, 8 January 2021, https://www.theguardian.com/world/2021/jan/09/kim-jong-un-calls-us-biggest-enemy-and-says-nuclear-submarine-plans-complete.

The Japan Times, "Shadowy North Korean IT group believed hiding out in Russian Far East: sources," *The Japan Times*, 18 February 2018, https://www.japantimes.co.jp/news/2018/02/18/world/politics-diplomacy-world/shadowy-north-korean-group-believed-hiding-russian-far-east-sources/.

The Maritime Executive, "South Korea Probes Possible Hack of DSME Computers," *The Maritime Executive*, 21 June 2021, https://www.maritime-executive.com/article/south-korea-probes-possible-hack-of-dsme-computers.

The US Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," 17 February 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and

United Nations, "United Nations Report of the Panel of Experts established

pursuant to resolution 1874, 30 August 2019," https://undocs.org/S/2019/691.

Van Der Werff Emily and Timothy B. Lee, "The 2014 Sony hacks, explained," *Vox*, 3 June 2015, https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea.

Wada, Haruki, *Kim Il Sung gwa Manju Hangil Chŏnjaeng*, Seoul: Changbi, 1992.

Ward, Alex, "Kim Jong Un made a surprise visit to China. It's mostly about Trump," *Vox*, 9 January 2019, https://www.vox.com/2019/1/8/18173792/north-korea-kim-trump-china-nuclear.

Williams, Martyn, "Russia Provides New Internet Connection to North Korea," *38 North*, 1 October 2017, https://www.38north.org/2017/10/mwilliams100117/.

Yun, Wan-Jun and Dong-Yeon Jung, "North Korean hackers withdraw from their hub in Shenyang," *Dong-A Ilbo*, 11 January 2018, https://www.donga.com/en/article/all/20180111/1186969/1/North-Korean-hackers-withdraw-from-their-hub-in-Shenyang.

〈국문초록〉

김정은의 병진노선에서 사이버의 역할:
북한의 정치문화, 해커, 해양전술

벤자민 영

북한의 사이버 능력은 세계 금융기관 및 외국정부(특히 미국정부, 한국정부)들에 비교적 새로운 위협이 되고 있다. 본 정성 논문에서는, 언론 기사, 학술 출간물과 같은 공개 원천들을 주로 이용하여, 북한 지도자 김정은이 자국의 비대칭 전력을 강화하고 병진노선(경제와 군사력의 동시 발전)을 진전시키는 방식을 분석한다. 특히 북한 공작원들은 사이버 분야와 해양 분야를 통합함으로써 체제에 더 많은 수익을 창출하고 있으며, 심한 제제에도 불구하고 북한 지도부가 권력을 유지하는 데에도 기여한다. 북한 해커들에 관한 국제적 관심이 높아졌지만, 북한의 국제정치 문화에서 사이버의 중요한 역할을 조사한 분석가는 거의 없으며, 특히 김정은의 병진노선 진전 부문에 있어서는 더 그렇다. 사이버는, 오래전부터 존재해 온 북한의 비정규전 및 게릴라 기반 무장투쟁 전통에 잘 맞아떨어진다. 또한, 사이버는 경제 혁신가 및 군사 전략가로서의 김정은의 북한 내 개인의 명성 역시 높인다. 본 논문은 이데올로기 맥락 및 해양 맥락에서 북한 사이버 작전의 역할에 초점을 맞춘다. 북한 해커들은 한국 조선산업을 타깃으로 해왔으며, '해양 체인(Marine Chain)'이라는 블록체인 사기도 개발했다. 북한 사이버 첩보원들은 활동에서 사이버 분야와 해양 분야의 연계에 점점 더 초점을 맞춰왔다.

주제어: 해커, 김정은, 병진, 사이버, 북한

투고일: 2021년 9월 16일 | **심사일:** 2021년 10월 27일 | **심사완료일:** 2021년 11월 25일