Cyber-hacking as a Means of "Self-reliance"

North Korea's Ransomware-based Cyber-hacking for Economic Gains in the Absence of Regulations on Cryptocurrencies in Global Finance

Dr. June Park

NCNK
The National Committee on North Korea

Wilson Center

UNDERSTANDING NORTH KOREA SERIES

The Understanding North Korea roundtable series is a joint program of the National Committee on North Korea and the Wilson Center's Hyundai Motor - Korean Foundation Center for Korean History and Public Policy. The roundtable series was established to enable emerging scholars of North Korea to share their research ideas with peers and experts in the field, and to publish their findings in a format accessible to a general audience.

The National Committee on North Korea is a non-governmental, non-partisan organization whose membership reflects a broad range of perspectives and subject-matter expertise related to North Korea. NCNK serves to share information among its members, advance their work, and provide the broader public with substantive and balanced information about North Korea. NCNK was founded in 2004 by Mercy Corps, a global aid and development organization.

The Wilson Center Hyundai Motor-Korea Foundation Center for Korean History and Public Policy was established in 2015 with the generous support of the Hyundai Motor Company and the Korea Foundation to provide a coherent, long-term platform for improving historical understanding of Korea and informing the public policy debate on the Korean peninsula in the United States and beyond. The Hyundai Motor-Korea Foundation Center for Korean History and Public Policy brings Korea to Washington through advanced research and programming that is rooted in history, informed by scholarship, and in touch with policy.

ABOUT THE AUTHOR

Dr. June Park is a 2021-22 Fung Global Fellow of the Princeton Institute for International and Regional Studies at Princeton University. She is a political economist by training and works on trade, energy, and tech conflicts with a broader range of regional focuses not just on the U.S. and East Asia, but also Europe. She studies economic pressures and conflicts, analyzing different policy outcomes based on governance structures – domestic institutions, leaderships, and bureaucracies that shape the policy formation process. Her current work pertains to post-pandemic geoeconomic conflicts in data governance and technology.

This paper reflects the views of the author alone and not those of the National Committee on North Korea, the Wilson Center, or any other organizations.

Abstract

This policy paper investigates North Korea's illicit financial activities in cyberspace as a means of 'self-reliance'. The paper is divided into three parts: first, it scrutinizes the evolution of North Korea's cryptocurrency thefts by ransomware attacks for bitcoins, followed by money laundering by the Lazarus Group (a.k.a. Hidden Cobra and Labyrinth Chollima), notably by its subgroups BeagleBoyz and Bluenoroff (a.k.a. APT 38 or Stardust Chollima) since 2014. The second part is on sanctions, whereby the paper examines the actions taken for recourse in the form of unilateral sanctions by the U.S. Treasury and other U.S. institutions under Trump and Biden, due to the difficulty of addressing the issue multilaterally. The failure to counter ransomware-based cybertheft under multilateral sanctions at the 1718 Sanctions Committee at the United Nations Security Council (UNSC) stems from dissent on enforcement by China and Russia – actors that have been perpetrating cyber-hacking at a broader scale and retracting contents on cryptocurrency theft and money laundering in the Panel of Experts reports. The third part on empirical findings suggests that the 'self-reliance' that North Korea has stressed at the 8th Congress of the Worker's Party is a recurring strategy that is currently built on exploitation of loopholes in current financial sanctions by planting ransomware, but not necessarily obtaining private keys or exploiting smart contracts. This method of circumvention and evasion of sanctions however may not be sustainable in the longer future if there are further punitive actions taken. The fourth part addresses the recent crackdowns on cryptocurrencies by the U.S. to sanction ransomware under the Biden administration. Lastly, the final section concludes with policy recommendations that suggest a focus on targeting ransomware attacks by reverse hacks/attacks and digital asset freezes upon determination of perpetrators of digital financial crime, to ensure that regulating DeFi does not preclude its positive effects such as financial inclusion, given the forecast that the CBDC's potential to curb cryptocurrency theft would be limited.

Introduction: North Korea's Cyber-hacking as a Means of "Self-Reliance"

Leading up to the 8th Congress of the Workers' Party of Korea in January 2021, North Korea emphasized the notion of 'self-reliance' to overcome its calamities under COVID-19. It emphasized science and technology as the key to the concept, asserting the importance of self-sufficiency and self-sustainability in the lessons of the socialist movement. While no specific strategies were laid out, the concept of 'self-reliance' was presented in ambiguous form to exert internal strife against external threats perceived from within. At present, the symbolic meanings of "self-reliance" based on North Korea's *Juche* philosophy continue to evolve based on the ever-changing situation on the Korean peninsula. As the pandemic unfolds and the digital economy expands, one of the biggest changes to the hermit kingdom's capacity to enable "self-reliance" is indeed its hacking mechanisms in cyberspace.

North Korea has engaged in various kinds of illicit activities – including drug production and tobacco counterfeiting to obtain foreign exchange to overcome chronic trade deficit and current account deficit – in the decades preceding multilateral and unilateral sanctions. In response to the changing international landscape, which had been quite lucrative, North Korea developed other methods of economic gains. Into the 2000s, it focused on counterfeiting currency notes – notably the U.S. dollar – and money laundering. With the rise of multilateral and unilateral sanctions, targeting even North Korea's overseas labor, North Korea sought out to evade sanctions. Ironically, licit commodity-based exports to China enabled North Korea to stay afloat in the early 2010s. As the world's digital transformation accelerated, North Korea saw an opportunity in cyberspace. In the last decade, it has developed domestic talent in computer skills and built an army of hackers focusing on data breach and cryptocurrency theft. The inability of existing sanctions to keep up with and punish North Korea's illicit activities in cyberspace enabled this shift, leaving the task of assessment largely to the expertise of cybersecurity firms. Only in recent years have U.S. authorities taken countermeasures, demonstrated by the U.S. Department of Treasury advisory on ransomware and the U.S. Department of Justice ruling on bitcoin trading activities for North Korea after years of investigation. The U.S. perceives that the money laundering process continues to be crucial for North Korea after obtaining the bitcoins at ransom and exchanging them into fiat currency.

The absence of a global regulatory mechanism on digital currency has also led to the difficulty of establishing a framework for countering North Korea's ransomware attacks. While the central bank authorities around the world have remained undecided on regulating crypto and emphasized the existing system of centralized finance (CeFi), decentralized finance (DeFi) expanded across the globe, and the exponential expansion of the crypto market has led to the loss

of momentum for establishing a multilateral regulatory framework to harness DeFi at the global level.[1] Whether North Korea can continuously depend on cryptocurrencies is largely contingent upon the direction of global governance on DeFi and digital currencies broadly. Cryptocurrencies carry intrinsic values but require convertibility with fiat currency for real world transactions. As North Korea's cyber-hacking activities grow, the policy moves to counter and penalize its bitcoin money laundering are gaining momentum.

The Evolution of North Korea's Cryptocurrency Theft and Recourse

North Korea's Motivations and Operations in Cyber-hacking in the Crypto World and North Korea's Shift to Cryptocurrency Theft from Counterfeited Notes

North Korea was actively counterfeiting banknotes in the 2000s[2], notably the U.S. dollar.[3] Into the latter half of the 2010s, it was reported that counterfeit currencies are still found in North Korea for domestic transactions. Reemerging counterfeit banknotes in North Korean domestic markets not only included local currency but also counterfeit renminbi alongside the dollar for border transactions, demonstrating the demand of the Chinese yuan in North Korea.[4][5] Before 2005, North Korea was heavily reliant on counterfeit notes, and utilized small banks for its finances. Although the U.S. Treasury froze North Korea's accounts in the Banco Delta Asia (BDA) based in Macau that year, North Korea was not totally disconnected from SWIFT, the key global messaging system used by banks to transmit financial transactions, until 2017. While North Korea was able to negotiate the return of funds in the Six Party Talks process, the incident struck a deep fear in North Korea that their financial assets could come under U.S. control.[6] North Korea's counterfeited notes do exist today, though the crackdown by its leadership makes their domestic use risky. On top of the BDA designation and the SWIFT disconnection, the push factors that led North Korea to change the main modus operandi for sanctions evasion from counterfeit notes to cryptocurrency theft were the immense possibilities in cyberspace as an unchartered territory and the utility of bitcoins.

---

[1] Countries are now pursuing their own paths on a) whether they will outlaw crypto currencies, and if so, which kinds; b) how digital currencies would be regulated; c) whether they will issue central bank digital currencies (CBDC) at all, and if yes, under what terms of operation and convertibility; d) which level of anonymity it will require for the trading of digital currencies.

[2] 'US says N Korea forged dollars,' *BBC*, October 13, 2015. http://news.bbc.co.uk/2/hi/asia-pacific/4337610.stm

[3] CRS Reports RL33324, 'North Korean Counterfeiting of U.S. Currency,' March 22, 2006 – June 12, 2009. Congressional Research Service. https://www.everycrsreport.com/reports/RL33324.html

[4] 'High quality counterfeit U.S. notes circulating in N. Korea: sources,' *Yonhap News Agency*, June 26, 2016. https://en.yna.co.kr/view/AEN20160626001700315

[5] '수퍼노트: 전 세계를 속인 북한산 초정밀 위조지폐,' *BBC Korea*, July 8, 2021. https://www.bbc.com/korean/international-57122476

[6] 'North Korea Cracks Down on Counterfeiting, on the Rise as Economy Worsens,' *Radio Free Asia*, July 8, 2021. https://www.rfa.org/english/news/korea/money-07082021165348.html

North Korea increased its interest in cyberwarfare with technological advances upon the collapse of the Soviet Union in the 1990s.[7] Under state guidance, North Korea developed cyber capabilities to overcome its relatively weak conventional military might and to gain benefits in cyberspace. It is worth noting that although concerns had been on the rise from the early 2010s about North Korea's cyber capabilities, its cybercrimes in DeFi did not come under scrutiny by multilateral oversight, as financial sanctions were focused on transactions in CeFi. Only since 2020 have they come to be penalized by U.S. authorities. A new task force targeting ransomware was launched by the U.S. Department of Justice in April 2021, with a mission statement citing that such activity 'not only dangers American businesses but the health and safety of the American people'. However, it is worth noting that U.S. legal action was taken only in the aftermath of a serious injury to U.S. industries, mainly by Russia.[8] Put another way, the North Korean ransomware attacks were not the core target of the initiative taken by the U.S. authorities – rather, the U.S. was responding to Russia's hacking of critical infrastructure and the overall increase in ransomware attacks during the COVID-19 pandemic.

The early hacks conducted by the Lazarus Group include Operation Troy in 2009,[9] Ten Days of Rain,[10] DDoS attacks against NH Bank in 2011[11], and DarkSeoul Cyberattack in 2013[12]. The major hack came in 2014, when Sony Pictures was hacked and demanded to withdraw the release of the film 'The Interview'.[13] The attacks in early 2010s were data breaches rather than cryptocurrency theft, although financial institutions such as banks were targeted. The use of ransomware and phishing attacks to rob banks have only come under scrutiny since the $81 million Bank of Bangladesh heist in 2016. The use of malware has also been evidenced by the WannaCry attacks in 2017 (Figure 1).[14] Cybersecurity firms note that the Lazarus Group[15] that was presumably formed in 2009 was operating for Bureau 121 (Figure 2), a reconnaissance bureau established in 1998.

---

[7] Pinkston, Daniel A. "Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the 'Sŏn'gun' Era." *Georgetown Journal of International Affairs* 17, no. 3 (2016): 60–76. http://www.jstor.org/stable/26395976

[8] 'Ransomware Targeted by New Justice Department Task Force,' *The Wall Street Journal*, April 21, 2021. https://www.wsj.com/articles/ransomware-targeted-by-new-justice-department-task-force-11619014158?mod=article_inline

[9] Ryan Sherstobitoff and Itai Liba, McAfee® Labs and James Walter, Office of the CTO, 'Dissecting Operation Troy: Cyberespionage in South Korea,' *McAfee White Paper*. https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf

[10] 'Ten Days of Rain: Expert analysis of distributed denial-of-service attacks targeting South Korea,' *McAfee White Paper*. https://www.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf

[11] https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

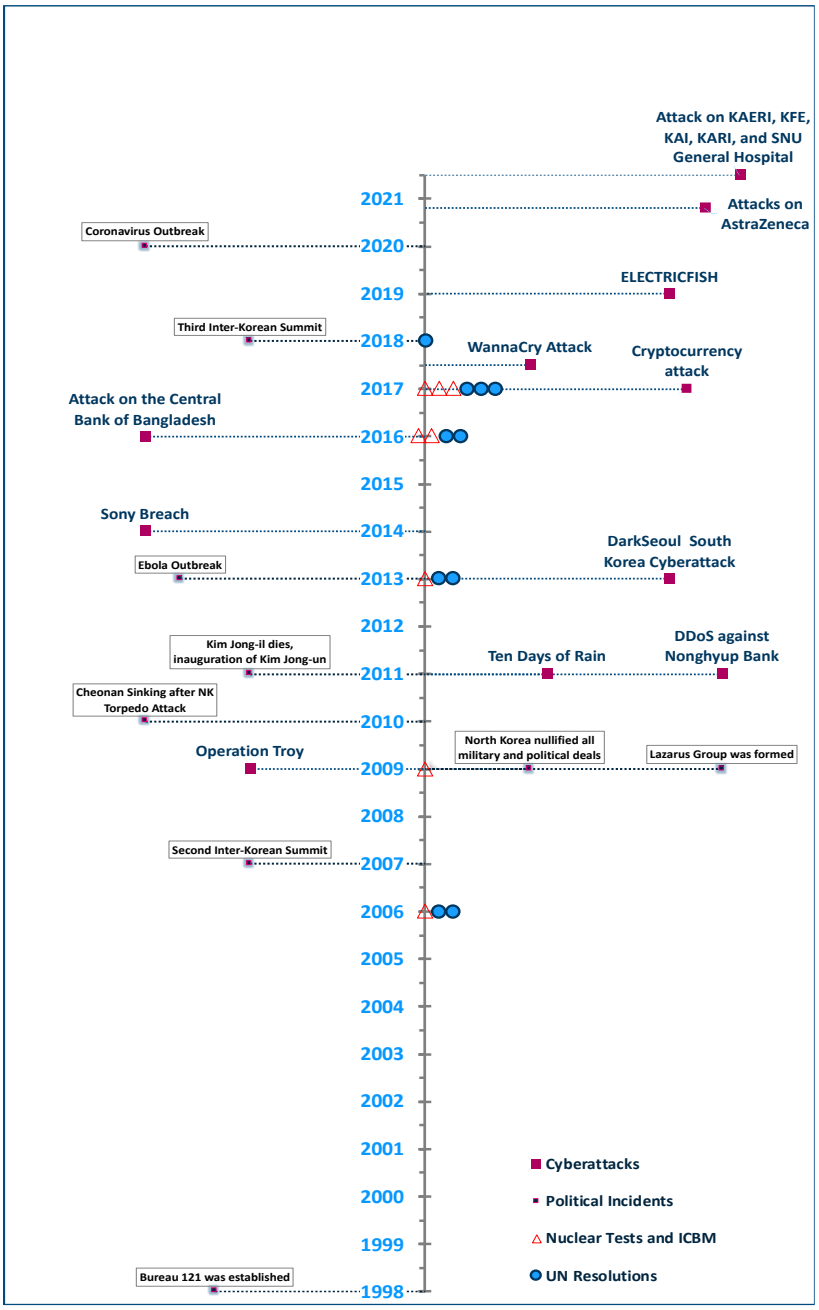
[12] David Martin, 'Tracing the Lineage of DarkSeoul,' *SANS Institute White Paper*, March 4, 2016. https://www.sans.org/white-papers/36787/

[13] 'What is known about the Lazarus Group: Sony hack, military espionage, attacks on Korean banks and other crimes,' Kaspersky Lab, February 24, 2016. https://www.kaspersky.com/blog/operation-blockbuster/11407/

[14] Threat Group Cards: A Threat Actor Encyclopedia. Permanent link APT group: Lazarus Group, Hidden Cobra, Labyrinth Chollima https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Lazarus%20Group%2C%20Hidden%20Cobra%2C%20Labyrinth%20Chollima

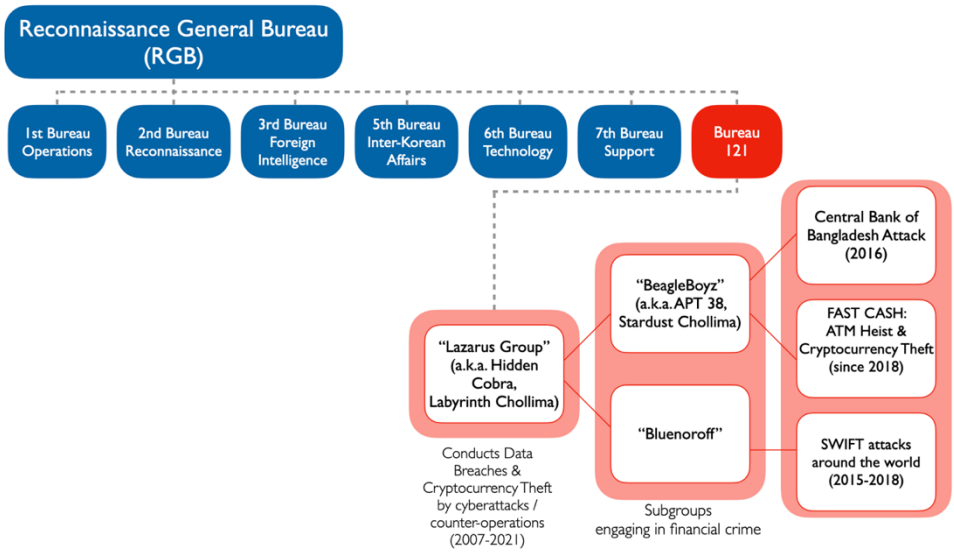
[15] Other names given to the Lazarus Group (Kaspersky) are Labyrinth Chollima (CrowdStrike), Group 77 (Talos), Hastati Group (SecureWorks), Whois Hacking Team (McAfee), NewRomanic Cyber Army Team (McAfee), Zinc (Microsoft), Hidden Cobra (Trend Micro), APT-C-26 (Qihoo 360), ATK 3 (Thales), SectorA01 (ThreatRecon), and ITG03 (IBM).

Figure 1. The Timeline of North Korea's Cyberattacks



Source: Updated by the author based on data by the Thailand Computer Emergency Response Team (CERT) and the Friedrich Naumann Foundation for Freedom (FNF) Seoul Office.

Figure 2. The Organizational Structure of North Korea's Cyber Programs under the Reconnaissance General Bureau (RGB) and Threat Actor Groups of "Lazarus Group"



Source: By author based on the 1718 Panel of Experts Reports, Industry reports by CrowdStrike, FireEye and Treasury reports and the Thailand Computer Response Team of the Government of Thailand and Matthew Ha and David Maxwell, 'Kim Jong Un's All-Purpose Sword', Foundation for Federal Democracies, October 3, 2018 (https://www.fdd.org/analysis/2018/10/03/kim-jong-uns-all-purpose-sword/). Another subgroup of the Lazarus Group – Andariel (FSI) or Silent Chollima (CrowdStrike) – are unmentioned in Figure 2, as they focus primarily on information/data breach and espionage.

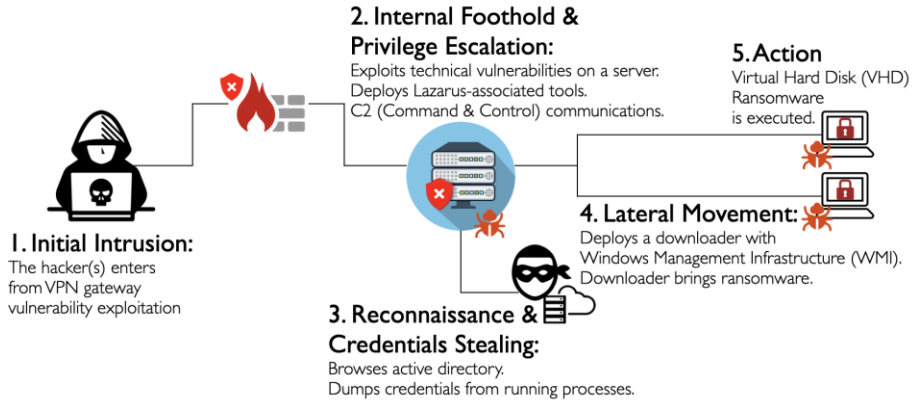
Stage 1: Malware (Ransomware) as a Tool for Paralyzing Computer Systems

The hacking of cryptocurrencies begins with the planting of malware in a targeted system. The use of malware in North Korea's cyber-hacking methods has garnered policy attention in recent years.[16] Notably, ransomware has been the main mode of operation for North Korea's cyber-hacking (Figure 3). Ransomware and viruses are both malwares, in that they are designed to damage, disrupt, or hack a device, ultimately causing adverse effects on the computer systems. The key difference is that while viruses are the sources of infections from one device to another, ransomware involves a paralysis of the targeted computer system and a demand for ransom (mainly bitcoins) in exchange for removal of the malware. The removal of ransomware is usually

[16] 'Lazarus Under The Hood,' The Kaspersky Lab, April 3, 2017. The Lazarus Group has been active since at least 2009, intruding the computer systems of financial institutions, casinos, software developers for investment companies and cryptocurrency businesses across 18 countries – Mexico, Costa Rica, Brazil, Uruguay, Chile, Nigeria, Gabon, Ethiopia, Kenya, Iraq, Poland, India, Bangladesh, Thailand, Vietnam, Taiwan, Indonesia and Malaysia. The most targeted and affected countries are Mexico, the United States, Brazil, Turkey, Saudi Arabia, Iran, India, Bangladesh, Russia, Malaysia, Indonesia, Vietnam, China, Taiwan, and South Korea. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood_PDF_final.pdf

very difficult, leaving victims reliant on the ransomware developer/planter and limiting options to regain access to the system.

Figure 3. North Korea's Bitcoin Hacking using VHD (Virtual Hard Disk) Ransomware



Source: Visualization regenerated and updated by author based on the report by the Kaspersky Lab (2016). https://securelist.com/lazarus-on-the-hunt-for-big-game/97757/

Stage 2: Economic Gains by Theft of Cryptocurrencies

North Korea has relied on bitcoin trading houses, or virtual currency exchange houses, to launder stolen cryptocurrencies into fiat currency since 2017. Bitcoin trading houses offer over-the-counter brokering services. Once the bitcoins have been cashed in via multiple addresses through bitcoin trading houses or exchanges (Figure 4), the returns in fiat cash are laundered in the traditional method using U.S. banks via the centralized financial system (CeFi), with Chinese entities and/or companies acting as enabling platforms.[17][18] The U.S. Department of Justice found a U.S. citizen, Vigil Griffith, guilty of transferring tech expertise on blockchains and cryptocurrencies to North Korea.[19] The U.S. indictment alleges that two Chinese nationals – 田寅寅 a.k.a. Tian Yinyin, and 李家东 a.k.a. Li Jiadong – have engaged in the exchanging act for

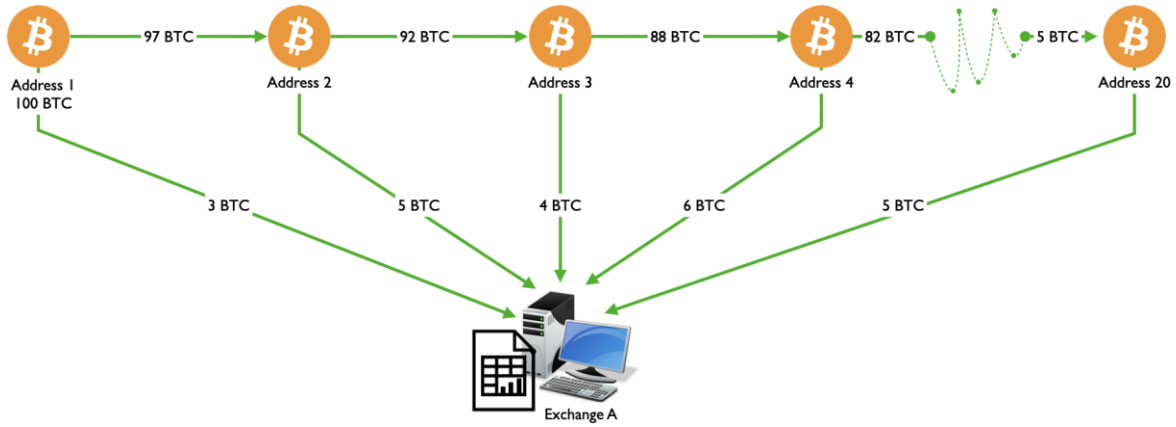
[17] 'FINCEN Files,' International Consortium of Investigative Journalists (ICIJ), September 20, 2020. https://www.icij.org/investigations/fincen-files/

[18] Jason Morris, 'Money Laundering and North Korea,' October 24, 2017. https://www.int-comp.org/insight/2017/october/money-laundering-and-north-korea/

[19] U.S. Attorneys Office, Southern District of New York, U.S. Department of Justice. 'United States Citizen Pleads Guilty To Conspiring To Assist North Korea In Evading Sanctions,' September 27, 2021. https://www.justice.gov/usao-sdny/pr/united-states-citizen-pleads-guilty-conspiring-assist-north-korea-evading-sanctions

North Korea, using several obfuscation techniques[20], ultimately depositing the proceeds into nine financial institutions.[21][22]

Figure 4. Example of a "Peel Chain" of Bitcoins (Stage 2)



Source: 'Annex 56: Laundering virtual currency into a fiat currency,' Report of the Panel of Experts established pursuant to resolution 1874 (2009), UNSC 1718 Sanctions Committee (S/2020/840), p.194. https://daccess-ods.un.org/TMP/6405249.83406067.html Visualization regenerated by the author due to low pixelation in the original Panel of Experts report.

To put this into perspective, North Korea's cryptocurrency theft between 2011 and 2020 totaled more than $1 billion[23][24] and its laundered amount of money from 2008 to 2017 more than $174.8 million[25], while in 2019, the South Korean government provided $9 million in assistance and in 2020, South Korean private entities provided $1.24 million in assistance. In sum, what South Korea provides is minimal compared to what for North Korea can obtain through cryptocurrency theft or money laundering.

[20] Press Release, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency From Exchange Hack: Forfeiture Complaint Details Over $250 Million Stolen by North Korean Actors," Office of Public Affairs, U.S. Department of Justice, March 2, 2020. https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

[21] Press Release, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Department of Treasury, March 2, 2020. https://home.treasury.gov/news/press-releases/sm924

[22] '中国比特币 OTC 兑换商回应受美财政部制裁一案：并不知情，自己也是受害者,' *Chaindd*, March 5, 2020. https://www.chaindd.com/3284691.html

[23] 'These are the largest cyber thefts of the past decade—and 80% of them involve Bitcoin,' *Fortune*, April 6, 2021. https://fortune.com/2021/04/06/cyber-thefts-bitcoin/

[24] 'Financial Hacks: The Biggest Financial Hacks of the Decade,' *Traders of Crypto*, April 2019. https://tradersofcrypto.com/financial-hacks/

[25] 'Secret documents show how North Korea launders money through U.S. banks,' *CNBC*, September 20, 2020. https://www.cnbc.com/2020/09/20/secret-documents-show-how-north-korea-launders-money-through-us-banks.html

Delayed Response at the Multilateral and Unilateral Levels

Multilateral Non-Reaction

As North Korea's cyber-hacking activities grow and expand, existing multilateral sanctions are not fit for the digital age and are no longer sufficient in countering North Korea's cyber threats. The digital age necessitates upgrading, updating and fortifying the sanctions mechanism both at multilateral and unilateral levels, given that the lion's share of North Korea's profit from illicit activities is gained through cryptocurrency thefts in cyberspace. There are two main challenges in adopting UNSC sanctions on cryptocurrency theft relations: a) it may be blocked by P5 members China and Russia, which also engage in cryptocurrency theft at even larger scales, and b) UN member states remain generally divided on how to approach and regulate digital currencies – cryptocurrencies, bitcoins, and central bank digital currencies--and those with trading houses may rebut such a sanctions.

As long-time advocates for partial sanctions relief for North Korea at the UNSC, China and Russia are highly likely to object to additional UNSC sanctions on North Korea. Even missile tests and nuclear weapons development have failed to move the UNSC to fulfill its mandate. For example, North Korea's recent tests of a hypersonic missile prompted a UNSC emergency meeting, but China and Russia opposed the adoption of a joint statement, as both countries are testing hypersonic missiles.[26] A UNSC sanctions resolution on cryptocurrency theft by North Korea will require more than fact-finding efforts by the UN Panel of Experts. Meanwhile, current multilateral sanctions will be unable to counter North Korea's nuclear weapons and ballistic missile proliferation if they cannot sufficiently counter North Korea's theft in cyberspace and the unchecked financing it derives from such activities.

U.S. Unilateral Actions

At the multilateral level, the U.S. government initially tried to pressure North Korea's financial activities via the inter-agency Financial Action Task Force (FATF)[27] given China's recalcitrance at the UNSC. Established in 1989, the FATF is a multilateral body that established international standards on anti-money laundering (AML) and counter-financing of terrorism (CFT). Currently, North Korea is on the FATF's blacklist, which requires countries to impose enhanced financial countermeasures against North Korea.

[26] 'North calls UN Security Council meeting 'intolerable provocation,' *The Joongang Daily*, October 3, 2021. https://koreajoongangdaily.joins.com/2021/10/03/national/northKorea/North-Korea-UN-Security-Council-denuclearization/20211003171749020.html

[27] The Financial Action Task Force, the U.S. Department of Treasury. https://www.fincen.gov/resources/international/financial-action-task-force

Nonetheless, their efforts have not deterred North Korea from engaging in money laundering. The efforts required now at the multilateral and unilateral sanctions levels are more multifaceted than previous methods of implementing financial sanctions. The ongoing investigations and indictments by the U.S. Department of Justice, the U.S. Department of Treasury, the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security, and the Federal Bureau of Investigation (FBI) reveal that even under U.S. unilateral sanctions, combatting North Korea's cyber-hacking activities would require a whole of government approach.

These investigations have led the U.S. to impose its first unilateral sanctions on North Korea's cybercrimes. The U.S. Department of Justice indicted three individuals associated with North Korea's cyber activities in recent years including the Sony Pictures hack in 2014. Most recently, the U.S. Treasury and U.S. Justice departments have entered a prosecution settlement with BMJ, an Indonesian entity, to settle with a payment of the criminal fine (Table 1, left column). In addition, the crackdown on entities that cooperate with North Korea on its money laundering and cyber-hacking schemes have come under scrutiny by Janet Yellen, Secretary of the Treasury Department and former chairwoman of the Federal Reserve Board. The Office of Foreign Assets Control (OFAC) at Treasury under her term has reached settlements with private entities for civil liability for cooperating with North Korean entities in their financial crimes. In February 2021, the CISA issued an advisory with an analysis of North Korea's cryptocurrency malware, AppleJeus, used by the North Korean APT Lazarus Group (Table 1, right column). The analysis was conducted jointly by the FBI, CISA, and Treasury, indicating that the U.S. financial sanctions efforts cannot be conducted by the U.S. Treasury alone. The Biden White House also announced a cross-government task force on ransomware[28], but it is expected that the administration seeks countering ransomware by regulating the entirety of DeFi, while not outlawing digital currencies, with speculations that it intends to protect the interests of CeFi.

[28] 'White House announces ransomware task force — and hacking back is one option,' *Politico*, July 14, 2021. https://www.politico.com/news/2021/07/14/white-house-ransomware-task-force-499723

Table 1. Unilateral Sanctions in the Absence of Multilateral Sanctions to Counter Cryptocurrency Theft by North Korea

	U.S. Judgement on North Korea's Ransomware-enabled cryptocurrency theft	U.S. Investigation on North Korea's Malware-enabled cryptocurrency theft
Operations	Cyber-hacking of the following targets: Entertainment companies (Sony Pictures), financial institutions, cryptocurrency companies (including cryptocurrency exchanges, traders, and marketplaces), online casinos, cleared defense contractors, energy utilities, and individuals	FastCASH (AppleJeus) Individuals and companies, including cryptocurrency exchanges and financial service companies, through the dissemination of cryptocurrency trading applications that have been modified to include malware that facilitates theft of cryptocurrency
North Korean Threat Actor and Individuals	Lazarus Group JON CHANG HYOK, aka "Quan Jiang," a.k.a. "Alex Jiang"; KIM IL, a.k.a. "Julien Kim," aka "Tony Walker"; and PARK JIN HYOK, a.k.a. "Jin Hyok Park," a.k.a. "Pak Jin Hek," a.k.a. "Pak Kwang Jin"	Lazarus Group (Individual names unannounced, investigations in progress)
Enforcement Date and Actors	Indictment on January 14, 2020 US Department of Justice US Department of Treasury	Joint Advisory on Malware AppleJeus on February 2021 CISA, Department of Homeland Security US Department of Treasury and the FBI
Sanctions Target	Bitcoin Trading Houses Bukit Muria Jaya (BMJ Indonesia), for 28 wires to North Korea in violation of Section 510.212 of North Korea Sanctions Regulations	Investigations in progress
Sanctions Method	Ruling Criminal fine of $1,016,000 to settle BMJ's potential civil liability	Pending

Source: By author based on official documents from the U.S. Department of Justice, U.S. Department of Treasury, U.S. Department of Homeland Security.

Argument: Lawlessness on Crypto in the Global Financial System and the Multilateral Sanctions Mechanism

Lawlessness, not Self-Reliance

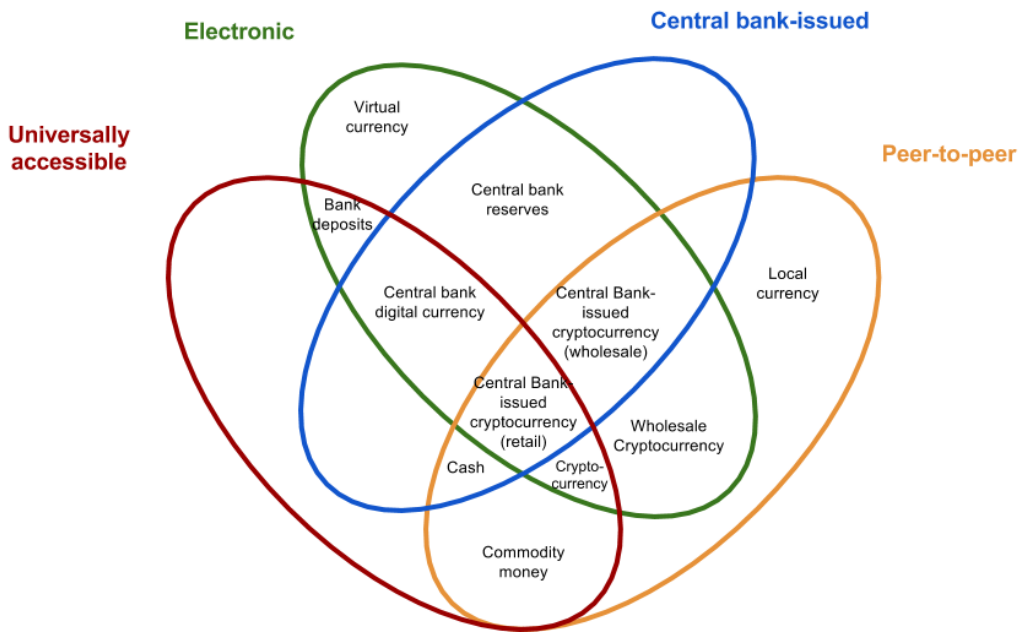
This policy paper contends that what North Korea is relying on is not exactly "self-reliance", but rather *lawlessness* emanating from the absence of governance regarding cryptocurrencies in global finance. The lack of uniform regulatory measures on cryptocurrencies beyond the SWIFT network under existing sanctions enable North Korea's economic gains in cyberspace. Moreover, when loopholes in DeFi are coupled with those in CeFi, it further emboldens North Korea's cryptocurrency theft, followed by money laundering via banks using the SWIFT network.

In the initial development of digital currencies, the deliberations in the private sector (i.e., Facebook's Libra, which is a wholesale digital currency; see Figure 6) for launching tokens were taken as a threat to the power of central banks. China swiftly acted on developing its own digital currency by its central bank, the People's Bank of China (PBOC). Central banks had been against the issuance of central bank digital currencies (CBDC) until 2018, but when it became very clear that China would be launching the digital yuan, the positions by the central banks of the world's major economies shifted. Furthermore, the explosive expansion of DeFi began to raise concerns for CeFi, given the enormous interests embedded in the financial world with decision-making. The response to the rise of DeFi in China was the development of CBDCs and outlawing of everything that is not a PBOC-backed digital renminbi.[29] China's CBDCs are centralized and not on blockchain, which enables the tracking of individual capital and assets, and the PBOC move to outlaw crypto consolidates state control of the people's wealth. The current U.S. moves against ransomware coupled with a hardening policy stance on cryptocurrencies indicate that the U.S. is also moving towards regulation of cryptocurrencies, but it is difficult to imagine the U.S. outlawing crypto entirely. In the U.S., concerns are raised in the financial sector that the U.S. may end up doing the same if it makes crypto illegal.

China's crackdown on cryptocurrencies will have an impact on North Korea's money laundering process of bitcoins using Chinese networks and bank accounts, but will not block or deter its ransomware hacking activities altogether. North Korea will continue to find trading houses to exploit to cash the cryptocurrencies it has obtained through ransomware, and vulnerable financial institutions to place its ransomware to demand bitcoins as ransom.

[29] Press Release, 'Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation (关于进一步防范和处置虚拟货币交易炒作风险的通知),' People's Bank of China, September 15, 2021.
http://www.pbc.gov.cn/en/3688110/3688172/4157443/4353814/index.html (English Version)
http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4348521/index.html (Chinese Version)

Figure 6. Situating Cryptocurrencies in the Financial System



Source: Taxonomy of money by Morten Linnemann Bech and Rodney Garratt, in 'Central bank cryptocurrencies,' Bank of International Settlements (BIS), 2017. p.60 (https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf)

Targeted Sanctions on Cryptocurrency Theft

It is highly likely that in the future, there will be as much policy and regulatory divergence in DeFi amongst jurisdictions as in CeFi (e.g., certain transactions are legal in certain jurisdictions while illegal in others). Countries will have a wide-ranging policy option to choose from: outlawing, partially allowing, or accepting all digital currencies including CBDCs, with varying degrees of convertibility and anonymity amongst different kinds of digital currencies. Upon the launch of CBDCs, countries would benefit from thinking about how they will coordinate internationally in the coexistence of DeFi and CeFi to harness the financial crime in cyberspace. Albeit the limited capabilities in AML and CFT, the launch of CBDCs will be an eventful timing for governments to deliberate the issue of cryptocurrency theft, given what's at stake: global financial risk. Despite the robust protective measures that are anticipated in deploying CBDCs, there are uncertainties regarding hacking and theft of blockchains for CBDCs. It would be the right time to consider under which circumstances cryptocurrency transactions should be voided, reported, and penalized, as in the case of the DOJ indictment on the Lazarus Group's activities.

Validating the Positive Effects of DeFi

However, this is not to suggest that DeFi should be abolished indefinitely, as DeFi has demonstrated that it can extend the benefits of finance beyond the capabilities of CeFi. It would

be important not to throw the baby out with the bathwater. There is a case for defending DeFi, given all its vices including speculative behavior by those that mine crypto and invest in it, that while DeFi is a brewing ground for cybertheft, it has also opened doors for those without bank accounts in CeFi, enabling financial inclusion. Additionally, CeFi has not been with its limitations when it comes to financial crime. The launch of CBDCs will neither prevent nor deter North Korea from engaging in cyber activities aimed at data breaches or cryptocurrency theft. The limits of CBDCs capability to counter anti-money laundering (AML) and counter financing of terrorism (CFT) based on tracking has been continuously raised by previous studies on CBDCs.[30] CBDCs are poised to rely on blockchains, which are tools also deployed in DeFi. The concerns in the future would be discerning whether blockchains are totally un-hackable, both in the realms of DeFi and CeFi. That is to say that the level of risks exists in both worlds.

Conclusion and Policy Recommendations

To explicate what truly enables North Korea's 'self-reliance', this paper has surveyed the landscape and evolution of North Korea's cryptocurrency theft, and the current limitations of sanctions at the multilateral level and unilateral U.S. actions taken. The lawlessness on digital currencies in global finance enables North Korea's illicit activities in cyberspace. This paper has also maintained that outlawing DeFi to protect the interests of the CeFi would do little to counter them and therefore would be unreasonable. Below are three tangible recommendations:

First, a coordinated mechanism of mandatory reporting of suspicious transactions should be built domestically and internationally (beyond the levels of FTAF), to include bitcoin cashing. If DeFi and CeFi are to coexist, it would mean the coexistence of various digital currencies with CBDCs – meaning it would mean more complication to investigating North Korea's cyberthefts. This is especially necessary if CBDCs inherently do not have a strong AML/CFT mechanism.

Second, the means, expertise and intelligence withheld by major U.S. cybersecurity firms should be shared with the U.S.-ROK Ransomware Working Group, launched in September 2021 at the National Security Council levels of the two countries, and North Korea's behavioral patterns in cyberspace must be thoroughly studied to build a preventive mechanism within the discretion of the alliance. Notably, the methods of reverse hacking (e.g., deployed in the case of Colonial Pipeline hack) to retrieve stolen bitcoins would be highly desirable for both sides.

[30] 'Central Bank Digital Currencies,' Committee on Payments and Market Infrastructures, Markets Committee of the Bank for International Settlements, March 2018. p. 9. It is noted that such capability may be limited especially in the case of a traceable CBDC, as it would not be the main conduit for illicit transactions if it is traceable.
https://www.bis.org/cpmi/publ/d174.htm

Third, as in the case of Colonial Pipeline ransomware attack, methods such as reverse tracing in the digital realm to target digital asset freezes of malicious actors should be deployed toward asset seizure, in the event of a ransomware attack and ransom handover.[3132] Determination of specific perpetrators of digital financial crime and paralyzing their interests would ensure that regulating cryptocurrency theft need not blanket regulation on DeFi, and would not preclude its positive effects such as financial inclusion.

[31] Office of Public Affairs, U.S. Department of Justice, 'Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,' June 7, 2021.
[32] 'First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers,' *CNN*, June 8, 2021. https://edition.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html

Cover Image: View of Pyongyang from North Korea's capital.
Photo by Omer Serkan Bakir via iStock