HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

BRIEF
belfercenter.org/project/korea-project

KOREA PROJECT | MAY 2022
NORTH KOREA CYBER WORKING GROUP POLICY MEMO NO. 1

North Korean Cryptocurrency Operations: An Alternative Revenue Stream

By Heeu Millie Kim, June Lee, and Rachel Paik

Executive Summary

As cryptocurrency has risen to prominence within the past decade, its widespread use has likewise created great potential for exploitation by malicious actors. With a cyber arsenal capable of reaching cryptocurrency platforms and users, North Korea has increasingly targeted virtual assets as a source of revenue for its regime. In its 2021 final report, the United Nations Panel of Experts estimated that North Korea stole approximately $316.4 million in virtual assets between January 2019 and November 2020. The decentralized nature of the cryptocurrency market is well-suited for a heavily-sanctioned and financially-isolated state like North Korea, especially given tighter trade restrictions and border closures during the COVID-19 pandemic. The ease of obscuring ownership

of virtual assets and the lack of regulatory oversight make cryptocurrency all the more attractive for North Korea.

Although North Korean cyber operations have been widely publicized, the purpose of this report is to focus on three ways North Korea obtains cryptocurrencies, specifically cryptomining, cryptojacking, and fraudulent initial coin offerings (ICOs). Given observed trends and changes in the cryptocurrency environment—namely, the rise of decentralized finance (DeFi) and over-the-counter brokers—this paper finds that North Korea's crypto operations are consistent with its national objectives and likely to continue. Second, North Korea's cryptocurrency operations offer an attractive and transferable model for other financially-isolated states and non-state actors. Finally, governments should work with law enforcement agencies, multilateral institutions, and non-traditional actors to mitigate the national security threat from North Korea's cryptocurrency activities.

Background

North Korea's state-sponsored cyber actors have already generated substantial revenue through operations targeting financial systems. In the FASTCash campaign that emerged around 2016, a group known as the BeagleBoyz stole tens of millions of dollars through fraudulent ATM cash-outs in multiple countries, including the United States. In 2018, the US Department of Justice (DOJ) charged a North Korean computer programmer, Park Jin Hyok, for his involvement in the 2017 WannaCry global ransomware operation, the 2016 theft of $81 million from Bangladesh Bank, and the 2014 attack on Sony Pictures Entertainment. These operations have not only undermined the integrity of international financial systems, but also demonstrated North Korea's ability to evade United Nations Security Council (UNSC) sanctions through cyber-enabled tactics. Since 2017, North Korea has increasingly engaged in illicit cryptocurrency activities alongside its cash withdrawal schemes and far-reaching ransomware attacks.

Estimates from the DOJ and the United Nations Panel of Experts (POE) confirm that cryptocurrency theft is indeed profitable and has great potential to become an effective and sustainable revenue stream for North Korea. In 2018 alone, North Korea's state-sponsored cyber actors reportedly stole more than $250 million dollars-worth of virtual currencies. Lazarus Group, a U.S.-designated North Korean state-sponsored malicious cyber group, was able to remotely access private keys to virtual currency wallets by hacking into the email of a crypto exchange employee. Two Chinese individuals played a critical role laundering the illicitly-obtained funds through cryptocurrency exchanges and bank accounts, rendering North Korea's cyber intrusion a success. This cryptocurrency heist accounted for nearly half of North Korea's estimated gains in virtual currency that year. For the first

time in the public eye, cryptocurrency theft was seen as a means for North Korea to rake in substantial amounts of money—largely undetected and through a loosely regulated financial system.

Since then, North Korean cyber actors have increasingly targeted cryptocurrency companies to illicitly accrue and launder significant amounts of virtual currencies. The 2021 UN report revealed that China-based individuals also laundered North Korea's proceeds from two hacks in July 2019 and September 2019, through which North Korea stole approximately $272,000 and $2.5 million, respectively. Income raised through crypto activities, often at the behest of the military's Reconnaissance General Bureau, is thought to support the regime's weapons of mass destruction (WMD) programs.

Estimation of Gains from Reported Cryptocurrency Theft

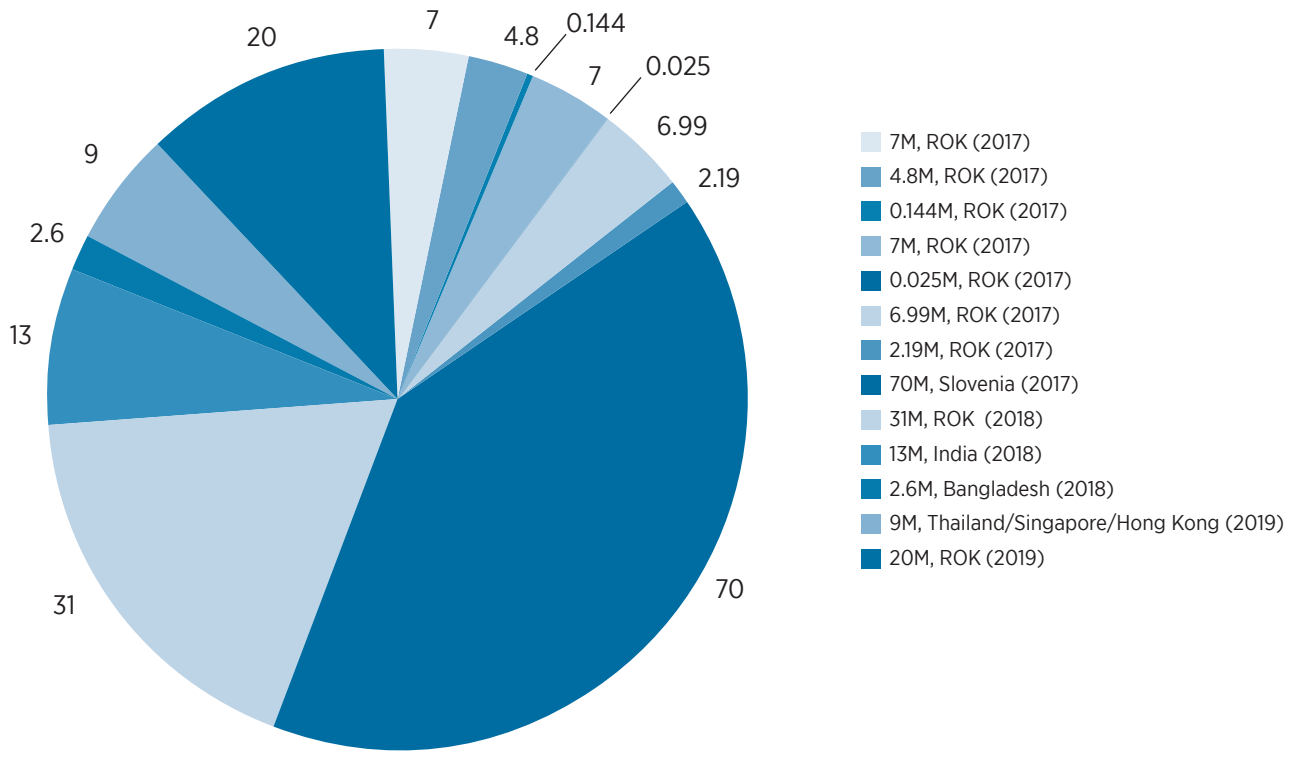
Exact figures of North Korea's total gains from cryptocurrency operations are unknown, given several barriers that complicate tracking and calculation. First, North Korea utilizes over-the-counter virtual asset brokers, many of whom are in third party countries like China. North Korea launders money through these peer-to-peer services that do not collect know-your-customer information to covertly convert gains in cryptocurrency. These brokers create shell companies in countries like China, Singapore, Cambodia, and the U.S. to move tens of millions of dollars through correspondent banking services and finally to North Korea.

Obfuscation techniques also create a money trail that is impossible to track. Chain-hopping, which the UN believes brokers used to launder proceeds from North Korea's 2019 July and September hacks, is a method where a broker rapidly converts virtual assets from one cryptocurrency to another through unregulated exchanges. This dilutes the traceability of transactions, even if initial records exist on the cryptocurrency's blockchain ledger. Another challenge to estimation is cryptocurrency that builds in anonymity from the start, such as Monero, Dash and Z-Cash, since transactions of these virtual assets are not associated with users to begin with. Finally, with transaction fees paid to brokers and third party actors, the final sum obtained by North Korea through cryptocurrency schemes is near impossible to calculate.

Though exact figures are unknown, a general discussion of estimated gains is important to understand how valuable cryptocurrency operations are to North Korea as a revenue stream. As these gains are unregulated, North Korea can continue to accrue significant amounts of cybertheft funds

to generate revenue for the regime. The 2021 UN Security Council report suggests that North Korea accumulated $316.4 million dollars in virtual currency between January 2019 and November 2020 alone. The Panel is currently investigating a cryptocurrency exchange hack from September 2020 with strong links to North Korea, which resulted in a theft of approximately $281 million worth of cryptocurrencies. The 2019 UN Panel of Experts mid-term report estimated that North Korea had raised $571 million in cryptocurrencies. North Korea extorted mainstream cryptocurrencies including Bitcoin and Ethereum, starting with an attack on South Korea's digital asset trading platform, Bithumb, in 2017. Targeting a range of cryptocurrency companies around the world, North Korea notably stole more than $70 million from a Slovenian company in December 2017; $24.9 million from an Indonesian company in September 2018; and $11.8 million from a New York financial services company in August 2020, among other cases.

Reported Revenue from Cryptocurrency Theft Operations (in millions of USD)



*Reported cryptocurrency theft from 2017 to May 2019. Numbers from the 2019 UN POE midterm report based on information from Member States, statements by government agencies, corporate statements, reports by cybersecurity firms and media articles.

As recently as February 2021, the US DOJ indicted two additional North Korean programmers who allegedly collaborated with Park Jin Hyok to extort more than $1.3 billion in money and cryptocurrency in a series of cyberattacks. Though challenging to estimate and verify, the potential value of stolen cryptocurrency indicates that North Korea will not be turning away from virtual assets anytime soon.

North Korean Cryptocurrency Activities

The following section examines three methods (both licit and illicit), by which North Korea obtains cryptocurrency, beyond attempts to hack cryptocurrency exchanges. While the regime may rely on alternate means to raise cryptocurrency, reports most frequently attribute the following techniques to North Korean hackers.

Crypto Mining

Put simply, crypto mining is a process of solving cryptographic equations to gain rewards in the form of cryptocurrency. The 'main actor' or miner seeks to solve a cryptographic function in order to validate a cryptocurrency transaction and add it to the blockchain, which is essentially a public record of all cryptocurrency transactions. In doing so, the miner competes to successfully solve the puzzle, verify the legitimacy of a cryptocurrency transaction, and earn a fixed amount of cryptocurrency. The reward for each block added to the blockchain depends on the type of cryptocurrency. For Bitcoin, the reward is currently 6.25 bitcoins for each verified transaction, although the reward amount is halved every 210,000 blocks (roughly every four years). As of March 2022, a single Bitcoin traded at around $46,000, which means one successful verification would have been worth about $287,500 USD. For Monero (XMR)—another cryptocurrency targeted by North Korea—the reward decreases as more Monero is mined. In March 2022, a miner would have gained 0.86 XMR or about $190 per verification, given the XMR price of $216.

North Korea allegedly began mining Bitcoin in May 2017, and its efforts have increased exponentially from no activity to hundreds of mining attempts per day. At the time, the reward was 25 Bitcoins per verified transaction, which means one successful addition to the blockchain amounted to around $54,000 ($2,170 was the price of Bitcoin in May 2017). That year alone, the price of Bitcoin increased by more than 1,000 percent. North Korea would have earned a whopping $326,550 per successful verification in December of 2017. In 2020, Recorded Future, a cybersecurity firm, reported that North Korea was mining Bitcoin at a small scale and relatively static rate as of November 2019. Comparatively, the traffic volume and rate of communication with peers for Monero mining increased tenfold between October 2018 and November 2019. As Monero is a privacy-oriented coin that uses cryptography to hide transaction information, North Korean hackers who seek to obscure the flow of money between users may prefer mining a coin like Monero to

Bitcoin. Indeed, Recorded Future observed an increase in the use of port 7777, a mining pool commonly used for Monero by higher-capacity machines.

A possible inhibitor to North Korean crypto mining is that it requires significant computing power and high-wattage power supplies. By the most recent 2021 metrics, one Bitcoin transaction requires approximately 1,810.31 kilowatt-hours (kWh) of energy. Put in perspective, this is the equivalent of roughly 62 days of electricity for the average US household. Thus far, North Korea's access to an abundance of cheap energy from coal has fueled its crypto mining. Yet, North Korea's computational capabilities are fairly constrained by IP challenges, its limited access to computers, and reliance on Kwangmyong, the domestic intranet that is isolated from the rest of the world. This may be another reason why North Korea has turned to Monero, which requires lower processing requirements.

Moving forward, the launch of blockchain platform Ethereum 2.0 in 2022 may be a gamechanger for cryptocurrency mining. Ethereum 2.0 will be far less energy-intensive from a computer processing standpoint because it will function on a proof-of-stake rather than a proof-of-work mechanism used by most cryptocurrencies. Users will be able to propose blocks and validate transactions through attestations rather than mining on the blockchain network. This will reduce Ethereum's power consumption by 99.9%. Given the scalability of this process, Ethereum 2.0 is projected to boast 100,000 transactions per second, which is much faster than Bitcoin's rate at 4.6 transactions per second. North Korea reportedly has not mined Ether, but the platform's lower hardware requirements and relative ease of processing may prove attractive for its future mining endeavors.

Though crypto mining is neither illegal nor restricted to certain actors, North Korea is likely to continue evading sanctions and hiding the flow of money into the regime through the mining and theft of cryptocurrency. Such an independent and loosely-regulated virtual asset system provides the ideal environment for a heavily-sanctioned and cash-strapped state like North Korea to move and obtain illicit funds.

Cryptojacking

Cryptojacking involves the deployment of malware to infect devices and surreptitiously use their computing power to mine for cryptocurrency. Hackers commonly gain access to their victims by compromising individual devices through phishing and spear phishing attacks, or injecting legitimate websites with mining script that runs on any browser that visits the site. Newly generated tokens are deposited in wallets owned by the attacker, while the victims bear the costs of mining, including electricity and wear and tear to computers. Early cryptojacking attacks caused a noticeable slowdown in device operation, as the mining process consumed significant computing power.

However, crypto mining malware has developed in ways that allow it to better conceal its presence, allowing malicious programs to persist undetected in victim devices for long periods of time.

Cyber criminals are increasingly taking advantage of the revenue generation opportunities offered by cryptojacking. In the first half of 2018, the number of detected samples of crypto mining malware increased by 950%. Following the growth in cryptocurrency prices in the first quarter of 2021, Kaspersky reported a surge of attacks involving illicit crypto mining. Cryptojacking malware has also been detected in the networks of industrial control systems, where increased processor and network bandwidth usage could have significant safety concerns. Some cyber criminal groups have paired crypto mining malware with ransomware attacks, creating versatile and potentially powerful tools for obtaining cryptocurrency.

North Korean hacking groups engage in cryptojacking as an additional means of generating revenue while evading financial sanctions through cyber means. While few instances of cryptojacking have been publicly attributed to North Korea, the regime's known operations have targeted users in South Korea but also globally. In the summer of 2017, North Korean hacking group Andariel seized control of a server at a South Korean company, using it to mine about 70 Monero coins (worth about $25,000 at the time). Andariel is known for conducting operations tailored to South Korean businesses and government agencies. According to a South Korean government report, the group has been involved in multiple illicit schemes to generate revenue, including stealing bank card information from ATMs and hacking online gambling sites to steal cash.

In April 2017, Kaspersky Labs reported that North Korean hacking group Bluenoroff (which overlaps with the BeagleBoyz group) infiltrated a server in France in order to install Monero mining malware on victim devices. The incident was only detected as server logs that indicated the group's advanced, persistent backdoor were not properly wiped, likely due to the hackers' installation of computationally-demanding crypto mining software. Kaspersky Lab says Bluenoroff's malware is likely to be secretly deployed in many other servers around the world.

North Korean universities also appear to be engaged in developing cryptojacking applications. In early 2018, researchers detected software for an application that mined Monero and sent it to Kim Il Sung University in Pyongyang. The address set to receive the mined crypto coins did not resolve, suggesting either that the application was developed as an early test of a cryptojacking attack or for educational purposes. The university's involvement in the cryptojacking scheme is consistent with reports that North Korean state hackers receive training at the country's elite universities.

Cryptojacking offers an attractive, persistent means for North Korea to evade international sanctions and generate funds for its WMD program, and the regime is likely to continue with such

activities. Exploiting victims' computing power allows the regime to engage in crypto mining at scale and overcome the challenge of its limited national computational capabilities. As governments globally begin to impose regulations on crypto activities, cryptojacking will become even more important as a means for the regime to conceal cyber crime operations and overcome first line cyber defenses.

Fraudulent Initial Coin Offerings (ICOs)

In 2021, the DOJ unsealed an indictment alleging that North Korean hackers had stolen millions of dollars worth of cryptocurrency by developing and marketing a fraudulent blockchain platform called Marine Chain. To date, Marine Chain remains one of the best known fraudulent initial coin offerings (ICOs) and the only one officially attributed to North Korea.

An ICO describes the process by which companies in the blockchain and cryptocurrency space raise capital to launch new tokens, apps, goods, or services. The end product of an ICO is called a token, of which there are several types. Utility tokens are the most common type, and Ethereum is one of the most popular utility tokens. Less commonly known are security tokens, or digital contracts for a fraction of an asset with tangible value, such as real estate, cars, or ships. As a result, the purchase or sale of a security token will often include the characteristics, economic value, and rights associated with these assets. As ICO investments are open to nearly anyone, the sale of security tokens through ICOs has become comparable to a traditional IPO with lower barriers to entry. This is one of the unique appeals of security tokens.

In the case of Marine Chain, North Korean hackers launched a fraudulent ICO for an asset-backed security token that tokenized shipping vessels. Marine Chain described itself as a "next-generation global maritime investment marketplace" that allowed individuals and institutions to purchase and trade the fractional ownership of marine assets, while allowing North Korea to "secretly obtain funds from investors, control interests in marine shipping vessels, and evade U.S. sanctions." What is notable about the choice to offer security tokens for shipping vessels is that North Korea is renowned for its illegal ship to ship transfers and disguising the ownership of its vessels to circumvent US and UNSC sanctions. The alleged CEO of Marine Chain, who identified himself as Captain Jonathan Foong Kah Keong, has also been connected to several other Singapore-based companies known to work with North Korea to circumvent sanctions. Pyongyang took advantage of high-risk investors who were willing to put digital capital into shipping vessels that may have been used to bring money and resources to North Korea in the real world.

The timing of the fraud scheme is also notable. Marine Chain was highly active in 2017 to 2018, well before the popularization of security token ICOs and increased SEC regulation, demonstrating North Korean hackers' exploitation of new trends in cryptocurrency to accrue capital for the regime. However, users on popular cryptocurrency forums like Reddit were quick to catch onto North Korea's first fraudulent ICO, noting that the Marine Chain website appeared to be a carbon copy of another website called Shipowner, which was also offering security tokens for shipping vessels.

In recent years, the US Securities and Exchange Commission has moved to approve tokens they evaluate as compliant with their standards, which could potentially increase interest in new blockchain-based token offerings. Investors are hopeful that regulation will stimulate the adoption and widespread use of security tokens, allowing them to function as a bridge between Wall Street and the cryptocurrency world.

Noteworthy Trends in the Crypto Environment

Two trends in digital currencies and illicit finance pose challenges for existing efforts at regulating the crypto environment, to the advantage of malicious North Korean actors, and demand greater attention from international policymakers.

1. Rise of Decentralized Finance (DeFi)

Decentralized finance, commonly referred to as DeFi, is a blockchain-based form of finance that does not rely on central financial intermediaries such as brokerages, exchanges, or banks to offer traditional financial instruments. Instead, DeFi utilizes "smart contracts," which are self-executing contracts between buyers and sellers, written into code, and stored on blockchains such as Ethereum. As the fundamental purpose of DeFi is to allow lenders and borrowers to engage directly with each other and remove the need for third-party institutions, DeFi applications seek to minimize oversight and regulation. As a result, the growth of DeFi may complicate the application of existing financial regulations. In a September 2020 cryptocurrency theft tied to North Korea, hackers reportedly sought to launder the stolen funds through decentralized exchanges. If DeFi continues to grow in prominence, it will become increasingly difficult for international and national

law enforcement to conduct oversight and regulation, making crypto an ever more viable funding source for heavily sanctioned states, including but not limited to North Korea.

2. Role of Over-the-Counter (OTC) brokers

US and international regulators should seek ways to track over-the-counter (OTC) brokers who have worked, or continue to work, with North Korea-associated crypto wallets. North Korean crypto activities involve a complex chain of transactions to launder and ultimately convert digital currency into funds that can be readily used. OTC brokers play a major role in each stage of this process, such as facilitating "layering" schemes (e.g., "peel chains" and "chain hopping") intended to move crypto coins into different wallets and currencies, obscuring the original source of the funds. North Korea also relies on OTC brokers willing to bypass legal requirements—frequently based in China—to convert their digital coins into cash. South Korea recently introduced legislation requiring crypto exchanges to register with its internet security agency, but the OTC broker issue remains a major problem. Increased analysis and monitoring of international crypto exchanges (such as know-your-customer rules and anti-money laundering programs) by South Korean, UN, and other international regulators could help inform both policymakers, banks, and the private sector.

Future Outlook for North Korean Crypto Activity

Facing financial peril due to decades of US and UN-led sanctions and even tighter trade restrictions and border closures to prevent the spread of COVID-19, North Korea will likely continue to engage in cyber-enabled crime to obtain cryptocurrency. With estimated gains in the hundreds of millions of dollars, cryptocurrency theft has proven to be a highly profitable endeavor for North Korea. There is currently little to prevent the regime from growing the breadth and sophistication of its already advanced cyber operations.

Despite indictments from the US government, North Korean cyber criminals remain at large, as North Korea does not extradite its citizens to face US charges. There may be some potential for North Korean cyber actors to be apprehended within their wide network of overseas cells. The March 2021 extradition of a North Korean citizen from Malaysia to the US on money laundering charges suggests that states may be increasingly willing to comply with sanctions and strengthen lax legal frameworks exploited by North Korean cyber criminals. Governments have also taken

direct steps to restrict the activities of cryptocurrency exchanges. In September, the US Treasury issued its first sanctions on a cryptocurrency exchange for facilitating ransomware payments by a cyber criminal group. China's recent announcement outlawing all crypto-related transactions will surely disrupt North Korean crypto operations in China.

Yet, even in an evolving regulatory environment, North Korea is likely to continue its illicit crypto activities, relying on an extensive cyber crime network and partnerships with nations such as Russia, Iran, and India.[1] North Korea can maintain a steady revenue stream from cryptocurrency theft by bargaining with select cryptocurrency exchanges, banks, or state regulators who facilitate their illicit activities in exchange for exemption from North Korean cyber attacks. As new regulations pose a potential challenge to the regime's crypto activities, North Korea will adapt, doubling down on existing networks and forging new international partnerships, to maintain alternative sources of funding for its WMD program.

This paper offers three key takeaways for international policymakers and network defenders.

1. **North Korea's crypto operations are consistent with its national objectives and therefore are likely to continue.** As the international community imposes increasing sanctions on the regime, crypto operations have provided a persistent means for North Korea to evade international sanctions and generate funds for its WMD program. While exact figures are unknown, the increasingly diverse means through which North Korea attempts to obtain cryptocurrency suggest that the regime will continue to invest in its crypto operations.

2. **North Korea's cryptocurrency operations offer a transferable model for other financially-isolated states and non-state actors**. North Korea's experience with cryptojacking, fraudulent ICOs, and other forms of cryptocurrency theft not only provides an alternative means for the regime to fund its WMD program, but can also serve as a viable model for other sanctioned and cash-strapped states seeking to move and obtain funds. Several states, including Iran, Venezuela, and Russia, have already used crypto activities to raise revenue outside of the traditional financial system. If North Korea continues to profit from cryptocurrency schemes, other financially and diplomatically isolated states will seek to develop the capabilities for illicit crypto theft as a means of generating wealth while circumventing sanctions. Moreover, nonstate actors may also look to illicit cryptocurrency activities for funding. Though technical capacity is still a limiting factor for state and non-state actors, North Korea's continued crypto operations and adaptation to the changing crypto environment could provide a model to overcome these challenges.

1 For instance, in 2020, North Korea joined a new "Group of Friends" within the United Nations, strengthening networks with China, Russia, and Iran, as well as Algeria, Angola, Belarus, Bolivia, Cambodia, Cuba, Eritrea, Laos, Nicaragua, Saint Vincent, Syria, Venezuela, and Palestine.

3. **Governments should work with law enforcement agencies, multilateral institutions, and other non-traditional actors to develop creative approaches to mitigate the national security threat from North Korea's crypto operations**. Sanctions and other traditional national security measures have proved ineffective in restricting the regime's crypto fraud and illicit operations. National security actors should consider hybrid approaches, such as working more closely with law enforcement and treating North Korea's revenue-generating cyber activities as cyber crimes, or strengthening financial crime or tracking capacities by working with banks and multilateral institutions.

Works Cited

Anti-Malware Research, Kaspersky Lab. "IT threat evolution Q1 2021. Non-mobile statistics." Secure List, May 31, 2021. https://securelist.com/it-threat-evolution-q1-2021-non-mobile-statistics/102425/.

"Bitcoin Energy Consumption Index." Digiconomist, 2021. https://digiconomist.net/bitcoin-energy-consumption/.

De, Nikhilesh. "Blockstack's Regulated Token Offerings Raise $23 Million." CoinDesk Latest Headlines RSS, September 10, 2019. https://www.coindesk.com/markets/2019/09/10/blockstacks-regulated-token-offerings-raise-23-million/.

Doman, Chris. "A North Korean Monero Cryptocurrency Miner." AT&T Business, January 8, 2018. https://cybersecurity.att.com/blogs/labs-research/a-north-korean-monero-cryptocurrency-miner.

Frankenfield, Jake. "Cryptojacking." Investopedia, October 28, 2021. https://www.investopedia.com/terms/c/cryptojacking.asp.

Frankenfield, Jake. "Initial Coin Offering (ICO)." Investopedia, November 3, 2020. https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp.

Frankenfield, Jake. "Smart Contracts: What You Need to Know." Investopedia, December 7, 2021. https://www.investopedia .com/terms/s/smart-contracts.asp.

Gill, Prabhjote. "Ethereum 2.0's first upgrade will happen this month — a step closer to denting the competitive advantage of 'Ethereum Killers'." Business Insider, October 8, 2021. https://www.businessinsider.in/investment/news/ethereum-altair-hard-fork-threatens-competitive-advantage-of-solana-cardano-and-others/articleshow/86863524.cms.

Gilbert, David. "North Korea's Bitcoin Crash Course Has Experts Worried." Vice, November 27, 2017. https://www.vice.com/en/article/a37xya/north-koreas-bitcoin-crash-course-has-experts-worried.

Global Research & Analysis Team, Kaspersky Lab. "Lazarus Under The Hood." Secure List, April 3, 2017. https://securelist.com/lazarus-under-the-hood/77908/.

Greig, Jonathan. "US Treasury Dept. Sanctions Russian Cryptocurrency Exchange for Work with Ransomware Groups." ZDNet, September 21, 2021. https://www.zdnet.com/article/us-treasury-dept-sanctions-russian-cryptocurrency-exchange-for-work-with-ransomware-groups/.

Insikt Group. "How North Korea Revolutionized the Internet as a Tool for Rogue Regimes." Recorded Future, February 9, 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0209.pdf.

Insikt Group. "North Korea's Ruling Elite Are Not Isolated." Recorded Future, July 25, 2017. https://www.recordedfuture.com/north-korea-internet-activity/.

Ioanes, Ellen. "North Korea Is the Most Isolated Country on the Planet, but It Still Finds Ways to Steal Billions of Dollars." Business Insider, March 3, 2021. https://www.businessinsider.com/how-north-korea-uses-hacking-and-cryptocurrency-to-avoid-sanctions-2021-3.

Jun, Jenny. "How North Korea's Cyber Power Can Undermine US Sanctions Enforcement." NK PRO, July 2, 2021. https://www.nknews.org/pro/how-north-koreas-cyber-power-can-undermine-us-sanctions-enforcement/?t=1641908476343.

Kasulis, Kelly. “For the First Time Ever, a North Korean Man Is Brought to the US to Stand Trial: NK News.” NK News - North Korea News, March 23, 2021. https://www.nknews.org/2021/03/for-the-first-time-ever-a-north-korean-man-is-brought-to-the-us-to-stand-trial/.

Kelly, Jemima. “Bitcoin’s murkier rivals line up to displace it as cybercriminals’ favourite.” Reuters, May 19, 2017. https://www.reuters.com/article/cyber-attack-bitcoin-idUSL8N1II1MV.

Kim, Christine. “North Korea hacking increasingly focused on making money more than espionage: South Korea study.” Reuters, July 28, 2017. https://www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO.

Kim, Sam. “North Korean Hackers Hijack Computers to Mine Cryptocurrencies.” Bloomberg, January 1, 2018. https://www.bloomberg.com/news/articles/2018-01-02/north-korean-hackers-hijack-computers-to-mine-cryptocurrencies?sref=QmOxnLFz.

Kutlu, Ovunc. “China, Russia, Iran, North Korea, Others Form Group.” Anadolu Agency, December 3, 2021. https://www.aa.com.tr/en/asia-pacific/china-russia-iran-north-korea-others-form-group/2173560.

L., Kenny. “The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed.” *Towards Data Science,* January 31, 2019. https://towardsdatascience.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44.

Lehren, Andrew, and Dan De Luce. “Secret documents show how North Korea launders money through U.S. banks.” *NBC News,* September 21, 2020. https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329.

Liebkind, Joe. “What Is North Korea’s Role in Bitcoin and Does It Affect Prices?” Investopedia, August 11, 2021. https://www.investopedia.com/news/what-north-koreas-role-bitcoin/#citation-2.

Millman, Rene, and Liam J. Kelly. “What is Ethereum 2.0 and Why Does It Matter?” Decrypt, September 10, 2021. https://decrypt.co/resources/what-is-ethereum-2-0.

“Monero (XMR) price stats and information.” Bit Info Charts, December 26, 2021. https://bitinfocharts.com/monero/.

Newman, Lily Hay. “Now Cryptojacking Threatens Critical Infrastructure, Too.” Wired, February 12, 2018. https://www.wired.com/story/cryptojacking-critical-infrastructure/.

Nichols, Michelle, and Raphael Satter. “U.N. Experts Point Finger at North Korea for $281 Million Cyber Theft, Kucoin Likely Victim.” Reuters, February 10, 2021. https://www.reuters.com/article/us-northkorea-sanctions-cyber/u-n-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-idUSKBN2AA00Q.

O’Neill, Patrick Howell. “North Korean Hackers Steal Billions in Cryptocurrency. How Do They Turn It into Real Cash?” MIT Technology Review, September 10, 2020. https://www.technologyreview.com/2020/09/10/1008282/north-korea-hackers-money-laundering-cryptocurrency-bitcoin/.

“Over 60 S.Korean Crypto Exchanges Set to Suspend Services next Week.” Reuters, September 17, 2021. https://www.reuters.com/technology/over-60-skorean-crypto-exchanges-set-suspend-services-next-week-2021-09-17/.

Park, Seongsu. “Andariel evolves to target South Korea with ransomware.” Secure List, June 15, 2021. https://securelist.com/andariel-evolves-to-target-south-korea-with-ransomware/102811/.

"R/Cryptocurrencyscams - Marine Chain.io: North Korea Scam Currency." reddit. Accessed December 31, 2021. https://www.reddit.com/r/cryptocurrencyscams/comments/8a23za/marine_chainio_north_korea_scam_currency/.

Sharma, Rakesh. "Decentralized Finance (DEFI) Definition and Use Cases." Investopedia, December 20, 2021. https://www.investopedia.com/decentralized-finance-defi-5113835.

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

Statista. "Bitcoin (BTC) price per day from October 2013 to December 14, 2021." Statista, December 2021. https://www.statista.com/statistics/326707/bitcoin-price-index/.

"The growing two-headed threat: cryptojackers paired with ransomware." Acronis. https://www.acronis.com/en-us/articles/cryptojacking/.

United Nations, Security Council. *Midterm report of the Panel of Experts submitted pursuant to resolution 2464*. S/2019/691 (30 August 2019), available from https://undocs.org/S/2019/691.

United Nations, Security Council. *Final report of the Panel of Experts submitted pursuant to resolution 2515*. S/2021/211 (4 March 2021), available from https://undocs.org/S/2021/211.

"US Charges Three North Koreans over $1.3bn Theft." BBC News. February 17, 2021. https://www.bbc.com/news/technology-56103921.

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

U.S. Department of Justice. "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." News release, September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

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

U.S. Department of Treasury. "Treasury Designates Shipping Network Engaged in Ship-to-Ship Transfers with North Korean Vessels." Press Release, August 30, 2019. https://home.treasury.gov/news/press-releases/sm762.

Yorio, Janine. "Security Tokens Are Back and This Time It's Real." CoinDesk Latest Headlines RSS, June 30, 2021. https://www.coindesk.com/business/2021/06/30/security-tokens-are-back-and-this-time-its-real/.

About the Authors

Heeu Millie Kim is a Graduate Research Analyst at the Center for Security and Emerging Technology and the Director of Research of the Korea Project's North Korea Cyber Working Group. Her research focuses on military applications of artificial intelligence, cybersecurity, and security in the Asia-Pacific region. She has previously conducted research on North Korea and security in East Asia for the Korea Chair at the Center for Strategic and International Studies and the Asian Studies Program at Georgetown University. Millie has an M.S. in Foreign Service from the School of Foreign Service at Georgetown University, where she received her B.S. in International Politics.

June Lee is a Program Coordinator and Research Assistant for the Tech and International Affairs Program at the Carnegie Endowment for International Peace, where her research focuses on cyber norms and financial sector cybersecurity. She co-leads the Korea Project's North Korea Cyber Working Group and has previously conducted research on cybersecurity and conflict resolution at the Atlantic Council's Cyber Statecraft Initiative and the State Department. June graduated Phi Beta Kappa from Stanford University, studying international relations and computer science.

Rachel Paik is a Project Associate on the DPRK Counterproliferation team at CRDF Global and a member of the North Korea Cyber Working Group. Prior to joining CRDF Global, she worked in fundraising and development at the Arms Control Association as well as the Council of Korean Americans. She was also a former Grants & Programs Officer at Partnership for a Secure America. Rachel developed her interests in nuclear and Korea issues as a NEREC international young fellow at KAIST in Daejeon, South Korea. She is passionate about Diversity, Equity, and Inclusion, and has worked on various leadership development and advocacy programs on Capitol Hill and within the nuclear policy community. Rachel graduated with honors from the University of Washington studying international and Korea studies.

About the Korea Project

The goal of the Korea Project is to foster a deeper understanding of rapidly evolving security challenges on the Korean Peninsula and to develop creative approaches to address them. The Korea Project also partners with interdisciplinary researchers to capture insights from the Peninsula's role as an oracle of global trends—from criminal cyber operations to pandemics to nuclear proliferation to economic statecraft.

Acknowledgments

The authors would like to thank the Korea Foundation for supporting this report.

Korea Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

belfercenter.org/project/korea-project