North Korea's Quest for Crypto: Implications for Cyber Policy and Regional Security

Sofiya Sayankina
Hankuk University of Foreign Studies

Abstract

The Democratic People's Republic of Korea (DPRK, North Korea) has repeatedly deployed hacking groups to pursue disruption, espionage, and data theft. Since the latest round of economic sanctions took effect in 2017, its cyber operations have increasingly focused on financially motivated attacks. The ambiguous legal status of cryptocurrencies, coupled with limited international regulation, has made them an attractive target for the DPRK. To obtain foreign currency, North Korea has adopted creative cyber tactics—from approaching crypto-exchange employees on social media to hijacking personal computers for cryptocurrency mining. By continually evolving methods and shifting targets, DPRK hackers have adapted quickly to geopolitical developments. This article recommends updating cryptocurrency and cybersecurity regulations and deepening minilateral cooperation in cyberspace to counter the rise of North Korean financial cybercrime and bolster regional security and stability.

Keywords: North Korea, Cryptocurrency, State-affiliated hacking, Cybersecurity, Cyber policy

Introduction

Access to cyberspace has opened the door to a diverse set of state and non-state actors who adopt and deploy new technologies faster than regulation can keep pace. Cryptocurrency (or virtual currency) is one such example. In a white paper, Bitcoin's creator, the person(s) known as Satoshi Nakamoto (2008), described it as a "system for electronic transactions without relying on trust," contrasting it with conventional transactions that pass through a third party and retain the possibility of reversal. The decentralized nature of cryptocurrency has been described as "fundamentally aimed at reducing the power of a centralized government" (McShane 2021). While most governments have now introduced cryptocurrency regulations—ranging from recognizing it as a legal medium of exchange to issuing outright bans on trading and mining—the decentralized, peer-to-peer blockchain system has also been exploited for money laundering, cybercrime, and the financing of illicit activities (Frankenfield 2024).

One state has fully embraced this dimension: the Democratic People's Republic of Korea (DPRK, North Korea). DPRK-affiliated hacker groups are known for rapidly adopting cyber techniques for espionage and disruption, but financially motivated operations have carved out a distinctive niche for the regime as a prominent state actor in cyberspace. A seeming contradiction arises between the common image of North Korea as an economically isolated state—where most citizens lack access to the global internet—and the reality that its hackers are among the quickest to adopt new techniques, from spear-phishing via social media to marketing a fake cryptocurrency business. According to Dmitri Alperovitch (co-founder of CrowdStrike), DPRK groups are more creative and aggressive than their Russian, Chinese, and Iranian counterparts (Johnson 2021). They are willing to cross boundaries of accepted state behavior for two reasons: (1) effective retaliation in cyberspace is difficult, especially against North Korea, given its isolation from global networks; and (2) sanctions-induced

economic isolation has incentivized the regime to seek revenue elsewhere and to evolve its cyber tactics.

Using content analysis, this article traces the evolution of North Korea's cyber capabilities and explains how the misuse of cryptocurrencies fits within the regime's broader geopolitical strategy. It addresses two questions: (1) how and why did North Korea develop such versatile tactics for cyber-enabled financial theft?, and (2) what role does DPRK hacking play in the global cybersecurity landscape?

The article proceeds as follows. First, an overview of North Korea's activity in cyberspace provides background for understanding the dynamics of DPRK hacking groups and the regime's strategic goals. Next, the analysis turns to DPRK cyberattacks for financial gain—particularly successful cryptocurrency operations—in the context of economic isolation. Finally, the article assesses how these attacks affect regional security and offers policy recommendations—grouped into cryptocurrency-specific measures, general cybersecurity practices, and DPRK-focused policies—to ensure mechanisms are in place to mitigate North Korea's cyber activity and, by extension, the threat landscape in East Asia.

Overview of North Korea's Cyber Activity

This overview of North Korea's cyber tactics, units, targets, purposes, and techniques provides background for the analysis of its exploitation of cryptocurrency. Although DPRK teams use versatile, up-to-date toolsets, their operations against cryptocurrency largely reuse the tactics and techniques they have deployed for espionage and data theft. Since the inception of North Korea's cyber program in the early 2000s, its hackers have become some of the world's most skilled and aggressive.

Kong et al. (2019) suggest that North Korea's cyber operations are conducted by the Reconnaissance General Bureau (RGB) and divisions of the General Staff Department (GSD). While the GSD primarily plans

wartime cyber strategy, the RGB focuses on clandestine activity in peacetime. The RGB reports directly to the State Affairs Commission and Supreme Leader Kim Jong Un, underscoring its strategic importance. Unlike many other states that actively employ offensive cyber capabilities, North Korea's hacking units are organized to minimize overlap and maximize efficiency by amplifying distinct skill sets.

There is no consensus on group naming, in part because it is unclear whether teams act independently or as subdivisions of a larger entity. The infamous Lazarus Group first surfaced as "Guardians of Peace" during the Sony Pictures hack and is also known as Hidden Cobra (by the US government), Labyrinth Chollima (by CrowdStrike), and Diamond Sleet or ZINC (by Microsoft). Some analysts split Lazarus into two components: a financial unit, Bluenoroff (also called BeagleBoyz by the US government, APT38 by Mandiant/FireEye, and Stardust Chollima by CrowdStrike), and a South Korea–focused unit, Andariel (Silent Chollima at CrowdStrike). Another group, APT37—also referred to as Reaper, Scarcruft, Group123, or Ricochet Chollima—targets private-sector firms and industries primarily in South Korea but also in Japan, Vietnam, and the Middle East. Kimsuky (Kaspersky; Velvet Chollima at CrowdStrike) is a leading global espionage unit. To avoid confusion, this article refers to three widely recognized names: Lazarus Group (encompassing both sub-units), Reaper, and Kimsuky.

According to earlier South Korean intelligence estimates, roughly 6,800 IT professionals were operating under state-affiliated organizations (Kim H. 2021), with later figures rising to about 8,400. Dispersed across China, Russia, Southeast Asia, and the Middle East, many pose as freelance developers available for coding gigs or full-time remote work (Caesar 2021). Such arrangements compound already thorny jurisdictional problems when nationals of Country A conduct an attack on Country B from the territory of Country C. With no comprehensive agreement on cybercrime, both non-state and state-affiliated entities—including DPRK hackers—exploit third-country residency to shield malicious activity.

Before North Korea turned to cryptocurrency theft, its hackers

primarily targeted South Korea, the United States, and Japan, occasionally striking countries with weaker cybersecurity. They also engaged in espionage against Russia's defense industry in 2020, an operation attributed to Kimsuky (RIA Novosti 2020). Typical targets included government services, research institutions, private firms, and individuals—particularly North Korean defectors. The purposes of state-affiliated operations have included espionage and data theft, financial gain, and ideologically driven psychological attacks, as in the Sony case.

Given severely limited domestic internet access, computer network operations (CNOs) likely constitute the bulk of DPRK cyber activity. CNOs are commonly categorized into computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE). Many CNAs begin as CNE because intelligence collection precedes effective attack. CND comprises measures to protect networks and devices against infiltration and disruption.

Because relatively few devices in North Korea are internet-connected, the country has only two primary external routes: a China Unicom (China United Network Communications) link and Russia's TransTeleKom (TTK). The TTK path was widely thought to have been added after US Cyber Command launched a denial-of-service operation against the RGB in 2017, severing the DPRK's only then-visible route. TTK officials, however, have stated that a connection to North Korea existed as early as 2009 (Pashinskaya 2017), with DPRK traffic previously appearing under TTK's general routing because it lacked a designated autonomous system. Telecommunications services were not included in UN Security Council Resolution 2375, which imposed the 2017 sanctions (Pashinskaya 2017). The second link gave Pyongyang redundancy against future disruptions and could plausibly increase the speed of its outward operations. More broadly, North Korea's poorly integrated network architecture reduces exposure to outside cyberattacks.

Since the early 2000s, North Korean cyber strategy has aimed to operate below the threshold of armed conflict (or outside it altogether), denying principal victims—chiefly South Korea and the United States—

clear justification for conventional retaliation. Cyberspace thus offers the regime a "low-risk, high-return" channel to pursue its goals. The absence of widely accepted norms and enforceable rules likewise benefits Pyongyang.

Tactics have evolved markedly from early website defacements of South Korean government portals. As international pressure mounted on traditional revenue streams—such as narcotics and counterfeit-goods smuggling—the regime pivoted toward cryptocurrency as a new lifeline (Ryall 2025). To trace how tactics shifted alongside cybersecurity changes, it is useful to review notable incidents formally attributed to DPRK actors by national agencies (primarily in South Korea and the United States) and leading cybersecurity firms.

The timeline of malicious activity—including Kimsuky campaigns, the Sony hack, and WannaCry 2.0—has been documented elsewhere (Kim and Polito 2019; Kong et al. 2019). These illustrate three broad categories of state-affiliated operations: cyber-terrorism/vandalism, information theft (including espionage), and financially motivated attacks. While earlier operations emphasized disruption of adversary networks and devices, the past five years have seen a pronounced shift toward financial operations. Espionage, present from the outset, has also broadened in scope and targeting. Although responsibilities are relatively delineated across groups, their toolsets overlap: distributed denial-of-service (DDoS) attacks, spear-phishing, and exploitation of zero-day vulnerabilities are common.

DDoS (Distributed Denial-of-Service). DDoS attacks, used to paralyze victim networks, are a staple of DPRK cyber-terror campaigns. Reported early operations in 2009 struck targets in South Korea and the United States, including the South Korean Presidential Office, the National Assembly, the White House, and the Pentagon. Subsequent campaigns hit NongHyup Bank's systems in 2011, and the 2013 "DarkSeoul" operation knocked all three major South Korean broadcasters offline (Kim and Polito 2019).

Zero-day exploitation. North Korean actors frequently exploit newly

discovered vulnerabilities in widely used software (e.g., Adobe Flash Player) and South Korea–specific formats (e.g., .hwp files) (Osborne 2018). WannaCry 2.0 leveraged a Windows vulnerability disclosed shortly beforehand by the Shadow Brokers (Schneier 2017). Reaper has repeatedly used zero-days to gather intelligence from South Korean government and private-sector networks, including via Windows Trojans enabling remote surveillance (Osborne 2018).

Spear-phishing and smishing. DPRK units are meticulous in target selection and may spend months preparing. Victims include defectors, cybersecurity professionals, private-sector employees, academics, and government officials. Tactics have evolved from basic email lures to prolonged engagement over social media to build rapport and trust. North Korea also employs "smishing," compromising Android devices through malware-laden packages targeting primarily SMS (Mun 2021).

Decoy documents. Decoy PDFs and Word files—often related to North Korea's nuclear program—exploit document vulnerabilities and appear in Korean, English, or Japanese (Glover 2021). Pyongyang adapts quickly to political developments—as shown by a phishing campaign launched one week after Yoon Suk-yeol's attempted martial law episode, using the lure "Disclosure of Defense Counterintelligence Command Martial Law Documents"—and can scale from highly targeted approaches to broad campaigns, such as one blasting 126,000 phishing emails across 30 promotional formats (Park 2025).

Sectoral targeting. DPRK hackers range widely and add new targets as geopolitics shift. Since 2018 they have targeted the aerospace industry following South Korea's successful test of a homemade booster engine. By mid-2020, alongside government agencies, defense units, transportation, financial institutions, and heavy industry, they increasingly struck biotech companies, universities, and research facilities working on COVID-19 (Kim N. 2021). The media outlet *Daily NK*, which has sources inside North Korea, reported the creation of a new unit, Bureau 325, tasked specifically with pharmaceutical and biochemical espionage to obtain COVID-19 data (Jang 2021).

Pre-crypto financial operations. Before pivoting to cryptocurrency theft, North Korea stole from banks in Vietnam, Poland, the Philippines, Turkey, Taiwan, and Mexico, with a well-known Bangladesh Bank heist as its most lucrative (Caesar 2021). Exploiting weaknesses in cybersecurity, the attackers stole SWIFT credentials and sent fraudulent transaction requests. From 2014 to 2018, Lazarus also executed ATM "cash-out" schemes across 30 countries in Asia and Africa using malware that, according to Symantec, infected "servers controlling the ATMs, allowing them to intercept their own fraudulent transaction requests and withdraw cash" (Porter 2018). Collectively stealing more than $2 billion from financial institutions, DPRK hackers demonstrated detailed knowledge of banking systems and transaction protocols as well as advanced technical skills. In 2022, North Korean ransomware victims included six US hospitals and healthcare companies, as alleged in the indictment of Andariel operative Rim Jong Hyuk (US Department of Justice 2024). The filing describes laundering through China-based facilitators and the redirection of proceeds into further intrusions—including against US Air Force bases, NASA-OIG, defense contractors in Taiwan and South Korea, and even a Chinese energy firm—suggesting Pyongyang's willingness to target broadly, including its main ally.

North Korea's cyber activity stands out for several reasons. First, despite strict sanctions and limited access to advanced technology, Pyongyang has cultivated a major state presence in cyberspace through careful selection and rigorous training of cyber professionals. Second, with constrained access to global networks and isolation from economic and governance processes, state-affiliated groups can pursue aggressive tactics that complicate timely attribution. And, because cyber operations generally fall below the use-of-force threshold, they often avoid punishment. For similar reasons, North Korea faces fewer incentives to invest heavily in domestic cyber defense; the geographic dispersion of its operators further complicates retaliation. Third, DPRK hackers adapt rapidly to new defensive protocols and shift targets quickly, exploiting unpatched vulnerabilities; during the COVID-19 pandemic, for example,

new units were established to focus on vaccine-related espionage, likely under orders from the State Affairs Commission. Finally, traditional bank heists (e.g., Bangladesh Bank) required extensive research, long lead times, and physical cash-handling, meaning the regime's turn toward more straightforward cryptocurrency targets was only a matter of time.

The next section examines North Korea's evolving cryptocurrency-theft operations and the regime's growing reliance on them.

North Korea's Cybercrimes for Financial Gain

In addition to providing privacy—where transaction details are known primarily to counterparties—a decentralized, highly encrypted virtual currency that bypasses traditional financial institutions can interfere with a state's legal and financial systems unless regulatory measures are introduced. The legal status of cryptocurrencies remains unsettled: although designed as virtual money, they can be classified as property or as financial assets (Bolotaeva et al. 2019). Agreement on a common status is difficult, because it would invite governments to regulate crypto as an analogous object. Moreover, since the transaction logic is embedded in software, states tend to regulate the actors and intermediaries involved in transactions and mining rather than the transactions themselves.

Regulatory approaches vary widely across states, leading to gaps in control over cross-border activity. China banned cryptocurrency transactions in 2021, officially targeting the facilitation of financial crime (Mathis 2021). Yet it does not prohibit circulation or possession, effectively recognizing crypto as commodity/property protected from seizure under Chinese law, while Hong Kong positions itself as crypto-friendly and Chinese investors continue to use exchange-hosted wallets (e.g., Binance, HTX/Huobi) and the stablecoin Tether (Chen and Liu 2021). The United States—currently the center of Bitcoin mining—

has begun tightening oversight, including a $41 million fine against Tether for misstatements about dollar-tied reserves (Nover 2021). South Korea considered an outright ban but instead imposed strict exchange requirements: cybersecurity certification and bank partnerships to enforce real-name verification, with non-compliant exchanges subject to closure (Reuters 2021).

South Korea's stringent crypto rules and comparatively complex internet banking can be attributed in part to North Korean threats: it was among the first to suffer DPRK crypto-focused attacks. A 2017 Bloomberg taxonomy grouped illicit crypto activity into money laundering, contraband transactions, tax evasion, and extortion (Kethineni and Cao 2019). North Korea had long been accused of drug trafficking, counterfeiting, and money-laundering schemes (Westcott 2014). After the WannaCry ransom did not yield proceeds as large as expected, Pyongyang began using cryptocurrency not only as a payout mechanism but as a direct target, rapidly adapting and evolving its tactics.

DPRK actors have compromised multiple exchanges by infiltrating internal networks with the same spear-phishing techniques used for espionage. In March 2019, they breached Singapore-based DragonEx via a meticulously planned social-engineering operation: the attackers built a fake wallet company with a website and LinkedIn personas that persuaded senior managers to install a "trial" trading bot—actually malware that yielded the wallet keys (Alper 2020). Other large-scale thefts attributed to North Korea include: Upbit (2019, $41 million), KuCoin (2020, $275 million, later mostly recovered), Ronin Bridge (2022, $600 million), and Atomic Wallet (2023, $100 million) (Tidy 2025).

Although the Lazarus Group has expanded globally, South Korean exchanges bore the brunt of the DPRK's early crypto campaigns. In 2017, Bithumb—then South Korea's largest exchange and fifth largest worldwide—lost approximately $30 million in crypto after months-long infiltration that began with compromising an employee's home computer, exposing thousands of transactions and customer records. Lazarus then

demanded $16 million to delete the data. Weeks earlier, Coinrail suffered losses exceeding $30 million, and Youbit ultimately shut down after losing 17 percent of its coins in a cyberattack.

DPRK operators have also engaged in cryptojacking. South Korea's National Intelligence Service reported malware designed to locate and hijack South Korean computers to mine the privacy-focused coin Monero, with proceeds routed to servers at Kim Il Sung University in Pyongyang (Lee 2018). Two additional tactics were launching an alternative coin ("HOLD") and promoting a fraudulent ICO, Marine Chain (a platform offering virtual tokens for partial ownership of marine vessels), which shut down after six months and disappeared with investor funds (Rotaru 2019).

As tactics evolved from zero-day exploitation to sophisticated social engineering, the victim set broadened. After initially striking decentralized projects with lower security barriers, DPRK actors in 2024 mounted successful attacks against centralized exchanges, including Japan's DMM Bitcoin and India's WazirX (once the country's largest, later filing for restructuring after the breach) (Japan Times 2025). Most notably, in February 2025, Lazarus stole a record $1.5 billion in digital tokens from Dubai-based Bybit by abusing Safe—a multi-signature wallet layer intended to enhance security (Ryall 2025). These attacks underscore the "low-risk, high-return" nature of targeting crypto reserves amid persistent regulatory ambiguity.

Although blockchain flows can be traced and some stolen assets have been recovered (US Department of Justice 2022), DPRK actors employ effective obfuscation: mixers and peel-chains (breaking funds into smaller tranches), chain-hopping across assets and blockchains, and over-the-counter (OTC) brokers. Because privacy coins like Monero lack liquidity for very large transfers, Lazarus has also turned to decentralized finance (DeFi) protocols such as THORChain to swap stolen Ether into Bitcoin, particularly when Ethereum-based assets risk being frozen (Morton 2025). They further refine laundering by using decentralized exchanges (DEXs) and privacy-enhancing tools while orchestrating

hundreds of false accounts and identities—often a more intricate endeavor than the initial theft (O'Neill 2020).

On end-use, a 2019 UN report estimated DPRK cyber operations had netted about $2 billion—including roughly $300 million in cryptocurrencies—to fund nuclear and ballistic-missile programs (Nichols and Satter 2021). While other illicit revenue streams persist (e.g., illegal coal trade, remote IT work, and more recently, weapons sales to Russia), several factors suggest that cyber-derived funds support nuclear and missile programs: (1) the theft units are state-affiliated, so proceeds accrue to the regime; (2) despite sanctions that should constrain hard-currency access for nuclear-supply payments, the programs continue; (3) Lazarus's pivot from disruptive operations to financial heists signals shifting regime priorities; and (4) even if funds are not used directly for procurement, they "free up" (Chiang 2023) other resources by covering debts and imports. Crypto also affords operational autonomy, reducing reliance on China and Russia, and an additional channel for transactions with them, while intimidating adversaries.

As governments tighten virtual-currency rules, North Korea adapts, attacking the very mechanisms designed to insulate crypto from state interference. Core attributes—blockchain settlement and user-level privacy—are leveraged to Pyongyang's advantage: encrypted transactions obscure treasury holdings; transaction finality can preclude reversals even after exchange compromises; decentralized mining enables hijacking of foreign devices; and the absence of a central authority denies victims a direct avenue of appeal. These features, together with the DPRK's targeting of private firms and individuals for profit, place its activity alongside criminal actors rather than typical state conduct.

The regime identified the opportunity quickly, turning a technology built for privacy and decentralization into both a target and a means for state criminal activity. Its move away from the disruptive, demonstrative operations of the early 2010s reflects a keen grasp of cybersecurity practice and fast responses to geopolitical change—contributing to the

weaponization of virtual currency for ransomware groups. Two factors, above all, shaped the evolution from opportunistic, ideologically tinged operations into one of the most creative and versatile theft-and-laundering enterprises in cyberspace, stealing and washing more than $2 billion in crypto.

Centralized state hacking system. As discussed earlier, DPRK tactics are diverse, inventive, and aggressive. After numerous successful data-theft campaigns—from military intelligence collection to industrial espionage—the regime recognized it could target financial reserves using similar tradecraft. Operations involving SWIFT and ATM cash-outs made the eventual pivot to crypto logical: crypto heists are cheaper, often require no physical access, and malware can be repurposed against other exchanges. They also tend not to trigger urgent interstate responses given legal ambiguity and irreversible settlement. State affiliation confers further advantages: effectively unlimited attempts and timelines with low prosecution risk abroad. Internally, discipline may be harsher than any foreign sanction, adding pressure to succeed. Current DPRK campaigns involve careful target selection after months of preparation, spear-phishing of specific employees via platforms like LinkedIn, and credible corporate-style personas—though English remains a relative weakness.[1] For a time, South Korea's public and private sectors were priority targets, aided by linguistic proximity and a surge in domestic crypto use—South Korean users tripled in the first four months of 2021 to 5.87 million (Yoon 2021)—incentivizing attacks despite tighter exchange security. Through constant iteration, DPRK teams have mastered both technical tools and social-engineering tradecraft. The RGB's rigid hierarchy under the State Affairs Commission and clear division of responsibilities keep operations aligned with national strategy without inter-unit interference.

Isolation from international processes. After the UN Security Council's

1 Personal communication with an IT professional targeted in a North Korean social engineering campaign.

2017 sanctions banned exports of coal, iron, lead, and seafood (De Luce and Mitchell 2019), cryptocurrency became essential to regime survival along with fraudulent vessel identities, ship-to-ship transfers of illicit cargo, and changes of visa types for its workers abroad (Lee and Hwang 2025). Beyond exchange hacks and crypto-denominated ransom, North Korea is believed to mine crypto domestically. Although coal exports to China were banned, cheap domestic coal can still generate electricity for mining—even amid periodic power shortages—and thus monetize a restricted resource without technically exporting it. Sanctions aimed at halting nuclear and missile programs have coincided with more frequent missile tests since 2017. State-affiliated hackers thus serve a dual role: tasked to steal sensitive technology and to finance its implementation. Earlier, Pyongyang timed cyberattacks to symbolic dates (e.g., the "Fourth of July" campaign or the DDoS attacks on the 63rd anniversary of the Korean War outbreak, or to protest the imposition of sanctions (such as Operation DarkSeoul in 2013). More recently, it has used missile tests to answer US–ROK strategic moves, shifting from ideological signaling toward practical revenue generation with its cyber operations.

The DPRK floated the idea of a state cryptocurrency, but with no visible progress—especially after the US banned transactions in Venezuela's "petro" (Wroughton and Alexander 2018)—it likely prefers intermediated channels. Despite mounting regulations, several countries in Southeast Asia, the Middle East, and Eastern Europe still allow crypto-to-cash conversion for a fee. A typical route reportedly moves ransomware takings from South Korea to Russia for black-market cash-out, which nonetheless reduces profitability due to intermediary fees (Kim H. 2021). Similarly, splitting Bitcoin into numerous small transfers through instant-exchange services incurs high cumulative fees, a burden individuals cannot bear but a state actor can absorb.

Thus, to sum up, DPRK targets, scope, and toolkits diverge from many other state-sponsored operations. While most state-affiliated actors prioritize espionage, industrial espionage, data theft, influence,

disinformation, and service disruption, North Korea also targets crypto exchanges and wallets for profit, and runs cryptojacking at scale. Because decentralized systems lack a central regulator, these activities occupy a legal gray zone. Few other state-affiliated actors conduct cyber operations purely for financial gain. The DPRK's conduct therefore resembles cybercriminal groups and illustrates how an isolated regime has no compunction about deploying cyber theft alongside traditional state operations. Building on this analysis, the next section considers the implications of North Korea's cryptocurrency campaign for regional security and global cyberspace.

Implications for Regional Security and Policy Recommendations

Under the conditions of North Korea's continuous cyberattacks and cryptocurrency theft, the effectiveness of sanctions imposed on the DPRK regime has been questioned. By extension, the ability of the North Korean regime to circumvent sanctions by relying on its cryptocurrency reserves to build its nuclear and ballistic missile programs has implications for regional security. By excluding the DPRK from international processes in which other states regularly participate, disengagement with North Korea as a nation-state has seemingly signaled to the regime that it is acceptable not to behave according to norms and to instead engage in illicit activity typically associated with non-state actors. In the case of cryptocurrency theft, hacker groups and hacktivist collectives might act in line with a state's interests but are rarely affiliated with state structures (unlike hackers conducting espionage and influence operations).

By using stolen cryptocurrency to develop its military programs and intelligence networks, North Korea further blurs the line between cyber and physical threats and between state and non-state activity in cyberspace. Another point of concern for regional security is North

Korea's growing reliance on practices and connections from the broader international cybercriminal ecosystem. For example, the Andariel subgroup, which until 2020 had only targeted South Korea, is "suspected to have operated as an initial access broker or affiliate for the Play ransomware operation, which is believed to have links to Russia" (Milenkoski et al. 2025). In the context of rapprochement between the two regimes, with North Korea sending its troops to participate in the war against Ukraine, such activity can indicate closer cooperation in other areas and at different levels, including cyberattacks targeting other states in the region. Tighter cooperation with Russia could mean there will be even fewer instruments to curtail DPRK activity in cyberspace, as its spectrum of tactics and tools grows enough to increase attacks on both South Korea and Japan.

While maintaining a minimal level of dialogue with the North Korean regime, policymakers could work on introducing comprehensive frameworks that protect cryptocurrency transactions and at the same time do not infringe on users' rights. All policy recommendations can be divided into three groups: cryptocurrency-specific measures, general cybersecurity practices, and North Korea-related policies. This approach will help ensure that regulatory mechanisms account for all actors—individual users, cryptocurrency businesses, financial institutions, and state systems—and contribute to regional and global cybersecurity.

First, there is a need for agreement on the legal status of cryptocurrency, which is currently recognized as property, commodity, or financial asset (but not money), or not recognized as an object of regulation at all. This causes confusion and legal hurdles in implementing effective policy mechanisms: a clear status would allow legal systems to treat cryptocurrency as a comparable object for which regulation is already in place, enabling prosecution of perpetrators in cases of cryptocurrency theft. Ideally, this should be done at the international level and applied by global financial institutions, which are still hesitant to recognize cryptocurrency as a legitimate financial object.

While controlling encrypted peer-to-peer, blockchain-based

transactions would be a complicated task for state-level regulatory agencies, requiring cryptocurrency exchanges to adopt a clear set of rules could help guard against money laundering and prevent large losses in the event of an exchange compromise. While privacy-focused cryptocurrencies like Monero benefit from inflows linked to illicit transactions, identifying trends and patterns of fraudulent activity can help prevent transfers into Monero at early stages. Possible requirements for businesses could include mandatory real-time identity confirmation for transactions exceeding a set amount, limits on the number of transactions within a period, storing a larger share of funds in cold wallets that are less vulnerable to hacking, and reserving the right to block all transactions in the event of suspicious activity. Although fully securing virtual currency against cyberattacks is impossible, exchanges can provide greater protection for users' funds and reduce the likelihood of shutdowns after an incident. Introducing regulation that prioritizes advanced blockchain intelligence within the compliance and risk-management frameworks of financial institutions, which allows monitoring and tracing of crypto transactions across multiple blockchains, could also help identify suspicious flows and subsequently flag or sanction them.

Although issuing a ban on cryptocurrency transactions and mining might seem like a certain way to avoid crypto-induced money laundering and cyber theft, traffic can be rerouted through a VPN to another country (Olcott et al. 2021).[2] Introducing strict cybersecurity measures, including regular training, as well as anti-money laundering regulations would likely have a more positive effect while still allowing users to enjoy the advantages of cryptocurrency's inclusivity.

The second set of recommendations involves improving cybersecurity practices and responses to ransomware. First, it is important to ensure that cryptocurrency-exchange systems are secure and up to date by

2 This is what some crypto miners in China are suspected to be doing after crypto mining was banned.

strengthening public-private cooperation. Second, frequent internal checks and commissioning external cybersecurity professionals should be prioritized. Third, educating employees and customers on basic cybersecurity hygiene—particularly on social engineering tactics used by hackers—can reduce the likelihood of successful spear-phishing attacks. Tactics used to counter misinformation, such as "pre-bunking," which issues early warnings based on patterns and early signs of fraudulent campaigns, can also decrease the success of phishing.

Due to complicated inter-Korean relations and the security situation on the Korean Peninsula, as well as sharing the same language with the attackers, South Korea has been one of the earliest and most frequent targets of North Korean state-affiliated groups, including attacks on its cryptocurrency exchanges. Exposure to a large number of cyber threats requires more rigorous cybersecurity measures across internet infrastructure and exchanges. Ensuring that businesses promptly contact KISA (Korea Internet & Security Agency) in cases of suspected compromise—and that KISA has sufficient resources and authority to help mitigate consequences—requires increases in personnel, given the DPRK's growing focus on cyber activity. Another policy some governments have considered is prohibiting ransomware payments, which would strip attackers of financial incentives. Legislation restricting transactions with users in countries lacking adequate anti-money laundering policies might also reduce the likelihood of funds being transferred to malicious actors. Finally, policies regarding North Korea's cyber activity focused on cryptocurrency should address two issues: the effects of economic sanctions, and the means of retaliation against continuous cyberattacks. Efforts to make North Korea adhere to international norms through sanctions have instead pushed the DPRK to evolve methods of funding its nuclear and missile programs rather than suspending them. It is also important to note that the share of for-profit cyberattacks launched by North Korea increased after sanctions went into force, helping the regime keep pace with its strategic objectives. Because cyberattacks originating from North Korea or conducted by North Korean hackers

abroad are clearly state-sponsored, implementing policies targeting illicit activity in cyberspace—and the actors facilitating such activity—would at least partially help contain North Korea within international norms.

Additionally, retaliating against the DPRK with cyber tools would likely not inflict considerable damage due to its very low connectivity and underdeveloped infrastructure. Stripping other states of incentives to aid North Korea in cyberattacks is difficult but likely more effective. However, the states that provide internet connectivity to North Korea and those hosting groups of North Korean hackers may see benefits from the disruption North Korea causes in global cyberspace and from its illicit cryptocurrency operations. Katagiri (2024) notes that, because Russia and China lack reciprocity or extradition agreements with the West, Russian and Chinese hacking groups "can operate without fear of repercussions, except for the possibility of detention and arrests by the authorities for behaviors inconsistent with state interest." Reaching an intergovernmental agreement on a cyber regime that defines rules of behavior and thresholds for state participation is necessary to begin much-needed regulation, but is hard to achieve.

However, minilateral cooperation among like-minded countries to investigate and prosecute individuals behind attacks is feasible, as shown by the 2021 joint operation by law-enforcement agencies from Ukraine, South Korea, and the United States. That operation resulted in the detention of multiple suspects in Kyiv believed to be linked to the Clop ransomware cartel accused of hacking South Korean retailer E-Land, with South Korean police physically present during the arrests—usually carried out solely by local authorities. Similar operations can be conducted with local law enforcement when dealing with "scam cities," such as those on the Thailand-Myanmar border. This, however, requires improving diplomatic ties with ASEAN and its member states.

Strengthening cybersecurity architecture and fostering ties with other countries could also be recommended for better bilateral cooperation and faster response. Programs similar to the one the Korean Institute of Criminology developed with the UNODC in 2008 for law-enforcement

and police officers in Vietnam and Thailand—teaching computer-related technologies and providing general information on cybercrime trends and legislation—could be implemented to raise awareness of cryptocurrency crimes. Finally, tackling cryptocurrency crime could be integrated into the cyber component of multi-domain joint military training or joint cyber-law-enforcement exercises, which could improve public-private cooperation and subsequent investigations when a cryptocurrency exchange is compromised.

To summarize, ensuring maximum protection of cryptocurrency reserves through robust cybersecurity measures and coordinated international action against perpetrators would not only help combat money-laundering practices and decrease ransomware attacks, but also potentially improve the effectiveness of restrictions on the North Korean regime by cutting off a major channel for funding its nuclear and missile programs.

Conclusion

North Korea shows no signs of slowing its nuclear and missile programs and continually adapts to new constraints, calling into question both the effectiveness of international sanctions and the rationale for imposing them. Concurrently, the DPRK has found a new revenue stream to support military development in a "low-risk, high-return" fashion characteristic of a pariah state: money theft in cyberspace, a domain enabled by anonymity and its cross-border nature. Difficult attribution and limited options for cyber retaliation complicate efforts to ensure adherence to international norms of conduct online.

Against this backdrop, North Korea has gone further than most state actors by crossing the boundary between the behavior of national governments and criminal entities: among the "Big Four" (Russia, China, Iran, and the DPRK), North Korea is the only country that conducts cyberattacks for financial gain at the state level through an

integrated government hacking system. Since the early 2020s, cryptocurrency-related attacks have become a go-to tactic for state-affiliated hackers, leveraging the core features of virtual currencies—privacy, encryption, peer-to-peer architecture, and blockchain settlement—that are not yet fully subject to national or international regulation. DPRK hackers have exploited these attributes by directly compromising cryptocurrency exchanges via spear-phishing and by demanding crypto transfers in ransomware campaigns.

This combination—a versatile toolkit, sensitivity to social and political developments, and state backing—interacts with uneven corporate cybersecurity and hesitant regulation to make it extremely hard to prosecute suspects in cryptocurrency theft. Moreover, because cryptocurrencies gain from rising volumes and users, imposing tighter rules and limits is unlikely so long as perceived benefits outweigh risks. In parallel, North Korea's cryptocurrency theft adds to an already chaotic cyber landscape characterized by ransomware, infrastructure attacks, disinformation, and election interference. By stretching already thin law-enforcement, intelligence, and often underfunded and understaffed military resources, malicious actors gain greater operational freedom.

Additionally, because the internet is not integrated into the DPRK's critical infrastructure and very few users have regular access to the global network, other states have comparatively little room to maneuver in cyberspace to retaliate in ways that would cause significant damage. Aware that it has little chance of surviving a conventional military conflict, the regime finds asymmetric capabilities in cyberspace relatively cheap, safely provocative, and consistently remunerative, offering a broad target set and virtually unlimited attempts. North Korea also benefits from the fact that cryptocurrency theft typically does not directly target other states but private companies, which, amid loosely enforced regulations and uneven cybersecurity, often have limited ability to recover stolen funds.

To counter North Korea's activity in cyberspace, states should work toward consensus on an intergovernmental cyber regime to overcome

the legal vacuum and discourage other governments from facilitating DPRK criminal activity. In parallel, while basic cybersecurity hygiene is a necessary first step to protect users, businesses, and infrastructure, promptly updating anti-money-laundering and cryptocurrency regulations in response to evolving tactics would help disincentivize attacks and keep pace with North Korea's rapidly adapting cyber operations.

References

Alper, Tim. 2020. "North Korea 'Used LinkedIn, Telegram' in USD 7m Crypto Exchange Hack." *Cryptonews*. February 5. https://cryptonews.com/news/north-korea-used-linkedin-telegram-in-usd-7m-crypto-exchange-5705.htm

Bolotaeva, O. S., A. A. Stepanova, and S. S. Alekseeva. 2019. "The Legal Nature of Cryptocurrency." IOP Conference Series: Earth and Environmental Science 272/3: 032166. https://doi.org/10.1088/1755-1315/272/3/032166

Caesar, Ed. 2021. "The Incredible Rise of North Korea's Hacking Army." *The New Yorker*. April 19. https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army

Chen, Conghui, and Lanlan Liu. 2021. "How Effective Is China's Cryptocurrency Trading Ban?" *Finance Research Letters* 46 (B): 102429. https://doi.org/10.1016/j.frl.2021.102429

Chiang, Sheila. 2023. "North Korean Hackers Have Allegedly Stolen Hundreds of Millions in Crypto to Fund Nuclear Programs." *CNBC*. September 6. https://www.cnbc.com/2023/09/06/north-korea-hackers-stole-crypto-to-fund-nuclear-program-trm-chainalysis.html

De Luce, Dan, and Andrea Mitchell. 2019. "U.N. Report: North Korea Smuggles Oil, Hacks Banks Despite Sanctions." *NBC* News. March 12. https://www.nbcnews.com/news/north-korea/u-n-report-north-korea-evading-sanctions-buying-oil-selling-n981821

Frankenfield, Jake. 2024. "Cryptocurrency Explained with Pros and Cons for Investment." *Investopedia*. June 15. https://www.investopedia.com/terms/c/cryptocurrency.asp

Glover, Claudia. 2021. "North Korean Cyberattacks on South Korea Increase." *Tech Monitor*. June 22. https://techmonitor.ai/technol-

ogy/cybersecurity/north-korean-cyberattacks-on-south-korea-kimsuky

Jang, Seulkee. 2021. "Kim Jong Un Is Directly Handling Results of New COVID-19 Hacking Organization's Work." *Daily NK*. February 5. https://www.dailynk.com/english/kim-jong-un-directly-handling-results-new-covid-19-hacking-organization-work/

Japan Times. 2025. "North Korea's $1.5 Billion Heist Puts the Crypto World on Notice." *Japan Times*. March 3. https://www.japantimes.co.jp/news/2025/03/03/asia-pacific/crime-legal/north-korea-billion-heist-crypto/

Johnson, Derek. 2021. "What Makes North Korean Hacking Groups More Creative?" *SC Media*. May 21. https://www.scmagazine.com/news/2021-rsa-conference/what-makes-north-korean-hacking-groups-more-creative

Katagiri, Nori. 2024. "From Prepaid Cards to Bitcoin: How Did Ransomware Hackers Adopt Cryptocurrencies?" *Journal of Cyber Policy* 9/2: 239–55. https://doi.org/10.1080/23738871.2024.2435956

Kethineni, Sesha, and Ying Cao. 2019. "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity." *International Criminal Justice Review* 30/3: 325–44. https://doi.org/10.1177/1057567719827051

Kim, Chong Woo, and Carolina Polito. 2019. "The Evolution of North Korean Cyber Threats." Asan Institute for Policy Studies—Issue Brief. February 20. https://en.asaninst.org/contents/the-evolution-of-north-korean-cyber-threats

Kim, Hwan-yong. 2021. "30 Countries Including the US and Korea, Declare Cooperation to Respond to Ransomware from Russia, North Korea, Etc." ["Mi·han Poham 30yeogaegug, Leosia·bughan Deung Laenseom-Weeo Daeeung Gongjo Seon-Eon"]. *Voice of America* (VOA Korean). October 15. https://www.voakorea.com/a/6271833.html

Kim, Nan-yeong. 2021. "North Korea Spear-Phishing on Cryptocur-

rency Industry… Also Attacks Vaccine Pharmaceutical Companies" ["Buk, Gasanghwapye San-Eob-e Seupieo Pising…Baegsin Jeyag Hoesa Gong-Gyeogdo"]. *Newsis*. October 5. https://newsis.com/view/?id=NISX20211005_0001602826&cID=10101&pID=10100

Kong, Ji Young, Jong In Lim, and Kyoung Gon Kim. 2019. "The All-Purpose Sword: North Korea's Cyber Operations and Strategies." CCDCOE. June. https://ccdcoe.org/uploads/2019/06/Art_08_The-All-Purpose-Sword.pdf

Lee, Joyce. 2018. "North Korea Appears to Be Mining Cryptocurrency, like Bitcoin, to Fund Regime: Report." *Global News*. January 9. https://globalnews.ca/news/3953855/north-korea-mining-cryptocurrency-to-fund-regime

Lee, Sang Yong, and Hyun-uk Hwang. 2025. "Digital Warfare: N. Korea's Evolving Cyber Arsenal and Global Threats." *Daily NK*. March 28. https://www.dailynk.com/english/digital-warfare-north-korea-evolving-cyber-arsenal-global-threats/?tztc=1

Mathis, William. 2021. "US Emerges as Biggest Bitcoin Miner after China Crypto Crackdown." *Al Jazeera*. October 13. https://www.aljazeera.com/economy/2021/10/13/bbus-emerges-as-biggest-bitcoin-miner-after-china-crypto-crackdown

McShane, Alex. 2021. "Tesla CEO Elon Musk: Bitcoin and Crypto Take Aim at Centralized Government." *Bitcoin Magazine*—NASDAQ. September 29. https://www.nasdaq.com/articles/tesla-ceo-elon-musk%3A-bitcoin-and-crypto-take-aim-at-centralized-government-2021-09-29

Milenkoski, Aleksandar, Jiro Minier, Julian-Ferdinand Vögele, Max Smeets, and Taylor Grossman. 2025. "Ransomware's New Masters: How States Are Hijacking Cybercrime." Virtual Routes—Pharos Series. April. https://virtual-routes.org/wp-content/uploads/2025/04/Virtual-Routes-Pharos-Report-Series-No.-3.pdf

Morton, Joseph. 2025. "North Korea Steals Enough Money to Rank in the Top 5 Crypto Owning Countries." *Mugglehead Investment*

Magazine. March 18. https://mugglehead.com/north-korea-steals-enough-money-to-rank-in-the-top-5-crypto-owning-countries/

Mun, Dong Hui. 2021. "North Korea's Kumsong 121 Recently Employed Social Media to Launch a Cyber Attack." *Daily NK*. September 13. https://www.dailynk.com/english/north-korea-kumsong-121-recently-employed-social-media-launch-cyber-attack

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-To-Peer Electronic Cash System." *Bitcoin.org*. October 31. https://bitcoin.org/bitcoin.pdf

Nichols, Michelle, and Raphael Satter. 2021. "U.N. Experts Point Finger at North Korea for $281 Million Cyber Theft, KuCoin Likely Victim." *Reuters*, February 10. https://www.reuters.com/article/us-northkorea-sanctions-cyber-idUSKBN2AA00Q

Nover, Scott. 2021. "The US Crackdown on Stablecoins Is Targeting Tether First." *Yahoo Tech*. October 20. https://finance.yahoo.com/news/us-crackdown-stablecoins-targeting-tether-121327177.html

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

Olcott, Eleanor, Sam Joiner, and Steven Bernard. 2021. "US Overtakes China as Biggest Bitcoin Mining Hub after Beijing Ban." *Financial Times*. October 13. https://www.ft.com/content/50acdea5-cad1-4f39-8e6a-9be7ab78485d

Osborne, Charlie. 2018. "North Korean Reaper APT Uses Zero-Day Vulnerabilities to Spy on Governments." *ZDNET*. February 2. https://www.zdnet.com/article/north-korean-reaper-apt-uses-zero-day-vulnerabilities-to-spy-on-governments

Park, Joon Ha. 2025. "North Korean Hackers Used Fake Martial Law Documents in Mass Phishing Attack." *NK News*. April 15.

https://www.nknews.org/2025/04/north-korean-hackers-used-fake-martial-law-documents-in-mass-phishing-attack/

Pashinskaya, Anastosiya. 2017. "The North Korean Internet: Why the DPRK Needs a Russian Provider" ["Internet Po-Severokoreyski: Zachem KNDR Rossiyskiy Provayder"]. *Deutsche Welle*. October 6. https://p.dw.com/p/2lDwA

Porter, Jon. 2018. "North Korea-Linked Hackers Stole Tens of Millions from ATMs across the World." *The Verge*. November 8. https://www.theverge.com/2018/11/8/18075124/north-korea-lazarus-atm-fastcash-hack-millions-dollars-stolen

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

RIA Novosti. 2020. "Experts on DPRK Hackers' Attacks on Russian Industry" ["Eksperty Rasskazali Ob Atakakh Hakerov Iz KNDR Na Rossiyskie Predpriyatiya"]. October 19. https://ria.ru/20201019/khakery-1580455239.html

Rotaru, Cristina. 2019. "The Curious Case of Marine Chain: The DPRK Cyberscam Behind a Blockchain-Powered Maritime Investment Marketplace." *VERTIC*. April 24. https://www.vertic.org/2019/04/the-curious-case-of-marine-chain-the-dprk-cyberscam-behind-a-blockchain-powered-maritime-investment-marketplace

Ryall, Julian. 2025. "North Korean Hackers Boost Pyongyang's Huge Crypto Reserve." *Deutsche Welle*. April 7. https://www.dw.com/en/north-korea-crypto-bitcoin-hackers-kim-jong-un/a-72162566

Schneier, Bruce. 2017. "Who Are the Shadow Brokers?" *The Atlantic*. May 23. https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/

Tidy, Joe. 2025. "North Korean Hackers Cash out Hundreds of Millions from $1.5bn ByBit Hack." *BBC*. March 10. https://www.bbc.com/news/articles/c2kgndwwd7lo

US Department of Justice. 2022. "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and Their Conspirators." DOJ Archives. July 19. https://www.justice.gov/archives/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors

US Department of Justice. 2024. "North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers." July 25. https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals

Westcott, Lucy. 2014. "North Korea's Illicit Economy Includes Fake Viagra and Smuggled Ivory." *The Atlantic*. April 15. https://www.theatlantic.com/international/archive/2014/04/north-koreas-illicit-economy-includes-fake-viagra-and-smuggled-ivory/360678

Wroughton, Lesley, and David Alexander. 2018. "U.S. Bans Transactions with Venezuela's Digital Currency." *Reuters*. March 20. https://www.reuters.com/article/technology/us-bans-transactions-with-venezuelas-digital-currency-idUSKBN1GV2OZ/

Yoon, L. 2021. "South Korea: Total User Number of Leading Cryptocurrency Exchanges 2021." Statista. September 24. https://www.statista.com/statistics/1250233/south-korea-user-numbers-of-leading-cryptocurrency-exchanges

Article submitted 2/5/25, revised 6/30/25, accepted 7/4/25.