MARCH 2026

Cross-Border Law Enforcement Collaboration for Countering North Korea's Crypto Plunder

By Joohui Park

Introduction

The Democratic People's Republic of Korea (DPRK) is exploiting cyberspace and decentralized cryptocurrency architecture in order to satisfy its craving for crypto assets, and it has become a global security concern.[1] This is reflected in the **final report** adopted in 2025 by the UN Open-Ended Working Group on "security of and in the use of information and communications technologies 2021–2025," which acknowledges growing member-state concerns that cryptocurrency theft may affect international peace and security. These concerns, expressed throughout the working group process, were incorporated into the collective threat assessment contained in the final report. Later in 2025, the Multilateral Sanctions Monitoring Team (MSMT) issued **recommendations** in response to violations of UN Security Council resolutions by North Korea, particularly regarding cryptocurrency theft and laundering practices used to circumvent sanctions.

North Korea's cryptocurrency theft and subsequent money-laundering activities are highly distinctive. First, they are conducted by state-directed criminal networks, often enabled by overseas-deployed information technology (IT) workers. Second, these activities rely on cryptocurrency laundering

1. According to FATF, a virtual asset is "a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations." Virtual assets can be classified based on diverse criteria; for instance, they can be centralized or decentralized, depending on whether a central issuing and controlling authority exists or not. Central bank digital currency is a widely recognized central digital currency. Cryptocurrency, including bitcoin, is the most well-known decentralized virtual asset.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

tools from third-party service providers outside of North Korea. Finally, facilitators operating in third countries covertly enable the conversion of stolen cryptocurrency into fiat currency.

To counter this emerging threat posed by North Korea, South Korea has undertaken a comprehensive set of countermeasures. These include strengthening **domestic regulation** of virtual-asset service providers, notably through (1) the introduction of **know-your-customer (KYC) and information sharing obligations** for cryptocurrency exchanges, (2) imposing targeted **sanctions** on individuals and entities involved in cryptocurrency theft and money-laundering activities, (3) enhancing **law enforcement cooperation** with domestic and foreign cryptocurrency exchanges to disrupt laundering flows, and (4) expanding international cooperation, particularly with **the United States and Japan** and **the Financial Action Task Force (FATF)**, an organization discussed in more detail later in this paper.

When it comes to enforcing laws against North Korea's crypto-related illicit activities, however, South Korea continues to face significant challenges. First, the inherently decentralized nature of virtual asset transactions complicates efforts by law enforcement authorities to identify and trace perpetrators involved in cryptocurrency theft. Second, uneven or absent international regulatory frameworks governing virtual-asset finance impede the ability of law enforcement agencies to obtain timely cooperation from foreign cryptocurrency exchanges. Third, the lack of an internationally coordinated framework for law enforcement cooperation in the investigation, freezing, seizure, or confiscation of proceeds derived from cryptocurrency theft constrains the ability of national authorities to secure swift cross-border assistance. Against this backdrop, this paper analyzes the potential of the UN Convention against Cybercrime (UNCC) as an international law enforcement framework for countering North Korea's crypto theft and laundering practices.

North Korea's Craving for Crypto Assets

North Korea's pursuit of cryptocurrency reflects a broader strategic adaptation to international sanctions and financial isolation. As conventional revenue streams were severed, the regime turned to cyberspace—exploiting decentralized crypto infrastructure to generate funds beyond the reach of traditional regulatory frameworks. This section examines why the regime shifted its cyber operations toward large-scale crypto theft, and the methods it employs to launder and cash out stolen assets.

A SHIFT IN PRIORITIES: THEFT TO SUSTAIN THE REGIME

Over the past decade, North Korea has systematically exploited cyberspace to acquire assets—both cryptocurrency and fiat currency—to finance its weapons programs and nuclear ambitions. Prior to this period, North Korea engaged in malicious cyber activities for objectives other than asset acquisition. A notable example is the **2013 Dark Seoul attack**, which targeted South Korean financial institutions and media outlets, causing extensive damage to data and information systems. The primary objective of the attack was to instill public panic through the disruption of critical services, although it also resulted in economic losses—approximately **48,700 PCs and servers** were disrupted, with estimated **losses of KRW 867.2 billion**.

Since the 2016 adoption of **UN Security Council Resolution 2270**, which imposed comprehensive sanctions on North Korea following its fourth nuclear test, the regime's primary use of cyberspace has shifted markedly toward the theft of funds. For example, in early 2016, DPRK actors **attempted** to steal fiat currency by exploiting vulnerabilities in the Bangladeshi central bank's SWIFT system. At that

time, the use of virtual assets was still nascent and had not yet become a viable vehicle for large-scale illicit finance. However, following the **complete exclusion** of DPRK banks from the SWIFT network in March 2017, the country lost all formal channels for transmitting or receiving U.S. dollars. Against this backdrop, cryptocurrency theft has emerged as a critical mechanism through which North Korea generates revenue while circumventing conventional financial regulations. While North Korea appears to continue maintaining units responsible for disruptive and destructive cyber operations, even these units are reportedly required to be **self-financing**, which in practice drives them to engage in cybercrime as a means of generating revenue for the regime.

The scale of cryptocurrency theft attributed to DPRK actors has become increasingly alarming. According to **a 2025 report** by the MSMT, North Korea stole approximately USD 1.19 billion in cryptocurrency in 2024 and at least USD 1.645 billion between January and September 2025. Notably, these figures do not include the alleged theft of an additional USD 30 million from **Upbit**, a major cryptocurrency exchange based in South Korea, in late 2025. Moreover, the value of crypto assets stolen in single incidents continues to reach unprecedented levels. In February 2025, North Korean cyber actors allegedly stole nearly **USD 1.5 billion** in Ethereum tokens (ETH) from Bybit, the world's second-largest cryptocurrency exchange. This incident constitutes **the largest cryptocurrency theft** on record, surpassing the 2022 Ronin Bridge hack, which had previously held that distinction with losses estimated at approximately **USD 620 million**.

MODUS OPERANDI: THE 2022 RONIN NETWORK THEFT

North Korea's crypto theft and subsequent money-laundering process are well-coordinated by its IT workers, resourced by crypto-laundering tools, and assisted by facilitators within safe havens. North Korea mobilizes IT workers abroad, masquerading as legitimate employers or employees, to implant malicious code. Diverse third-party crypto-laundering tools, such as mixing and bridging services, are used to obfuscate tracing. Further, facilitators in third countries are contributing to the conversion of stolen cryptocurrencies into fiat currencies. In the course of an attack, North Korean actors commit numerous types of criminal activities, including identity theft, cybercrime (e.g., illegal access and misuse of tools), and money laundering.

To understand the challenges in law enforcement in relation to these criminal activities by North Korean actors, it is worth following North Korea's primary patterns of behavior in crypto thefts and money laundering. The Ronin Network theft in 2022 represents a general playbook carried out by North Korea for crypto theft and laundering.

The first step is cyber-enabled theft. North Korean cyber operators deploy the full spectrum of available methods to obtain assets, including cutting-edge technical capabilities (e.g., AI) and refined social engineering tactics. In early 2022, employees at Sky Mavis, the developer of Axie Infinity game, were targeted by threat actors impersonating recruiters of a fictitious company who solicited job applications through LinkedIn. A fraudulent job offer was then delivered via a weaponized PDF document. Upon download, the file deployed malware that infiltrated the Ronin Network's bridge infrastructure, which enables cross-chain asset transfers for Axie Infinity. This initial compromise enabled the attackers to gain control of **four of the nine validators** securing the Ronin Network, leaving them one validator short of achieving complete network control. Using these validators, the actors authorized two fraudulent withdrawal transactions: **173,600 ETH and 25.5 million USD Coin**, equivalent to more than USD 600 million.

The second step is cryptocurrency laundering using a multistage methodology. Once stolen cryptocurrency is located in wallets under their control, DPRK actors initiate an extensive money laundering operation, using a diverse array of tools such as mixing, swapping, and bridging.[2] According to Chainalysis, the laundering scheme has utilized over **12,000 distinct crypto addresses**, demonstrating the group's highly sophisticated obfuscation capabilities. In the Ronin case, the cyber operators first sent stolen crypto assets to intermediary wallets. Subsequently, crypto assets were mixed in batches through Tornado Cash, a decentralized mixing service which contributed to laundering over **USD 455 million** worth of crypto stolen from this Ronin Network theft. Obfuscated crypto assets in ETH were swapped for bitcoin (BTC) to exploit inter-blockchain tracing complexities. The crypto assets in BTC underwent additional batch mixing to further obscure transaction provenance.

The final stage is the "cash out" phase, which constitutes the critical end goal for DPRK operators converting illicit cryptocurrency holdings into liquid fiat currency that can fund state activities. In most cases, hackers enter a dormant state, waiting for suitable timing to cash out. For six months, a large portion of the crypto assets stolen from the Ronin Network heist remained unmoved in cryptocurrency wallets under the DPRK actors' control. With the collaboration of law enforcement authorities and Chainalysis, **10 percent** of stolen funds were recovered in September 2022.

THE HIDE-AND-SEEK CHASE FOR CRYPTO THEFT

From a law enforcement perspective, investigating, prosecuting, and recovering assets from cryptocurrency theft attributed to North Korean actors presents significant challenges. This section examines the key obstacles confronting law enforcement, from the decentralized and pseudonymous architecture of the cryptocurrency ecosystem to the exploitation of third-country facilitators, as well as the steps South Korea has taken to confront these challenges.

THE DECENTRALIZED AND PSEUDONYMOUS ARCHITECTURE

The principal challenges in investigating and prosecuting criminal activities associated with cryptocurrency theft stem from the structural features of the cryptocurrency ecosystem itself. Cybercrime, in most cases, is inherently transnational in nature and therefore already presents significant obstacles for cross-border law enforcement. Beyond this general difficulty, however, cybercrimes involving cryptocurrencies give rise to distinct challenges derived from two defining characteristics of the crypto ecosystem: the decentralized and pseudonymous nature of transactions.

First, cryptocurrency transactions are decentralized by design. Cryptocurrencies function as a medium of exchange whose issuance, transfer, and ownership are recorded through distributed ledger technologies, most notably blockchain. For law enforcement authorities, such distributed ledgers constitute a double-edged sword. On the one hand, every cryptocurrency transaction is immutably recorded on a publicly accessible ledger. This transparency enables investigative authorities to trace and analyze financial flows with a degree of precision. On the other hand, transactions recorded on distributed ledgers do not intrinsically require intermediaries. This does not mean that there exist no intermediaries; of course, intermediaries such as crypto exchanges exist for other purposes,

2. A virtual currency wallet is a software-based tool that connects to a particular blockchain network, enabling the creation, storage, and management of users' addresses and private keys. It also enables the sending and receipt of virtual currencies. A single wallet may contain multiple virtual currency addresses. Wallets operated by third-party service providers are commonly referred to as "hosted wallets," as the provider maintains custody of users' funds until a transaction is initiated. By contrast, "unhosted wallets" grant users full and autonomous control over their assets without reliance on an intermediary.

including facilitating cryptocurrency transactions. However, transactions based on blockchain do not by design necessitate any intermediaries as a prerequisite for concluding transactions. With only wallet addresses, parties can transact directly on a peer-to-peer basis. In such transactions, law enforcement can hardly expect the cooperation they have with regard to centralized transactions—for instance, identity verification of transaction parties—which are conducted under the control of traditional banks. Moreover, stolen crypto assets may be stored in unhosted wallets. Because only the wallet holder can exercise control over assets stored in such wallets, law enforcement authorities are **unable to freeze, seize, or recover** these funds in the absence of access to the relevant private keys.

Second, cryptocurrency transactions are **pseudonymous**. Wallet addresses required to conduct transactions consist merely of alphanumeric strings, and the verification of a user's real-world identity is not a prerequisite for participation in the network. As a result, while investigative authorities may be able to trace the movement of cryptocurrency across the blockchain, they are unable to ascertain the identity of the individuals or entities controlling the relevant wallets, or it is extremely challenging to do so.

These architectural features of cryptocurrencies significantly enhance North Korea's incentives to target crypto assets, as they allow state-sponsored actors to evade detection or, at minimum, delay and complicate tracing efforts in the cyber domain. Such incentives are further amplified by the development of sophisticated obfuscation techniques—including mixing, swapping, and cross-chain bridging—designed to limit or effectively eliminate transactional traceability. In addition, the emergence of **anonymity-enhanced cryptocurrencies**, which are specifically engineered to obscure transactional linkages between wallet addresses and thereby undermine blockchain analytics, further impedes law enforcement efforts.

Consequently, blockchain-specific technical expertise has become indispensable for effective law enforcement. Cross-border cooperation in crypto-related investigations frequently depends on a requesting authority's ability to present credible, technically substantiated evidence demonstrating that stolen assets are located within the jurisdiction of the requested state. In practice, however, most law enforcement agencies lack the specialized expertise required to conduct such analyses independently. While assistance from private blockchain analytics firms—such as Chainalysis and Elliptic—remains valuable, investigative authorities must also develop and institutionalize in-house cryptocurrency and blockchain analytical capabilities to ensure sustainable and effective enforcement.

TARGETING CASH-OUT POINTS

Although the cryptocurrency ecosystem is predominantly decentralized, centralized exchanges (CEXs) exist to facilitate transactional convenience for users.[3] They serve as fiat-to-crypto gateways that enable users to trade fiat currencies for virtual assets with ease, and vice versa. Also, they provide user-friendly asset management for those unable or unwilling to manage private keys independently and play a critical role in providing a wide range of crypto-related services.

3. A centralized exchange (CEX) is a custodial, intermediary-operated virtual asset trading platform that performs exchange and related services as a business on behalf of users. In comparison, a decentralized exchange (DEX) is a blockchain-based trading mechanism that enables the exchange of virtual assets directly between users through automated smart contracts, without reliance on a centralized intermediary or custodial entity. However, it should be noted that the term "exchange" may be somewhat imprecise in the decentralized context, since blockchain-based virtual asset transactions can occur directly via smart contracts on a distributed ledger without the need for a trading venue or institutional marketplace. For the convenience of comparison with centralized exchanges, this paper uses the term DEX.

Criminal actors exploit these CEXs primarily to convert crypto assets into fiat currency. Consequently, law enforcement agencies have targeted these cash-out points as nodes for tracing, freezing, seizing, and confiscating stolen cryptocurrency. In several jurisdictions, cryptocurrency CEXs are subject to **anti-money laundering and counter-financing of terrorism** obligations, including KYC requirements comparable to those imposed on traditional banks and financial institutions.

By capturing the moment when DPRK actors use crypto exchanges to cash out stolen money, it is possible to identify, freeze, seize, or even recover the stolen crypto money. For example, the approximately 10 percent of stolen funds recovered from the 2022 Ronin Bridge heist were seized by targeting cash-out points within the cryptocurrency ecosystem. This operation marked the first recorded seizure of stolen cryptocurrency, demonstrating the feasibility of asset recovery through law enforcement intervention at centralized exchange chokepoints. Blockchain analysis provided by Chainalysis was used to trace the stolen funds to **specific cash-out points**.

In another example, a portion of the cryptocurrency stolen in **the 2019 Upbit heist** was recovered in 2024. In that incident, the exchange suffered the theft of approximately USD 41 million ETH. This case represents the first substantiated instance in which a South Korean investigative authority formally attributed the theft of cryptocurrency from a domestic exchange to DPRK operatives. The South Korean Police Agency (SKPA) worked closely with the FBI and **concluded** that the heist had been perpetrated by DPRK actors. The SKPA ultimately recovered approximately 4.8 BTC, valued at roughly USD 400,000, which were subsequently returned to Upbit.

However, the recovery process undertaken by South Korean law enforcement authorities illustrates the challenges inherent in cross-border investigations of cryptocurrency-related crimes. After determining that a portion of the stolen cryptocurrency had been converted into bitcoin and held at a Switzerland-domiciled cryptocurrency exchange, the SKPA submitted compelling evidence to Swiss prosecutorial authorities demonstrating that these assets were linked to the theft from Upbit. What followed was an extensive **multiyear campaign** of asset recovery efforts. The SKPA encompassed numerous virtual and telephonic consultations alongside direct engagements at **the Swiss Federal Prosecutor's Office**. Working in concert with the South Korean Supreme Prosecutors' Office and the Ministry of Justice, the SKPA maintained persistent cross-border legal cooperation with Switzerland for nearly four years. Unfortunately, the foreign cryptocurrency exchanges **largely declined** to respond to South Korean law enforcement entities' overtures seeking the return of the illicitly obtained assets. This case demonstrates that close and timely cooperation with foreign virtual asset service providers and national financial intelligence units is imperative for effectively addressing cryptocurrency theft and recovering stolen crypto proceeds.

FACILITATORS OPERATING IN THIRD COUNTRIES

There are facilitators in third countries that contribute to money laundering and cash-out by DPRK actors. Mostly, these actors rely substantially on Chinese-based facilitators. Some Chinese facilitators collaborated with North Korean actors to procure fake identifications and operate a peer-to-peer cryptocurrency trader. Others even worked as **brokers** for money laundering and cashing out by purchasing crypto assets from DPRK actors and delivering converted funds in fiat currency in exchange for a certain amount of money in crypto or fiat form. In 2020, two Chinese nationals were **indicted** by the U.S. Department of Justice for laundering North Korean–linked cryptocurrency. In 2023, Sim

Hyon-Sop, working for North Korean Foreign Trade Bank, was **charged** by the Department of Justice in three different indictments for his money laundering activities. He allegedly received cryptocurrencies stolen through hacking, remitted them to multiple wallets, and handed them to **brokers he contacted** in China or the United Arab Emirates. Without cooperation from states where facilitators operate, however, the justice process cannot proceed, and the charged individuals have never been arrested or tried. Information on the facilitators based in China, including ones involved in cryptocurrency laundering, has been delivered to China by **the participating states in the MSMT**. Unfortunately, there has been no indication that China took any action in response to such information.

Financial infrastructures in Southeast Asian countries often serve as a critical conduit for North Korean cryptocurrency laundering. For instance, between 2022 and 2024, a North Korean national with connections to Reconnaissance General Bureau **regularly met** in person with officials from Huione Pay, a Cambodia-based payment service, to convert cryptocurrency into fiat currency and execute international transfers. Further, North Korean actors based in Cambodia allegedly **used accounts** registered at Huione Pay in 2023 to move funds from the Ronin Bridge theft. No criminal indictment in relation to Huione Pay has yet been filed. Instead, the U.S. Treasury Department **excluded** Huione Group from the U.S. financial system. Several states **expressed concerns** to the Cambodian government regarding Huione Pay's activities facilitating North Korean actors' money laundering. Subsequently, the National Bank of Cambodia **revoked** Huione Pay's payments license; notwithstanding this action, the company seems to **continue its operations** within Cambodia.

SOUTH KOREA'S EFFORTS IN THE CHASE

South Korean crypto exchanges have been hit by North Korean malicious activities in cyberspace. In 2017, Youbit was hacked **two times** and entered insolvency. In addition to **the 2019 attack**, Upbit also had Solana-based crypto assets valued at **KRW 44.5 billion** stolen in 2025. In order to combat crypto theft by DPRK actors, South Korea has taken key steps in the right direction, which include introducing or reforming several crypto-related policies—including amending the Act on Reporting and Using Specified Financial Transaction Information (**SFTI Act**) and passing into law the Act on Virtual Asset Users Protection (**VAUP Act**)—and deepening international cooperation with the United States, Japan, and the FATF.

First, information sharing among virtual asset service providers (VASP), Korea Financial Intelligence Unit (KoFIU), and investigative entities has improved. On April 19, 2022, dedicated **direct communication lines** were established between the SKPA and five major domestic virtual asset exchanges—Gopax, Bithumb, Upbit, Korbit, and Coinone. Later that year, on October 13, the SKPA concluded an **MOU** with these exchanges to facilitate investigative cooperation in virtual asset-related crimes and to enhance measures for victim protection and harm prevention. The information-sharing obligations of VASP and the KoFIU were also strengthened by amending the SFTI Act. In accordance with this act, VASP must report transactions suspected of involving illicit assets to the KoFIU (SFTI Act, Article 4). The KoFIU must provide information regarding specified financial transactions to investigative, financial, or intelligence entities—including the prosecutor general, director of the National Intelligence Service, and other relevant entities—where deemed necessary for including criminal investigations related to illicit proceeds or money laundering (SFTI Act, Article10). In accordance with the principle of reciprocity, the KoFIU may provide information on specified financial transactions to foreign financial intelligence units and receive such information in return (SFTI Act, Article 11).

Second, crypto exchanges' authority and responsibility in managing virtual assets under their custody have been expanded. Exchanges have been vested with discretionary authority to block virtual asset deposits and withdrawals without users' consent (VAUP Act, Article 11). Under this authority, exchanges can suspend deposits and withdrawals without users' consent where there are reasonable grounds to suspect involvement in money laundering activities. Exchanges are also required to hold no less than 80 percent of the economic value of users' virtual assets **isolated from the internet for security**, including in cold wallets (Decree to the VAUP Act, Article 11; Financial Service Commission Notice on the Supervision of Virtual Asset Business, Article 9).

Third, South Korea has worked together with the United States to counter North Korea's crypto theft. In 2022, South Korea established **a joint working group** with the United States to comprehensively address and respond to North Korea's lucrative activities in the cyber domain. This working group is composed of multiple agencies from the foreign affairs, intelligence, finance, and justice fields. In 2024, South Korea and the United States jointly imposed **sanctions** on the same person, Sim Hyon-Sop, for his money laundering activities. In 2025, South Korea, the United States, and Japan issued **a joint statement** on DPRK cryptocurrency thefts, where the three nations specifically emphasized the collaboration among the public and private sectors. Further, FATF members, including South Korea, have maintained North Korea's designation as **a high-risk jurisdiction** and called on all jurisdictions to cut off or restrict financial relationships with North Korea, implement enhanced financial monitoring, and strictly enforce UN sanctions.

Seeking International Law Enforcement Framework for Countering Crypto Theft

As illustrated above, South Korea has realigned its domestic policies to bring the virtual asset financial system within the scope of existing anti-money laundering/countering the financing of terrorism (AML/CFT) frameworks, and has deepened international cooperation with the United States, Japan, and the FATF to counter the North Korea's cryptocurrency theft. Nevertheless, absent effective cooperation at the global level—particularly from jurisdictions that enable North Korea's money-laundering activities—North Korea's pursuit of cryptocurrency will remain largely unconstrained. Accordingly, there is a pressing need for an international cooperation framework that enables states to collaborate swiftly in identifying, freezing, seizing, and recovering stolen cryptocurrency, as well as in investigating and prosecuting cyber-enabled cryptocurrency theft. This section assesses the extent to which existing multilateral instruments—including the UN Convention against Transnational Organized Crime (UNTOC), the UN Convention against Corruption (UNCAC), the FATF recommendations, and the newly adopted UN Convention on Cybercrime—provide an adequate legal basis for such cooperation.

ASSESSING EXISTING FRAMEWORKS

The Budapest Convention on Cybercrime does not regulate money laundering. **UNTOC** and **UNCAC** do so, but are not fully suitable to regulate cyber-enabled crypto theft. The FATF provides **practical guidance** for states to invoke when requesting mutual legal assistance in investigations and prosecutions related to crypto theft and laundering. However, this guidance is not legally mandated, and thus implementation remains voluntary for each state.

UNTOC and UNCAC

The UNTOC and the UNCAC include provisions requiring parties to impose customer identification, record-keeping, and suspicious transaction reporting obligations on financial institutions (UNTOC Article 7[1][a]; UNCAC Article 14[1][a]). The treaties further oblige parties to ensure that competent authorities responsible for combating money laundering—including administrative, regulatory, law enforcement, and, where appropriate, judicial bodies—are legally and institutionally empowered to cooperate and exchange information at both the domestic and international levels, subject to the conditions prescribed by domestic law (UNTOC Article 7[1][b]; UNCAC Article 14[1][b]). In addition, both treaties provide mechanisms enabling interstate cooperation for the identification and confiscation of criminal proceeds (UNTOC Article 13; UNCAC Article 55). The UNTOC has 195 parties, including South Korea, North Korea, the United States, and China, while the UNCAC has 192 parties, including South Korea, the United States, and China. Despite their near-universal participation, however, neither treaty offers an effective legal basis for seeking interstate cooperation specifically in cases of DPRK cryptocurrency theft and laundering, given their limited material scopes—the UNTOC to organized crime, and the UNCAC to corruption-related offenses.

FATF Recommendations

As highlighted above, timely cooperation from foreign financial institutions (i.e., cryptocurrency exchanges), is key for law enforcement authorities to identify, freeze, seize, or recover stolen cryptocurrency in their custody. For the purpose of law enforcement, cooperation from cryptocurrency exchanges can be sought based on **international AML/CFT standards** developed by the FATF. The FATF is an intergovernmental body established in 1989, **the objectives** of which are to protect financial systems from money laundering and the financing of terrorism and proliferation. Thirty-eight countries including South Korea, the United States, the United Kingdom, China, and Japan are FATF members. FATF has upgraded its international standards on AML/CFT regularly, in particular, to make virtual assets subject to the standards. The latest update's Recommendation No. 15 **makes clear** that "countries should ensure that virtual asset service providers are regulated for AML/CFT purposes."

FATF's recommendations associated with law enforcement provide practical guidance where countries can offer mutual legal assistance to each other in relation to crypto laundering. The FATF recommended that countries should ensure that investigative powers and techniques relating to the production, search, and seizure of information from financial institutions including crypto exchanges are available for use in response to requests from mutual legal assistance (Recommendation No. 37). In addition, countries should have measures to take expeditious action in response to requests by foreign countries seeking assistance to identify, trace, evaluate, investigate, freeze, seize, and confiscate criminal property, which includes recognizing and enforcing foreign orders on freezing, seizing, or confiscating (Recommendation No. 38). While the recommendations adopted by FATF are a practically valuable instrument on which law enforcement entities of each country can rely for cooperation, it is not legally binding.

Framework Under the UN Convention Against Cybercrime

Ultimately, the UNCC is the only internationally binding instrument to date that provides substantive and procedural rules for global cooperation to combat crypto theft and laundering by DPRK actors. Interestingly, both the DPRK, the primary perpetrator of cyber-enabled cryptocurrency theft, and China, the principal jurisdiction providing a safe haven for DPRK-affiliated actors, have signed the

UNCC. The UNCC, adopted by the UN General Assembly in December 2024, remains unsigned by the United States and its like-minded countries, including South Korea, due to a range of unresolved controversies. One major concern is that the procedural provisions governing access to electronic data are perceived to lack sufficient human rights safeguards, thereby creating the risk that authoritarian states (including China, Russia, and North Korea) could exploit these mechanisms for surveillance purposes. Nevertheless, the UNCC does contain substantive and procedural rules that could contribute to seeking cooperation from foreign crypto exchanges (albeit indirectly) and countries that facilitate North Korea's crypto theft and subsequent laundering processes. In this context, the value that the convention adds for countering North Korea must be assessed.

Eliminating Safe Havens by Criminalizing Crypto Laundering

As illustrated above, DPRK actors' laundering of stolen cryptocurrency and cashing out is facilitated by third-party laundering services and enablers located in third countries. Thus, there is a need for globally harmonized rules where activities related to cryptocurrency laundering are criminalized and punishable. The UNCC requires parties to criminalize money laundering of proceeds of cybercrimes (Article 17) ("Cybercrimes" here refer to the offenses established under Articles 7–16 of the convention). Under the convention, proceeds of crime refer to "**any property**" derived from or obtained, directly or indirectly, through the commission of an offense. This convention makes clear that "property" means "assets of every kind," and includes "virtual assets" (Article 2[i]). Based on these provisions, parties are obligated to criminalize acts of laundering cryptocurrency stolen through hacking.

This criminalization obligation is linked to obligations for international cooperation. For instance, in accordance with the convention, parties must cooperate with each other for the purpose of sharing e-evidence relating to the offences established under the UNCC, namely, not only cyber-enabled criminal activities, but also crypto laundering (Article 35[1][b]). Further, parties must take effective measures to cooperate with each other in conducting inquiries concerning the movement of criminal proceeds (Article 47[1][b]). In sum, these clauses can function as a legitimate basis to ensure that countries providing safe havens to facilitators assisting North Korea's crypto laundering activities can no longer do so. Instead, they are legally obligated to cooperate with other treaty parties in sharing e-evidence related to cryptocurrency laundering and conducting inquiries into the movement of stolen cryptocurrency.

International Cooperation Framework for Identifying, Freezing, Seizing, and Recovering Stolen Assets

The UNCC contains rules on international cooperation for the purpose of confiscating crypto proceeds generated through cybercrime. Parties first must adopt a domestic legal framework where criminal proceeds can be identified, traced, frozen, seized, and confiscated. In other words, parties are required to implement measures within their legal frameworks to confiscate criminal profits as well as equipment involved in the offenses (Article 31[1]). To facilitate confiscation, they must also adopt measures to enable authorities to identify, trace, freeze, or temporarily seize such items (Article 31[2]).

Second, The UNCC sets forth procedures through which parties may request the confiscation of criminal proceeds in cryptocurrency located in other parties. When proceeds of crime are situated in one party state, another party state that has jurisdiction over the predicate offenses can request the confiscation of the proceeds from it. In such a request, the requesting country must submit information on a description of the property to be confiscated, the location, and a statement of fact to the extent

possible. Subsequently, after this request, the requested country is obligated to take measures to identify, trace, and freeze or seize proceeds of crime for such confiscation (Article 50).

Third, there is a provision where investigative entities could indirectly gain cooperation from foreign crypto exchanges. Each party must empower its courts or other competent authorities to order that bank, financial, or commercial records be made available or be seized for the purpose of international cooperation for confiscation (Article 31[7]). Based on this clause, a party can gain information regarding allegedly stolen cryptocurrency in the custody of foreign exchanges. Given that the SKPA encountered the foreign cryptocurrency exchanges' **refusal** to respond to the agency's requests in order to seek the return of the assets unlawfully obtained from the 2019 Upbit hack, these provisions may provide a legal ground on which a party can rely to draw cooperation from foreign crypto exchanges.

In Sum

This assessment of existing international frameworks shows that the UNTOC and the UNCAC offer useful legal tools, but their limited scope prevents them from adequately addressing the specific challenges posed by cyber-enabled asset theft. The FATF recommendations similarly provide practical guidance for states, yet their nonbinding character means that implementation ultimately depends on each country's willingness to comply. As a result, even well-developed domestic regulations and strong bilateral partnerships are insufficient to fully address a threat that exploits gaps between national jurisdictions. In light of these limitations, the UNCC marks an important shift toward a binding global framework. By requiring the criminalization of cryptocurrency laundering and establishing coordinated procedures for asset recovery, the convention advances international cooperation.

Conclusion

The decentralized and pseudonymous nature of cryptocurrency transactions provides North Korea with incentives to target crypto assets. This structural advantage is further compounded by sophisticated obfuscation techniques—including mixing, swapping, and cross-chain bridging—and anonymity-enhanced cryptocurrencies, all of which significantly reduce or eliminate transactional traceability. In response, law enforcement agencies have targeted cash-out points on CEXs that criminal actors exploit primarily to convert crypto assets into fiat currency, with a view to tracing, freezing, seizing, and confiscating stolen cryptocurrency. However, the absence of a global framework through which law enforcement authorities can seek cooperation from foreign cryptocurrency exchanges makes it difficult for the authorities to effectively and swiftly address cryptocurrency theft and recover stolen assets. Furthermore, facilitators operating within third countries are providing assistance in the money laundering process involving cryptocurrency stolen by North Korea. Unless law enforcement action is taken against those involved in money laundering who operate in safe havens, it will be difficult to prevent North Korea from laundering funds illicitly obtained through cyber activities.

From this perspective, law enforcement responses to North Korea's cyber-enabled theft of cryptocurrency and subsequent money laundering require global cooperation. In particular, states should seek harmonization at the level of interstate criminalization by defining cybercrime and money laundering of proceeds generated by cybercrime as criminal offenses. In addition, a framework is needed to ensure that law enforcement cooperation in identifying, freezing, seizing, and recovering stolen funds can be carried out swiftly and effectively. While the UNCC remains a subject of intense

debate regarding human rights and surveillance, it nonetheless presents a significant opportunity to anchor a multilateral law enforcement regime. By mandating the criminalization of cryptocurrency-based money laundering and institutionalizing international cooperation for asset recovery, the convention could provide a more coherent and binding legal framework to address DPRK crypto theft and money laundering practices. ■

Joohui Park *is a senior researcher on the Cybersecurity Policy Research Team at the National Security Research Institute in the Republic of Korea.*

This report is made possible through support from the National Security Research Institute (NSR) of Korea. CSIS and NSR conducted scholarly research on U.S.-ROK cyber resilience. The analysis presented here was independently authored by researchers at NSR.