
The North Korean Crypto Threat

Juan C. Zarate

Executive Summary

- The North Korean threat to the crypto ecosystem is the highest form of immediate risk to the crypto-economy driven by a regime that seeks to profit from its misuse to reinforce its regime and fuel all its programs – without concern for the integrity, security, or stability of the evolving crypto economy and technologies.
- Policymakers, regulators, and enforcement agencies are focused on North Korea’s pivot to crypto – which represents a dangerous convergence of national security, cyber, and financial integrity risks. This comes at a time of heightened regulatory scrutiny over the sector and ongoing global debates on the treatment of cryptocurrencies, blockchain technologies, and DeFi.
- The North Korean threat presents itself at a time when risk management of the crypto ecosystem must mature on all fronts, including tackling the highest risks. There needs to be a commitment by all stakeholders to more careful risk management and to distinguish where risks lie. This is critical as regulators consider how to regulate the sector in all its forms – and as crypto stakeholders decide how, where, and with whom they will operate. There should be a sober recognition that this technology presents enormous opportunities for financial and commercial innovation, but it will be exploited by bad actors – including those threatening the integrity, security, and sustainability of the system.
- Herein lies the challenge and opportunity for the crypto ecosystem. A rogue and dangerous nation state has made it a business and security imperative to exploit and corrupt the emerging crypto economy and technologies – with real world consequences as North Korea resumes missile tests and rattles its nuclear saber. This challenge requires those who care about the legitimacy, growth, and promise of the crypto economy and related innovations to target North Korea as a preeminent risk.

Introduction

North Korea (the Democratic People’s Republic of Korea “DPRK”) presents a fundamental and growing international security challenge – and now represents the most serious nation-state risk to the crypto ecosystem. Over the last two decades, the regime in Pyongyang has expanded its nuclear and ballistic missile programs; threatened South Korea (including the sinking of a South Korean naval vessel), its neighbors, the United States, and political opponents; and accelerated its cyber capabilities and attacks against government agencies, banks, and the private sector.

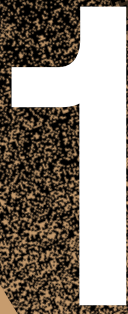
Kim Jong-un, the latest in the dynastic leadership of North Korea’s totalitarian regime, has been explicit about the use of cyber capabilities in the country’s arsenal: “Cyber warfare, along with nuclear weapons and missiles, is an ‘all-purpose sword’ that guarantees our military’s capability to strike relentlessly.”¹ These capabilities have expanded over time, coupled with an ability to access and subvert international systems for the regime’s advantage.

To fund their ambitions and ensure regime survival, North Korea has operated as a

mafia state – leveraging criminal enterprises, rogue networks, and illicit financing to raise funds and evade scrutiny beyond its borders. In the face of two decades of sanctions and pressure, the regime in Pyongyang has adapted – finding novel ways to access, raise, and move money into the regime’s coffers surreptitiously.

With the advent of the crypto economy, the North Korean regime has taken full advantage of its ability to engage in cyber heists and obtain cryptocurrencies as a means of accessing capital. This has been both a means of funding the regime and an asymmetric posture to attack enemy systems. Exploiting the crypto ecosystem has now become a consistent source of revenue for the regime as well as being another weapon to be wielded against its enemies.

The North Korea threat to the crypto ecosystem is the highest form of immediate risk to the crypto-economy driven by a regime that seeks to profit from its misuse to reinforce its regime and fuel all its programs – without concern for the integrity, security, or stability of the evolving crypto economy and technologies.



1

The Moment for Maturing Crypto Risk Management

The fundamental challenge of DPRK misuse of crypto presents an important moment for maturing the management of risk in the crypto economy. Broadly speaking, we have now crossed the Rubicon of legitimacy for the crypto sector, with cryptocurrencies and underlying technologies gaining acceptance and adoption as a new asset class; the potential for alternative payment, trading, and commercial systems; and serving as fonts of creativity, innovation, and financial freedom and inclusion. Even in the face of market headwinds and a crypto winter, there is no going back to a world where a crypto economy doesn't exist.

In that vein, there needs to be a commitment by all stakeholders to maturing risk management in this domain. It is clear that not all cryptocurrencies or stablecoins are the same, not all VASPs operate equally, not all jurisdictions regulate harmoniously, and not all technologies present the same challenges. This means that there needs to be more careful risk management in the crypto domain to distinguish where risks lie.

This is critical as regulators consider how to regulate the sector in all its forms and developments – and it is equally important as crypto stakeholders decide how, where, and with whom they will operate. Consideration

of risk should affect the design of new technologies, the application of controls, and the adaptation of regulations and principles of good governance to technologies that present new opportunities. And there should be a sober recognition that this technology and innovation, like all others, can and will be exploited by bad actors – including those who do not care about the integrity, security, or sustainability of the underlying system.

In the crypto ecosystem and in other domains, North Korea is a rogue regime that has historically found illicit ways to profit, circumvent controls, and misuse and threaten systems.



2

The Mafia State



The regime's ability to adapt and leverage financial and commercial networks is well-practiced. Despite its moniker as "The Hermit Kingdom," the regime does not exist in full isolation, relying heavily on banks, front companies, shippers, and smuggling networks beyond its borders to access the capital it needs to maintain its military, missile, and nuclear programs and to maintain the regime leadership's luxurious lifestyles.

North Korea has long relied on the illicit economy for funding -- organized criminal enterprises like narcotics production and distribution, trafficking of endangered species, counterfeiting currency, and manufacturing and smuggling counterfeit cigarettes.² The best counterfeit U.S. \$100 bills -- called "The Supernote" -- are produced by the North Korean regime, with North Korean diplomats and counterparties using counterfeit globally. Supernotes have appeared in exchange houses, banks, and casinos as far afield as Peru, Yemen, and Las Vegas.

In the early 2000s, the U.S. government focused its enforcement and regulatory

attention on North Korean criminal activities, especially its abuse of the financial system -- an effort I helped lead. The intent of this project was to squeeze the regime's financial lifelines, increase the chances of success for nuclear negotiations, and protect the integrity and security of the financial system.

In 2005, the U.S. Treasury Department cut off one of North Korea's principal financial lifelines by designating Macau-based Banco Delta Asia SARL (BDA) as a "primary money laundering concern" under Section 311 of the PATRIOT Act. The bank had been "a willing pawn for the North Korean government to engage in corrupt financial activities,"³ and had been serving as an all-purpose bank for North Korean illicit transactions and money laundering. As a result of the regulatory action, BDA was cut off from the U.S. and international financial system.

With the exposure of its illicit activities and direct consequences leveled against a facilitating bank, North Korean financial and commercial relationships were severed or put at risk Pyongyang's institutions, agents, and fronts were severely impacted

by lost access to accounts, transactions, and commercial networks as financial institutions, including in China, severed ties due to tainted entanglement in North Korean illicit activities and potential expulsion from the international financial system.⁴ For more than two years, the price of reentry into the Six-Party Nuclear Talks leveled by North Korea was the return of its money frozen in BDA and renewed access to the financial system.⁵

More UN and national sanctions and enforcement actions have been leveled against the North Korean government, sectors of the economy upon which it relies (e.g., coal and minerals), and various nodes and enablers over time, especially in the wake of continued North Korean provocations and testing of its nuclear and missile programs. DPRK has adapted to the pressure, by moving its activities further into the illicit sphere. Sanctions evasion and masked transactions, in the form of creating front companies and using ship-to-ship transfers, has become common practice for North Korea, along with reliance on cyber attacks and proxies that challenge attribution.⁶



3

Crypto Rogue

North Korea has pivoted to exploiting evolving financial platforms and technologies, such as cryptocurrency and blockchain technology to compensate for closed channels in the formal financial system and losses because of economic sanctions on more traditional forms of commercial activity.⁷ Beyond their obvious financial benefit, cyber attacks and heists also provide “plausible deniability” to the DPRK, thereby “reducing the risk of retaliation and allowing it to operate in the gray zone between peace and war.”⁸ Indeed, North Korea has demonstrated that it can successfully operate in the cyber and crypto domains with little consequence and rich rewards, while other channels of revenue and financial flows are closed. Crime is paying for North Korea as it exploits the crypto economy using cyber tools and proxy networks.

North Korea’s hacking capabilities allow it to steal financial resources from central banks, financial institutions, and virtual currency exchanges and users. The 2020 UN report on North Korea states that Pyongyang’s cybercrime capabilities have generated up to \$2 billion in total revenue through August 2019 for its weapons of mass destruction programs using “widespread and increasingly sophisticated” cyber attacks.⁹ Since the report was written, there has been more evidence to indicate that the pace and the ingenuity of North Korea’s online threat have accelerated.¹⁰

- The Lazarus Group, a Pyongyang-led cybercrime organization in operation since 2014 and sanctioned in 2019, has been instrumental in these attacks, compromising major national financial networks and stealing hundreds of millions of dollars’ worth

of cryptocurrency.¹¹ One notable cyber attack orchestrated by the Lazarus Group was in 2016, against the Bank of Bangladesh. The Lazarus Group hacked the bank’s network, stole its credentials for the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a financial messaging system, and issued requests through the Federal Reserve of New York to send funds from the Bangladeshi bank to accounts the hackers held.¹² In the end, the Lazarus Group got off with \$81 million, with the intent to steal nearly a billion dollars if not for their own mistake and diligence by attentive officials at the NY Fed.¹³ Besides Bangladesh, the Lazarus Group has conducted successful heists against financial institutions in India, Mexico, Pakistan, Philippines, South Korea, Taiwan, Turkey, Chile, and Vietnam.¹⁴

- A more recent attack perpetrated by the Lazarus Group involving cryptocurrency occurred in March 2022, when it stole \$620 million in crypto from the video game Axie Infinity through its underlying blockchain, Ronin.¹⁵ This exploit was fruitful for the DPRK, considering its annual total cryptocurrency theft in 2021 was worth around \$400 million, according to blockchain analytics firm Chainalysis.¹⁶ In June 2022, the Lazarus group was allegedly behind another successful attack, this time stealing \$100 million from California blockchain, Harmony.¹⁷ Hackers then laundered almost all of the funds using Tornado Cash, a virtual currency mixer sanctioned by the U.S. Treasury Department in August 2022 for laundering over \$7 billion worth of

virtual currency (including \$455 million stolen by the Lazarus Group).¹⁸

- Another recent ploy by North Korean hackers involves perusing job sites like LinkedIn and Indeed and copying job experiences from real profiles to build plagiarized resumes and secure jobs at U.S. cryptocurrency firms.¹⁹ By gleaning information from crypto firms, North Korea’s government could collate information about future cryptocurrency trends, including sanctions controls and evasion tactics. The DPRK is getting more sophisticated and better at infiltrating target networks and systems – directly and indirectly.
- As North Korea’s economy continues to deteriorate amid sanctions and its response to COVID-19, “cybercrime remains a key source of revenue.”²⁰ A UN report claimed that North Korean hackers stole more than \$50 million between 2020 and mid-2021 and launched seven further attacks on cryptocurrency platforms to help fund their nuclear program.²¹ The number of DPRK attacks and exploits will only grow.

Herein lies the challenge for the crypto ecosystem and all those who want to see the crypto economy flourish. A rogue and dangerous nation state has made it a business and security imperative to exploit and corrupt the emerging crypto economy and technologies – with real world consequences as North Korea resumes missile tests and rattles its nuclear saber. This challenge requires those who care about the legitimacy, growth, and promise of the crypto economy and related innovations to focus on North Korea as a preeminent risk.



4

North Korea as a Preeminent Crypto Risk

Policymakers, regulators, and enforcement agencies are focused on North Korea's pivot to crypto – which represents a dangerous convergence of national security, cyber, and financial integrity risks. This comes at a time of heightened regulatory scrutiny over the sector and ongoing global debates on the treatment of cryptocurrencies, blockchain technologies, and DeFi.

U.S. authorities are targeting North Korea's crypto activity more aggressively.

- The recent designation of Tornado Cash by the Office of Foreign Assets Control (OFAC) was likely animated by the twin factors of North Korean/Lazarus Group misuse of the technology to tumble \$455 million in stolen crypto and the laundering of more than \$7 billion in virtual currency globally through the use of Tornado Cash.²² This action has garnered much attention and controversy regarding the ramifications and appropriateness of the use of IEEPA authorities to designate an open-source protocol. This powerful sanctions tool was used in part because North Korean

leveraged and profited through the enabling technology.

- The recent designation of Blender.io (a Bitcoin mixer) by OFAC in May 2022, also signaled the desire by OFAC authorities to use sanctions tools to isolate and mark a part of the crypto economy that was being misused by the North Koreans. According to OFAC, the Lazarus Group used Blender.io to launder over \$20.5 million in illicit proceeds derived from the Group's Axie Infinity/Ronin attack.²³
- In May 2022, the Biden administration sanctioned Far Eastern Bank and Bank Sputnik for doing business with North Korea and supporting its efforts to develop WMD and ballistic missile programs.²⁴ This marks the first time that Russian banks were sanctioned for facilitating North Korea's evasion of sanctions. With a desire to address sanctions evasion across sanctions programs, the Biden administration will no doubt consider sanctions on additional Chinese or Russian

companies directly linked to North Korea sanctions evasion.²⁵ As John Detmers, then Assistant Attorney General for the National Security Division at the U.S. Department of Justice noted in February 2021, "the time is ripe for Russia and China, as well as any other countries whose entities or nationals play a role in the D.P.R.K. revenue-generation efforts, to take action."²⁶

U.S., South Korea, Japan, and other allies realize that the North Korean risk has bled into the crypto domain, and they will attach more resources and attention to targeting illicit North Korean cyber and crypto activity and will attempt to deter and prevent exploitation of these systems and technologies. This presents an important moment then for the crypto ecosystem, with North Korea representing the most serious and material nation-state risk to the integrity of this budding system. North Korea should become a test case for how authorities and legitimate crypto and tech players manage and counter the rogue misuse of the crypto economy.



5

Test Case for Cooperation & Concerted Action

Deterring and neutralizing North Korea's cyber attacks and exploitation of the crypto economy should be a core goal of international cooperation.²⁷ This requires a strategy that attempts to challenge DRPK in the crypto domain, with purposeful cooperation between the public and private sectors.

- Tactically, this will require task forces and combined efforts to discover and react to where the North Korean government and its proxies are operating in the crypto domain. Blockchain analysts, compliance teams, regulators, virtual asset service providers, and law enforcement, among others, can help track and trace where North Korean-signed actors are operating and where they may be infiltrating systems. There can be concerted efforts to track the stolen funds, to freeze and recover assets, and ultimately to close avenues or channels of abuse by DPRK hackers.
- With more calls for the use of regulatory measures and sanctions to affect misuse of cryptocurrencies, there will be more attention to tracking and confiscation of cryptocurrencies by North Korea as a part of the future sanctions landscape. Going forward, we will see the U.S. focus its attention on finding networks and connections that help North Korea evade sanctions. This will include the targeting of rogue actors, networks, and platforms that facilitate North Korean activity, "including foreign over-the-counter (OTC) brokers and telecommunications companies that provide to North Korea technical services, know-how, and equipment that its hackers use to conduct malicious cyber operations."²⁸
- There should be continued attention on strengthening and clarifying the U.S. regulatory regime, so regulation is not guided solely by enforcement actions and companies are not incentivized to engage in regulatory arbitrage. This includes identifying and isolating rogue actors that are not playing by the rules, even if they prove systemically relevant. Understanding the landscape and how regulation and enforcement affect technology should be the subject of ongoing public-private dialogues.
- The importance of the crypto economy, new payment systems, and the innovations stemming from these technologies should be viewed as a national security and economic asset – to be tended to carefully and with an eye toward competition with other state actors like China. This is critical as China continues to prove a financial and commercial outlet and backstop for North Korea and fears the loss of central control in state-authoritarian capitalist system.
- Crypto and digital payment technologies will continue to be a source of growth, innovation, and economic freedom. The private sector and technology innovators should help design new technologies – around identity management and identification of anomalous or suspicious behavior – that will be able to manage risk in the system – including discovering and preventing rogue players from exploiting the system. While there may be a low maturity to managing this risk, efforts in this area are increasing as some companies approach innovation with compliance at the core of their product design and market offerings.
- There is a need for more innovative public-private partnership models, which continue to evolve and need to grow more operational. If cooperative efforts in this domain are to take hold, there needs to be a challenge to the old models of information exchange to enable real and concerted actions. We have seen this in the cyber domain in recent years, where government and industry actors have collaborated more effectively in the face of fast-moving cyber threats from sophisticated state and non-state actors. Proactive industry commitments of tech and talent, such as law enforcement initiatives with blockchain analytics firms are a start, along with examples of collaboration well underway with the FS-ISAC, the Financial Consortium, and the National Cyber-Forensics and Training Alliance (NCFTA).²⁹

Ultimately, the efforts to track, target, and prevent North Korea's abuse of the crypto ecosystem will determine if such threats – with clear international security and systemic implications -- can be addressed and managed effectively.

All crypto stakeholders must be clear-eyed about the risks and the opportunities in the new crypto economy – and learn to balance both. The challenge of doing this thoughtfully amidst blazing innovation, opportunity, as well as abuse represents a common challenge for national security professionals, regulators, and the crypto industry and technologists alike. In this regard, North Korea presents an opportunity to focus attention and innovation on the highest form of risk in this domain -- and how we will collectively address it.

The Honorable Juan C. Zarate was the first-ever Assistant Secretary of the U.S. Treasury for Terrorist Financing and Financial Crimes and former Deputy Assistant to the President and Deputy National Security Advisor for Combatting Terrorism (2005–2009).

He is the Chairman of the Center on Economic and Financial Power at the Foundation for Defense of Democracies (FDD); Chairman and Co-Founder of Consilient; and Global Co-Managing Partner and Chief Strategy Officer for K2 Integrity. He is the author of numerous articles and books, including “Treasury’s War: The Unleashing of a New Era of Financial Warfare” (PublicAffairs 2013). Since 2014, he has been an independent advisor to Coinbase, and for eight years, he was a Lecturer on Law at the Harvard Law School.

Endnotes

- 1 <https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/>
- 2 <https://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf> p15
- 3 <https://home.treasury.gov/news/press-releases/js2720>
- 4 <https://www.nytimes.com/2007/01/18/world/asia/18iht-north.4255039.html>
- 5 Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare*, 2013
- 6 <https://c4ads.org/reports/black-gold/>; https://home.treasury.gov/system/files/126/05142020_global_advisory_v1.pdf; <https://rusi.org/explore-our-research/publications/commentary/un-panel-experts-report-north-korea-more-advanced-weaponry-better-sanctions-evasion>; <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf>
- 7 <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BlockchainAnalysisEES.pdf?mtime=20220216090240&focal=none> p1
- 8 https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf p7-8
- 9 https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf (30 August 2019), p26
- 10 <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>
- 11 <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BlockchainAnalysisEES.pdf?mtime=20220216090240&focal=none> p1
- 12 https://www.fdd.org/wp-content/uploads/2018/09/REPORT_NorthKorea_CEEW.pdf p23
- 13 <https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>
- 14 <https://home.treasury.gov/news/press-releases/sm774>
- 15 <https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/>; <https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea>
- 16 <https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/>
- 17 <https://www.bloomberg.com/news/articles/2022-06-29/north-korean-hackers-suspected-in-100-million-harmony-heist?sref=Pw1Mp35R>
- 18 <https://home.treasury.gov/news/press-releases/jy0916>
- 19 <https://www.yahoo.com/news/north-korean-fraudsters-suspected-copying-153907880.html>

-
- 20 The Attack on America's Future: Cyber-Enabled Economic Warfare, Edited by Samantha F. Ravich and Annie Fixler, Foundation for Defense of Democracies, Forthcoming fall 2022, Chapter: North Korea: The Evolution of Kim Jong Un's 'All-Purpose Sword,' By Mathew Ha, p43
 - 21 <https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf> p80
 - 22 <https://home.treasury.gov/news/press-releases/jy0916>
 - 23 <https://home.treasury.gov/news/press-releases/jy0768>
 - 24 <https://home.treasury.gov/news/press-releases/jy0801>
 - 25 <https://n.news.naver.com/mnews/article/020/0003433973>
 - 26 <https://www.justice.gov/opa/pr/assistant-attorney-general-john-c-demers-delivers-remarks-national-security-cyber>
 - 27 <https://n.news.naver.com/mnews/article/020/0003433973>
 - 28 <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BlockchainAnalysisEES.pdf?mtime=20220216090240&focal=none> p2
 - 29 <https://regtechconsulting.net/aml-regulations-and-enforcement-actions/314b-information-sharing-a-valuable-but-underutilized-tool/>

The North Korean Crypto Threat

Questions? Please email us at:
info@cryptoforinnovation.org

© 2022 Crypto Council for Innovation