Penn State Journal of Law & International Affairs

Volume 12 | Issue 2

October 2024

Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme

Kole Zellers

ISSN: 2168-7951

Penn State
Journal of Law & International Affairs

2024 VOLUME 12 NO. 2

HACKED! NORTH KOREA'S BILLION-DOLLAR CRYPTO HEISTING SCHEME

By: Kole Zellers[*]

TABLE OF CONTENTS

[*] Kole Zellers is a Student Works Editor for the Penn State Journal of Law & International Affairs and a 2024 J.D. Candidate at Penn State Law in University Park, PA.

I. INTRODUCTION

When most people are asked about cryptocurrency, they probably think about a big-name digital currency like Bitcoin, a buzzword like the "blockchain," or perhaps a hooded figure in a dark room, sitting behind a laptop screen filled with rapidly flashing numbers. In any case, it is unlikely that most people who have heard of cryptocurrency truly understand how it works or fully grasp its impact on the global economy over the past ten years. Even with the extreme devaluation of cryptocurrency since the beginning of 2022, its total market value remains at around $1 trillion, and in November of 2021, crypto's global market value peaked at nearly $3 trillion,[1] making it 7% of the world's money by one estimation.[2] Even if these economic statistics fail to impress you, few would argue against the gravity of cryptocurrency's social and cultural impact, principally in the United States and other countries with high-speed Internet access. A study from July shows that 89% of U.S. adults have heard of Bitcoin and that 22% of adults (46 million Americans) own at least some amount of Bitcoin.[3] On a global scale, the study estimates that roughly 1 billion people will use cryptocurrencies around the world in 2022.[4]

For a service that is available exclusively online, cryptocurrency has managed, with unprecedented speed and efficiency, to become a fundamental part of national economies all over the world, especially in poor and developing countries, where decentralized currency can be used to combat inflation or lack of access to a traditional banking

---

[1] Elizabeth Howcroft, *Cryptocurrency market value slumps under $1 trillion*, REUTERS (June 13, 2022, 12:56 PM), https://www.reuters.com/business/finance/cryptocurrency-market-value-slumps-under-1-trillion-2022-06-13/.

[2] Nathan Reiff, *How Much of All Money Is in Bitcoin?*, INVESTOPEDIA (Nov. 26, 2021), https://www.investopedia.com/tech/how-much-worlds-money-bitcoin/.

[3] Josh Howarth, *How Many People Own Bitcoin? 95 Blockchain Statistics (2022)*, EXPLODING TOPICS (July 12, 2022), https://explodingtopics.com/blog/blockchain-stats.

[4] *Id.*

system.[5] While the global access to digital currency brought about by the decentralized nature of cryptocurrency has numerous benefits, it also raises several concerns, particularly concerning traceability, user identification, and other transparency issues that do not arise with traditional currency.[6] Many "tech-savvy" individuals from all over the world, whether they are working for a government, a corporation, or independently, have mastered the art of exploiting the transparency issues of the decentralized digital currency system for their own economic benefit. In the year 2021 alone, "crypto scammers" stole a record $14 billion in cryptocurrency, marking a 79% increase in losses from "crypto-related crime" from 2020.[7]

The rapid increase in crypto crime is largely attributed to the rise of decentralized finance (DeFi) platforms.[8] DeFi platforms were created to replace the "middlemen" of traditional currency, like banks and stock exchanges, with software that does the work of creating the market, initiating the transaction, and verifying the legitimacy of users.[9] The open-source software used to create DeFi platforms, otherwise known as crypto exchanges, permits people to trade directly and rapidly with one another on the blockchain.[10] However, because DeFi is not subject to the same consumer protections and safeguards as the traditional banking system, it is a major target for fraud.[11] In fact, the FBI reports that 97% of cryptocurrency stolen from January to March

---

[5] *See Bitcoin adoption and its impacts on the developing world*, THE GUARDIAN (Oct. 28, 2021, 6:12 AM), https://guardian.ng/opinion/outlook/bitcoin-adoption-and-its-impacts-on-the-developing-world/.

[6] Mackenzie Sigalos, *Crypto scammers took a record $14 billion in 2021*, CNBC (Jan. 7, 2022, 4:31 AM), https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html#:~:text=Scammers%20around%20the%20world%20took,%243.2%20billion%20worth%20of%20cryptocurrency.

[7] *Id.*

[8] Mengqi Sun, *DeFi Increasingly Popular Tool for Laundering Money, Study Finds*, WALL ST. J. (Jan. 26, 2022, 8:00 AM) https://www.wsj.com/articles/defi-increasingly-popular-tool-for-laundering-money-study-finds-11643202002

[9] Kevin Roose, *What is DeFi?*, N.Y. TIMES, https://www.nytimes.com/interactive/2022/03/18/technology/what-is-defi-cryptocurrency.html?auth=register-google1tap&register=google1tap (last visited Oct. 21, 2022).

[10] *Id.*

[11] *Id.*

of 2022 was stolen from DeFi platforms.[12] As part of this report, the FBI recommends that investors take significant caution and conduct extensive research before investing on a DeFi platform.[13] Despite the statistics that suggest the dangers of DeFi, these platforms are reportedly still growing in popularity, with more than 4.5 million unique wallets (virtual storage spaces for cryptocurrency) used in DeFi at the end of the first quarter of 2022.[14] The popularity of DeFi, according to its proponents, is due in large part to low barriers for entry, the public nature of DeFi blockchain information, and the economic autonomy brought about by the user's ability to hold his or her own assets.[15]

While immensely efficient and undoubtedly popular for that reason, it is clear that DeFi will continue to be the subject of the overwhelming majority of cryptocurrency thefts for years to come. Since the emergence of DeFi, knowledgeable and properly equipped bad faith actors have acquired immense wealth through the art of stealing from crypto exchanges, and with the severe lack of effective regulation, they have little incentive to stop. The particular bad faith actor subject to the analysis of this article is the Democratic People's Republic of Korea (DPRK). Under the leadership of Kim Jong-Un, North Korea has routinely found itself at odds with the governments, societal values, and cultural identities of Western nations, more particularly, the United States. As part of this opposition, North Korea has made its nuclear weapons program a top priority in countering the U.S., and has even recently declared itself a "nuclear weapons state".[16] As increasingly harsh economic sanctions have been imposed on the

---

[12] *Cyber Criminals Increasingly Exploit Vulnerabilities in Decentralized Finance Platforms to Obtain Cryptocurrency, Causing Investors to Lose Money*, FBI, https://www.ic3.gov/Media/Y2022/PSA220829#:~:text=Between%20January%20and%20March%202022,30%20percent%20in%202020%2C%20respectively. (last visited Oct. 21, 2022).

[13] *Id.*

[14] Max Crawford, *Bitcoin DeFi: Unpacking the Key Drivers Behind the Popularity of DeFi Technologies*, HIRO (July 25, 2022), https://www.hiro.so/blog/bitcoin-defi-unpacking-the-key-drivers-behind-the-popularity-of-defi-technologies.

[15] *Id.*

[16] *North Korea declares itself a nuclear weapons state*, BBC NEWS (Sept. 9, 2022), https://www.bbc.com/news/world-asia-62845958.

country in response to its nuclear missile program, North Korea has been forced to tap into alternative, less regulated sources of revenue, such as decentralized digital currency. And over the past few years, the government has mastered the art of weaponizing its acutely tailored cyber infrastructure to exploit the weaknesses of DeFi platforms.[17] Through these attacks, the DPRK has managed to steal unprecedented amounts of cryptocurrency, totaling over $1 billion in theft from DeFi protocols in the year 2022 alone.[18] But why has North Korea's crypto heisting scheme been so successful, and what can be done to stop it?

A. North Korea: A Hacker's Success Story

In the 21st century, particularly since Kim Jong-Un became the Supreme Leader of North Korea in 2011,[19] the country has been exceedingly popular in the news media and world renowned for its "anti U.S." policies, its "communist government", and, of course, for its commitment to a military nuclear weapons program, which has advanced greatly since its formation in the 1980s.[20] Many people, especially adults in the U.S., also know North Korea for its role in the infamous "Sony Pictures hack" in 2014, a malware attack launched on the employees of Sony that stole terabytes of private information, erased an enormous amount of data, and forced the company offline until its network was rebuilt.[21] Perhaps less famous, but undoubtedly more impactful, was the 2017 WannaCry 2.0 global ransomware attack launched by a North Korean hacker organization known as the

---

[17] *See* Ji Da-gyum, *N. Korean hackers steal $1b in crypto from DeFi protocols this year: report*, THE KOREA Herald (Aug. 17, 2022, 9:59 PM), https://www.koreaherald.com/view.php?ud=20220817000755.

[18] *Id.*

[19] Mark Memmott, *Kim Jong Un Declared To Be 'Supreme Leader' Of North Korea*, NPR (Dec. 29, 2011, 7:15 AM), https://www.npr.org/sections/thetwo-way/2011/12/29/144420122/kim-jong-un-declared-to-be-supreme-leader-of-north-korea.

[20] *Nuclear Weapons Program*, GLOBAL SECURITY, https://www.globalsecurity.org/wmd/world/dprk/nuke.htm (last accessed Oct. 21, 2022).

[21] Andrew Blankstein, *U.S. indicts three North Koreans in massive WannaCry, Sony hacks*, NBC NEWS (Feb. 17, 2021, 11:43 AM), https://www.nbcnews.com/politics/justice-department/u-s-indicts-three-north-koreans-massive-wannacry-sony-hacks-n1258096.

"Lazarus Group", which infected 300,000 computers in 150 nations, and caused billions of dollars in damage.[22] More recently, the same group was linked to a $625 million crypto theft from the Ronin Network, an Ethereum-based blockchain project that powers the popular "play-to-earn" video game Axie Infinity.[23]

In response to these attacks and others, the United States Department of Justice (DOJ) launched an investigation and successfully identified a North Korean citizen who was allegedly involved in these attacks, Park Jin Hyok.[24] In 2018, Hyok was charged with "conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money and other resources." [25] And in 2021, three other North Korean computer programmers were indicted for their alleged participation in these attacks and in other illicit activities, including cryptocurrency heists, bank heists, and spear-phishing campaigns.[26] This indictment, however, has clearly not deterred North Korea from continuing to conduct high profile cyberattacks, as evidenced by its very recent ransomware attacks on multiple healthcare facilities.[27] Although the DOJ was able to recover

---

[22] *Cyber-attack: US and UK blame North Korea for WannaCry*, BBC NEWS (Dec. 19, 2017), https://www.bbc.com/news/world-us-canada-42407488.

[23] Carly Page, *US officials link North Korean Lazarus hackers to $625M Axie Infinity crypto theft*, TECH CRUNCH (Apr. 15, 2022, 10:53 AM), https://techcrunch.com/2022/04/15/us-officials-link-north-korean-lazarus-hackers-to-625m-axie-infinity-crypto-theft/.

[24] *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*, U.S. DEP'T JUSTICE (Sept. 6, 2018), https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[25] *Id.*

[26] *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe*, U.S. DEP'T JUSTICE (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks and#:~:text=A%20federal%20indictment%20unsealed%20today,and%20companies%2C%20to%20create%20and.

[27] Kevin Collier, *North Korea is targeting hospitals with ransomware, U.S. agencies warn*, NBC NEWS (Jul. 6, 2022, 4:25 PM), https://www.nbcnews.com/tech/security/north-korea-targeting-hospitals-ransomware-us-agencies-warn-rcna36896.

$500,000 of the stolen funds in this case[28], there have been numerous attacks over the last few years that have not been accounted for, with a 2019 report estimating that North Korea had stolen $2 billion from crypto exchanges and banks to fund its nuclear missile program.[29] Since 2019, there has been no shortage of success for North Korean hackers, which is in large part due to the meteoric rise of cryptocurrency and the emergence of DeFi platforms.

To contextualize how immensely successful North Korea's crypto heisting scheme has been over the past five years, it is most helpful to turn to real dollar amounts. Between January of 2017 and September of 2018, North Korea is estimated to have stolen $571 million from cryptocurrency exchanges.[30] From 2019 to November of 2020, the number dropped to $316 million, but this statistic is still staggering when compared to the country's revenue from official exports, which totaled a mere $89 million in 2020.[31] In 2021, North Korean hackers successfully stole nearly $400 million in cryptocurrency, and as referenced earlier, the country has already stolen an estimated $1 billion from DeFi protocols as of August of 2022.[32] These numbers certainly raise alarm, especially in light of the country's continuously expanding nuclear weapons program, which,

---

[28] *Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators*, U.S. DEP'T JUSTICE (Jul, 19, 2022), https://www.justice.gov/opa/pr/justice-department-seizes-and-forfeits-approximately-500000-north-korean-ransomware-actors?mkt_tok=NzEwLVpMTC02NTEAAAGFvFgo66jTOL7xvecSin27m5dwjBRUCDjCb5BO8B4z_XSlbjZyJx826WjiCzuRW2oNFgbJRqvpKQ1g36gKFz0.

[29] Michelle Nichols, *North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report*, REUTERS (Aug. 5, 2019, 2:28 PM), https://www.reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX.

[30] *See* Choe Sang-Hun et al., *How North Korea Used Crypto to Hack Its Way Through the Pandemic*, N.Y. TIMES (June 30, 2022), https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html#:~:text=Its%20hackers%20are%20accused%20of,from%202019%20to%20November%202020.

[31] *Id.*

[32] Ji Da-gyum, *supra* note 17.

according to the Korea Institute for Defense Analyses in Seoul, tested a record number of missiles in 2022, costing the country $620 million.[33]

As shocking as these values may seem, the 2022 crypto crash has undeniably had an extremely detrimental impact on the profitability of these heists. One source notes that the recent crash has "wiped out millions of dollars in funds stolen by North Korean hackers . . . threatening a key source of funding for the sanctions-stricken country and its weapons program[s]."[34] According to Chainanalysis, a New York-based blockchain analytics firm, $170 million in old, unlaundered North Korean crypto holdings has decreased in value to $65 million since the beginning of 2022, illustrating how gravely impactful this year's crypto crash has been.[35] Further, according to U.S. authorities, if the aforementioned attack on project Ronin by the Lazarus Group were to happen today, the group would have stolen a meager $230 million in Ethereum, nearly a third of what was stolen earlier this year.[36]

Despite the ongoing economic crisis, the Korea Institute for Defense Analyses notes that North Korea plans to resume nuclear testing.[37] These plans beg the question: how will the DPRK pay for it? According to South Korean government sources, the plunge in crypto value may affect the DPRK's plans for funding the program, meaning that the country may turn to alternative revenue streams, like attacks on traditional currency systems.[38] Aaron Arnold of the Royal United Services Institute (RUSI) think-tank in London asserts that the crash of the crypto market will have little impact on North Korea's nuclear program, as Pyongyang has larger sources of funding that it can rely on, like the continued smuggling of coal and other major exports

---

[33] Josh Smith, *Crypto crash threatens North Korea's stolen funds as it ramps up weapons tests*, REUTERS (June 29, 2022, 9:03 AM) https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

banned by Security Council resolutions to countries like China.[39] From another angle, an Indian software firm's cybersecurity division reports that North Korea may be ramping up attacks on conventional banks, as evidenced by an increase in phishing emails received in recent months.[40] However, according to Chainanalysis, North Korea's crypto behavior has not changed in a major way since the crash, and analysts do not expect that crypto heists will slow down any time soon.[41] North Korean hackers are well renowned for their sophisticated laundering techniques, and according to a Center for a New American Security (CNAS) author, they are also known to wait out rapid dips in the crypto market before converting these funds to cash.[42] This information suggests that North Korea may feel very little impact from the 2022 crypto crash and. Therefore, there is pressing demand for legitimate policy action, not a reliance on economic downturn, to solve the problem.

B. Thwarting Crypto Heists: A Modern Approach

It has become plainly evident, based on the information from the last five years alone, that North Korea has contrived an extremely effective strategy of evading its economic sanctions. Due to the profitability of cryptocurrency thieving, the DPRK has continued to fund its nuclear missile program as if it were not harshly sanctioned by the United States, the United Nations, and the European Union. North Korea's immensely successful crypto heisting enterprise is the product of an issue that is two-fold. On the one hand, the nature of a decentralized system of currency gives rise to transparency and accountability issues, which, for individuals with the proper experience, provide the innate benefit of incognito and anonymity. There is no denying that a large part of North Korea's success in this space has been the product of its natural characteristics. On the other hand, the policy decisions, or lack thereof, by countries most concerned with North Korea's nuclear program and most intimately involved with the development of cryptocurrency as a legitimate

---

39 Josh Smith, *supra* note 17.
40 *Id.*
41 *Id.*
42 *Id.*

system of decentralized currency have allowed the country to take total advantage of the transparency issues inherent to such a system. Therefore, while it would be foolish to assert that the prevalence of crypto theft is an issue born exclusively of failed policy, it would be even more unwise to decree that, due to the nature of the crypto space, any effort to thwart bad actors through regulatory changes would be in vain. In fact, quite the opposite is true, as the only way bad actors in the crypto space are stopped or brought to justice is through the implementation of sound policy.

Going forward, this comment will focus on the specific strategies employed by North Korean cyber operatives to exploit the lack of regulation around decentralized finance platforms and the steps that need to be taken by the United States and the United Nations to better regulate them. First, it will argue in favor of several amendments to existing UN sanctions so that they more explicitly address and punish entities that are directly or indirectly supporting North Korea's cybercrime efforts. Next, it will call for a U.S. strategy that not only strengthens the security of its domestic exchanges but also bolsters international regulations and promotes a universal system of licensing for all companies that process cryptocurrency. Further, it will explore the need for a permanent division within the Justice Department for the purpose of facilitating seizures of cryptocurrency and tracing down crypto heists, both successful and unsuccessful, by actors at home and abroad. Finally, it will argue in support of a third-party intelligence agency to be created through a multilateral treaty or through one between the United States and South Korea. This arrangement would allow for North Korea's maneuvers within the cyber space to be more acutely monitored so that state-sponsored hackers could be more effectively exposed and brought to justice.

II. BACKGROUND

A. The Meteoric Rise of Cryptocurrency

The idea of "cryptocurrency" was originally conceptualized in the 1980s by an American cryptographer, David Chaum. Chaum published a paper about a digital, untraceable currency that could be

sent and received without using a centralized bank.[43] It was not until over 40 years later, however, that the cryptocurrency market would take shape with the help of Satoshi Nakamo, a pseudonym person or persons who purchased Bitcoin.org in 2008 and mined the first block of Bitcoin in 2009.[44] In the early 2010s, when compared to today's price, Bitcoin still had extremely minimal value, but the coin grew exponentially over a four year period, from just pennies in 2010 to several hundred dollars by the end of 2014.[45] During this time, the crypto market began to diversify as numerous other cryptocurrencies, such as Litecoin, entered the market.[46] From 2014 to 2016, in response to a number of scams and thefts, the security of the most popular cryptocurrency exchanges was drastically improved.[47] Also during this time, the use of a virtual "crypto-wallet" became a standard practice for most traders.[48] In the two-year period between 2016 and 2018, Bitcoin's price rose with unprecedented speed, going from $434 in 2016 to just shy of $20,000 in December of 2017. Ethereum also quickly emerged as the second most popular coin during this period.[49] Throughout 2018, the price of Bitcoin dropped drastically, in large part due to financial regulations and security concerns resulting from exchange hacks, valuing at a mere $3,700 by the end of the year.[50] Throughout 2020 and 2021, primarily due to large investments in Bitcoin by companies like MicroStrategy and Tesla, the price of Bitcoin surged, reaching a record high value of $69,000 in November of last year.[51]

Since the beginning of 2022, the price of Bitcoin, like many other cryptocurrencies, has rapidly declined in what many are calling

---

[43] Evan Jones, *A Brief History of Cryptocurrency*, CRYPTO VANTAGE (Sept. 21, 2022), https://www.cryptovantage.com/guides/a-brief-history-of-cryptocurrency/.

[44] Wayne Duggan, *The History of Bitcoin, the First Cryptocurrency*, U.S. NEWS (Aug. 31, 2022, 3:21 PM) https://money.usnews.com/investing/articles/the-history-of-bitcoin.

[45] Evan Jones, *supra* note 43.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Evan Jones, *supra* note 43.

the "2022 Crypto Crash".[52] The price of Bitcoin has fallen by at least 60 percent ($23,000) while Ethereum has plummeted by an enormous 75 percent ($1,500).[53] It is estimated that from May to June, cryptocurrencies have lost approximately $1 trillion in total value.[54] Many are attributing the crash to anti-inflation measures, which have led to rising interest rates and a tightening of the money supply.[55] The volatile state of the global economy as a result of the Covid-19 pandemic has undoubtedly contributed greatly to the crash as well.[56] This enormous blow to the value of major cryptocurrencies has been devastating for millions of investors, mining companies, and crypto-thieves, too.[57] While the crash has certainly done its part in deterring crypto thieves from continuing their attacks, there are a number of key policy measures that have been effective as well.

B. The Evolution of Crypto Regulation: Home and Abroad

In the early years of cryptocurrency, few governments expressed concern for market regulation, but as the exchanges grew and more people invested, it became an unavoidable necessity.[58] Now, detailed and extensive regulations of crypto exchanges, currencies, users, and more have become commonplace in many countries and even on a global scale. In the United States, there are numerous federal

---

[52] Jessica Sier et al., *What caused crypto to crash this time (in five charts) and will it survive?*, FINANCIAL REVIEW (Aug.1, 2022, 7:00 AM), https://www.afr.com/technology/what-caused-crypto-to-crash-this-time-in-five-charts-and-will-it-survive-20220711-p5b0ps.

[53] *Id.*

[54] Ruth Strachan, *Can Bitcoin miners recover from the 2022 crypto crash?* INVESTMENT MONITOR (Aug. 5, 2022, 9:52 AM), https://www.investmentmonitor.ai/crypto/bitcoin-miners-recover-crypto-crash-2022.

[55] Kevin Voigt et al., *How to Navigate a Crypto Crash in 2022*, NERD WALLET (Sept. 23, 2022), https://www.nerdwallet.com/article/investing/crypto-crash.

[56] Forbes Staff, *Bitcoin's Coronavirus Crash; Blockchain In A Pandemic*, FORBES (Mar. 15, 2022, 9:00 AM), https://www.forbes.com/sites/cryptoconfidential/2020/03/15/bitcoins-coronavirus-crash-blockchain-in-a-pandemic/?sh=ffd61982a5bf.

[57] Ruth Strachan, *supra* note 54.

[58] *The evolution of cryptocurrency and regulations since the inception of Bitcoin*, ETN-NETWORK, https://news.electroneum.com/the-evolution-of-cryptocurrency-and-regulations-since-the-inception-of-bitcoin (last accessed Oct. 21, 2022).

agencies that are tasked with imposing cryptocurrency laws and regulations, including the Securities and Exchange Commission (**SEC**), the Commodity Futures Trading Commission (**CFTC**), the Federal Trade Commission, the Department of the Treasury, the Internal Revenue Service (**IRS**), the Office of the Comptroller of the Currency (**OCC**) and the Financial Crimes Enforcement Network (**FinCEN**).[59] However, despite the large number of agencies involved in cryptocurrency, very few official rules have been formally drafted.[60] In fact, most U.S. laws on cryptocurrency are proposed or passed at the state level.[61] Cryptocurrency is only subject to regulation in the U.S. when it constitutes a security, which includes "an investment contract" as defined under *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).[62] Following the precedent established by *W.J. Howey Co.*, the SEC will evaluate the substance of a transaction to determine whether a cryptocurrency is an "investment contract" and therefore subject to regulation under the Securities Act.[63]

If the SEC does determine that a digital currency is a security, the currency's issuer must register it with the SEC.[64] Once a cryptocurrency is determined to constitute a security, for that coin to be traded or sold, two requirements must be met.[65] First, the SEC requires that the currency's broker-dealer be licensed with the SEC and also be a member of the Financial Industry Regulatory Authority (FINRA).[66] Second, the currency can only be traded on a "licensed securities exchange of alternative trading system" ("ATS") approved by the SEC.[67] Unfortunately, very few cryptocurrencies are traded on

---

[59] Joe Dewey et al., *Blockchain & Cryptocurrency Laws and Regulations 2022 USA*, GLOBAL LEGAL INSIGHTS,https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa#:~:text=Sales%20regulation,-Back%20to%20top&text=The%20sale%20of%20cryptocurrency%20is,MSB%E2%80%9D)%20under%20Federal%20law (last accessed Oct. 21, 2022).

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] Joe Dewey et al., *supra* note 59.

[66] *Id.*

[67] *Id.*

ATS platforms, even though the SEC's Chair Gary Gensler has publicly stated that "most cryptocurrencies are securities" and would therefore be subject to the SEC's regulation requirements.[68] Gensler has gone on to publicly state that because most crypto tokens are securities and because so few are registered with the SEC, most of them are operating illegally.[69] However, the SEC has lagged behind with respect to prosecuting these cryptocurrencies, meaning that many continue to operate under very minute regulatory pressure.[70] There have also been issues with the process of harmonizing traditional securities laws as applied to stocks and bonds, for example, and those that would apply to a currency system that does not depend on intermediaries.[71]

With respect to cryptocurrency exchanges—or digital marketplaces that permit users to buy, sell, and trade cryptocurrencies,[72]—the FinCEN is in charge of regulation, as required under the Bank Secrecy Act.[73] Specifically, the Financial Crimes Enforcement Network (FINCEN), applies the Bank Secrecy Act to regulate money service businesses (MSBs).[74] According to the guidelines issued by FinCEN in March of 2013, virtual currency exchanges and persons who issue and redeem virtual currency from a central repository are considered MSBs.[75] Further, all MSBs that are money transmitters are required to conduct a risk assessment for

---

[68] Tobi Opeyemi Amure, *Most Cryptocurrencies Are Securities, Says SEC Chair*, INVESTOPEDIA (Sept. 8, 2022), https://www.investopedia.com/gensler-on-crypto-6544288#:~:text=U.S.%20Securities%20and%20Exchange%20Commission%20Chair%20Gary%20Gensler%20said%20most,and%20other%20crypto%2Drelated%20issues.

[69] Scott Nover, *The head of the SEC says most cryptocurrencies are operating illegally*, QUARTZ (Sept. 8, 2022, 5:18 PM), https://qz.com/the-head-of-the-sec-says-most-cryptocurrencies-are-oper-1849513471#:~:text=The%20SEC%20says%20most%20cryptocurrencies%20are%20unregistered%20securities.

[70] *Id.*

[71] Joe Dewey et al., *supra* note 59.

[72] *Id.*

[73] *Id.*

[74] *Fact sheet on MSB Registration Rule*, FINCEN https://www.fincen.gov/fact-sheet-msb-registration-rule (last accessed Nov. 18, 2022).

[75] Joe Dewey et al., *supra* note 59.

exposure to money laundering and to implement an anti-money laundering (AML) program accordingly.[76] This is a requirement of FinCEN that further demands these MSBs to "develop, implement, and maintain a written program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities."[77] The AML program is quite exhaustive, requiring that the MSB assure compliance through written policies and a designated compliance officers in addition to personnel training.[78]

Another governmental department that specializes in anti-money laundering efforts is the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), which has formulated the Specially Designated Nationals and Blocked Entities List (SDN List). The SDN List includes a record of certain individuals and companies who are engaging in transactions with sanctioned countries.[79] This list must be followed by all U.S. citizens engaged in the business of money transmission.[80] The SDN is an extensive sanction list that has played an increasingly key role in combating money laundering, especially within the cryptocurrency sector recently.

With the rise of DeFi platforms since 2018, it has become significantly more difficult for the U.S. to combat money laundering strategies employed by individuals, companies, and governments both at home and abroad, as they now have the capability to make anonymous trades using decentralized currencies on platforms that enforce little to no vetting process or customer ID requirements.[81] The most prominent and relevant example of this is the cryptocurrency mixer named Tornado Crash, which in August of 2022 was sanctioned by the OFAC for its service that allowed users to send unvetted funds to their mixer in exchange for a cryptographic note that could be used

---

76 *Id.*
77 *Id.*
78 *Id.*
79 *Id.*
80 *Id.*
81 Joe Dewey et al., *supra* note 59.

to withdraw their mixed funds to a new address.[82] Most notoriously, OFAC exposed Tornado for its critical role in the laundering of over $455 million worth of cryptocurrency from the aforementioned Axie Infinity's Ronin Bridge Protocol.[83]

Outside of cryptocurrency mining and taxation, the policies and organizations mentioned above are largely the extent to which the U.S. government regulates domestic exchanges and transactions at the federal level. The only exception to this is the Market Integrity and Major Frauds Unit (MIMF) within the Department of Justice.[84] The MMIF Unit was specially created in order to prosecute events of fraud and market manipulation that involve cryptocurrency.[85] The Unit has been highly successful in prosecuting individuals found guilty of stealing funds from investors both in the U.S. and abroad, charging over $2 billion to defendants since 2019 alone.[86] The strategies of the MMIF are of great importance to this comment because they utilize blockchain data analytics to uncover unregistered cryptocurrency exchanges involved in fraud schemes, which is something this comment calls for on a global scale through an international enforcement regime.[87] An example of the effectiveness of this strategy came to light on November 7, 2022, when the DOJ announced a historic $3.36 billion cryptocurrency seizure in connection with a dark web fraud.[88]

At the state level, numerous states have passed extensive legislation with respect to cryptocurrencies and blockchain technology.[89] But because in the United States there is no universal definition for the terms "cryptocurrency," "digital assets," and so on,

---

[82] *Id.*

[83] *Id.*

[84] *Market Integrity and Major Frauds Unit*, U.S. DEP'T JUSTICE (Sep. 26, 2022), https://www.justice.gov/criminal-fraud/crypto-enforcement.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Cryptocurrency Laws and Regulations by State*, BLOOMBERG LAW (May 26, 2022), https://pro.bloomberglaw.com/brief/cryptocurrency-laws-and-regulations-by-state/.

the number of restrictions and protocols that are legislated varies greatly from state to state.[90] And while stronger, more universal state regulation may play an important role in combating domestic crypto heisting, it will do little to prevent the attacks carried out by North Korea, especially because the large majority of the crypto exchanges that fall victim to these heists operate outside of the United States. This is clearly an issue of international significance, but unfortunately, little to no international regulation currently exists with respect to cryptocurrency, meaning that state actors do not have the tools necessary to thwart the actions of the DPRK.

The United States is by no means the only country that has made an effort to establish a large number of domestic regulations around cryptocurrency and crypto exchanges. In fact, most European and Nordic countries have considerable crypto regulation, especially with respect to crypto exchanges and firms.[91] France, for example, has adopted the Financial Market Authority (AMF), which subjects crypto firms to mandatory registration with the government and stricter "Know Your Customer" (KYC) regulations.[92] The AMF also imposed new requirements that prohibit anonymous accounts from being created on crypto exchanges.[93] Both exchanges and firms are subject to AML requirements.[94] Germany has also been a prominent regulator of crypto since the early days, requiring that all buying, selling, and trading of crypto-assets be done through licensed exchanges and that all firms be licensed with the German Federal Financial Supervisory Authority.[95] And in the UK, crypto exchanges are required to register with the UK Financial Conduct Authority (FCA), the authority that has also banned the trading of cryptocurrency derivatives outright.[96] Additionally, the UK does not consider cryptocurrencies to be legal

---

[90] *Joe Dewey et al., supra note 59.*

[91] Susannah Hammond et al., *Cryptocurrency regulations by country*, THOMAS REUTERS (2022).

[92] *Id* at 14.

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id* at 23.

tender, meaning that it is treated like a foreign currency for most purposes and subject to considerable taxes.[97]

The Nordic countries are also highly regulatory of crypto exchanges. Sweden's Financial Supervisory Authority (FSA) has imposed registration requirements through the Swedish Currency Exchange Act, which requires that wallet providers and providers of virtual currency exchange services comply with the country's AML provisions.[98] Similarly, Norway's Ministry of Finance has established regulations of virtual currency exchanges and storage services in an effort to combat money laundering via exchanges that convert cryptos to fiat currency.[99]

Based on the exhaustive nature of the regulations enacted in these countries, it is clear that western Europe is just as concerned about crypto as the U.S. is, especially within their own borders. And while there is little evidence to suggest that China and North Korea have ever seriously considered enacting any crypto regulation, they certainly do not speak for all of Asia. Japan is commonly described as having one of the most advanced regulatory schemes for crypto in the world.[100] The government requires that all exchanges be registered and comply with the AML and Combating the Financing of Terrorism (CFT) Regulations.[101] Further, the country has enacted the Payment Services Act (PSA) and the Financial Instruments and Exchange Act (FIEA), which regulate crypto derivatives trading and crypto custody service providers.[102] More impressively, Japan became the first country to create self-regulatory bodies in 2020: the Japanese Virtual Currency Exchange Association (JVCEA) and the Japan STO Association, which together promote compliance with regulations.[103] Since 2021, South Korea has also made significant efforts in the realm of crypto

---

97 *Id.*
98 *Id* at 21.
99 *Id* at 19.
100 *Id* at 26.
101 Susannah Hammond et al., *supra* note 91, at 26.
102 *Id.*
103 *Id.*

regulation, due in large part to several large exchange hacks.[104] Like many other countries, these regulations were passed to strengthen AML regulation and obligations for crypto service providers.[105] The regulations also require these providers to register with the Korean Financial Services Commission.[106]

The efforts by Japan and South Korea alone reflect that North Korea does not represent the position of Asia with respect to crypto regulation in the slightest. In fact, the data on crypto regulations by country suggests that the large majority of developed nations have made at least some effort to regulate crypto, whether that is with respect to exchange regulation, tax policy, or AML enforcement. The prevalence of and similarities between crypto regulations enforced by countries all across the world are unsurprising. It is clear that KYC, AML, and crypto exchange registries have been highly successful at the domestic level for the dozens of countries that have implemented them. However, it is also clear that, due to the anonymity, speed, and interconnectedness of cryptocurrency exploitation, domestic policy by itself is incapable of quelling the tactics of well-equipped state actors. And yet, the international community has failed to establish any agreement, treaty, or regime that would begin to implement these types of regulations on a global scale.

Outside of the sanctions imposed on North Korea by the United Nations and the European Union beginning in 2006, few to no recognizable efforts have been made by the international community to enforce anything specifically related to cryptocurrency in general or more specifically against North Korea. In the last few months, however, the European Union has taken its first steps towards regulating cryptocurrency with the introduction of a new crypto regulation legislation called Markets in Crypto-Assets (MiCA).[107] MiCa, on its surface, appears to be exactly what this comment argues for: an

---

104 *Id* at 29.

105 *Id.*

106 *Id.*

107 *Cryptocurrency Alert*, AKIN GUMP STRAUSS HAUER & FELD LLP (Oct. 27, 2022), https://www.akingump.com/a/web/pFc2jfvKX3HSkiqm2GvDri/4FGDpY/cryptocurrency-alert.pdf.

attempt at a global, harmonious regulation of cryptocurrency markets.[108] The primary purpose of the bill is to regulate money laundering, promote consumer protection, and ensure crypto company accountability across the globe.[109] What is most important about the proposed bill is its emphasis on "transparency, disclosure, authori[z]ation and supervision of transaction."[110] While a large focus of MiCa is ensuring that the consumer is informed of all the risks, costs, and charges associated with crypto assets, it also introduces measures "to tackle market manipulation and prevent money laundering, terrorist financing and other criminal activity."[111] MiCa's authority also directly applies to persons engaged in the provision of crypto-asset services, meaning that the regulation would include crypto trading platforms and exchanges.[112] MiCa will create, what is in essence, a registry for authorized crypto-asset service providers, otherwise known as "CASPs," which will require these persons to meet particular compliance criteria before they are permitted to provide their services within the EU.[113] MiCa certainly looks promising, as it touches on some of the most important areas for combating the shroud of DeFi and the lack of accountability for exchanges.

While the European Union has made waves with this newly approved crypto-assets regulation, it is certainly not all-encompassing or globally applicable. It does undoubtedly make the EU the world leader for international cryptocurrency regulation, however, as the United States, the United Nations, and other countries have offered little insight on how to move forward. The UN did have a conference on trade and development in August of 2022 during which cryptocurrency was a central topic, but its main focus was the risks and costs of crypto in developing nations, not the methods to introduce international regulation of crypto exchanges. [114] This conference,

---

108 *Id* at 1.

109 *Id.*

110 *Id.*

111 *Id* at 2.

112 *Cryptocurrency Alert*, *supra* note 107, at 2.

113 *Id* at 3.

114 Alex Pugh, *UN calls for comprehensive crypto regulation in developing countries*, FINTECH FUTURES (Aug. 15, 2022), https://www.fintechfutures.com/2022/08/un-calls-for-comprehensive-crypto-regulation-in-developing-countries/#:~:text=

officially known as the United Nations Conference on Trade and Development (UNCTAD) called on these developing nations to introduce many of the same key regulations implemented by developed nations with respect to crypto exchanges, digital wallets, and other aspects of decentralized finance.[115] So, while the UN has yet to legislate any actionable policy, if it can promote to developing nations the importance of implementing crypto regulation, it would serve not only to help their domestic economy in the short term but also to bolster international security in the long run.

C. Dissecting the DPRK: Government, Economy, and Cyber Infrastructure

When North Korea is so often depicted as agrarian, developing, or a "nuclear weapons state", it certainly comes as a shock to hear that the country has a remarkably advanced cyber infrastructure that has proven to be capable of causing billions of dollars in damage to companies, individuals, and governments all over the world in just a few short years. The DPRK's cyber infrastructure, like its nuclear program, has been funded largely by illicit, sanction-evading strategies.[116] And while these strategies have changed over time, especially recently with the rise of crypto, former member of the North Korea Panel of Experts at the United Nations Security Council, Stephanie Kleine-Ahlbrandt, notes that North Korea has long relied on illicit funding methods of this nature.[117] She notes also that the decision by Kim Jong Un's regime to develop the government's cyber capabilities aligns closely with its nuclear military strategy, which "aims to overcome its relative conventional military inferiority."[118]

The government of North Korea places great emphasis on its military preparedness, and a significant portion of the economy is

---

It%20calls%20on%20developing%20nations,financial%20institutions%20from%20holding%20crypto.

115 *Id.*

116 Eun DuBois, *Building resilience to the North Korean cyber threat: Experts discuss*, BROOKINGS (Dec. 23, 2020), brookings.edu/blog/order-from-chaos/2020/12/23/building-resilience-to-the-north-korean-cyber-threat-experts-discuss/.

117 *Id.*

118 *Id.*

contributed toward military spending to ensure a high level of preparedness.[119] Since the leader of Kim Jon Il in the late 1990s, one of North Korea's central goals has been to build a strong military, and this has remained the case under the leadership of Kim Jong Un.[120] In fact, the most recent estimates project that the DPRK may have the material for over 100 nuclear weapons and that it has tested missiles capable of striking the United States with a nuclear warhead.[121] Further, North Korea's military is ranked as the fourth largest in the world, with over 1.2 million personnel and a growing number of ballistic missile tests, despite continued sanctions by the West.[122] In fact, just at the beginning of November, 2022, it was reported that North Korea fired a minimum of 23 missiles into the sea near South Korea's coast.[123] The military, at least as it is classically defined, is by no means the only focus of the DPRK. According to the former director of South Korea's National Intelligence Service, Nam Jae-joon, Kim Jong Un himself has equated the importance of developing cyber capabilities to that of nuclear power and has claimed that "cyber warfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our [North Korea's] military's capability to strike relentlessly."[124]

Kim Jong Un's emphasis on cyber capability as a military weapon (and not a social tool) is most obviously reflected in the country's network infrastructures, which leave the vast majority of its citizens without Internet access, and even those that are sufficiently "elite" to be given access are given an extremely limited one.[125] In

---

[119] The Editors of Encyclopedia Britannica, *North Korea Government and Society*, BRITANNICA, https://www.britannica.com/topic/Democratic-Party-of-Korea (last accessed Nov. 18, 2022).

[120] *Id.*

[121] CFR.org Editors, *North Korea's Military Capabilities*, COUNCIL ON FOREIGN RELATIONS (June 28, 2022, 11:40 AM), https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities.

[122] *Id.*

[123] *Id.*

[124] Jason Bartlett, *Why Is North Korea So Good at Cybercrime?* THE DIPLOMAT (Nov. 13, 2020), https://thediplomat.com/2020/11/why-is-north-korea-so-good-at-cybercrime/.

[125] Donghui Park, *North Korea Cyber Attacks: A New Asymmetrical Military Strategy*, HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES (June 28, 2016),

addition to infrastructural investments for cyber development, the DPRK has heavily invested in finding, educating, and training cyber experts so that they are capable of hacking, attacking, and exploiting infrastructures all over the world, with a primary focus on the U.S. and South Korea.[126] This includes both training programs within the military and the funding of universities within Pyongyang that specialize in technology.[127] A headline from the Daily NK from May, 2022 best illustrates this recruiting strategy that has been ongoing for over 30 years.[128] The article reports that 100 of the best graduates from the top tech schools in the country have been recruited to the military shortly after Kim Jong Un mentioned the deployment of "a 'new strategic weapon"'.[129] Furthermore, it is alleged that North Korea has cooperated with China, Russia, Iran, and other "few friendly countries" in an effort to improve its cyber capabilities by sending students abroad to receive additional training.[130] Although there are few sources available, it is believed that these specially trained cyber operatives are headquartered in the Reconnaissance General Bureau (RGB), which serves as a central hub for the DPRK's covert military operations.[131] It is estimated that between 3,000 and 6,000 North Korean hackers have been fully trained and now serve as staff for the RGB, or the Korean People's Army (KPA).[132]

The majority of the most complete literature focuses on cyberattacks conducted by, or alleged to have been conducted by, North Korea, rather than instances of crypto heisting, but it is still important to understand the ways in which these attacks are traced back to the DPRK. The most prominent example is the infamous

---

https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/.

126 *Id.*

127 *Id.*

128 Jeong Tae Joo, *Around 100 Top Technology University Graduates Join Military*, DAILY NK (May 15, 2020, 1:30 PM), https://www.dailynk.com/english/around-100-top-technology-university-graduates-join-military/.

129 *Id.*

130 *See* Donghui Park, *supra* note 125.

131 Emma Chanlett-Avery et al., CONG. RSCH. SERV., R44912, NORTH KOREAN CYBER CAPABILITIES: IN BRIEF (2017).

132 *Id.*

WannaCry attack from 2017 that was discussed earlier.[133] Here, the NSA was able to trace this attack back to North Korea's RBG via a Chinese IP address that was known to be used by the RBG.[134] While this attack happened six years ago, it stole the digital asset Bitcoin, $140,000 of which were left unconverted to hard cash.[135]

It is clear that North Korea's economy has suffered from both the ongoing, harsh economic sanctions and the substantial, global hikes in inflation since the beginning of 2022. However, it is also clear that this economic downturn has not been realized within the DPRK's military or its cyber infrastructure, as the government has continued to test more nuclear missiles and deploy more cyberattacks without skipping a beat. The only thing that remains unclear is whether and to what degree concerned nations will work together in the international community to legislate a functional solution to the problem.

III. ANALYSIS

A. The Impact of Sanctions on DRPK's Funding Strategies

As we have seen over the past sixteen years, the economic sanctions imposed by the United Nations and the European Union have had significantly less impact on North Korea's ability to harass, abuse, and exploit both private and public infrastructure outside of it borders than expected. North Korea's ability to forge on in light of these sanctions reflects a long history of masterful sanction evasion, and at the same time, calls for an alternative strategy to be employed to stop this behavior. In the new age of decentralized markets, we must implement enforcement mechanisms that regulate not just the buying and selling of physical goods or the use of the conventional banking system but also the selling, trading, and exchanging of digital currency.

One of the primary ways by which North Korea evades sanctions through the use of cryptocurrency is in non-banking sectors, or Designated Non-Financial Businesses and Professions (DNFBPs),

---

133 *See Cyber-attack: US and UK blame North Korea for WannaCry*, *supra* note 22.
134 *Id.*
135 *Id.*

which are industries that exist outside the financial sector, making them a primary target for money laundering.[136] The business most commonly considered to be DNFBPs are: gambling services, insurance, high-risk corporates, real estate, independent legal services, precious metals/stones trade, trust and investment funds, external audit and accounting, and lending.[137] In recent years, the use of cryptocurrency in DNFBPs has grown dramatically, and North Korea's involvement in this scheme is made most obvious through examples such as Kim Jong-Un's possession of a yacht[138], which indicates a flagrant evasion of DPRK sanctions against luxury goods as imposed by the UN.[139] North Korea has been known to use this sector in the past, specifically in its 2016 Bangladesh Bank Heist which involved the laundering of $81 million through the gambling sector.[140] And now that many casinos accept both fiat currency and cryptocurrencies and permit bank transfers, there exists the possibility that crypto-jackers can launder their illegitimate through these casino services.[141] Furthermore, with the emergence of cryptocurrency and DeFi platforms, money laundering schemes will be undoubtedly become more common and more difficult to track down.

While some measures have been put in place by organizations operating internationally, such as the Financial Action Task Force (FATF)[142], these measures are not harsh enough, as they give a great deal of deference to DNFBP businesses who are expected to express

---

136 *What Is DNFBP?*, DEP'T OF COMMERCE & INVESTMENT, https://www.dci.gov.ky/what-is-dnfbp (last accessed Nov 18, 2022).

137 *Designated Non-Financial Businesses and Professions: FinTech Are Not the Only Ones to Care About AML*, THE SUMSUBER (Oct. 24, 2021), https://sumsub.com/blog/designated-non-financial-businesses-and-professions/.

138 Sasha Erskine et al., *Compliance Harmony: How North Korean Cryptocurrency Abuse Is Expanding*, RUSI (Jul. 14, 2022), https://rusi.org/explore-our-research/publications/commentary/compliance-harmony-how-north-korean-cryptocurrency-abuse-expanding.

139 *Id.*

140 *Id.*

141 *Id.*

142 *The Financial Action Task Force*, FINANCIAL CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/resources/international/financial-action-task-force (last accessed Nov 18, 2022).

"due diligence" in complying with the FATF requirements.[143] Rather, the FATF should require that all cryptocurrency transaction that exceed $1000 be reported, subject to a $500 fine if the exchange is not reported within thirty days. Further, this requirement should become internationally mandated through a larger treaty rather than applying only to the thirty-two countries that have become members of the FATF.[144] A multilateral treaty would be a highly effective tool for moving global crypto regulation in the right direction, as it would create a system of actionable accountability for all member states. It would also serve to establish an inter-governmental policymaking body that would focus specifically on legislating international standards for crypto-related financial crimes. This policymaking body could, and probably should, possess the ability to threaten sanctions or fines for non-compliance with "FATF-type" regulations and policies, including (but not limited to): failure to implement domestic, crypto-oriented AML regulations, failure to prosecute or extradite known crypto-thieves or cyber operatives involved in state-sponsored crypto heisting or laundering, and failure to review the compliance of crypto exchanges with AML requirements at regular intervals chosen by the policymaking body.

The treaty may also require member states to impose harsher taxes on cryptocurrency when it is processed or converted into traditional currency. And it will also be in the policymaking body's best interest to enforce measures for the purpose of countering tax evasion in the crypto space. Taking the U.S. Treasury for example, there currently exist serious problems with cryptocurrency and tax evasion, and the department is combatting these by requiring all transfers of cryptocurrency assets worth $10,000 or more to be reported to the IRS.[145] In addition to higher taxes, which will cut into the profitability of crypto laundering, obligatory reporting of crypto asset transfers above a certain dollar amount to the international governing body will

---

143 Sasha Erskine et al., *supra* note 138.

144 *The Financial Action Task Force*, *supra* note 142.

145 Thomas Franck, *U.S. Treasury calls for stricter cryptocurrency compliance with IRS, says they pose tax evasion risk*, CNBC (May 20, 2021, 4:03 PM), https://www.cnbc.com/2021/05/20/us-treasury-calls-for-stricter-cryptocurrency-compliance-with-irs.html.

greatly bolster transparency. Further, the treaty could require that any business involved in the processing of cryptocurrency operating within the borders of a member state to apply and be approved by the "FATF-type" policymaking body before they are permitted to operate within the borders of any member state, much like the requirement for cryptocurrency brokers to register with the SEC before they can operate in the United States.[146]

While "FATF-type" regulations would make up only a portion of a multilateral treaty imposed for the purpose of crypto regulation, it would certainly be an important one, as it would serve to directly combat and punish money laundering, terrorist financing, and so on. It would also play a major role in bolstering the transparency of cryptocurrency transactions throughout the world by requiring harsher and more harmonious regulation standards of all member states.

With respect to the current sanctions imposed upon North Korea, it is evident that their effectiveness has been severely undermined by the DPRK's ability to exploit the crypto market. In order to combat this, the international community must work together to enforce stricter sanctions that will hinder the country's access to cryptocurrency, and by doing so, its ability to fund a nuclear program. Over the past decade, there have been several occasions upon which the U.S. Treasury has taken drastic measures to sanction particular cryptocurrencies and cybergroups that maliciously use them.[147] One prominent example of this occurred in September of 2019 when the U.S. Treasury's Office of Foreign Assets Control (OFAC) specifically sanctioned three cyber groups operating within and being supported by North Korea.[148] One of these groups was the aforementioned

---

146 *See* Joe Dewey et al., *supra* note 59.

147 *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. DEPT. TREASURY (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.

148 *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, U.S. DEPT. TREASURY (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774.

Lazarus Group, which was responsible for both the 2017 WannaCry 2.0 ransomware attack and the attack on project Ronin in 2022.[149]

These sanctions were imposed upon North Korea in addition to and in accordance with Executive Order 13722, which enforced blocks upon government and the Workers' Party of North Korea for the primary purpose of hindering the country's pursuit of a more developed nuclear and missiles program.[150] More specifically, E.O. 13722, which was imposed upon North Korea in March of 2016, prohibits imports and exports of several goods and services, including financial services and technology.[151] It also prohibits new investment and financing in North Korea by U.S. persons.[152] By specifically identifying the Lazarus Group and three other North Korean hacking groups, the OFAC extended the prohibitions of E.O. 13722 to deter these actors from continuing to perpetrate cyber-attacks within the U.S. and abroad. And while it is clear that existing sanctions have been largely ineffective, it is nevertheless an important measure of deterrence for governments to identify and condemn these groups on the world stage.

Three years later, OFAC took an even more direct money laundering counter-measure by sanctioning a cryptocurrency service (or "mixer") known as Tornado Cash for its involvement in the laundering of over $7 billion in virtual currency since 2019, which included $455 million stolen by the Lazarus Group.[153] This action came three months after OFAC's action against Blender.io, a virtual currency mixer routinely used by the DPRK's Lazarus Group to launder cryptocurrency, marking the first-ever sanction on a mixer.[154] This is not the first time the U.S. Treasury has taken action against a business involved in the cryptocurrency market. In September of 2021,

---

149 *See Cyber-attack: US and UK blame North Korea for WannaCry*, *supra* note 22.

150 Exec. Order No. 13,722, 81 C.F.R. 53 (2016).

151 *Id.*

152 *Id.*

153 *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, *supra* note 147.

154 *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. DEPT. TREASURY (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768.

the Department sanctioned a cryptocurrency exchange for an alleged role in the laundering of funds stolen via cyberattack.[155] These enforcement actions, which were carried out in collaboration between OFAC and FinCEN, involved a cryptocurrency exchange called Bittrex, Inc., which was found to have willfully violated the reporting requirements of the Bank Secrecy Act's anti-money laundering (AML) requirements and suspicious activity report reporting requirements (SAR).[156] As a result, the exchange was sued by OFAC and FinCEN for $24 million and $29 million, respectively.[157] This substantial fine, and more broadly, this action by the U.S. government, is a key example of highly effective crypto currency regulation and enforcement at the domestic level. Furthermore, it is the sort of enforcement the most likely can be translated to the global level and retain the same effectiveness.

With respect to the sanctions on cryptocurrency mixers, according to Chainalysis, a "mixer" is a service used to anatomize the origin and owner of crypto funds by blending the currencies of many users together.[158] Further, it was reported in 2022 that ten percent of all illicitly held cryptocurrencies were laundered through a mixer, indicating that mixers have become a key aspect of the crypto laundering process in very recent history.[159] This action by OFAC to sanction Tornado Crash, which marked the second sanction on a virtual currency mixer, was done in accordance with E.O. 13694, which was amended to both block all entities that are fifty percent or more owned by Tornados Crash and also to block all "property and interest in property" of Tornado Crash in the U.S. or in the possession of U.S.

---

155 Lauren Feiner, *U.S. Treasury sanctions cryptocurrency exchange for alleged role in ransomware attacks*, CNBC (Sep. 22, 2021, 7:31 PM), https://www.cnbc.com/2021/09/21/us-treasury-sanctions-cryptocurrency-exchange-suex.html.

156 *Treasury Announces Two Enforcement Actions for over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc.*, U.S. DEPT. TREASURY (Oct. 11, 2022), https://home.treasury.gov/news/press-releases/jy1006.

157 *Id.*

158 *See* Chainanalysis Team, *Crypto Mixers and AML Compliance*, CHAINALYSIS (Aug. 23, 2022), https://blog.chainalysis.com/reports/crypto-mixers/#:~:text=A%20crypto%20mixer%20is%20a,is%20otherwise%20hard%20to%20achieve.

159 *Id.*

persons.[160] The U.S. government has laid the groundwork for the type of crypto-oriented sanctions that will have a meaningful impact on the efforts of cybercriminals to obfuscate their proceeds from heists and other illicit cyber activities, especially if it is enforced through a multilateral treaty with global support.

In accordance with the sanctions already enforced by the U.S., the UN, and the EU, if the member states of these organizations were able to direct themselves as a unified force for the sake of international crypto regulation, there is little doubt that they will be able to make substantial progress in eliminating the most predominant shortcomings within the market. What will play a fundamental role in this process is the ability for governments most well-equipped to moderate cryptocurrency usage within their borders to multilaterally impose sanctions against cyber-criminal groups, virtual currency mixers, exchanges, currency conversion businesses, DNFBPs, and other organizations most commonly involved in the theft and laundering conducted by governments such as North Korea. This could be brought about either by amending UN and EU sanctions as they currently exist, or through the creation of an entirely new international governmental body for the sake of cryptocurrency regulation.

What would likely be the most immediately impactful and achievable step would be to amend the existing sanctions imposed upon North Korea by the United Nations. More specifically, United Nations Security Council Resolution 2270,[161] which was imposed to add new items to the luxury goods ban established by United Nations Security Council Resolution 2094, could be amended to include sanctions on "Designated Non-Financial Business and Professions" (DNFBPs) that are failing to comply with anti-money laundering efforts as applied domestically by the government of any member state.[162] The addition of a DNFB sanction would fit well within Resolution 2270 because these business and professions are composed

---

160 *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, *supra* note 147.

161 S.C. Res. 2270, U.N. Doc. S/RES/2270 (Mar. 2, 2016).

162 S.C. Res. 2094, U.N. Doc. S/RES/2094 (Mar. 7, 2013).

primarily of luxury good vendors, many of which are used by North Korea to evade sanctions with cryptocurrency purchases.[163] These additional sanctions would be imposed in coordination with the "FATF-type" regulations brought about by the ratification of a multilateral AML treaty as explained at the beginning of this section. Alternatively, just as the UN Security Council imposed Resolution 2270 to supplement and extend Resolution 2094, the Council could impose a new Resolution with a specific focus on DNFBPs, especially if it is able to identify particular offenders.[164] While this action will not have a direct effect on North Korea's nuclear missile program, if the UN is able to successfully identify and sanction DNFBPs that are routinely used by North Korea, it will undoubtedly hinder the country's ability to launder money through the exploitation of negligent vendors in this sector. Over time, this will have a drastic impact on the viability of a crypto-oriented funding strategy for the DPRK nuclear missile program.

In addition to DNFBP sanctions, the UN could, like the United States, identify and sanction state-sponsored cyber groups operating within North Korea, such as Lazarus Group," "Bluenoroff," and "Andariel."[165] This would serve to bolster the blocks and prohibitions imposed upon North Korea by the United States. It would also elevate the issue to one of global magnitude and hopefully persuade countries all across Europe and Asia to reform their domestic regulations of the crypto market so that they are better equipped to counter crime conducted by well-equipped, state-sponsored cyber groups. Furthermore, the United States' sanctions on North Korea block all property and interests in property held by entities that are directly or indirectly owned by any of the three listed cyber groups.[166] This extends to all property and interests in property in possession or control of any U.S. person as well, and it requires these persons to report these interests to OFAC.[167] By doing so, the U.S. has put itself

---

163 S.C. Res. 2270, *supra* note 161.

164 *Id.*

165 *Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups*, *supra* note 148.

166 *Id.*

167 *Id.*

in a strong position to prevent, counter, and prosecute any cybercrime conducted by these groups within the United States. If the UN Security Council was able to adopt a similar sanction, this would have a substantial global impact, as it would both motivate all member states to enforce these sanctions domestically and also deter these groups from conducting cybercrime within any member state's borders out of fear of suffering harsher economic limitations.

A final UN sanction amendment or addition that would deliver a substantial blow to North Korea's crypto heisting-tactics would involve the imposition of blocks on cryptocurrency exchanges and mixers that either cooperate with North Korea or neglect KYC, AML, or other licensing and customer identification requirements to a degree such that crypto assets are at risk of being stolen or laundered. What would be most effective is the standardization and universalization of these requirements through UN action, such as the establishment of a regulatory measure like the EU's Markets in Crypto-Assets (MiCA) so that the Security Council can easily identify violations.[168] Once identified, violators would then be subject to sanctions such as those imposed by the United States on virtual currency mixers like Tornado Cash and Blender.[169] Members of the United Nations would then be obligated to enforce these sanctions against any exchange, mixer, or other cryptocurrency related business operating within their country. This would undoubtedly motivate all crypto-related businesses to fully comply with licensing and security requirements, as UN supported sanctions could be economically devastating. As a result of this near-universal compliance, North Korean cyber-crime groups would face a much greater challenge in concealing their identities and bypassing the security of these platforms, which would now follow universally recognized licensing and security requirements.

Regardless of the path taken by the international community with regard to universal crypto policing, the implementation of amendments to existing sanctions, the ratification of entirely new sanctions, or a mix of both strategies by the UN Security Council is a necessary first step. Any action taken to explicitly condemn and punish

---

168 *Cryptocurrency Alert*, *supra* note 107.

169 *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, supra* note 154.

shady dealings in the crypto sector will serve to hamstring the DPRK economy and counter the country's sanction evasion strategies. Through DNFBP sanctions, the UN will substantially reduce North Korea's ability to exploit loopholes, negligence, or bad faith actors that exist within the luxury good market. Furthermore, by identifying and blocking all entities associated with state-sponsored cyber groups operating within North Korea and abroad, the UN will subject these groups and their allies to significant costs and penalties all throughout the world. And finally, by sanctioning exchanges and mixers that fail to comply with AML, licensing, KYC, and other requirements, it will bolster the security of these platforms on a global scale, thereby reducing the likelihood that organized hacker groups continue executing large-scale crypto heists.

B. How the Regulatory Policies of the U.S. and Japan Should be Applied Globally

Of all the countries that have taken steps to regulate cryptocurrency, the U.S. and Japan stand above the rest as the most proactive and thorough regulatory bodies in the world. They have taken steps not only to bolster the transparency of the transactions occurring on exchanges, mixers, and conversion businesses that operate within their borders but also to identify, sanction, and prosecute entities who violate these requirements. For the international community to have a tangible impact on the DPRK's crypto heisting scheme, the regulatory efforts of Japan and the U.S. should be mirrored and implemented on a global scale. This would be most effectively brought about through new policy measures employed and directed by The United Nations Conference on Trade and Development body (UNCTAD), The International Monetary Fund (IMF), and The World Bank. Alternatively, an entirely new regulatory body outside of the United Nations could be established for the sole purpose of decentralized currency regulation. Regardless of the chosen path, it is important that the international community adhere closely to the regulatory methods of the U.S. and Japan, as they show the most promise for thwarting the DPRK.

Focusing first on the Japan as a model and UNCTAD as the international regulatory body, there are several key measures that the

organization should apply to cryptocurrency. First, it is important to understand UNCTAD's role within the UN and how it can have an impact on crypto regulation. UNCTAD primarily works with the governments of developing countries to ensure that they can fairly participate in the global economy.[170] This is brought about through efforts that eliminate tariffs and other trade barriers that prevent young and poor nations from growing in a globalized market.[171] With respect to policymaking, the UNCTAD body known as the Conference meets every four years to analyze, coordinate, and implement new strategies for developing trade, technology, infrastructure, and other areas crucial to the success of young and poor nations.[172] The organization also routinely publishes policy analyses, which offer data and policy recommendations for developing nations, usually focusing on "trade, investment, finance and technology."[173] Beginning in the Summer of 2022, UNCTAD has released several policy briefs that focus specifically on cryptocurrency and its primarily negative impact on the economies of developing nations.[174] On June 13, 2022, for example, UNCTAD released a policy brief about the rapid rise of cryptocurrency usage during the COVID-19 pandemic and how this has created substantial costs for national monetary sovereignty and economic stability in developing countries .[175] Importantly, this brief includes three policy recommendations, the first of which emphasizes the importance of requiring crypto-exchanges and digital wallets to register with a central regulatory body.[176] Furthermore, the first recommendation advises developing nations to reduce the financial incentives for cryptocurrency usage by imposing transactional taxes on

---

[170] Karen Mingst, *United Nations Conference on Trade and Development*, BRITANNICA (Apr. 16, 2002), https://www.britannica.com/topic/United-Nations-Conference-on-Trade-and-Development.

[171] *Id.*

[172] *Id.*

[173] *Publications*, UNCTAD, https://unctad.org/publications (last accessed Feb. 5, 2023).

[174] *UNCTAD spells out actions to curb cryptocurrencies in developing countries*, UNCTAD (Aug. 10, 2022), https://unctad.org/news/unctad-spells-out-actions-curb-cryptocurrencies-developing-countries.

[175] *Policy Brief No. 100*, UNCTAD (June 13, 2022), https://unctad.org/system/files/official-document/presspb2022d9_en.pdf.

[176] *Id.*

trading and entry fees for exchanges and wallets.[177] This recommendation aligns strongly with the Japan system of regulation, which focuses on transparency requirements for crypto businesses. However, the policy brief stops short of several regulatory measures that are imposed upon decentralized cryptocurrencies in the Japan that have undoubtedly played a role in combating the DPRK's heisting efforts.

Most significantly, the UNCTAD policy brief fails to recommend that a centralized government agency be tasked with managing the registration process and ensuring compliance. As explained in the background section, under the Payment Services Act (PSA), the Japanese government defines what constitutes a cryptocurrency and accordingly regulates major utility tokens like Bitcoin, Ethereum, and so on.[178] Businesses that participate in the buying, selling, or exchanging of cryptocurrencies or crypto assets are required to register themselves as a provider of Crypto Asset Exchange Services (CAES) with the Financial Services Agency of Japan (FSA).[179] Further, the Financial Instruments and Exchange Act (FIEA) regulates shares, bonds, or fund interests in tokens by requiring businesses involved in the buying, selling, or exchanging of these "security tokens" to register as well. And most recently, Japan has taken measures to regulate stablecoins, digital currencies with a value tied to that of government-issued currency, by requiring businesses that make use of these coins to register with the FSA.[180] It is evident that Japan understands the value of enforcing a central registration system to combat the exploitation of a naturally covert currency system.

In its next policy brief concerning cryptocurrency, the UNCTAD should adjust its policy recommendations to more directly emphasize the importance of creating a centralized system of registration for all businesses involved in the purchase, sale, or transfer

---

177 *Id.*

178 Takeshi Nagase et al., *Blockchain & Cryptocurrency Laws and Regulations 2023 | Japan*, Global Legal Insights, https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/japan (last accessed Feb. 5, 2023).

179 *Id.*

180 *Id.*

of digital currencies and crypto assets, including stablecoins. Furthermore, while Non-Fungible Tokens (NFTs) are not a crypto asset or a security by definition, if Japan decides to subject these tokens to the same regulatory requirements, UNCTAD should include them in its recommendations.[181] By stressing the importance of regulating decentralized currency in the policy brief, UNCTAD will help to put developing nations on the correct path forward from the get-go. Registration requirements are an effective way for these countries to ensure that shady dealings are not occurring through backdoor, unregulated channels. If these requirements become a standard practice for developing nations, there is little doubt that the DPRK's ability to thieve crypto will be thwarted.

The International Monetary Fund (IMF), like the UNCTAD, plays a key role in the economic development of young and poor countries across the world. The IMF works closely with the World Bank to support the long-term financial goals of these countries.[182] More specifically, the IMF provides support by advising governments on development strategies and providing them with short and medium-term loans.[183] In collaboration with this effort, the World Bank provides infrastructural and environmental aid through projects such as schools, running water, electricity, disease prevention, and so on.[184] The World Bank, like the IMF also supports development by lending to the governments of its poorest member countries.[185] Importantly to the issue at hand, the IMF conducts annual analyses on the financial development of the world which are then published in several different forms of reports.[186] The Global Financial Stability Report is an assessment of the global financial market published by the IMF semiannually.[187] Its considerations are made on a global scale, and

---

[181] *Id.*

[182] *The IMF and the World Bank*, INTERNATIONAL MONETARY FUND, https://www.imf.org/en/About/Factsheets/Sheets/2022/IMF-World-Bank-New (last accessed Feb. 5, 2023).

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Global Financial Stability Report*, INTERNATIONAL MONETARY FUND, https://www.imf.org/en/Publications/GFSR (last accessed Feb. 5, 2023).

[187] *Id.*

they provide key insight into both the welfare of the market and the most prominent risks it is facing at the time of publishing.[188] This report is an extremely useful tool for both governments and private investors across the world who use its data models to inform their financial decision-making. The IMF also publishes a wide variety of reports on the 190 countries that are members of the organization.[189] These reports are of great significance, as they provide key insight into each country's political and economy stability, taxation and banking laws, legal system, and many other factors that shape global identity.[190]

When a country receives a loan from the IMF, it is sure to face stringent use and conduct requirements that must be complied with for the loan to be disbursed in full. The IMF conditionalities are quite straightforward, requiring the country to modify its economic policy to resolve the problem that caused the need for financial aid in the first place and making the borrower responsible for the loan's effectiveness[191]. There a several compliance assessment strategies employed by the IMF, focusing on specific and quantifiable criteria, spending targets, and broader markers for financial achievement.[192] The IMF Executive Board is tasked with assessing a borrowing country's compliance with requirements and performance on the benchmarks.[193] One example of a structural benchmark as provided by the IMF website is the improvement of a borrowing country's financial sector operations.[194] To ensure that borrowers are making progress with cryptocurrency, the IMF Executive Board should modify this benchmark to focus more directly on the country's development of a regulatory scheme for digital currencies and assets. If, as previously called for, the UNCTAD publishes an updated list of crypto-policy recommendations for developing nations based on the Japanese

---

188 *Id.*

189 *IMF Country Information*, INTERNATIONAL MONETARY FUND, https://www.imf.org/en/Countries (last accessed Feb. 5, 2023).

190 *Id.*

191 *Factsheet*, INTERNATIONAL MONETARY FUND, https://www.imf.org/en/About/Factsheets/Sheets/2016/08/02/21/28/IMF-Conditionality (last accessed Feb. 5, 2023).

192 *Id.*

193 *Id.*

194 *Id.*

model, the Board's assessment should use this list as a framework for determining the borrowing country's performance. And while the structural benchmarks, unlike the other forms of compliance assessment, are evaluated only "in the context of overall program performance", the IMF should reserve the right to withhold loan rollouts or increase borrowing costs if a country persistently falls shorts of the UNCTAD regulatory framework.[195] This assessment will give developing nations are very strong financial incentive to prioritize cryptocurrency regulation while growing their financial sector with the help of an IMF loan. And because of increased regulation, crypto security will be bolstered across the world, counter the efforts of the DPRK in the process.

With respect to the IMF's Global Financial Stability Report, the organization should adjust its assessment to address the impact of investments more directly in cryptocurrency on the global market. In 2021, the IMF talked in great lengths about the "crypto ecosystem" in its annual report, which emphasized the volatility of the crypto market, its impact on global financial stability, and the financial risks of a world with inconsistent regulatory standards.[196] Importantly, the 2021 report emphasizes the need for national regulators in all jurisdictions to implement robust governance and disclosure standards for all forms of cryptocurrency.[197] It also includes significant data on the volatility of crypto, borrowing rates for stablecoin, trading activity on exchanges, and other key indicators.[198]

This report has undoubtedly gone a long way to inform the public on the impact of crypto on a global scale, but it is important that the inclusion of these figures becomes a standard practice for the organization. By including this information every year, the IMF will help government leaders around the globe to become better informed on the volatility of the crypto market and the risks associated with faulty regulation. Furthermore, the IMF's extensive reporting on the

---

195 *Id.*

196 *Global Financial Stability Report*, INTERNATIONAL MONETARY FUND, 54 (Oct. 6, 2021).

197 *Id.*

198 *Id.* at 43.

financial welfare of its 190 member countries should include at least one annual report on each nation's investments in cryptocurrency and efforts made to regulate the market. This will be an extremely useful tool for private investors around the world, as it will serve to eliminate the uncertainty associated with investing in a country for which the decentralized currency market is unknown. From another perspective, it will encourage countries to effect more stringent regulatory measures, as these measures will increase the likelihood of foreign investment in developing countries. Market transparency is a key factor in evaluating country risk when an investor considers investing internationally. For the IMF, and more broadly the UN, to bolster investment in poor and young countries, it should prioritize the publication of well-researched data on the crypto market. In response, IMF nations will implement regulations that bolster investor confidence, leading to more rapid economic development, all while countering the efforts of crypto thieves around the world, including North Korea.

Alternatively, or more preferably in addition to UNCTAD and IMF policy reform, the execution of an intrastate agreement or treaty for the purpose of gathering intelligence and prosecuting crypto thieves would make for an effective tool of deterrence. A treaty executed for such a purpose should, as explained at the beginning of this section, adhere closely to the U.S. methods for fighting cryptocurrency crime, as they have been proven to yield tangible consequences for lawbreakers. In order for such a treaty to effect change, however, South Korea's involvement is a must, as their National Intelligence Service (NIS) has played a fundamental role in gathering nearly all information that is currently known about the DPRK's crypto heisting scheme.[199] If the prosecutorial power of the U.S. Department of Justice is combined with the highly successful data gathering techniques of the NIS, there is little doubt that the DPRK will be strongly deterred from continuing its crypto thieving strategies. But is such a treaty realistic? And if so, what can be done to ensure its execution?

---

[199] *Intelligence on North Korea*, NIS, https://eng.nis.go.kr/EAF/1_2.do (last accessed Feb. 5, 2023).

C. Impact of a Bilateral Treaty Between the U.S. and South Korea

As things currently stand, there exists significant cooperation and partnership between the United States and South Korea, both from an economic and a governance standpoint.[200] And while South Korea has been much slower than the U.S. when it comes to enforcing cryptocurrency regulation, there is no doubt that the country understands the growing need for better policies.[201] Regulation is less relevant to the execution of a bilateral treaty, however, as its focus would be on identifying and prosecuting cybercriminals, not preventing them from breaking the law. In fact, the only role South Korea would need to play in such a treaty would involve intelligence gathering and the sharing of that information with the U.S. Department of Justice. More specifically, the aforementioned Market Integrity and Major Frauds Unit of the DOJ, as well as the FBI, would work with the South Korean National Intelligence Service (NIS) so that the agencies can more effectively prosecute fraud, market manipulation, and other crimes occurring within the U.S. crypto market. And while on its face this treaty appears to serve only the U.S. interest in protecting citizens from domestic cybercrime, countries everywhere would benefit from a system that streamlines the process of identifying and prosecuting cybercrime. First, through the publicity of the treaty alone, North Korea would assuredly be deterred from continuing its criminal activity in general, at least to some degree. Furthermore, once the agreement begins to produce tangible results in the form of indictments, or perhaps even with South Korea's help, arrests, the DPRK will start to reconsider its nuclear missile funding strategies. And finally, from a financial standpoint, if the intelligence received from South Korea aids the U.S. in more effectively seizing cryptocurrency ransoms, the DPRK will suffer a direct economic blow that is sure to impact the prosperity of its nuclear missile program.

---

[200] *U.S. Relations With the Republic of Korea*, U.S. DEP'T OF STATE (Sept. 22, 2020) https://www.state.gov/u-s-relations-with-the-republic-of-korea/.

[201] Cheyenne Ligon et al., *South Korean Lawmakers Are Gearing Up to Regulate Crypto. What Could That Look Like?*, COINDESK (Jan. 26, 2023, 1:00 PM), https://www.coindesk.com/consensus-magazine/2023/01/26/south-korea-national-assembly-crypto-debate-regulations/.

Given the markedly positive relationship between the governments of the U.S. and the Republic of Korea (ROK), the formulation of such a treaty agreement is most certainly within the realm of possibility. After the Korean War, a U.S.-South Korea Alliance was formed for the primary purpose of helping South Korea to defend itself from the DPRK.[202] This alliance involves a sizable U.S. military presence within South Korea, as well as related military activities to deter North Korean aggression.[203] Importantly, the Biden Administration has recently called for more robust cooperation between the two countries under the U.S.-ROK Alliance and has even advocated for the addition of Japan to the alliance.[204] This ambition supports the likelihood of a successful negotiation between the two countries with respect to prosecuting cryptocurrency crime, especially because the main focus of the alliance is DPRK deterrence. One of the first steps that should be taken in promulgating this arrangement should be taken by the United States Congress, and it involves the negotiation of an amended treaty agreement with the ROK. Given the overwhelming bipartisan support for an alliance between the U.S. and South Korea, it is likely that such an amendment to the U.S.-ROK Alliance would be approved without issue.[205] However, if an amendment fails to be approved by the Senate, the President should use his foreign relations powers to enact an executive agreement with South Korea, as this would not require the advice or consent of the Senate, but it would still have the same force as a ratified treaty.[206] In any case, bolstering cooperation between the U.S. and the ROK for the purpose of identifying and prosecuting North Korean cybercriminals will play a direct and critical role in dismantling the funding of the country's nuclear missile program. In an ideal world, this cooperation would be extended to include other countries in the

---

[202] Cong. Rsch. Serv., IF11388, *U.S.-South Korea Alliance: Issues for Congress* (Mar. 14, 2022).

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] The Editors of Encyclopedia Britannica, *Executive Agreement*, BRITANNICA (Apr. 5, 2002), https://www.britannica.com/topic/executive-agreement.

Asia-Pacific, namely Japan, as its vast knowledge of the crypto market would serve the U.S. interest in prosecuting thieves.

IIII. CONCLUSION

In conclusion, if the United States, the members of the United Nations, and other countries concerned by North Korea's ability to fund a nuclear program through crypto heisting schemes want to effect meaningful change, they must act quickly to harshen regulations and bolster education. This will require, at a minimum, persistent and explicit emphasis on the need for all countries to enact more stringent regulations for crypto exchanges and their users, businesses that process crypto currency, and sectors that accept cryptocurrency as a form of payment. Moreover, a successful regulatory overhaul necessitates cooperation from a multitude of actors on the world stage to create far-reaching, transparent, and well-established regulatory standards for cryptocurrency. The current sanctions have proven to be severely lacking in efficacy, arguably doing more to incentivize the DPRK to fund its nuclear program in covert, more difficult to trace ways than to cripple it. Since the rise of crypto heisting a few years ago, it has become evident not that the UN sanctions are insufficiently aggressive, but rather, that they attack the wrong sectors. These sanctions should not be replaced but broadened to include North Korea's cyber infrastructure, identified cyber operatives, and crypto exchanges or processing businesses that cooperate with North Korea. In addition to harsher sanctions, the U.S. must improve its domestic regulation of cryptocurrency. This would include harsher regulations of domestic exchanges, a significant broadening of Congress' power to regulate crypto, more deference given to decisions made by the SEC, and an expansion of the Justice Department's involvement in exposing and prosecuting cyber operatives.

To augment improved U.S. regulation, the world must work together to better regulate cryptocurrency. This will require, most importantly, the establishment of international standards for crypto exchanges. While the UN cannot force a non-lawbreaking country to adjust its domestic regulatory scheme to bolster crypto security, it certainly can help create the financial and social incentives for doing so. Through organizations like the IMF, the UN can create serious

economic motivation for developing nations to follow suit and comply with international crypto regulation. And of course, the UN Security Council reserves the right sanction members states for non-compliance with any of its peacekeeping operations.[207] Further, crypto related crime will be reduced drastically if the international community collaborates to identify and prosecute crypto thieves. One way to instigate this collaboration is through the modification of the current U.S.-ROK Alliance so that the countries may begin working together to track down North Korean cyber operatives and indict them for their crypto-related crimes.[208] In doing so, the two countries will ideally set in motion a global effort to counter the DPRK's heisting scheme through prosecutorial deterrence measures. More harmonious regulatory efforts coupled with more aggressive legal action against the DPRK will serve not only to bolster worldwide confidence in the safety of decentralized currency but also to impede North Korea's ability to fund its nuclear missile program. Together, these undertakings will help to create a modernized world that is safer, more economically prosperous, and better educated.

---

[207] *See Sanctions*, United Nations Security Council, https://www.un.org/securitycouncil/sanctions/information (last accessed Feb. 5, 2023).

[208] *See* Cong. Rsch. Serv., *supra* note 201.