NOTE

EVADING, HACKING & LAUNDERING FOR NUKES: NORTH KOREA'S FINANCIAL CYBERCRIMES & THE MISSING SILVER BULLET FOR COUNTERING THEM

*Seongjun "Spencer" Park**

ABSTRACT

North Korea has employed various means to evade international sanctions and launder its illicit funds. It has expanded such activities into cyberspace in recent years with astounding adaptability as well as tactical and operational maturity. Whereas upward harmonization of anti-money laundering standards on a global scale would be more potent than other suggested solutions such as increasing cybersecurity resilience and replacing cryptocurrencies entirely with central bank digital currencies, North Korea likely will remain largely undeterred. Instead of looking for a "silver bullet," the international community must focus on building financial incentive structures that could induce nations' participation in the upward regulatory harmonization.

* J.D. Candidate, 2023, Fordham University School of Law; M.P.P., 2018, University of Virginia; B.A., 2017, University of Virginia; Staff Editor, *Fordham International Law Journal*, Volume 45.

I. INTRODUCTION

North Korea's nuclear program and its destabilizing military provocations against its neighbors[1] have led the international community to impose numerous economic sanctions on Pyongyang. To overcome these sanctions, North Korea has increasingly employed advanced cyber capabilities to conduct ransomware attacks,[2] digital bank heists, cryptocurrency theft,

1. There have been five major conventional military provocations by North Korea between 1999 and 2010, including three naval battles, the shelling of Yonpyong Island, and the sinking of ROKS Cheonan. *See* Taehee Whang, *Detecting Patterns in North Korean Military Provocations: What Machine-Learning Tells Us*, 18 INT'L RELS. ASIA-PAC. 193, 197–200 (2018).

2. Ransomware attack generally involves infecting a victim's computer with an access-denying malware and then demanding payments in cryptocurrency in return for granting the victim access to his or her computer. For a more in-depth explanation, see *infra* Section III.B.

crypto-based cyber scams,[3] and cryptojacking schemes[4]—all of which include money laundering components. The cyber-based nature of these financial crimes challenges the international community's attempt to curb North Korea's continued sanctions evasion and money laundering activities that are often assisted by individuals and organizations of many nations.

Several proposed solutions exist, but they are not without drawbacks. Increasing global cybersecurity resilience is a solution that is far too limited and insufficient.[5] Banning cryptocurrency entirely and promoting the adoption of central bank digital currencies ("CBDC")[6] instead is a distant solution with too many uncertainties.[7] It also comes with a risk that China might exploit CBDC infrastructure to aid North Korea in evading sanctions.[8] With the absence of a "silver bullet," a more potent and quickly actionable solution is an upward harmonization of global anti-money laundering ("AML") regulatory standards that principally entail the implementation of the latest AML laws and practices by countries through which North Korea channels its illicit transactions.[9] However, given these countries' lack of urgency to implement such standards, and, more importantly, China's reluctance to assist in AML measures against North Korea, global efforts to counter this problem will likely be ineffective, if not futile.[10]

These challenges notwithstanding, the leading AML countries and international community should still aim to achieve incremental gains in upward regulatory harmonization by proactively incentivizing countries with weak AML regimes to adopt the latest standards. Ongoing efforts and some recent successes regarding climate change action could serve as a

3. North Korea's alleged attempt to lure investors to its dubious Marine Chain Vessel Token Offering represents this type of cyber scam. For a more in-depth explanation, see *infra* Section III.C.

4. Cryptojacking refers to the act of using malware-infected computers' computing power to mine cryptocurrency. For a more in-depth explanation, see *infra* Section III.C.

5. *See* discussion *infra* Section IV.A.

6. CBDCs are digital currencies issued and backed by central banks unlike cryptocurrencies that are issued by private enterprises. For a more in-depth explanation, see *infra* Section IV.B.

7. *See* discussion *infra* Section IV.B.

8. *See id.*

9. *See* discussion *infra* Section IV.C.

10. *See id.*

benchmark for building effective financial incentive structures to induce such positive changes.[11]

II. OVERVIEW OF NORTH KOREA'S ILLICIT ACTIVITIES

A. Geopolitical Background

Since the end of the Cold War, the Kim regime has found itself in an increasingly tenuous position. The disappearance of economic aid from the Soviet Union—combined with floods, mismanagement, and the breakdown of the public distribution system—resulted in a period of crippling famine throughout North Korea in the mid-1990s.[12] As many as three-and-a-half million North Koreans are estimated to have died from starvation and malnutrition[13] during what is known as the "Arduous March."[14] The event not only "traumatized North Korean society from bottom to top," [15] but also severely undercut the regime's legitimacy.[16] In addition, the exceedingly more prosperous South Korea has reversed the conventional military superiority that North Korea had once enjoyed,[17] increasing the regime's sense of insecurity.[18]

The regime has developed nuclear weapons and ballistic missiles to counter this dynamic, and such focus has paid off for Pyongyang. North Korea's nuclear weapons program has been a

11. *See* discussion *infra* Part V.

12. *See How Did the North Korean Famine Happen?*, WILSON CTR. (Apr. 30, 2002), https://www.wilsoncenter.org/article/how-did-the-north-korean-famine-happen [https://perma.cc/TLK9-ALKZ] [hereinafter WILSON CTR.].

13. *Id.*

14. Zhuoran Li, *North Korea's Food Shortage is a Lesson for U.S. Policymakers*, DIPLOMAT (Oct. 28, 2021), https://thediplomat.com/2021/10/north-koreas-food-shortage-is-a-lesson-for-us-policymakers/ [https://perma.cc/H2N6-7H6K].

15. WILSON CTR., *supra* note 12.

16. *See id.*

17. *See generally* Min-Seok Kim, *The State of the North Korean Military*, *in* KOREA NET ASSESSMENT: POLITICIZED SECURITY AND UNCHANGING STRATEGIC REALITIES 19 (Chung Min Lee & Kathryn Botto eds., Carnegie Endowment for Int'l Peace 2020) (discussing that North Korea's numerical advantage but quality shortfalls render its conventional military force—Korea People's Army—inferior to that of South Korea's Republic of Korea Armed Forces).

18. *See* Young-taek Park, *The Structural Elements of North Korea's Insecurity Applying the "Regional Security Complex Theory"*, 24 KOR. J. DEF. ANALYSIS 321, 322–25 (2012) (attributing causes of North Korea's insecurity to internal political and economic inefficiency, failed competition with South Korea, and environmental transformation in terms of regional and international security).

"game changer in the South-North military balance," [19] and its newly acquired asymmetrical military assets have allowed the regime to both remain a viable threat to its neighbor to the south and become a direct threat to the United States.[20] After conducting six increasingly sophisticated nuclear tests since its first in 2006,[21] Pyongyang tested its first intercontinental ballistic missile in July 2017 and claimed that it could hit the "heart of the United States."[22]

Pyongyang's strategy of accumulating asymmetrical assets goes beyond nuclear warheads and extends to cyberspace. North Korea now possesses "advanced cyberwarfare prowess surpassed by only a few nations" [23] with reportedly over 7,000 cyber operatives[24] who are thought to have been responsible for major distributed denial-of-service ("DDos") attacks[25] on South Korean media, financial, and military infrastructure in 2011[26] and the Sony Pictures hacking in 2014. [27] Most recently, North Korea was

19. Kim, *supra* note 17, at 19.

20. *See id*. at 25 ("[I]f North Korea is able to master SLBM technology with nuclear warheads, that cannot but be seen as a major threat to the ROK, Japan, and the United States.").

21 . *See North Korea Overview*, NUCLEAR THREAT INITIATIVE (Oct. 19, 2021), https://www.nti.org/analysis/articles/north-korea-overview/ [https://perma.cc/A67Z-NQ25].

22. Sang-Hun Choe, *U.S. Confirms North Korea Fired Intercontinental Ballistic Missile,* N.Y. TIMES (July 4, 2017), https://www.nytimes.com/2017/07/04/world/asia/north-korea-missile-test-icbm.html [https://perma.cc/MD84-CX52].

23. Morten Soendergaard Larsen, *While North Korean Missiles Sit in Storage, Their Hackers Go Rampant*, FOREIGN POLICY (Mar. 15, 2021), https://foreignpolicy.com/2021/03/15/north-korea-missiles-cyberattack-hacker-armies-crime/ [https://perma.cc/VL6L-7GZJ] (quoting Bruce Klingner—a former CIA deputy division chief and current Heritage Foundation senior research fellow).

24. U.S. DEP'T HEALTH & HUM. SERVS., OFF. INFO. SEC., NORTH KOREAN CYBER ACTIVITY 3 (2021), https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf [HTTPS://PERMA.CC/UG8C-SYY5].

25. A DDos attack is a "malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server." *Distributed Denial of Service Attack (DDos) Definition*, IMPERVA, https://www.imperva.com/learn/ddos/ddos-attacks/ [https://perma.cc/DE8D-VPFM] (last visited Jan. 12, 2022).

26. *See* U.S. DEP'T HEALTH & HUM. SERVS., OFF. INFO. SEC., *supra* note 24, at 6.

27 . *See id.* The 2014 malware attack on Sony Pictures, which came after the company's release of a dark comedy satirizing the North Korean leader Kim Jong-un called *The Interview* despite threats from Pyongyang, junked 3,262 of Sony's 6,797 personal computers and 837 of its 1,555 servers. Some see it as a direct predicate for Russia's cyberattacks against the Democratic National Committee and the Hilary Clinton campaign during the 2016 U.S. presidential election. Richard Stengel, *The Untold Story of the Sony Hack: How North Korea's Battle with Seth Rogen and George Clooney Foreshadowed Russian*

reportedly responsible for targeted cyberattacks on major healthcare and pharmaceutical companies involved in COVID-19 research and vaccine development.[28]

B. Imposition of Sanctions Against North Korea

The United Nations Security Council[29] has responded to North Korea's nuclear weapons program by imposing nine economic sanctions, listed in Table I below.

Table I: List of UN Sanctions

Resolution	Date	Key Measures
1718	Oct. 2006	Prohibits the import of some military supplies and luxury goods
1874	June 2009	Broadens the arms embargo
2087	Jan. 2013	Clarifies a state's right to seize and destroy materials headed to North Korea
2094	Mar. 2013	Imposes travel ban on certain individuals and freezes their assets
2270	Mar. 2016	Prohibits UN members from opening North Korean bank accounts and banking offices and from providing vessels and aviation fuel to North Korea
2321	Nov. 2016	Prohibits mineral exports and directs member states to limit the number of bank

Election Meddling in 2016, VANITY FAIR (Oct. 6, 2019), https://www.vanityfair.com/news/2019/10/the-untold-story-of-the-sony-hack [https://perma.cc/944M-ECD7].

28. *See* U.S. DEP'T HEALTH & HUM. SERVS., OFF. INFO. SEC., *supra* note 24, at 4; *see also* Robert Hart, *Report: North Korean Hackers Tried to Steal Covid-19 Vaccine Tech from Pfizer*, FORBES (Feb. 16, 2021), https://www.forbes.com/sites/roberthart/2021/02/16/report-north-korean-hackers-tried-to-steal-covid-19-vaccine-tech-from-pfizer/?sh=88d0d944102c [https://perma.cc/6T6W-98ZB] (elaborating that it is unclear whether the alleged hacks were successful or when they may have occurred).

29. The UN Security Council consists of five permanent members—China, France, Russia, the United Kingdom, and the United States—and ten non-permanent members elected for two-year terms by the General Assembly. *See Current Members*, U.N. SEC. COUNCIL, https://www.un.org/securitycouncil/content/current-members [https://perma.cc/P94D-WYVD] (last visited Dec. 31, 2021).

		accounts held by North Korean diplomats and missions
2371	Aug. 2017	Prohibits coal and iron ore exports and bans joint ventures between North Korea and other nations
2375	Sept. 2017	Restricts crude oil and natural gas imports with additional asset freezes
2397	Dec. 2017	Directs states to expel North Korean laborers and imposes additional trade restrictions concerning petroleum, minerals, and heavy equipment

Source: Arms Control Association[30]

In addition to these UN sanctions, the United States, the European Union, South Korea, Japan, Australia, and other countries have imposed additional independent sanctions to further serve their State's security interests.[31] In particular, the United States Office of Foreign Assets Control ("OFAC") not only bans US nationals from engaging in financial activities with Pyongyang and targeted North Korean nationals, but also imposes secondary sanctions against governments, businesses, and nationals of third countries that engage in those prohibited activities.[32] The US government also enforces the Bank Secrecy Act of 1970 ("BSA") that was amended by Title III of the USA PATRIOT Act, which requires financial institutions to assist law enforcement against money laundering by filing currency transaction reports ("CTR"), suspicious activity reports ("SAR"), and other related reports to help government agencies in identifying transactions connected to money laundering schemes.[33]

30. *See* Kelsey Davenport & Elizabeth Philipp, *UN Security Council Resolutions on North Korea,* ARMS CONTROL ASS'N (Apr. 2018), https://www.armscontrol.org/factsheets/UN-Security-Council-Resolutions-on-North-Korea [https://perma.cc/P94D-WYVD].

31. *See* Eleanor Albert, *What to Know About Sanctions on North Korea*, COUNCIL ON FOREIGN RELS. (July 16, 2019, 8:00 AM), https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea [https://perma.cc/8BHN-JQEK].

32. *See* KING MALLORY, NORTH KOREAN SANCTIONS EVASION TECHNIQUES 15 (RAND Corp. 2021).

33. *See Bank Secrecy Act (BSA) & Related Regulations*, OFF. COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-

C. North Korea's Longstanding Sanctions Evasion & Money Laundering Techniques

The Kim regime, however, has become "very adept at evading [these] sanctions"[34] by employing four types of entities: diplomats, overseas laborers, front and shell companies,[35] and trusted third-country intermediaries.[36] Through these entities, North Korea has generated hard income in dollars and euros through prohibited trade and criminal activities, acquired restricted materials and technology, smuggled goods, covertly financed these evasive operations, and laundered money.[37] Crimes committed by North Korea to generate hard currency include, but are not limited to: narcotics trafficking,[38] imposition of forced overseas labor on its nationals,[39] counterfeiting of US dollars[40] and cigarettes,[41] and illicit engagement in the arms[42] and wildlife trades.[43] Money laundering is especially important to North Korea as it reduces the

related-regulations/index-bsa-and-related-regulations.html [https://perma.cc/237V-ED8F] (Nov. 13, 2021, 4:33 PM).

34. MALLORY, *supra* note 32, at 19.

35. A front company is a fully functioning business that disguises obscure illicit activity using legitimate business operations, while a shell company is a business without independent operations, significant assets, ongoing business activities, or employees. *See id.* at 20.

36. *See id.* at 20. Around 150 nationals of third countries have been identified to have knowingly acted as intermediaries for North Korea's sanctions evasion operations, and they especially play a significant role in countries that require its citizens to own a majority share in business entities. *See id.*

37. *See id.* at 19.

38. *See* Max Fisher, *Report: North Korea Ordered Its Foreign Diplomats to Become Drug Dealers*, WASH. POST (Mar. 22, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/03/22/report-north-korea-ordered-its-foreign-diplomats-to-become-drug-dealers/ [https://perma.cc/9LCA-28XJ].

39. *See* U.S. DEP'T STATE, TRAFFICKING IN PERSONS REPORT 295-97 (20th ed. 2020).

40. *See* Mike Eckel, *New $100 Bill: Why North Korea Won't Be Very Happy*, CHRISTIAN SCI. MONITOR (Oct. 8, 2013), https://www.csmonitor.com/World/2013/1008/New-100-bill-why-North-Korea-won-t-be-very-happy [https://perma.cc/2BKT-XDCD].

41. *See* Emma Reynolds, *Illicit Cigarette Trade Helps Pay for North Korea's Nukes*, N.Y. POST (Nov. 1, 2017), https://nypost.com/2017/11/01/illicit-cigarette-trade-helps-pay-for-north-koreas-nukes/ [https://perma.cc/6WXW-L7N5].

42. *See* Samuel Ramani, *North Korea's Military Partners in the Horn of Africa*, DIPLOMAT (Jan. 6, 2018), https://thediplomat.com/2018/01/north-koreas-military-partners-in-the-horn-of-africa/ [https://perma.cc/LG5S-E5DH].

43. *See* Rachel Nuwer, *North Korean Diplomats Accused of Smuggling Ivory and Rhino Horn*, NAT'L GEOGRAPHIC (Oct. 16, 2017), https://www.nationalgeographic.com/animals/article/wildlife-watch-north-korea-illegal-wildlife-trade [https://perma.cc/B5M8-NLV6].

risk of detection of its entire evasive operations by supervisory authorities.[44]

North Korea's money laundering operations—like those by other criminal organizations—are conducted in three stages: placement, layering, and integration. Placement, in its simplest form, involves North Korean agents—usually under diplomatic cover—opening bank accounts in their host and neighboring countries to deposit the regime's illicit funds and thereby introduce them into the financial system.[45] Agents use their own name or the name of their family members and front companies when opening these accounts.[46] In countries with less stringent regulatory frameworks and more resource-constrained banks, North Korea often opens accounts using the name of non-North Korean nationals and entities for which it has signing authority under business or employment contracts, purchase joint ownership in non-North Korean financial institutions, or use casinos for placement.[47]

In the layering stage, the placed funds are moved across several accounts at different financial institutions in different jurisdictions to hide their origin. North Korea often uses bank accounts held by joint ventures with international trading companies to achieve this. It further obscures these layering operations by ensuring that international wire transfer messages do not contain any information that might hint at the funds' connection to Pyongyang.[48] In the final stage of integration, placed and layered funds are used in seemingly legitimate purchases that conceal the fact that North Korea is the buyer in these transactions. North Korea allegedly does this by using false names on invoices, hiding the name of its designated banks, and pooling funds from several sources when making a single large payment.[49]

While North Korean agents often direct their money laundering transfers to accounts in legal jurisdictions that shield information about the accounts' owners,[50] a sizeable amount of

44. *See* MALLORY, *supra* note 32, at 40.
45. *See id.*
46. *See id.*
47. *See id.* at 40–41.
48. *See id.* at 41.
49. *See id.*
50. *See id.*

North Korea-linked funds have also reportedly passed through US banks—which in theory have far greater resilience to money laundering activities than those in less-regulated jurisdictions. In 2020, the US Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") Files—a cache of secret SARs leaked by BuzzFeed—shockingly revealed that between 2008 and 2017, US banks, including JPMorgan Chase and the Bank of New York Mellon, cleared over US$174.8 million worth of transactions likely associated with North Korean money laundering schemes.[51] The leaked documents state, for example, that a Chinese national by the name of Xiaohong Ma and her company Dandong Hongxiang Industrial Development Corp.—indicted by US authorities in 2016 and 2019 on charges of money laundering—used multiple shell companies to route more than tens of millions of dollars to North Korea through China, Singapore, Cambodia, and the United States.[52] BNY Mellon reported to FinCEN that it had cleared US$85.6 million worth of Ma's suspicious transactions, which contained typical North Korean money laundering features such as obscure recipient companies based in high-risk jurisdictions like Cambodia, initiation of several batches of transfers in round amounts over a short period of time, and lack of clear commercial reasons.[53] Even more perplexingly, BNY Mellon cleared these transactions despite media coverages of Ma's open affiliations with Pyongyang,[54] including her appearances in the Stimson Center's newsletter[55] and an Associated Press article.[56]

---

51. Andrew W. Lehren & Dan De Luce, *Secret Documents Show How North Korea Launders Money Through U.S. Banks*, NBC NEWS (Sept. 20, 2020), https://www.nbcnews.com/news/world/secret-documents-show-how-north-korea-launders-money-through-u-n1240329 [https://perma.cc/B2DG-QJ4H].

52. *See id.*

53. *See id.*

54. *See id.*

55. *See* Paul White, *DPRK Business Monthly Volume 1, No. 2,* NORTH KOREAN ECON. WATCH (2010), http://www.nkeconwatch.com/nk-uploads/dprkmonthly2.pdf [https://perma.cc/5NP2-JHSK] (featuring Ma's interview with the China Daily about her anticipation of greater trade volume and faster transportation of goods between China and North Korea following the construction of a new bridge over the Yalu River).

56. *See* Didi Tang, *North Korean Ebola Policies Hit Tourism Businesses,* FED. NEWS NETWORK (Oct. 31, 2014), https://federalnewsnetwork.com/health-news/2014/10/north-korean-ebola-policies-hit-tourism-businesses/ [https://perma.cc/4T8C-7KAL] (stating that Ma's trading activities with North Korea has not taken a hit despite the regime's Ebola-related trade restrictions because most of her businesses are conducted over the phone).

JPMorgan Chase also reported that it had facilitated more than US$89.2 million worth of transactions between 2011 and 2013 that benefitted eleven companies and individuals associated with North Korea's sanctions evasion.[57] Some of these companies included Faith Surplus Trading Ltd. and Dandong Sanjiang Trading Co. Ltd., both of which are based in China.[58] The former made fourteen wire transfers worth US$3.76 million to China Oil Singapore—a subsidiary of state-owned China National United Oil Corp.—that has an extensive track record of suspected sanctions evasion on behalf of North Korea and Iran, while the latter has made at least eighty suspicious shipments to North Korea.[59] Similarly to BNY Mellon's failure to block Ma's transactions despite news reports of her background, it is unclear why JPMorgan Chase completed these transfers even though the bank had "internal intelligence"[60] about these companies.

FinCEN Files signal that there are serious sanctions and AML enforcement problems even for generally more capable US financial institutions, especially when correspondent banking is involved. Correspondent banking routinely occurs when US banks provide their international counterparts with currency exchange and other related services, and vice versa, and plays an essential role in facilitating cross-border transactions.[61] However, the US Treasury notes that money launderers have frequently exploited correspondent banking because US correspondent banks do not have an account relationship with a transfer's or payment's international originator; when the originator is the non-domestic respondent bank's direct or indirect client, US banks are hence unable to conduct effective Know Your Customer ("KYC") processes and are thus limited in their knowledge about the transaction.[62] The sheer volume of international transactions that US correspondent banks intermediate also makes it difficult for them to more thoroughly examine each transfer or payment.[63] Other factors including the absence of a requirement to collect a

57. Lehren & De Luce, *supra* note 51.

58. *See id.*

59. *See id.*

60. *Id.*

61. *See* U.S. DEP'T TREASURY, *National Strategy for Combating Terrorist and Other Illicit Financing* 21 (2020).

62. *See id.*

63. *See id.* at 13.

company's beneficial ownership information at its formation and change of ownership,[64] and the lack of comprehensive AML requirements on some financial institutions like state-chartered banks,[65] further contribute to US financial institutions "unwittingly process[ing] these [suspicious and likely illicit] transactions."[66]

As of 2021, North Korea has deployed its effective sanctions evasion techniques in at least 107 countries.[67] Such undertakings are most prevalent in Asia, with over 540 identified entities assisting Pyongyang in its endeavor in thirty-one of the region's forty-eight countries.[68] Consistent with FinCEN Files' identification of heavy Chinese entity involvement in North Korean money laundering operations, an overwhelming majority of these evasive activities in Asia occur in China.[69] Europe has the second highest concentration of such activities—160 identified entities in twenty-nine of forty-four countries—with Russia as the region's leading location of sanctions evasion.[70] Although Africa comes in third with 150 identified entities in thirty-eight of fifty-four countries, it is becoming a focal point of concern because the illegal sale of North Korean weapons to Africa for the Kim regime's hard currency generation is exacerbating the region's arms proliferation.[71]

D. Status Quo of Sanctions Enforcement

Ultimately, existing sanctions have failed to deter Pyongyang from continuing its nuclear and ballistic missile programs, as North Korea has become a "de-facto nuclear state."[72] The Kim regime's evasive moves very likely reduced the sanctions' potency and compromised their desired effect of compelling Pyongyang to make genuine, fundamental changes to its behaviors. A short period of détente—in the form of successive summits between Kim Jong-un, South Korean President Moon Jae-in, and US President

64. *See id.* at 12.
65. *See id.* at 13.
66. *Id.* at 12.
67. *See* MALLORY, *supra* note 32, at 5.
68. *See id.* at 6.
69. *See id.*
70. *Id.*
71. *See id.* at 6–8.
72. Chung Min Lee, *The Chimera of Peace on the Korean Peninsula*, *in* KOREA NET ASSESSMENT: POLITICIZED SECURITY AND UNCHANGING STRATEGIC REALITIES 5 (Chung Min Lee & Kathryn Botto eds., Carnegie Endowment for Int'l Peace 2020).

Donald Trump—took place in 2018 following North Korea's expression of its willingness to "denuclearize" under certain conditions.[73] But "Trump's and Moon's [overly] rosy appraisals of the chances of a nuclear deal and lasting peace" [74] did not materialize and North Korea soon reverted to aggression and self-isolation, as many experts had anticipated.[75] The sanctions remain in place as of March 2022.

III. NORTH KOREAN ILLICIT FINANCIAL ACTIVITIES IN CYBERSPACE

A. Cyberspace as Pyongyang's New Avenue for Evading Sanctions

While Pyongyang continues to evade sanctions and launder money, cyberspace has drawn the regime's attention as a new, more efficient avenue for evading sanctions. This is because cybercrimes, especially with the growth of the cryptocurrency industry, offer "low-risk, high-return" [76] opportunities to make money. Compared to North Korea's more traditional hard currency-generating crimes such as narcotics trafficking and arms trade,[77] cybercrimes offer their perpetrators greater protection from investigation through high levels of anonymity. Cybercriminals could easily use Tor network—a free, open-source software for enabling anonymous communication—and other technologies to hide their identity and even impersonate other criminals and organizations to make it "difficult to place [the]

73. Sang-Hun Choe & Mark Landler, *North Korea Signals Willingness to 'Denuclearize,' South Says*, N.Y. TIMES (Mar. 6, 2018), https://www.nytimes.com/2018/03/06/world/asia/north-korea-south-nuclear-weapons.html [https://perma.cc/D3ET-4GLJ].

74. Lee, *supra* note 72, at 2.

75. *See generally* Lee, *supra* note 72 (discussing that, despite Moon's optimism, Korea's strategic landscape has not changed and that North Korea has not taken meaningful steps to reduce its military threat against the South); *see also* Donald Kirk, *Moon Wants a Legacy on North Korea That Isn't Coming,* FOREIGN POL'Y (May 13, 2021), https://foreignpolicy.com/2021/05/13/moon-north-korea-legacy-biden/ [https://perma.cc/79XN-9PBZ] (pointing out that every previous deal with North Korea since 2000 had ended in failure and quoting Victor Cha's and David Maxwell's criticisms of Moon's appeasement strategy towards North Korea).

76. So-hyun Kim, *NK Stole Up to $2B by Hacking Financial Networks: Report*, KOR. HERALD (Sept. 4, 2020), http://www.koreaherald.com/view.php?ud=2020090400057.

77. *See* discussion *supra* Section II.C.

suspect behind the keyboard."[78] In addition, cybercriminals are not constrained by national borders, "yet police [and investigators] still have to work within these borders,"[79] giving rise to problems of varying privacy laws and policing priorities among nations.[80] The incredible speed with which cybercrimes valuing tens of millions of dollars could take place—a few seconds in many cases—further explains their appeal.[81]

The impact of the COVID-19 pandemic on global trade and economy probably makes cyber-based sanctions evasion even more attractive for North Korea. The drastic decreases in global trade due to the pandemic,[82] the 2021 global supply chain crisis,[83] and North Korea's own pandemic border lockdown that caused its trade volume with China to plummet by eighty percent[84] suggest that the regime's smuggling and trafficking-driven activities were likely negatively affected like any other transportation-dependent economic activities. Simultaneously, explosive growth in reliance on networked technologies—data system technologies used to manage and send digital resources over a computer network—and cloud-based companies has created an environment of "ubiquity and concentration [that] provides an exceptional opportunity for cybercriminals."[85] Given these conditions, it is natural that the regime would turn to cybercrimes that are not only lucrative but also more easily executable to evade sanctions. Indeed, the number

78. Sarah Coble, *How Cybercrime Has Changed Criminal Investigations*, INFOSECURITY (May 26, 2020), https://www.infosecurity-magazine.com/magazine-features/cybercrime-criminal-investigations/ [https://perma.cc/TB73-G4VB].

79. *Id.*

80. *See id.*

81. *See id.*

82. *See COVID-19 Drives Large International Trade Declines in 2020,* UNCTAD (Dec. 9, 2020), https://unctad.org/news/covid-19-drives-large-international-trade-declines-2020 [https://perma.cc/4NWR-JC2Z].

83. *See* Matt Egan, *The Global Supply Chain Crisis is About to Get Worse,* CNN (Oct. 13, 2021), https://www.cnn.com/2021/10/12/business/global-supply-chain-nightmare/index.html [https://perma.cc/7KGJ-QCTM].

84. Andrew Yeo, *North Korea is Addressing the Pandemic in Its 'Style.' That Means Leaving A Lot of People Hungry*, WASH. POST (Nov. 17, 2021), https://www.washingtonpost.com/politics/2021/11/17/north-korea-is-addressing-pandemic-its-style-that-means-leaving-lot-people-hungry/ [https://perma.cc/JY3M-4J7D].

85. Misha Glenny, *Pandemic Accelerates Growth in Cyberspace*, FIN. TIMES (Apr. 27, 2021), https://www.ft.com/content/49b81b4e-367a-4be1-b7d6-166230abc398 [https://perma.cc/XWV6-9BML].

of cybercrimes perpetrated globally soared during the pandemic,[86] although it is unclear how much of this increase can be attributed to North Korea.

As previously discussed in Section II.A, North Korea fields a massive army of cyber operatives as part of its asymmetrical strategy, which it also uses for conducting cyber-based financial crimes as part of its sanctions evasion strategy. Most of the commercial hackers that focus on financial crimes operate under the command of the Reconnaissance General Bureau, North Korea's key military-intelligence division, and its subunits of hackers like the Lazarus Group.[87] While "nobody seems to have a firm grasp on how many people work for each [subunit] or which group makes the most money,"[88] experts have identified several of these groups as shown in Table II.

Table II: Identified Hacking Subunits Affiliated to the General Reconnaissance Bureau

Unit Name	**Other Names**	**Targets**	**Attack Vectors**
HIDDEN COBRA	Lazarus Group, Guardians of Peace, ZINC, NICKEL ACADEMY	Finance, aerospace & defense, manufacturing, healthcare, telecom, and media sectors	Adobe Flash player and Hangul Word Processor, fake job offers via LinkedIn and WhatsApp, and phishing emails that exploit Microsoft Word and zero-day vulnerabilities[89]

86. *See id.*; *see also Cybersecurity Investment Grows in 2020, But Organizations Face Record Data Breaches*, CANALYS (Mar. 29, 2021), https://www.canalys.com/newsroom/cybersecurity-investment-2020 [https://perma.cc/ZTK5-GAG5] (stating that more digital records were compromised from data breach in 2020 than in the previous fifteen years combined).

87. *See* Ed Caesar, *The Incredible Rise of North Korea's Hacking Army*, NEW YORKER (Apr. 19, 2021), https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army [https://perma.cc/5QAB-V4AS].

88. *Id.*

89. A zero-day vulnerability refers to a "software vulnerability discovered by attackers before the vendor has become aware of it." *What is a Zero-day Attack?—Definition and Explanation*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/zero-day-exploit [https://perma.cc/YNX5-6BVQ] (last visited Dec. 29, 2021).

Andariel (Lazarus Group subunit)	Silent Chollima, Dark Seoul, Rifle, Wassonite	South Korea's and western nations' financial institutions and governments	Vulnerabilities in local South Korean software including ActiveX, watering hole attacks,[90] spear phishing,[91] Antivirus and PMS products, and installers and updaters
APT38	Bluenoroff, Stardust Chollima, BeagleBoyz, NICKEL GLADSTONE	Banks, financial institutions, and cryptocurrency exchanges	Drive-by compromise,[92] watering hole schemes, out-of-date versions of Apache Struts2,[93] and access Linux servers

Source: HHS Office of Information Security[94]

North Korea is undoubtedly an extremely rare case of a nation state so actively and conspicuously harnessing state resources to commit financial crimes in cyberspace. The US Department of

90. A watering hole attack refers to a "security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit[,] . . . [with the goal of] infect[ing] a targeted user's computer and gain access to the network at the target's workplace." Gavin Wright, *Watering Hole Attack*, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/watering-hole-attack [https://perma.cc/9T9X-7KZR] (last visited Dec. 29, 2021).

91. Spear phishing refers to "an email or electronic communications scam targeted towards a specific individual, organization[,] or business . . . often intend[ing] to steal data for malicious purposes . . . [or] to install malware on a targeted user's computer." *What is Spear Phishing?—Definition*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/spear-phishing [https://perma.cc/57L8-SLVF] (last visited Dec. 29, 2021).

92. A drive-by compromise refers to "malicious programs that install to . . . devices without [the user's] consent." *What is a Drive by Download*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/drive-by-download [https://perma.cc/698R-LFGG] (last visited Dec. 29, 2021).

93 . Apache Struts is a free, open-source framework for creating Java web applications. *See Welcome*, APACHE STRUTS, https://struts.apache.org/ [https://perma.cc/PZ6W-L76L] (last visited Dec. 29, 2021).

94. *See* U.S. DEP'T OF HEALTH AND HUMAN SERVICES, OFF. OF INFO. SEC., *supra* note 24, at 6–15.

Justice has thus fittingly labeled the regime as a "criminal syndicate with a flag."[95]

B. Types & Characteristics of Pyongyang's Non-Primary Financial Cybercrimes: Ransomware Extortion Campaigns & Digital Bank Heist

There are at least five types of cyber-based financial crimes perpetrated by North Korea: ransomware extortion campaigns, digital bank heists, cryptocurrency theft, crypto-based cyber scams, and cryptojacking. The former two have become relatively less common in recent years than the latter three and hence could be considered non-primary financial cybercrimes. Cryptocurrency—a tradable blockchain-based virtual asset like Bitcoin or Ethereum[96]—plays a heavy role in all but the digital bank heist, although digital bank heists might also involve the use of cryptocurrency in their perpetration.

Ransomware extortion campaigns—the first type—are arguably the least sophisticated of North Korea's cyber operations, the most infamous case being the May 2017 WannaCry 2.0 ransomware attack.[97] During the attack, over 200,000 systems across 150 countries were infected by a Windows hacking technique stolen from the US National Security Agency.[98] The ransomware denied the owners' access to their computer or its data, demanding a payment of US$300 worth of Bitcoin or more to unlock the contents of the computers.[99] Some of the most heavily

95. Press Release, U.S. Dep't of Just., Assistant Attorney General John C. Demers Delivers on the National Security Cyber Investigation into North Korea Operatives (Feb. 17, 2021), https://www.justice.gov/opa/pr/assistant-attorney-general-john-c-demers-delivers-remarks-national-security-cyber [https://perma.cc/7GA8-VR76].

96. *What is Cryptocurrency?*, COINBASE, https://www.coinbase.com/learn/crypto-basics/what-is-cryptocurrency [https://perma.cc/34QB-84QH] (last visited Jan. 12, 2022).

97. *See Cyber-attack: US and UK Blame North Korea for WannaCry*, BBC (Dec. 19, 2017), https://www.bbc.com/news/world-us-canada-42407488 [https://perma.cc/ZE6X-EK66].

98. *See* Thomas Brewster, *Microsoft Just Took a Swipe at NSA Over the WannaCry Ransomware Nightmare*, FORBES (May 14, 2017), https://www.forbes.com/sites/thomasbrewster/2017/05/14/microsoft-just-took-a-swipe-at-nsa-over-wannacry-ransomware-nightmare/?sh=7fec72133585 [https://perma.cc/6UMS-N93R].

99. *See* Alex Hern & Samuel Gibbs, *What is WannaCry Ransomware and Why is it Attacking Global Computers?*, GUARDIAN (May 12, 2017),

hit targets were the United Kingdom's National Health Service and Telefónica, one of Spain's largest companies.[100]

Although the extensive nature of the WannaCry attack was shocking, cyber experts soon discovered that the attack was in fact "sloppy" [101] with several poor design ideas and errors; these defects included a web-based "kill-switch" [102] that limited its spread, hardcoded Bitcoin addresses that enabled law enforcement to easily track attempts to cash out the profits, and a malware design that disallowed the perpetrators from checking who actually paid the ransom. [103] The WannaCry attack hence generated just over US$55,000, a "catastrophic failure [from a ransom perspective with] . . . the lowest profit margin seen from any moderate or even small ransomware campaign."[104] This could be one of the reasons why North Korean hackers since "have avoided ransomware [and instead focused] more on efforts to breach international financial payment systems such as SWIFT [wire transfer] or cryptocurrency entities."[105] Nonetheless, North Korea is still occasionally launching ransomware extortion campaigns such as the Lazarus Group's two VHD ransomware-based attacks on systems in France and Asia in early 2020.[106]

---

https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 [https://perma.cc/942S-6SUU].

100. *See id.*

101. Andy Greenberg, *The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes*, WIRED (May 15, 2017), https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/ [https://perma.cc/4EBR-A96Y].

102. *Id.* ("[The hackers] inexplicably built a "kill switch" into their code, designed to reach out to a unique web address and disable its encryption payload if it makes a successful connection. Researchers have speculated that the feature might be a stealth measure designed to avoid detection if the code is running on a virtual test machine. But it also allowed a pseudonymous researcher who goes by the name MalwareTech to simply register that unique domain and prevent further infections from locking up victims' files.").

103. *See id.*

104. *Id.* The average ransom payment in 2020 was $312,000, which increased to $570,000 in the first half of 2021. *See also* Molly Clancy, *The True Cost of Ransomware*, BACKBLAZE (Sept. 9, 2021), https://www.backblaze.com/blog/the-true-cost-of-ransomware/ [https://perma.cc/25VN-RKC3].

105. Shannon Vavra, *North Korean Hackers are Stepping Up Their Ransomware Games, Kaspersky Finds*, CYBERSCOOP (July 28, 2020), https://www.cyberscoop.com/north-korea-ransomware-lazarus-group-kaspersky-vhd/ [https://perma.cc/HM23-8MWF].

106. *See id.* ("In two incidents earlier this year affecting two businesses—one in France and one in Asia—hackers tied to the Lazarus Group deployed a little-known ransomware strain called VHD, which is designed to steal money from victims.").

North Korea's digital bank heists—the second type—are more complex than its ransomware attacks, and the heist of Bangladesh Bank in February 2016 was perhaps the first incident that showed the world that North Korea's cyber operatives could inflict serious financial damages beyond simple hacking attacks of "cartoonish quality" like the 2014 Sony Pictures breach.[107] Now infamously known as the Bangladesh Bank heist, the attempt to steal close to a billion dollars from Bangladesh's central bank began in January 2015 when the Lazarus Group sent the bank's employees job-seeking emails with CV and cover letter attachments containing a virus.[108]

Once the virus infected the employees' computers and gained access to the bank's internal system, the hackers "began stealthily hopping from computer to computer" and eventually made their way to the digital vault—a process which took about a year.[109] At the same time, they established conduits for the money by opening up four accounts in the Jupiter Street branch of Rizal Commercial Banking Corporation ("RCBC") in the Philippines using fake driver's licenses; RCBC failed its KYC check regarding these four accounts even though the four supposed owners had the exact same title and salary at different workplaces.[110]

Then on Thursday February 4, 2016 at 8:36 p.m. Dhaka time, the hackers initiated thirty-five transfers of US$951 million—nearly the entire contents of the bank's New York Fed account—to their RCBC accounts.[111] Much of these transfers were blocked by the Fed because "Jupiter" fortunately coincided with the name of a sanctioned Iranian shipping business, but US$81 million still made it to RCBC accounts—of which US$65 million was successfully laundered through a Manilla casino before being sent to North Korea through a Chinese man named Weikang Xu and North Korean operatives based in Macau.[112]

In contrast to the Sony Pictures hack and WannaCry attack, the Bangladesh Bank heist was "flashy" in terms of its technical

107. Caesar, *supra* note 87.

108. *See* Geoff White & Jean H. Lee, *The Lazarus Heist: How North Korea Almost Pulled Off a Billion-dollar Hack*, BBC (June 21, 2021), https://www.bbc.com/news/stories-57520169 [https://perma.cc/VN7J-A46G].

109. *Id.*

110. *See id.*

111. *See id.*

112. *See id.*

intricacy with "a larger tactical and operational maturity."[113] For one, the Lazarus Group meticulously chose Thursday evening Dhaka time to initiate the transfers to exploit the fact that the Bangladeshi weekend runs from Friday to Saturday.[114] This had the effect of delaying the full discovery of the heist by three days; Bangladesh Bank was closed for two days while New York Fed was trying to unravel the situation, and the Fed was closed when Dhaka finally came back on line on Sunday.[115]

Another brilliant maneuver displayed by the Lazarus Group was how they ensured that their fraudulently authenticated SWIFT transfers would not get noticed by the bank. The hackers not only installed a network update that prevented Bangladesh Bank from reading the SWIFT messages,[116] but also took the bank's tenth floor printer—which recorded every single transaction for the paper back-up system—out of action by hacking into its operating software.[117] No other digital bank heist of this scale and ingenuity has been reported, although it is alleged that North Korea did attempt similar but much smaller-scale heists in Vietnam, Taiwan, Mexico, Malta, and Africa around the same time period.[118]

C. Types & Characteristics of Pyongyang's Primary Financial Cybercrimes: Cryptocurrency Theft, Crypto-based Cyber Scams, & Cryptojacking

Of the remaining three types of cyber-based financial crime, cryptocurrency theft warrants more attention given that it has become North Korea's primary tool of evading sanctions and laundering money in cyberspace. Cryptocurrency in general is also trickier to tackle for the AML authorities. Though crypto-based cyber scams and cryptojacking are not as prevalent as cryptocurrency theft, their discussion in this Part is warranted

113. Caesar, *supra* note 87.
114. *See* White & Lee, *supra* note 108.
115. *See id.*
116. *See* Caesar, *supra* note 87.
117. *See* White & Lee, *supra* note 108.
118. *See* U.S. DEP'T JUST., *Three North Korean Military Hackers Indicted in Wide-Range Scheme to Commit Cyberattacks and Financial Crimes Across the Globe* (Feb. 17, 2021), https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and [https://perma.cc/E2KC-9UBM].

given their relatively recent emergence and their possibility of complementing cryptocurrency theft.

Of these three, cryptocurrency theft is the predominately employed cybercrime and is estimated to have generated over US$1.75 billion for Pyongyang as of February 2021. [119] Cryptocurrency exchanges—online marketplaces where cryptocurrencies are traded [120] —have been common targets. Though small-sized exchanges with low levels of security resources are "low-hanging fruit for professional [North Korean] hackers,"[121] North Korea is alleged to have stolen US$49 million and US$275 million worth of cryptocurrency from South Korea's UpBit and Singapore's KuCoin—two of the largest exchanges in the world—respectively. [122] Considering that North Korea made a meager gain of US$55,000 from the WannaCry attack and that Bangladesh Bank heist's US$65 million was the outcome of extremely intricate planning and year-long patience, it is clear why cryptocurrency theft is the regime's preferred method of evading sanctions in cyberspace.

What is more important and intriguing about this activity than the theft itself, however, is how North Korea launders the stolen cryptocurrency with the goal of eventually cashing it out at the exchanges. This is because, even without stealing cryptocurrency, North Korea can still funnel and launder its illicit funds acquired by engaging in traditional, non-cyber-based activities through the cryptocurrency space. Cryptocurrency's unique advantage for money launderers is that cryptocurrency transactions are pseudonymous and are not tied to registered names of individuals or entities. [123] Transactions are recorded on the publicly decentralized blockchain, but it is enormously challenging for the authorities to match a transaction to an individual or entity

119. *Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options*, CHAINANALYSIS BLOG (Feb. 9, 2021), https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack [https://perma.cc/94JT-JJM3] [hereinafter CHAINANALYSIS].

120. *See What is Cryptocurrency?*, *supra* note 96.

121. Tim Alper, *Small Crypto Exchanges 'Low-hanging Fruit' for North Korea Hackers*, CRYPTONEWS (Oct. 15, 2019), https://cryptonews.com/news/small-crypto-exchanges-low-hanging-fruit-for-north-korean-ha-4858.htm [https://perma.cc/NZ6W-8F8W].

122. Chainanalysis, *supra* note 119.

123. *See* Nick Oberheiden, *Crypto Laundering: Bitcoin + Money Laundering*, NAT'L L.REV. (Oct. 14, 2021), https://www.natlawreview.com/article/crypto-laundering-bitcoin-money-laundering [https://perma.cc/4RDB-UMZW].

because only the transaction's initiator has access to the account and cryptocurrency wallet; without having access to these two, the matching process is time- and labor-intensive.[124] There is simply no reason why North Korea would shy away from laundering many if not most of its illicit funds as cryptocurrency—even if generated outside of cyberspace—given these characteristics.

Yet, hurdles still exist for laundering illicitly attained cryptocurrency as depositing a substantial volume at different exchanges raises red flags, and tracking pseudonymous transactions on the blockchain—although difficult—is not impossible.[125] Furthermore, even though many virtual wallet providers and exchanges have few or no implemented AML programs and KYC procedures,[126] those in certain jurisdictions, including the United States, are required to keep track of their customers' identities.[127]

To bypass these hurdles, North Korean money launderers rely on peel chains, a tactic in which stolen cryptocurrency is moved in "rapid and automated transactions [of small pieces of Bitcoin peeled from the whole] from one wallet to new addresses . . . in a way that both hides the source of money and lessens the risk of setting off red flags."[128] Money launderers often further complicate this by peeling a new chain from an already peeled Bitcoin piece, thus generating "peel chains of peel chains,"[129] and by using a chain-hopping tactic in which the money is converted from Bitcoin to more private cryptocurrencies.[130]

---

124. *See id.*

125. *See* Mike Orcutt, *This is How North Korea Uses Cutting-Edge Crypto Money Laundering to Steal Millions*, MIT TECH. REV. (Mar. 5, 2020), https://www.technologyreview.com/2020/03/05/916688/north-korean-hackers-cryptocurrency-money-laundering/ [https://perma.cc/8LXY-6E2W].

126. *See* Oberheiden, *supra* note 123.

127. *See* Tracy French & Barbara Stettner, *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches, in* THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: ANTI-MONEY LAUNDERING 2019 14, 16–20 (Joel M. Cohen & Stephanie Brooker eds., Glob. Legal Grp. 2019).

128. Patrick H. O'Neill, *North Korean Hackers Steal Billions in Cryptocurrency. How Do They Turn It Into Real Cash?*, MIT TECH. REV. (Sept. 10, 2020), https://www.technologyreview.com/2020/09/10/1008282/north-korea-hackers-money-laundering-cryptocurrency-bitcoin/ [https://perma.cc/5422-4ZZM].

129. Orcutt, *supra* note 125.

130. *See* O'Neill, *supra* note 128.

When the laundered cryptocurrency is finally ready to be cashed out, it is usually sent to rogue over-the-counter ("OTC") brokers who use their legitimate-looking accounts at exchanges to sell and turn it into fiat currency like dollars or euros.[131] This allows North Korean operatives to complete their money laundering process without exposing their identity to exchanges in jurisdictions where KYC is mandated. For instance, in March 2020 the United States charged two Chinese nationals, Yinyin Tian and Jiadong Li, for using their 113 exchange accounts to launder more than US$100 million worth of stolen cryptocurrency on behalf of their North Korean co-conspirators.[132]

The most recent trends, meanwhile, reveal that North Korean cryptocurrency-based money laundering operations are responding to the authorities' increased targeting of rogue OTC brokers like Tian and Li in a way that would make AML policing even more difficult. Lazarus Group, for example, is spreading out its funds by opening more accounts directly or soliciting more OTC brokers to mitigate the risk of getting its accounts frozen or seized; the number of Lazarus Group-associated accounts that had received at least US$1,000 worth of cryptocurrency at the top twenty exchanges jumped from 470 in December 2019 to 2,078 in December 2020.[133]

A potentially more threatening response by the Lazarus Group is its declining use of mainstream exchanges and increasing use of Decentralized Finance ("DeFi") platforms, which nearly doubled in 2020.[134] DeFi platforms, dubbed the "Wild West" of the cryptocurrency industry,[135] are a collection of initiatives taken by "hordes of computer programmers trying to bring traditional financial products such as loans to the blockchain."[136] The particular vulnerability that these platforms present is that they

131. *See* Orcutt, *supra* note 125.

132 . *Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack,* U.S. DEP'T JUST. (Mar. 2, 2020), https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack [https://perma.cc/BC7Y-RGDP].

133. CHAINANALYSIS, *supra* note 119.

134. *See id.*

135. Ryan Browne, *DeFi—the 'Wild West' of Crypto—is Next on Regulators' Hit List*, CNBC (Nov. 4, 2021), https://www.cnbc.com/2021/11/04/defi-the-wild-west-of-crypto-is-set-to-face-regulatory-crackdown.html [https://perma.cc/S5YZ-V2ZM].

136. *Id.*

are, as the name implies, even more decentralized than mainstream exchanges, permitting users to "swap one type of cryptocurrency for another without a centralized platform ever taking custody of the users' funds" [137] and without any KYC procedures in place. All these trends exemplify North Korean operatives' high adaptability to changing AML environment, once again showing their tactical and operational maturity already revealed by the Bangladesh Bank heist.

Though comparatively much smaller in scale than cryptocurrency theft, crypto-based cyber scams and cryptojacking also pose substantial risks to international AML efforts because the way they help Pyongyang evade sanctions and launder money in cyberspace is nearly identical to that of cryptocurrency theft; the only material difference is the method through which North Korean hackers generate illicit crypto-funds before the money laundering steps. In terms of crypto-based cyber scams, North Korea was allegedly behind Marine Chain, an Ethereum blockchain-based platform offering partial ownership of maritime vessels in exchange for tradeable digital tokens.[138] The platform—registered in Hong Kong in April 2018—attempted to attract investors to participate in the Vessel Token Offering. Its Singaporean CEO Jonathan Foong Ka Keon abruptly shut the program down when the UN Panel of Experts ("POE") began their inquiry into the platform. Foong had an extensive prior history of advising Singaporean shipping companies that have been accused of helping North Korea evade sanctions.[139] The POE also reported that North Korea used cryptojacking—the act of using malware-infected computers' computing power to mine cryptocurrency—in several instances,[140] including a case in which Andariel took over the server of a South Korean company to mine the cryptocurrency

137. CHAINANALYSIS, *supra* note 119.

138. *See* Cristina Rotaru, *The Curious Case of Marine Chain: The DPRK Cyberscam Behind a Blockchain-Powered Maritime Investment Marketplace*, VERTIC (Apr. 24, 2019), https://www.vertic.org/2019/04/the-curious-case-of-marine-chain-the-dprk-cyberscam-behind-a-blockchain-powered-maritime-investment-marketplace/ [https://perma.cc/DT4N-XEAE].

139. *See id.*

140. *See* U.S. DEP'T JUST. ET AL., DPRK CYBER THREAT ADVISORY: GUIDANCE ON THE NORTH KOREAN CYBER THREAT 2 (Apr. 15, 2020) [hereinafter DPRK CYBER THREAT ADVISORY].

Monero and sent the mined virtual coins to a server located in Kim Il Sung University in Pyongyang.[141]

Cryptocurrency-based financial crimes are likely to remain North Korea's primary sanctions evasion and money laundering operations in cyberspace. The regime has shown remarkable willingness and ability to embrace blockchain technology and possesses advanced levels of adaptability and maturity in deploying its schemes that have been displayed in its digital bank heists as well. Members of the international community, therefore, need to respond with urgency.

IV. EVALUATION OF PROPOSED SOLUTIONS

A. Limited & Insufficient Solution: Increasing Cybersecurity Resilience

Several potential solutions have been proposed to counter North Korea's financial crimes in cyberspace and similar activities perpetrated by numerous other groups, but it is questionable whether they could fundamentally resolve the problem. The most obvious, yet limited and insufficient solution is that the international community work together to enhance overall cybersecurity resilience. The United States, for example, "strongly urge[s] governments, industry, civil society, and individuals to take all relevant actions . . . to protect themselves from and counter the DPRK cyber threat," and recommends implementing cybersecurity best practices, raising awareness, and sharing technical information of North Korean schemes in cyberspace.[142] Congress passed the Cybersecurity Information Sharing Act of 2015 as part of a US nation-wide effort to respond to cyber threats from North Korea and other forces, and to promote the sharing of classified cyber threat indicators and defensive measures between federal and non-federal entities.[143] The Act makes it easier for non-federal entities such as private companies to share relevant cybersecurity information by granting greater protection from liability. [144]

141. *See* Arjun Kharpal, *Hackers Have Found a Way to Mine Cryptocurrency and Send It to North Korea*, CNBC (Jan. 9, 2018), https://www.cnbc.com/2018/01/09/north-korea-hackers-create-malware-to-mine-monero.html [https://perma.cc/D85L-2FZC].

142. DPRK CYBER THREAT ADVISORY, *supra* note 140.

143. Cybersecurity Information Sharing Act, 6 U.S.C. §§ 1501–1510 (2015).

144. *See* 6 U.S.C. § 1505 (2015).

However, despite some advancements since the Act's enactment,[145] there has been a "lack of progress in improving the quality of information [the Cybersecurity and Infrastructure Security Agency ("CISA")] shares."[146]

There may be reasonable steps US policymakers can take to further US cybersecurity resilience against North Korean cybercrimes. These include fixing the pitfalls observed by CISA in administering the existing regulations and guidelines [147] and delivering on their promises of improving the current system with the new Vulnerability Disclosure Platform ("VDP").[148] Additionally, policymakers could encourage more informed decision-making by passing the Risk-Informed Spending for Cybersecurity Act[149] to require agencies to invest in cybersecurity tools based on a new risk-based budgeting model.[150]

However, such reactive cybersecurity measures would only be temporary solutions before North Korean hackers devise yet another new malware or other innovative means to exploit unforeseen vulnerabilities. They have already proved this numerous times with their increasingly elaborate cyberspace tactics and adaptability. Even without considering North Korea specifically, the "arms race between cybercriminals and businesses has reached a fever pitch." [151] Global cybercrime damages are expected to grow by fifteen percent annually between 2020 and

145. *See* OFF. OF INSPECTOR GEN., DHS MADE LIMITED PROGRESS TO IMPROVE INFORMATION SHARING UNDER THE CYBERSECURITY ACT IN CALENDAR YEARS 2017 AND 2018 7–9 (Sept. 25, 2020) (stating that CISA met the Act's guidelines and periodic review requirements, successfully increased the number of classified threat indicators shared with non-federal entities, accurately accounted for the security clearances of private sector users, and increased the number of non-federal AIS participants).

146. *Id.* at 6.

147. *See id.* at 6–7 (explaining that CISA faced factors including limited numbers of AIS participants sharing cyber indicators with CISA, delays receiving cyber threat intelligence standards, and insufficient CISA office staff).

148. *See* Jason Miller, *CISA's Still Overcoming Challenges 5 Years After Cybersecurity Information Sharing Act Became Law*, FED. NEWS NETWORK (Oct. 6, 2020), https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/10/cisas-still-overcoming-challenges-5-years-after-cybersecurity-information-sharing-act-became-law/ [https://perma.cc/G2HA-TY3E].

149. S. 4785, 116th Cong. (2019).

150. *See* Miller, *supra* note 148.

151 . Daniel Petrillo, *Are Threat Actors Winning the Cybersecurity Arms Race?*, MORPHISEC BREACH PREVENTION BLOG (Mar. 18, 2021), https://blog.morphisec.com/are-threat-actors-winning-the-cybersecurity-arms-race [https://perma.cc/55RY-GMSL].

2025 [152] despite exponential growth in global spending on cybersecurity solutions.[153]

Even more proactive approaches so often endorsed by cybersecurity experts[154] are unlikely to be capable of satisfactorily resolving the problem. The South Korean government took an unusually stringent measure of completely segregating the country's intranet from the internet, [155] but this network separation policy has conflicted with Seoul's ambitious Fourth Industrial Revolution Policy[156]—predicated on cloud services and private data transfers—without meaningfully enhancing the country's safety from Pyongyang's cyber threat.[157] Furthermore, as discussed previously, even if cybersecurity is enhanced to effectively prevent hacking and malware attacks, North Korea could still actively try to launder a substantial portion of the regime's non-cyber-generated funds by using cryptocurrency. Hence, strengthening cybersecurity resilience—while necessary—can never be regarded as sufficient by itself.

---

152. Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [https://perma.cc/B626-Z6FZ].

153. *See* Petrillo, *supra* note 151.

154. *See* Mike Elgan, *What is Proactive Cybersecurity?*, SEC. INTEL. (Oct. 20, 2021), https://securityintelligence.com/articles/what-is-proactive-cybersecurity/ [https://perma.cc/EFY8-J9WH] (discussing ethical hacking, automated intelligence, zero trust policy, and focus on indicators of behavior as proactive cybersecurity measures); *see also* Dudu Mimran, *What is Proactive Cyber Defense?*, MORPHISEC BREACH PREVENTION BLOG (Oct. 29, 2020), https://blog.morphisec.com/what-is-proactive-cyber-defense [https://perma.cc/SP6C-LSGD] (discussing a comprehensive approach that encompasses measures like frequently updating patches, implementing moving target defense, and hardening end points against known attacks).

155. *See* Somang Yang, *Network Separation Rules Pose Problems for South Korea*, PS-ENGAGE (June 24, 2021), https://ps-engage.com/network-separation-rules-pose-problems-for-south-korea/ [https://perma.cc/YC2H-J8JX] ("The network separation regulation requires the separation of internal workloads connected to the internal networks (intranet) from the external communication network, such as the internet. The reason for the separation is security. Initially implemented in the public sector, after a large-scale computer network scare, it was introduced in the financial sector.").

156. *See* Eun DuBois, *Building Resilience to the North Korean Cyber Threat: Experts Discuss*, BROOKINGS INST. (Dec. 23, 2020), https://www.brookings.edu/blog/order-from-chaos/2020/12/23/building-resilience-to-the-north-korean-cyber-threat-experts-discuss/ [https://perma.cc/56DE-X94R]. South Korea's Presidential Committee on the Fourth Industrial Revolution's policy objectives are centered around "bolster[ing] the data-based digital economy" including artificial intelligence and digital healthcare. *About PCFIR*, PRESIDENTIAL COMM. ON THE FOURTH INDUS. REVOLUTION, https://www.4th-ir.go.kr/en/greetings [https://perma.cc/582U-8EJ5] (last visited Dec. 30, 2021).

157. *See* DuBois, *supra* note 156.

B. Distant, Uncertain, & Exploitable Solution: Adopting CBDC While Illegalizing Cryptocurrency

Some have proposed that governments should take the hardline step of banning cryptocurrencies altogether and adopting central bank digital currencies ("CBDC") in preparation for the impending digital economy,[158] a solution that is not only distant and uncertain but also entails risks of being exploited by Beijing to aid Pyongyang. Critics of the cryptocurrency industry argue that cryptocurrencies like Bitcoin are nothing but a "libertarian fantasy" [159] that are unstable, [160] essentially valueless, [161] and environmentally hazardous. [162] They believe that it is the government's duty to "guarantee safe, usable, and stable money," and instead advocate CBDC as a solution that fulfills this principle. [163] The Bank of International Settlements ("BIS") agrees with this contention, stating that cryptocurrencies are "speculative assets rather than money [that] in many cases are used to facilitate money laundering, ransomware attacks, and other financial crimes, . . . with few redeeming public interest attributes . . . considering its wasteful energy footprint." [164] The BIS further contends that with adequate international cooperation, mutual recognition, and some degree of harmonization, CBDCs of different

158. *See, e.g.*, Martin Wolf, *The Time to Embrace Central Bank Digital Currencies is Now*, FIN. TIMES (July 20, 2021), https://www.ft.com/content/7a93fb0a-ae95-44fc-a3d2-1398ef0ce1af [https://perma.cc/24GN-933B]; Robert A. Manning, *Bye-bye, Bitcoin: It's Time to Ban Cryptocurrencies*, HILL (July 25, 2021), https://thehill.com/opinion/cybersecurity/564696-bye-bye-bitcoin-time-to-ban-crypto-currencies?rl=1 [https://perma.cc/TH7L-E59V].

159. Wolf, *supra* note 158.

160. Manning, *supra* note 158 ("[T]he risks and chaos of a wild world of unstable private money is a libertarian fantasy. According to a recent Federal Reserve paper, there are already some 8,000 cryptocurrencies. It's a new mom-and-pop cottage industry.").

161. Manning contends that unlike dollars, euros, and yen that are backed by nation's respective treasuries, any value assigned to cryptocurrency is "based solely on convincing others it has value." *See id*.

162. *See id.* Another source suggests that Bitcoin mining operations used as much energy as Denmark, or enough to power more than three million U.S. households in 2017, thereby rending it environmentally unsustainable and wasteful. *See* Chris Mooney & Steven Mufson, *Why the Bitcoin Craze is Using Up So Much Energy*, WASH. POST (Dec. 19, 2017), https://www.washingtonpost.com/news/energy-environment/wp/2017/12/19/why-the-bitcoin-craze-is-using-up-so-much-energy/ [https://perma.cc/DU49-XRKU].

163. Manning, *supra* note 158.

164. Bank of Int'l Settlements [BIS], *BIS Annual Economic Report 2021*, at 67, (June 29, 2021).

nations could effectively improve cross-border payments and limit the risks of currency substitution.[165]

CBDC is not merely a theoretical construct but an increasingly materializing reality in many parts of the globe. China has taken an early lead in this field, completely banning cryptocurrency mining and transactions in September 2021 as it rolled out pilot programs for its CBDC in select cities.[166] As of October 2021, over 140 million people have reportedly spent more than US$9.5 billion using e-CNY—the Chinese CBDC's official name—with over one-and-a-half million merchants accepting e-CNY payments.[167] With the People's Bank of China ("PBOC") ahead of the game, CBDCs could potentially disrupt the current international monetary system predicated on the US dollar.[168] The European Central Bank,[169] the Bank of England,[170] and the Bank of Japan[171] have also embarked on the process of developing their own CBDCs. Besides these largest central banks, the Indian government has signaled that it wants to ban cryptocurrency in the near future to adopt its own CBDC[172] and the US Federal Reserve is also expected to soon begin its

165. *See id.* at 85–90.

166. *See* Kenneth Rapoza, *China 'Banned' Crypto. Can SEC Try Doing the Same?*, FORBES (Oct. 11, 2021), https://www.forbes.com/sites/kenrapoza/2021/10/11/china-banned-crypto-can-the-sec-try-doing-the-same/?sh=57dd3b09455c [https://perma.cc/NR2C-CYJX].

167. Mark Potter, *$9.5 Billion Spent Using Chinese Central Bank's Digital Currency—Official*, REUTERS (Nov. 3, 2021), https://www.reuters.com/technology/95-billion-spent-using-chinese-central-banks-digital-currency-official-2021-11-03/ [https://perma.cc/AC7Q-GK68].

168. *See* Manning, *supra* note 158 (stating that China's CBDC sets renminbi in the direction of rivaling the dollar as international reserve currency in the distant future).

169. Press Release, European Central Bank, Eurosystem Launches Digital Euro Project (July 14, 2021), https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html [https://perma.cc/WZ6H-NVGE].

170. Press Release, Bank of Eng., Statement on Central Bank Digital Currency Next Steps (Nov. 9, 2021), https://www.bankofengland.co.uk/news/2021/november/statement-on-central-bank-digital-currency-next-steps [https://perma.cc/FS9Q-GNX6].

171. *See* Namrata Shukla, *Japan's CBDC Plans to 'Speed Up' in Light of Other Countries 'Moving Ahead' with Theirs*, AMBCRYPTO (Dec. 1, 2021), https://ambcrypto.com/japan-ramping-up-political-pressure-as-chinas-digital-yuan-inches-closer-to-launch/ [https://perma.cc/5BUV-CSTH].

172. *See* Jeanette Rodrigues & Suvashree Ghosh, *Is India Banning Cryptocurrency? How Can It Do That?: Quick Take*, BLOOMBERG (Nov. 28, 2021), https://www.bloomberg.com/news/articles/2021-11-28/is-india-banning-cryptocurrency-how-can-it-do-that-quicktake [https://perma.cc/4R9A-CG38].

review of a possible digital dollar issuance.[173] This trend shows that the proposal of illegalizing or at least more heavily regulating cryptocurrency and adopting CBDC has some merits for even the leading central banks to seriously contemplate, although almost all CBDC projects are "moving at a sluggish pace" and are a long way from becoming reality except for that of China.[174]

It is unclear as to whether banning cryptocurrency to facilitate an environment for CBDC adoption is going to work. Besides the blatant fact that illegalizing the now gigantic and thus "unspookable" [175] cryptocurrency industry entirely could have devastating economic consequences; it is highly unlikely that it could achieve its intended outcome. The Chinese cryptocurrency ban has shown that the industry is remarkably resilient, and that cryptocurrency miners and traders will simply move elsewhere or go underground.[176] Chinese market players of all types—from small cryptocurrency peer-to-peer lending startups[177] to giant e-commerce companies and digital financial firms like Alibaba, Yillion Group, and Hande Group—had already relocated their crypto-based operations months overseas before Beijing's strongest crackdown in late 2021.[178] The global Bitcoin mining

173. *See* Andrew Ackerman, *Fed Prepares to Launch Review of Possible Central Bank Digital Currency*, WALL ST. J. (Oct. 4, 2021), https://www.wsj.com/articles/fed-prepares-to-launch-review-of-possible-central-bank-digital-currency-11633339800 [https://perma.cc/3BNJ-N6VZ].

174. Ryan Browne, *Central Bank Digital Currencies are a Long Way from Becoming Reality—Unless You're in China*, CNBC (Nov. 12, 2021), https://www.cnbc.com/2021/11/12/central-bank-digital-currencies-are-moving-slowly-but-not-in-china.html [https://perma.cc/4RLJ-42NA] [hereinafter Browne, *CBDCs are a Long Way from Becoming Reality*].

175. *See* Rapoza, *supra* note 166.

176. Sadie Williamson, *Why China's Ban was the Best Thing for Bitcoin in 2021*, BITCOIN MAG. (Jan. 7, 2022), https://bitcoinmagazine.com/business/how-china-ban-improved-bitcoin-in-2021 [https://perma.cc/B3FL-EDUL].

177. Peer-to-peer lending firms facilitate the borrowing and lending of loans between two users without the intermediation of banks. Crypto-based peer-to-peer lending has loans denominated in cryptocurrency and executed on a blockchain network that processes the loan agreement. *What is Peer-to-Peer Lending?*, GEMINI (Mar. 14, 2021) https://www.gemini.com/cryptopedia/peer-to-peer-lending-loans#section-crypto-based-peer-to-peer-lending [https://perma.cc/5CCW-N92X].

178. Singapore accepted over three hundred cryptocurrency license applications from those Chinese businesses in July 2021 alone. *See* Ralph Jennings, *How China's Ban on Cryptocurrency Will Ripple Overseas,* VOICE OF AM. (Oct. 2, 2021), https://www.voanews.com/a/how-china-s-ban-on-cryptocurrency-will-ripple-overseas-/6254329.html [https://perma.cc/GWF7-EN9C].

activity, measured in computing power used for mining, also fully recovered in only a few months from its abrupt crackdown-induced drop as Chinese mining operations moved to hubs like the United States or new underground mining sites located on small farms across China.[179]

Whether CBDC adoption itself could adequately address the current money laundering problem is unclear as well. CBDCs' higher traceability and other technical aspects may certainly help governments combat some money laundering operations compared to physical cash, but they are still likely to "nevertheless be [a] tempting target for bad actors, both state and non-state, who will adapt their methods accordingly."[180] Some predict that CBDCs, by adding unique technical features such as wallet programmability and microtransactions to fiat money, may in fact "enable more intricate money laundering schemes,"[181] rather than help the international community eradicate money laundering and other related financial crimes. This concern has already been partially vindicated by the fact that the Chinese authorities have already uncovered at least two CBDC-based money laundering schemes during its e-CNY pilot phase.[182]

Adding more to this lack of clarity about CBDC's AML efficacy is that governments have many things to sort out before they can adopt CBDCs on a wide scale. Even the CBDC advocates accept that there are too many uncertainties and controversies associated with CBDC as of now, including CBDC's ambiguous relationship with existing fiat currency, impact on private banks, and the question of privacy and surveillance.[183] All these issues are "way

179. MacKenzie Sigalos, *Bitcoin Mining Has Completely Recovered from Chinese Ban,* CNBC (Dec. 10, 2021), https://www.cnbc.com/2021/12/10/bitcoin-network-hashrate-hits-all-time-high-after-china-crypto-ban.html [https://perma.cc/HJP5-PFEV].

180. Yaya J. Fanusie, *Central Bank Digital Currencies: The Threat from Money Launderers and How to Stop Them*, LAWFARE BLOG (Dec. 14, 2020), https://www.lawfareblog.com/central-bank-digital-currencies-threat-money-launderers-and-how-stop-them [https://perma.cc/ZD4J-434H].

181. *Id.*

182. *See China Catches Fraudsters Using Central Bank Digital Currency for Money Laundering*, LEDGER INSIGHTS (Nov. 15, 2021), https://www.ledgerinsights.com/china-catches-fraudsters-central-bank-digital-currency-cbdc-for-money-laundering/ [https://perma.cc/7WLF-MF4S].

183. *See* Manning, *supra* note 158.

above the paygrade of every central banker."[184] The most contentious issue of financial censorship—a negligible hurdle for PBOC but a major policy topic for almost all other central banks—will most likely slow down the already sluggish progress with CBDC adoption outside of China.

But the real danger with CBDC concerning North Korea specifically is that Beijing could abuse the global CBDC infrastructure to aid Pyongyang's money laundering operations. As discussed in previous Parts, detailed descriptions of North Korean sanctions evasion and money laundering operations are consistently accompanied by external, Chinese co-conspirators such as Xiaohong Ma, Faith Surplus Trading Ltd., Dandong Sanjiang Trading Co. Ltd., China Oil Singapore, Weikang Xu, Yinyin Tian, and Jiadong Li.[185] Whereas one might easily brush this off as a natural occurrence due to North Korea's geographic proximity to China as well as its heavy economic dependence on China, the international community has reasonable grounds to believe that the Chinese state is actively assisting the Kim regime in committing cybercrimes and laundering its funds—an allegation which Beijing has repeatedly denied.[186] Although Beijing is "not excited about an overly aggressive North Korea,"[187] it also does not want the Kim regime to collapse because it has traditionally viewed North Korea as a crucial buffer state between itself and South Korea, and also sees its aid to Pyongyang as "chip[ping] away at American strength and prestige."[188]

Given these circumstances, Beijing's greater control over transactions and payments through e-CNY's "controlled anonymity" and the government's ability to program each e-CNY according to

184. Browne, *CBDCs are a Long Way from Becoming Reality*, *supra* note 174 (quoting Garrick Hileman, head of research of Blockchain.com and visiting fellow at the London School of Economics).

185. *See* discussions *supra* Section II.C, Section III.B, Section III.C.

186. *Senior U.S. Official Accuses China of Aiding North Korea Cyber Thefts*, REUTERS (Oct. 22, 2020), https://www.reuters.com/article/us-usa-northkorea-china/senior-u-s-official-accuses-china-of-aiding-north-korea-cyber-thefts-idUSKBN2772RX [https://perma.cc/473H-PGX4].

187. *Id.*

188. John Pomfret, *Opinion: The Real Reason China Won't Turn Against North Korea*, WASH. POST (Sept. 8, 2017), https://www.washingtonpost.com/news/global-opinions/wp/2017/09/08/the-real-reason-china-wont-turn-against-north-korea/ [https://perma.cc/WMQ4-VBCV].

its need[189] may not actually be helpful for the international community in tackling North Korean cyberspace financial crimes and money laundering. Rather, it may result in Beijing's selective AML enforcement under which the Chinese regulators could clamp down on money laundering activities that do not serve its interests while turning a blind eye to those committed by Pyongyang or even facilitating them. If PBOC does achieve its objective of reorganizing the global financial industry with its CBDC infrastructure supplanting the dollar in the long run, or at the very least significantly increasing the role of e-CNY in global transactions, then it could potentially open new avenues for Beijing to continue assisting Pyongyang with even greater independence from the current US-led global AML regime.

This does not mean, however, that CBDC adoption is an undesirable policy that needs to be opposed at all costs. Though CBDC is "the future of money,"[190] there is going to be a long period before its widespread adoption, during which North Korea will continue to commit cybercrimes and launder funds generated from those activities. The international community needs a solution that will serve the world both in the meantime and after CBDCs arrive in full force.

C. The More Potent Yet Still Likely Futile Solution: Upward Harmonization of Global AML Regulatory Standards

An upward harmonization of global AML regulatory standards is probably a more potent policy proposal compared to the other suggested solutions, although efficacy is likely limited due to many countries' lack of urgency to actively participate. Currently, AML regulatory standards have some degree of global harmonization efforts undertaken by the Financial Action Task Force ("FATF"), which has issued risk-based AML/CFT policy recommendations followed by a series of updates since 2012.[191]

189. Shruti Gupta, *China's Digital Yuan is All About Data—and, Perhaps, Control*, INDUS. WEEK (Sept. 1, 2021), https://www.industryweek.com/the-economy/trade/article/21174069/chinas-digital-yuan-is-all-about-dataand-perhaps-control [https://perma.cc/BJ7P-MFFV].

190. Fanusie, *supra* note 180.

191. *See The FATF Recommendations,* FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-

The FATF also monitors individual countries' level of compliance with its recommendations and regularly issues a "grey list" and "black list" which, respectively, contain the names of jurisdictions subject to increased monitoring and the names of high-risk jurisdictions subject to call for action.[192] North Korea and Iran are the only two countries on the black list as of January 2022.[193]

The emergence of the cryptocurrency industry and blockchain technology has complicated the matter, however, to which the FATF responded in June 2019 by issuing an Interpretive Note to Recommendation 15 that pushes governments to extend their existing AML measures to virtual assets and their service providers.[194] The Interpretive Note strongly urges countries to apply the same level of regulations as directed by Recommendations 1, 10–16, and 35 and to require virtual asset service providers to be either licensed or registered.[195] Yet, nations are still displaying "salient differences" in the following areas of crypto-AML regulations: (1) the existence of special licensing requirements for cryptocurrency exchanges; (2) the extent to which the regulations cover administrators and wallet services; (3) whether initial coin offerings ("ICOs") are regulated under securities laws; and (4) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange.[196]

Even the leading nations with the highest AML standards are struggling to maintain their regulatory consistency across the board while keeping up with changing dynamics and ever more innovative cybercriminals and money launderers. In the United States, the very question of whether cryptocurrency is a currency,

---

recommendations.html#UPDATES [https://perma.cc/XLJ2-AVLU] (last visited Dec. 13, 2021).

192. *See Topic: High-risk and Other Monitored Jurisdictions*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate) [https://perma.cc/84SY-SKTZ] (last visited Jan. 30, 2022).

193. *See High-risk Jurisdictions Subject to a Call for Action—21 February 2020*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html [https://perma.cc/YF8U-KVAH] (last visited Jan. 30, 2022).

194. *See* French & Stettner, *supra* note 127, at 16.

195. FIN. ACTION TASK FORCE, THE FATF RECOMMENDATIONS: INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 76–77 (2021).

196. French & Stettner, *supra* note 127, at 16.

a security, or a commodity remains unsettled along with the issue of whether a person handling cryptocurrency counts as "financial institution" according to the registration requirements of FinCEN, the Securities and Exchange Commission ("SEC"), and the Commodity Futures Trading Commission ("CTFC").[197] Overlapping regulations and nonexistence of bright line tests challenges US regulators and compliance personnel and "mak[es] ascertaining the regulatory status of particular customer types and activities labor-intensive."[198]

The European Union adopted the Fifth AML Directive (EU) 2018/843 ("5MLD") in 2018, which added heightened risk-based approaches to the prior Fourth AML Directive (EU) 2015/849 ("4MLD"). [199] 5MLD broadened the AML-regulated entities' requirement to examine the background and purpose of a wider range of transactions and also mandated that they apply enhanced due diligence ("EDD") measures to transactions involving select high-risk third countries. [200] These EDD measures include obtaining additional information about the ultimate beneficial owner ("UBO"),[201] increasing the number and timing of control for monitoring, and requiring senior management approval for establishing and continuing a business relationship with a high-risk third country. [202] Nevertheless, EU member nations show varying degrees of 5MLD application and extension to the cryptocurrency space, [203] potentially giving rise to the same problems that US regulators and compliance personnel are facing. Harmonizing these different AML regulatory frameworks—both

197. *See id*.

198. *Id.* at 17.

199. *See* Peter Burrell & Michael Thorne, *The Fifth EU Money Laundering Directive: What Does This Mean for the "Risk-Based" Approach" to Due Diligence?*, WILLKIE FARR & GALLAGHER 2 (Feb. 20, 2019) https://www.willkie.com/-/media/files/publications/2019/02/the_fifth_eu_money_laundering_directive_what_does_this_mean_for_the_risk_based_approach_to_due_diligence.pdf [https://perma.cc/C9X2-ZKF9].

200. *See id.*

201. An Ultimate Beneficial Owner refers to a person who is the ultimate beneficiary of a transaction initiated by an institution. A jurisdiction typically considers an individual holding a minimum of 10-25 percent of capital or voting rights in the institution as a UBO. *What is an Ultimate Beneficial Owner (UBO)?*, SWIFT, https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/ultimate-beneficial-owner-ubo [https://perma.cc/M54V-MGG2] (last visited Mar. 8, 2022).

202. *See* Burrell & Thorne, *supra* note 199, at 2–3.

203. *See* French & Stettner, *supra* note 127, at 18–20.

for traditional and non-traditional assets with focus on cryptocurrency—could substantially enhance international efforts against North Korean money laundering operations by resolving the confusing coexistence of overlapping and conflicting policies. It would also promote coordinated global AML policymaking and enforcement.

This promising solution could be potent only if the AML standards are harmonized upward, with particular emphasis on bringing the high-risk developing countries—through which North Korea channels its illicit transactions—on board. The critical cybersecurity and AML vulnerabilities of these countries, in addition to Chinese co-conspirators, have been instrumental in enabling Pyongyang's financial cybercrimes and subsequent money laundering schemes.[204] Among the cases discussed in the previous Parts, the arguably most egregious example is the Filipino bank RCBC's utter failure to take the most basic KYC steps regarding the Lazarus Group's account openings during the Bangladesh Bank heist.[205] Unsurprisingly, except for Indonesia, the Basel Institute of Governance[206] has evaluated Southeast Asian developing countries—the non-Chinese jurisdictions most actively approached by Pyongyang's agents to launder funds—to be below both regional and global averages in terms of AML/CFT risk preparedness.[207] Cambodia and Myanmar, the two riskiest Southeast Asian jurisdictions, are on the FATF grey list as of January 2022.[208]

Unfortunately, it is unlikely that getting these high-risk countries on board is going to be easy. Many high-risk countries

204. *See* discussion *supra* Part III.

205. *See* discussion *supra* Section III.B.

206. The Basel Institute on Governance is a non-profit foundation based in Switzerland that conducts research and advises international private and public partners with respect to many anti-corruption issues such as asset recovery, collective action, corporate governance and compliance, and public governance. *See About Us,* BASEL INST. ON GOVERNANCE, https://baselgovernance.org/about-us [https://perma.cc/2HAW-SMPY] (last visited Dec. 30, 2021).

207. *See* BASEL INST. ON GOVERNANCE, BASEL AML INDEX 2021: RANKING MONEY LAUNDERING AND TERRORIST FINANCING RISKS AROUND THE WORLD 31–32 (10th ed. 2021) [hereinafter BASEL AML INDEX 2021].

208. *See Jurisdictions Under Increased Monitoring—October 2021*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-october-2021.html [https://perma.cc/8MZ4-DEZ5] (last visited Dec. 13, 2021).

and regions are riddled with political and economic problems associated with high AML/CFT risks.[209] Such factors include bribery and corruption, political instability, and low public and financial transparency and accountability.[210] The FATF's analysis of Cambodia's AML/CFT implementation efforts, for example, states that the country's lagging AML system is due to multiple factors including its dollarized and largely cash-based economy, systemic capacity and resource constraints, and high levels of corruption.[211] The US Department of the Treasury, in particular, has attributed Cambodia's poor AML infrastructure to corruption, which it describes as "endemic."[212] High-risk countries in other regions may have additional unique reasons for lacking the urgency to implement and enforce heightened AML standards against North Korea. As discussed previously, some African governments and related entities are thought to be acting together with Pyongyang in arms proliferation and thus are unlikely to jeopardize such ongoing relationship with North Korea.[213]

But the issue of stopping North Korea's financial cybercrimes and sanctions evasion ultimately depends on whether China—whose pivotal role in facilitating most of Pyongyang's illicit conducts has been discussed exhaustively in this Note—would withdraw its ambivalent support for the Kim regime. Given that Beijing is highly unlikely to do so in the foreseeable future,[214] harmonizing global AML regulatory standards upwards is likely futile despite its possible potency.

---

209. *See* BASEL AML INDEX 2021, *supra* note 207 at 31-36, 39-42 (showing that East Asia and Pacific, Latin America and Caribbean, Middle East and North Africa, South Asia, and Sub-Saharan Africa regions have meaningfully higher risk scores for the mentioned political and economic factors than Europe and North America).

210. *See id.* at 4, 46-47.

211. *See* ASIA PACIFIC GRP. ON MONEY LAUNDERING, CAMBODIA MUTUAL EVALUATION REPORT 3-6 (Sept. 2017).

212. U.S. DEP'T OF THE TREASURY, CONSIDERATIONS FOR U.S. COMPANIES AND ORGANIZATIONS THAT CONDUCT BUSINESS IN CAMBODIA WITHIN KEY SECTORS OR IN PARTNERSHIP WITH HIGH RISK ENTITIES 1-4 (Nov. 10, 2021), https://home.treasury.gov/system/files/126/cambodia_advisory_11102021.pdf [https://perma.cc/RD95-2R3H].

213. *See* discussion *supra* Section II.C.

214. Eleanor Albert, *The China-North Korea Relationship*, COUNCIL ON FOREIGN RELATIONS (June 25, 2019, 8:00 AM), https://www.cfr.org/backgrounder/china-north-korea-relationship [https://perma.cc/9JBQ-LNCX] (describing the resilience of China's supportive relationship with North Korea and stating that China's close ties with Pyongyang also helps Beijing in managing its relationship with the United States).

V. ACHIEVING INCREMENTAL GAINS IN UPWARD AML REGULATORY HARMONIZATION THROUGH FINANCIAL INCENTIVE STRUCTURES

Notwithstanding these immense challenges, however, failing to enforce AML/CFT measures against North Korea is likely to generate even more disturbing results by emboldening Pyongyang and other rogue nations that are testing the waters. It may even send a wrong signal to financial institutions—which have either tacitly or unwittingly processed North Korea's laundered funds[215]—and weaken their appetite for regulatory compliance. Therefore, even if China's and other North Korean trading partners' cooperation is hard to obtain, the international community must still aim for incremental gains in upward regulatory harmonization by proactively incentivizing countries with weak AML regimes to adopt the latest AML standards. Whereas increasing political and economic pressure against countries with lagging AML systems and commitments is a possible strategy, such approach could backfire at a time when China is increasingly seeking to rearrange the world order by forming its own network of allies opposed to the US-led democratic value system, respect for the rule of law, and human rights.[216] Countries may find international pressure intended to compel their participation in upward AML regulatory harmonization to be distasteful "bullying and interference"[217] and in return swerve to Chinese sphere of influence. Therefore, the focus should be on formulating financial incentive structures that could induce these nations' participation, especially where the lagging AML regime is due to resource constraints.

Ongoing efforts and some recent successes regarding climate change action could serve as a benchmark for these incentive structures. Though in a different context, financial incentives provided by developed, high-income countries have been

215. *See* discussion *supra* Section II.C.

216. *See* Steven L. Myers, *An Alliance of Autocracies? China Wants to Lead a New World Order*, N.Y. TIMES (Mar. 29, 2021), https://www.nytimes.com/2021/03/29/world/asia/china-us-russia.html [https://perma.cc/A3WL-Y5B7].

217. *Id*. (describing Chinese foreign minister Wang Yi's characterization of U.S. foreign policy during his summit with Russian foreign minister Sergey V. Lavrov at Guilin, China in late 2021).

projected to be effective at systematically decreasing developing, middle-, and low-income countries' carbon emissions where sanctioning mechanisms against violators of governing international agreements are deficient.[218] In the late 2000s, growing awareness led to discussions about encouraging developing countries to mitigate greenhouse gas emissions through financing.[219] The Canada-based independent think tank International Institute for Sustainable Development's ("IISD") 2009 report outlined two possible financing methods: (1) a wholesale "fund of funds"—a new institution that would collect funds from various sources before distributing them to smaller and more-focused climate mitigation funds and projects[220]—and (2) a set of self-standing funds each with its own funding sources and specific purpose.[221]

Whereas the wholesale approach has unique advantages including flexible and optimal fund aggregation and allocation, the IISD report explained that the approach does come with a disadvantage: [222] The additional layer of bureaucracy and political complexity associated with the creation of a new institution.[223] In 2010, member states of the United Nations Framework Convention on Climate Change ("UNFCCC")—a multilateral environmental agreement which came into effect in 1994[224]—established the Green Climate Fund ("GCF") to finance developing countries under the wholesale approach with funds provided by developed UNFCCC member governments.[225] Despite its shortcomings,[226] the GCF approved US$23.4 billion worth of mitigation projects and

218. Yali Dong et al., *Financial Incentives to Poor Countries Promote Net Emissions Reductions in Multilateral Climate Agreements*, 4 ONE EARTH 1141, 1141–42 (2021).

219. DEBORAH MURPHY ET AL., ENCOURAGING DEVELOPING COUNTRY PARTICIPATION IN A FUTURE CLIMATE CHANGE REGIME 2 (Int'l Inst. for Sustainable Dev. 2009).

220. *Id*. at 45.

221. *See id*. at 46.

222. *See id.*

223. *See id.*

224. *See What is the United Nations Framework Convention on Climate Change?*, U.N. CLIMATE CHANGE, https://unfccc.int/process-and-meetings/the-convention/what-is-the-united-nations-framework-convention-on-climate-change [https://perma.cc/7T7W-FZXJ] (last visited Dec. 31, 2021).

225. *See* U.N. Doc. FCCC/CP/2010/7/Add.1, at ¶ 102 (Mar. 15, 2011).

226. Sanjay Kumar, *Green Climate Fund Faces Slew of Criticism*, 527 NATURE 419–20 (2015) (asserting that GCF has not only failed to meet its fund aggregation objectives but also lacks transparency and is seriously understaffed).

successfully disbursed over US$1.5 billion for projects under implementation between 2015 and 2020.[227]

Meanwhile, the self-standing funds approach is also actively being implemented. As of December 2021, the Biden administration has announced its plan to double the financing of developing countries for climate mitigation compared to that of the Obama administration.[228] The World Bank is also planning on committing thirty-five percent of its total Group financing for climate mitigation projects through 2025.[229]

The international community could emulate the climate change financing efforts to establish incentive structures for inducing target countries' upward AML regulatory harmonization. In fact, the wholesale approach for boosting harmonization would likely not require creating an entirely new funding delivering institution like the GCF, as there are already existing AML/CFT assistance programs such as the FATF and the World Bank's Financial Integrity unit which provide client countries with AML policy development, assessment, and other technical assistance.[230] Revamping these existing AML/CFT assistance programs by adding funding functions to their operations could incentivize nations to increase their political commitment to improving their AML regime and grant them greater access to the financial resources necessary for implementing those improvements. Simultaneously, the United States and other leading AML countries, the United Nations, and the World Bank could make a separate self-standing funds approach by reformulating their external aid and international development programs around AML/CFT. This could encompass funds being directed towards anti-corruption and AML/CFT infrastructure in developing countries or the delivery of

227. GREEN CLIMATE FUND, CLIMATE ACTION DURING THE PANDEMIC 10 (2020).

228. Press Release, White House, Executive Summary: U.S. International Climate Finance Plan (Apr. 22, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/executive-summary-u-s-international-climate-finance-plan/.

229. Press Release, World Bank Grp., World Bank Group Increases Support for Climate Action in Developing Countries (June 22, 2021), https://www.worldbank.org/en/news/press-release/2021/06/22/world-bank-group-increases-support-for-climate-action-in-developing-countries [https://perma.cc/PX9Z-Q3P5].

230. *Financial Integrity*, WORLD BANK GRP., https://www.worldbank.org/en/topic/financialmarketintegrity [https://perma.cc/5QPD-6Z78] (last visited Dec. 31, 2021).

certain aid packages conditioned on material enhancements in the recipient nation's AML environment.

VI. CONCLUSION

North Korea has relentlessly engaged in financial crimes and money laundering activities to evade international sanctions and has recently expanded these illicit operations into cyberspace through ransomware extortion campaigns, digital bank heists, cryptocurrency theft, crypto-based scams, and cryptojacking. Not only are these activities funneling money into the Kim regime's nuclear programs and other destabilizing military buildups, but they are also inflicting serious monetary losses and cybersecurity breaches on victim nations, financial institutions, cryptocurrency exchanges, and many other organizations and individuals. The decentralized, pseudonymous, and largely unregulated nature of cross-border cyberspace, coupled with Pyongyang's reliance on third-party international intermediaries and the growing sophistication of North Korean cyber operatives' tactical and operational adaptation to the changing AML/CFT environment, complicates international regulatory response.

There is unfortunately no silver bullet when it comes to North Korea. Building cybersecurity resilience and forcefully phasing out cryptocurrency in favor of CBDC adoption are too weak, distant, or exploitable to be adequate strategies for countering Pyongyang's ever more cunning, innovative, and adaptive criminal activities in cyberspace. As long as China and certain other nation-states are slow at or opposed to implementing and enforcing the highest AML standards against North Korea, Pyongyang will remain largely undeterred. However, such difficulties do not justify letting the Kim regime continue its rampant sanctions evasion and financial cybercrime operations. The international community should instead aim to achieve incremental gains by building financial incentive structures that would encourage vulnerable nations to make material advancements with respect to their AML regime. The successes of both wholesale and self-standing funds in promoting carbon mitigation efforts in the developing world can serve as a promising benchmark. They also optimistically suggest that achieving upward regulatory harmonization may not be a Sisyphean task after all.