38 NORTH

North Korea's Illicit Cyber Operations: What Can Be Done?

Stephanie Kleine-Ahlbrandt
February 2020

It should surprise no one that the DPRK is a sophisticated cyber actor. Over the past several years, Kim Jong Un's regime has earned up to $2 billion through illicit cyber operations, providing North Korea with a significant cushion against the effects of international sanctions imposed on it and the efforts to leverage sanctions to generate greater pressure on Pyongyang to reach an acceptable agreement on denuclearization. The proportion of revenue generated by the DPRK through cyber operations has grown in relation to income generated through other illicit activities and its ability to adapt and move into areas such as cryptocurrency and the cybercrime underground make attacks harder to prevent and trace. This essay puts forward recommendations to achieve greater success in curbing this activity. The appendix provides a historical overview of the North's illicit cyber operations and a description of the various methods Pyongyang has used to continually improve its cyber capabilities to generate revenue in evasion of sanctions.

Background

The DPRK's advanced capabilities are consistent with the country's national objectives, state organizations and military strategy. Given the relative weakness of its conventional military, the ability to carry out asymmetric and irregular operations is key to the North's strategic objectives. The low cost of entry and high yield, the difficulties in attribution, a lack of effective deterrents, and the international community's high level of monitoring traditional weapons capabilities—such as nuclear weapons—also make cyber capabilities a natural regime focus.

Furthermore, cybercrime is a logical extension of the country's reliance on activities to evade sanctions such as counterfeiting, smuggling of precious metal, gems and cash, arms trading, gambling and illegal shipping operations. As a consistent innovator in sanctions evasion, it would have been surprising if the DPRK didn't take advantage of the vulnerabilities inherent in cyberspace, including the anonymity it provides, to generate illicit income. North Korean cyber actors have committed dozens of cyber attacks targeting financial institutions and cryptocurrency exchanges in at least 17 countries. The United Nations Panel of Experts stated in its 2019 midterm report that these actors raise money for the country's weapons of mass destruction

programs and that the increasing scale, capacity and sophistication of attacks show the DPRK's ability to continually adapt and develop its capabilities.

It is also worth keeping in mind that the new strategic domain of cyber is not just a question of financial crimes but also speaks to a larger set of DPRK strategic assets. These assets are applicable to cyber espionage, disruptive attacks in the United States and its allies, and the use of the internet to access prohibited knowledge and skills enabling the development of its nuclear and ballistic missile programs.

If the United States is going to have a serious approach to North Korea in the cyber domain it needs to recognize this reality and take the necessary steps to get ahead of Pyongyang's capabilities. Catch-up does not work in cyberspace where the attacker always has the advantage. Moreover, that approach needs to be integrated into the broader strategy to deal with North Korea including diplomacy, sanctions and military measures. This will require developing a coherent understanding of how to deter and respond to North Korean cyber attacks and the role and responsibilities of federal agencies in this process. However, to date, the international community's approach to North Korea continues to focus more narrowly on its WMD capabilities and a list of sanctioned commodities, while its cyber capabilities remain unaddressed.

Some Options

It is time for policymakers to devise an approach to deal with the DPRK's growing cyber capabilities by adopting measures to mitigate the country's sophisticated and lucrative attacks to gain foreign currency and evade sanctions. While private security firms and intelligence agencies prioritize North Korea's cyber attacks, policymakers lag far behind. They seem almost oblivious to the financial gains from these attacks that comprise an increasing proportion of revenue from the country's overall illicit activities as well as the North's movement into areas such as cryptocurrency and the cybercrime underground.[1] Given the characteristics of cyber, diplomacy should play a critical role in laying the groundwork for curtailing actions in this new strategic domain.[2]

It is critical that the United States develop in deed, not just word, an actual whole-of-government approach to North Korea that includes cyber. While there are questions about whether or not the National Security Council (NSC) should be "operational," the fact remains that it is the only element of government that has both the convening power and the ability to arbitrate across the entire government. Therefore, the NSC should lead a task force to address how to integrate cyber

[1] This piece focuses on the cyber operations carried out by DPRK actors in an attempt to generate illicit finance in evasion of sanctions.
[2] With regard to the issue of China's theft of US intellectual property, it was only after it was made a priority by the US, including through the 2015 Sino-US agreement on economic espionage, that the economic IP theft abated for a period. Diplomacy is key given that deterrence does not work in cyberspace (see Appendix).

with broader North Korea policy, bringing together cyber command, the intelligence community, the US Department of State, US Department of the Treasury, and other elements of the US government.

The task force would serve three objectives. First, it would signal that Washington intends to place greater priority on this issue. Second, and more important, it would develop the array of policy options needed to integrate cyber into any strategy to deal with North Korea. One area that will require special attention is the reality that it is increasingly meaningless to attempt to structure sanctions to leverage WMD negotiations without addressing how North Korea is obtaining its funds and the knowledge to advance these programs. These issues are now all intertwined since punitive and isolating sanctions only drive DPRK to cyber operations, as opposed to deterring them from them. The Task Force would develop a multilayered strategy drawing on all instruments of US national power given that deterrence operates completely differently in the cyber domain than in military domains (see Appendix). Finally, an NSC-led task force would provide an opportunity to review and assure that sufficient resources are devoted to the issue, through the intelligence community, the military and elsewhere. It would also ensure that significant efforts are directed at disrupting the virtual currency financing that the DPRK is using to continue to build its cyber infrastructure, and de-anonymizing cryptocurrency.

Energize Multilateral Diplomacy

Given that many DPRK attacks involve the most vulnerable institutions worldwide, the US government, led by the State Department, should actively engage partners, allies and other relevant countries (including in Southeast Asia) as well as industry to identify emerging technologies that North Korea could exploit to evade sanctions and facilitate cyber attacks. An example of such a technology is the dark web—a network designed for anonymity and frequented by criminals that the DPRK uses to buy and sell malware, hire hackers, launch cyber attacks and trade in virtual currencies completely undetected.

One model which could be considered in assisting other countries would be the Belt and Road Initiative (BRI) "strike teams" deployed by the United States to help educate countries and provide technical assistance, expertise and capacity building to better negotiate (and renegotiate) BRI deals with China. Interagency teams should be deployed to assist weak links identified in cyberspace as well. This approach will require making cyber a major focus in sanctions consultations with like-minded and other countries, allocate significantly more funding to this issue, and require the State Department to share information with relevant countries on attacks carried out by DPRK actors against their nationals, banks and cryptocurrency exchanges.

Law Enforcement

Efforts to build capacity, share information and encourage local law enforcement in relevant countries to investigate and take action on cyber activity are key. Law enforcement officials in countries used and targeted by DPRK cyber actors in their operations require the knowledge and tools to investigate attacks as well as shut down the infrastructure in countries being used to launch attacks. For example, Bulletproof Hosting Servers (BPHS) are hosting facilities for malicious content that can be used by the DPRK and other Advanced Persistent Threat (APT) actors to launch attacks. They generally operate in countries with lax regulations that may not have the tools to determine if BPHPs are in their country, and/or lack the will or capacity to shut them down (especially where officials have been bribed by them).

Cooperating with foreign law enforcement is also important to tackle the issue of the hundreds of DPRK programmers working abroad, many of whom are subordinate to the UN-designated Munitions Industry Department (MID). These individuals generate revenue for the DPRK through operations in China, Russia, Africa, Southeast Asia and the Middle East (see Appendix section, "DPRK programmers study and work abroad"). Hackers are generally more adept at collaborating across geographies than law enforcement.

Cryptocurrency

Better regulation of cryptocurrency markets is essential to clarify responsibility for attacks and laundering of funds, monitoring suspicious transactions, providing governments with information on attacks, and blocking transactions from accounts controlled by or associated with sanctioned actors. While regulation is usually the task of government regulatory agencies, cryptocurrencies are designed to be financially autonomous, operate with various degrees of anonymity, and do not require interaction with fiat (government-issued) currency including the US dollar (upon which most methods of regulating currency depend).

Given these facts, self-regulation should be encouraged to bridge the gap between the status quo and future government regulatory actions and involves the cryptocurrency exchange industry adopting its own guidelines and codes of conduct, which can eventually create market pressure to adopt best practices. For examples of how this is done, see Appendix section, "Self-Regulation of Cryptocurrency." Some countries are creating a regulatory sandbox to experiment with fintech and cryptocurrency regulation such as Switzerland. A larger proportion of the State Department grant money currently dedicated to training local government officials and financial institutions in developing countries on how to better enforce sanctions regimes should be dedicated to regulatory best practices for cryptocurrency.

Information Sharing

Banks, governments, cryptocurrency exchanges and other targets have been reluctant to share information on cyber attacks despite the utility of such information in helping to thwart and reduce the damage of attacks (see Appendix section, "Need for Information Sharing"). While more information sharing has taken place in recent years, including through the Financial Services Information Sharing and Analysis Center (FS-ISAC), convincing industry and government to share information on cyber threats is still a heavy lift. The US should model such information sharing itself while supporting other countries to establish inter-agency working groups to enable policymakers, regulators, supervisors, law enforcement authorities and other relevant authorities to cooperate with each other to develop and implement effective policies, regulations, and other measures to address cyber attacks with a view to addressing security gaps, developing regulatory approaches to cryptocurrencies, and sharing information on investigations. Public-private partnerships for information sharing should also be supported and expanded.

Enhanced Cybersecurity Measures

The US should also support efforts to improve cybersecurity protocols in financial institutions, cryptocurrency exchanges, and other potential targets worldwide to mitigate, thwart, delay and reduce the damage of attacks.[3] While these measures will not in themselves curb cyber attacks unless and until the United States fully integrates cyber issues into its broader North Korea policy, the US should nevertheless do all that it can to ensure that financial institutions, including central banks, private financial institutions (FIs), and designated non-financial businesses and professions (DNFBPs) including cryptocurrency exchanges, take independent steps to adopt enhanced cybersecurity measures and protect against malicious DPRK cyber activities worldwide.

With a small investment, financial institutions could enforce defensive measures as part of "defense in depth"—a cybersecurity principle whereby multiple security controls are employed to thwart cyber attacks from sophisticated actors such as the DPRK. Such measures include: 1) performing regular asset inventories; 2) maintaining strong access controls; 3) developing and regularly testing incident response plans; and 4) determining how, when and with whom information about security incidents should be shared. While incurring more cost, banks could also institute better network segmentation (limiting an attacker's movement across the network), deploy next-generation Intrusion Prevention Systems (IPSs), and integrate data-logging infrastructure such as Security Information and Event Management (SIEM) systems. These latter

[3] See Interagency Guidelines Establishing Information Security Standards, Board of Governors of the Federal Reserve System; Joint Statement on Heightened Cybersecurity Risk, January 16, 2020, by the Federal Deposit Insurance Corporation (FDIC) Office of the Comptroller of the Currency; and resources provided by the Federal Financial Institutions Examination Council (FFIEC).

two examine network traffic flows to detect and prevent vulnerability exploits while empowering security operations analysts to respond to incidents quickly and effectively.

Finally, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) could mandate members to adopt, institute and enforce policies designed to frustrate social engineering attacks, the DPRK's primary attack vector. By encouraging the use of free, online anti-social engineering tools, such as policy templates, training exercises and demonstration videos, members will be better situated to reduce and/or delay successful DPRK network penetrations, thereby decreasing the overall risk to the SWIFT messaging system.

Conclusion

In the end, containing and constraining North Korea's cyber activities will require a wholescale rethinking of how to integrate cyber defense, starting with the financial services sector, into both measures the international community needs to take in its own defense as well as into a broader strategy for dealing with North Korea. Pyongyang has already proven that it is determined to forge an asymmetric advantage in this new strategic domain. So far, the United States and the international community have been slow to recognize how this fast-developing problem affects broader efforts to cope with the security challenge posed by North Korea. The only remaining question is whether the international community will be resilient, agile and cohesive enough to finally deal with this challenge.

Appendix

Background

The DPRK's cyber capabilities today are the result of decades of focus by the country to develop them. The cybercrime group known as the Lazarus Group was responsible for the 2014 Sony attack as well as the 2017 WannaCry ransomware attacks affecting more than 200,000 computers in over 150 countries using exploits developed by the US National Security Agency (NSA) and subsequently leaked by the "Shadow Brokers."[1] The Lazarus Group was created by the DPRK as early as 2007, subordinate to the country's now-designated spy agency and arms dealer, the Reconnaissance General Bureau. It has been conducting attacks on South Korea since the mid-2000s that are consistent with North Korean objectives, doctrine and tactics.[2] Furthermore, ongoing and persistent cyber operations tend to track entrenched international disputes.[3]

Yet, long before the Lazarus Group came into existence, North Korea was already laying the foundation of its future cyber power. These efforts date back to the early 1980s, a time that many scholars consider to be North Korea's most backward period. In 1979, the DPRK sought the development of an integrated circuit plant through a project sponsored by the United Nations Development Program (UNDP) and the UN Industrial Development Organization (UNIDO).[4] In 1983, it established its first computer assembly plant and two years later an electronic computation college.[5] In 1986, it established the Pyongyang Informatics Center (PIC) with support from the pro-North Korean General Association of Korean Residents in Japan and the UNDP. It reportedly hired 25 Soviet instructors to train military students in "Cyber warfare."[6]

The main agency responsible for North Korea's information technology strategy, the Korea Computer Center (KCC), was established in 1990 at an estimated cost of $530 million. Throughout the 1990s, the Korean People's Army (KPA) studied the "electronic intelligence warfare" concepts formulated by China's People's Liberation Army, based on observations from the first Persian Gulf War and North Atlantic Treaty Organization (NATO) operations in the Balkans. Kim Jong Il promoted cyber capabilities as a way to both alleviate economic

[1] While highly destructive, with total damages ranging from hundreds of millions to billions of USD, Wannacry only generated around $140,000 in illicit finance.
[2] Daniel A. Pinkston, "Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the Sŏn'gun Era," *Georgetown Journal of International Affairs* 17, no. 3, (Fall/Winter 2016), 60-76.
[3] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015).
[4] Peter Hayes, "DPRK Information Strategy—Does It Exist?" in *Bytes and Bullets: Information Technology Revolution and National Security on the Korean Peninsula*, Alexandre Y. Mansourov (Honolulu: APCSS, 2005), chapter 4.
[5] Ibid.
[6] Yoon Kyu-sik, "The Prospects of North Korean Cyber War Capabilities and Threats", Military Forum, no. 68, Winter 2011 cited in Daniel A. Pinkston, "North Korean Cyber Threats, " in *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, Fabio Rugge (Milan: Ledizioni LediPublishing, 2018), 96.

deprivation and to resolve national security challenges, and in 1995, issued a directive for the KPA General Staff to develop cyber capabilities. He reportedly said, "In the 20th century, war is with bullets over oil. But in the 21st century, war will be [fought as] information warfare."[7] "In 1996, Kim visited the [State] Academy of Sciences to emphasize the need to acquire foreign software technology."[8] In 1996, an Internet link with the outside world was established through the Pyongyang UNDP office and fiber optic cables were laid to connect military installations. And in 1998, Kim issued another directive to the KPA General Staff to pursue cyber warfare capabilities.[9] Backward North Korea appears to have recognized early on the opportunities that cyber offered, and to have focused with strategic intent.

The country's focus on cyber warfare only strengthened under Kim Jong Un, who with a degree in computer science and the military, picked right up where his father left off. In February 2013, in a visit to cyber units of the Reconnaissance General Bureau (RGB), he proclaimed that "With intensive information and communication technology, and the brave RGB with its [cyber] warriors, we can penetrate any sanctions for the construction of a strong and prosperous nation." That year he reportedly also stated, "Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles." It has been estimated that North Korea devotes 10-20 percent of its annual military budget to its cyber warfare specialists, which have been numbered at 6,800. Many experts agree that despite its isolation and weak economy, North Korea is now one of the top global cyber threats.

The internet has become a more regular tool in the daily lives of North Korea's senior leadership, with a 300 percent increase in volume of activity in the past three years. This development reflects a normalization and professionalization of elite internet use facilitated by increased bandwidth and capacity routed through Russia's TransTelekom infrastructure, in addition to the DPRK's own allocated .kp range and a range assigned by China Netcom, which has been in use since 2010. More importantly, the operational apparatus of the cyber program includes hundreds of operators and programmers working overseas to generate foreign income.

The crux of North Korea's program has always been its human resources, starting with an elaborate system for selecting the most promising young students for computer science training in high school and then at one of the top technical universities, including Kim Il Sung University, Kim Chaek University of Technology, Pyongyang Computer Technology University and the Kim Il Sung Military Academy. This indigenous education and training combined with an impressive international pipeline to send them abroad for further education, training and work followed by more specialized training by the military and secret services. Already by the early

[7] Ibid.
[8] Daniel A. Pinkston, "North Korean Cyber Threats, " in *Confronting an "Axis of Cyber"? China, Iran, North Korea, Russia in Cyberspace*, Fabio Rugge (Milan: Ledizioni LediPublishing, 2018), 96.
[9] Pinkston, "Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the Sŏn'gun Era," 62.

1990s, DPRK nationals were being sent under diplomatic cover to study information technology (IT) in the US and Europe, often using accreditation and cover provided by multilateral organizations as well as embassies. The UN Panel of Experts investigated a case involving a family of Reconnaissance General Bureau agents responsible for illegal financial activities in Europe who were able to use the cover of a position at the United Nations Educational, Scientific and Cultural Organization in Paris to help the son obtain two master's degrees in Telecommunications and IT from the École Nationale Supérieure des Telecommunications de Paris (ENST) and the Institut Supérieur d'électronique de Paris (ISEP). He then secured a position of responsibility in the IT Department at the World Food Programme in Rome—all while undertaking financial operations on behalf of the RGB.[10]

By 2019, there were hundreds of DPRK programmers abroad generating revenue for the regime, including operations in China, Russia, Africa, Southeast Asia and the Middle East. Many are subordinate to the UN-designated Munitions Industry Department (MID). They operate by disguising their identities and using local citizens as nominal heads of IT companies actually controlled by DPRK developers, or else work for legitimate foreign companies doing non-malicious work alongside their cyber operations. The Panel of Experts investigated several IT service companies based in Southeast Asia that are linked to a North Korean designated entity. This included activity in Malaysia, which recently reopened the DPRK embassy in Kuala Lumpur. Some of the better-known operations of North Korean programmers have been based out of China, notably Shenyang, from which these operators were able, *inter alia*, to sell their services and products through US technology and social media sites to clients all over the world. (In 2018, the US Department of the Treasury designated a China-based and a Russia-based company for facilitating North Korean software sales.)

Cyber Operations to Generate Foreign Income

The DPRK has been able to develop sophisticated capabilities to carry out at least three types of attacks for the generation of foreign currency: attacks using the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging system, attacks involving the exploitation of cryptocurrency, and other types of opportunistic attacks.

Attacks Aimed at the SWIFT Messaging System

North Korea has successfully manipulated the SWIFT messaging system to generate foreign income through 26 attacks to date which have generated $248 million. In February 2016, attackers undertook a series of cyber attacks on Bangladesh Bank using SWIFT messages transmitted to the Federal Reserve Bank of New York to force the transfer of $81 million dollars

[10] United Nations, Security Council, *Report of the Panel of Experts Pursuant to Resolution 2345,* S/2018/171, March 5, 2018, Annex 44. His WFP contract was not renewed pursuant to the Panel's investigation although he continued to own property in Rome up until at least 2019.

from Bangladesh Bank's accounts to accounts in the Philippines and Sri Lanka and other parts of Asia (it would have been $851 million if not for a typographical error). In addition to the sizeable amount of funds stolen, the attack was notable for getting the US Federal Reserve to unknowingly authorize 5 of the 35 fraudulent payment requests, for the attackers' exploitation of bank holidays, and for their manipulation of specific bank operating procedures. Additionally, the attackers' international transfer of funds to the Philippines, which is known for its bank secrecy laws and a gambling industry operating outside anti-money laundering regulations, enabled the money to be laundered through Philippine casinos by Chinese nationals. Moreover, it took another two and a half years (until September 2018) for the attack to be publicly attributed to the DPRK in a US criminal complaint filed in federal court in Los Angeles on June 8, 2018.[11]

Need for Information Sharing

Following the attack, financial institutions and concerned governments had significant difficulties in acquiring relevant information from SWIFT and the US, both of which downplayed the attack as an isolated incident. Just three months later, in May 2016, Vietnam's Tien Phong Bank admitted it had interrupted a similar attempt to use fraudulent SWIFT messages to transfer more than 1 million dollars in December 2015. (Tien Phong admitted the incident only after BAE Systems released information on it.) That same month, SWIFT announced a Customer Security Programme with a new emphasis on security.

Such secrecy surrounding the attacks increases both the risk and negative impact of future attacks. Sharing information on attacks increases awareness about the tactics being used[12] and can facilitate the recovery of stolen funds post-intrusion before transfer to the final destination (as seen in the ability of several banks to thwart attacks after SWIFT messages were sent). Reputational harm and fear of loss of confidence contribute to the reluctance of financial institutions[13] and governments to divulge attacks, in addition to governments' concerns about sharing classified intelligence and sources. Chile's Redbank only admitted to a December 2018 attack against it when Senator Felipe Harboe revealed it on Twitter. The Redbanc attack, which connects Chile's entire automated teller machine (ATM) infrastructure, involved a sophisticated social engineering scheme in which hackers approached an employee through LinkedIn with a

[11] On March 21, 2017, former Deputy Director of the National Security Agency Richard Ledgett noted research that "forensically" tied this incident to the Sony attacks, and said that if North Korea's role in the bank robbery was confirmed, it would represent a troubling new capability. See Jonathan Spicer and Joseph Menn, "U.S. may accuse North Korea in Bangladesh cyber heist: WSJ," *Reuters*, March 22, 2017, http://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN16T2Z3, cited in Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins and Catherine A. Theohary, "North Korean Cyber Capabilities: In Brief," *Congressional Research Service*, August 3, 2017, https://fas.org/sgp/crs/row/R44912.pdf.

[12] To gain an initial foothold, North Korea uses standard social engineering attacks, including spear phishing, watering holes and customized personal attacks, leading to the target downloading a weaponized document attached to a spear phished email as was the case for Redbanc, Bancomext, Bangladesh and Cosmos Bank. DPRK attackers also use "watering holes," fake websites that closely resemble another legitimate site, which in several attacks mimicked financial regulation sites in Poland, Mexico, Turkey and Uruguay.

[13] Unlike traditional warfare, the targets are private companies with shareholders.

job opportunity followed by an entire Skype interview in Spanish to build trust before requesting the download of a weaponized file. Similar tactics were used against Malta's Bank of Valletta, where hackers pretended to be French regulators over the phone. Sharing this information amongst potential future targets is important given that employees are a critical control point for a financial institution's cybersecurity program and social engineering is the primary attack vector used to gain entry to systems.

Following the attack on Bangladesh Bank, there was a significant increase in the cyber threat facing the global financial industry, as noted by SWIFT in a joint report with BAE Systems in August 2018. Further attacks were carried out using similar methods on targets in various other countries, including Mexico, Philippines, Malaysia, Kenya, India and Nigeria, all countries that were likely targeted due, in part, to weaker security controls. The June 2018 US criminal complaint and September 2018 indictment of 34-year old DPRK cyber operator Park Jin Hyok refers to a pattern of computer intrusions and cyber heists in Asia, Africa, North America and South America between 2015-2018, putting attempted thefts at over $1 billion.[14] It appears that Southeast Asia was used to build up capabilities before expanding into Latin America and then Africa (early-to-mid 2016 through 2018) and then Europe and North America (October 2016 to October 2017). The criminal complaint reports 26 attacks for a total of $248 million. Many of the attacks were preceded by extremely thorough reconnaissance activities including lengthy access to the victim's environment to understand the network layout (an average of 155 days), necessary permissions and system technologies to tailor the attack to the bank's unique habits and conventions. This level of reconnaissance is what makes DPRK actors such a threat: They know their target better than the target knows itself. They research normal behavior, watching and learning how daily operations are conducted and then develop a customized attack methodology for that target.

As the attacks progressed, North Korea refined its tools and developed additional tactics, including measures to evade detection. A May 2018 attack on Banco de Chile forced the transfer of $10 million from accounts mainly in Hong Kong via fraudulent SWIFT transactions alongside a simultaneous ransomware attack rendering nearly 10,000 systems inoperable and forcing resources to be diverted to system restoration as a diversionary tactic through the use of a "wiper" (again, the full extent of the attack was only acknowledged by the bank after press reporting). Similar tactics had been seen in an attempted DPRK theft of $110 million in January 2018 on Bancomext, which had also tried to keep the attack a secret. Then, in August 2018, in an attack against Cosmos Bank in India, $13.5 million was withdrawn in more than 14,000 simultaneous ATM withdrawals in 28 countries over five hours, in an operation that required significant assets on the ground in those countries. The Cosmos attack was an advanced, well-planned and highly coordinated operation that bypassed three layers of defense in International

[14] United States District Court, Central District of California, *United States of America v. PARK JIN HYOK, also known as ("aka") "Jin Hyok Park", aka "Pak Jin Hek," Defendant,* MJ18-1479, Criminal Complaint, paragraph 8, www.justice.gov/opa/press-release/file/1092091/download.

Criminal Police Organization (INTERPOL) banking/ATM attack mitigation guidance.[15] Not only were the actors able to compromise the bank's network to send fraudulent SWIFT messages to transfer funds to accounts in Hong Kong, but they simultaneously compromised internal bank processes to bypass transaction verification procedures to order the massive simultaneous external physical withdrawals. This required a much more large-scale use of assets on the ground than in the Bangladesh heist. The attacks on Bancomext, Far Eastern International Bank and Banco de Chile all involved North Korea registering the receiving accounts under false names of NGOs and charities, further minimizing the appearance of fraud.

Sanctions Evasion

The key way in which cyber attacks on financial institutions allow the DPRK to evade financial sanctions is by rendering ineffective one of the most powerful tools in the financial sanctions toolkit: the assets freeze. Such attacks also render futile the requirement in UN resolutions for Member States to prevent the transfer of assets which could contribute to the DPRK's WMD. When a designated entity—such as the Reconnaissance General Bureau, which plays an important role in many of the DPRK's cyber attacks—is able to launch a successful cyber attack on a bank (often through the SWIFT network) to steal funds, it doesn't have to rely on the traditional steps of using front companies, false documents or complicit foreign nationals to use the traditional tools to request a transfer, which might trigger the bank's compliance mechanisms. Instead, it directly hacks into bank computers and infrastructure to send fraudulent SWIFT transfer messages—and then destroys the evidence. The destruction of the evidence is primarily anti-forensic, i.e., to prevent detection long enough to ensure that the funds are transferred.

Cryptocurrency Exchange Theft

By 2017, the DPRK started to move beyond attacks on financial institutions for fiat currency to exploiting cryptocurrencies,[16] allowing it to generate illicit income in ways that are harder to trace because transactions take place through total or partial anonymity to users and in an uneven international regulatory environment. Cryptocurrency exchanges are not subject to any of the standards of banks, such as security standards, financial institution sector reporting, "know your customer" or "due diligence" policies, or the requirement to report theft or fraud.

This lack of regulation has made it easier for DPRK actors to employ similar Tactics Techniques and Procedures (TTPs) on cryptocurrency exchanges and users as attacks on financial

[15] Oleg Kolesnikov, Securonix Threat Research Team, "Securonix Threat Research Report: Cosmos Bank SWIFT/ATM US$13.5 million cyber-attack detection using security analytics," *Securonix*, August 27, 2018, https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/.

[16] Uncontrolled by any central authority, a cryptocurrency is an internet-based medium of exchange in which financial transactions are conducted in a decentralized manner using blockchain technology.

institutions, including spear-phished emails and waterholes to get weaponized files downloaded by employees, credential theft, and lateral movement within the system.[17] Exploitation of this decentralized environment has allowed North Korea to steal upwards of $700 million from 11 cryptocurrency exchanges since 2015. Since July 2017, the DPRK has been implicated in large-scale theft from South Korean cryptocurrency exchanges, cryptocurrency scams, cryptojacking and cryptocurrency mining. The DPRK has mined, stolen or generated coins in at least three cryptocurrencies: Bitcoin, Litecoin, and Monero.

Cryptomining

The DPRK has engaged in low scale cryptomining operations, the process by which cryptocurrency is generated by verifying and adding existing cryptocurrency transactions to a "blockchain" or digital ledger. A tenfold increase in Monero mining activity by DPRK actors was reported between 2018 and May 2019. While analyzing North Korean network traffic in May 2017, the private security firm Recorded Future saw a sudden surge of traffic related to crypto mining operations, which it argued was unlikely to be possible without government authorization. The UN Panel of Experts stated in its 2019 midterm report that a "professional branch of the DPRK military" was engaged in cryptocurrency mining.[18] During the summer of 2017, North Korean hackers hijacked a South Korean server to mine $25,000 in cryptocurrency via an illegal process called "cryptojacking." However, there are only two additional known instances of similar attacks and it is unclear how much revenue has been generated through this activity.

Laundering Schemes

The WannaCry ransomware attacks in May 2017 had demanded ransom payments in Bitcoin which were then laundered through multiple virtual currencies and jurisdictions, including Monero using a Swiss-based cryptocurrency exchange called ShapeShift.[19] The proceeds of a third attack on Bithumb in June 2018 were transferred through YoBit, an exchange based in the Russian Federation, in a complex series of hundreds of transactions with the aim of converting and cashing out the entirety of the stolen cryptocurrency. The UN Panel of Experts stated in their 2019 midterm report that cryptocurrency attacks allow the DPRK more readily to use the proceeds of their attacks abroad and that the DPRK goes to great lengths to evade attempts to track the funds. This includes the increasing use of virtual-to-virtual layering schemes that attempt to further obfuscate transactions in a comparatively easy, cheap, and secure manner. One example of a digital version of "layering" is where cyber actors create thousands of transactions

[17] These TTPs were seen in attacks on Coincheck (2018), Upbit (2019) and DragonEx (2019), Yobit (2017) and Bithumb (2019).
[18] Regarding DPRK Bitcoin mining operations, Recorded Future states, "…given the relatively small number of computers in North Korea coupled with the limited IP space, it is not likely this computationally intensive activity is occurring outside of state control."
[19] See Criminal Complaint filed to the US District Court for the Central District of California against Park Jin Hyok.

in real time through one-time use cryptocurrency wallets. The Panel of Experts reported on a case in which stolen funds following one cyberattack in 2018 were transferred through at least 5,000 separate transactions and further routed to multiple countries before eventual conversion to fiat currency, making it highly difficult to track the funds.

The DPRK's attack methodology is opportunistic, as opposed to the more structured approach of China or Russia, which have set targets (DNC, OPM etc.), thus allowing North Korea to adopt its attacks to the targets that are available. For example, if DPRK actors cannot access one bank or cryptocurrency exchange instead of standing down they will go to another in a country with less regulation. The DPRK targets cryptocurrencies that provide the most anonymity, which are also the most unregulated, with the desire for anonymity, less to prevent attribution and more to buy time to ensure that the money is transferred or laundered before discovery. In the end, there is currently little if any cost to the DPRK government for launching such attacks; perversely, in fact, the DPRK has every incentive to undertake these actions given the current structure of sanctions.

Cryptocurrency Regulation

Better regulation of cryptocurrency markets is essential to ensure responsibility for laundering of funds, monitoring suspicious transactions and providing governments with information on attacks. But cryptocurrency regulation is a complex and controversial political issue. Cryptocurrency is designed to be financially autonomous, not requiring interaction with fiat currency. Further, most methods of regulating traditional currency come from its interaction with the US dollar.

Bringing order to an unregulated financial ecosystem is usually the task of government regulatory agencies, but cryptocurrencies do not easily lend themselves to asset freezing, blocking transactions or the other sanctions obligations that banks are expected to perform. Even as the use of cryptocurrencies increases, many countries remain unsure about how to classify them (as an asset or currency) as well as whether and how to regulate them. Many fear that regulation would stifle innovation in a developing industry and disincentivize operation in their jurisdiction. For example, in order to operate in New York state, cryptocurrency exchanges are required to obtain a BitLicense, which has been a source of controversy and debate. While regulators see these controls as key to reducing the risks of dealing in cryptocurrency, others see it as expensive and intrusive, a violation of end-user privacy, and a contributing factor to regulatory arbitrage where currency exchanges base themselves out of jurisdictions with less oversight.

In June 2019, the Financial Action Task Force (FATF) released virtual asset guidelines, with operating procedures for virtual asset service providers (VASPs) which go beyond customer due diligence rules to align more closely with bank regulations. These have left cryptocurrency

exchanges around the world uncertain of how to protect privacy if they implemented the guidelines and how to adjust their business models to avoid services subject to the guidelines.

Self-Regulation of Cryptocurrency

Given these drawbacks, some countries are pursuing self-regulation, where the cryptocurrency exchange industry adopts its own guidelines and codes of conduct, which can create market pressure within the industry to adopt best practices. For example, following attacks on their cryptocurrency exchanges, Japan and South Korea, the first and third most-traded cryptocurrency markets in the world, adopted self-regulation in cryptocurrency exchanges. India created a Blockchain and Cryptocurrency Committee (BACC) and in the United Kingdom, seven companies have formed CryptoUK, a trade body with a self-regulatory code of conduct. Ideally, self-regulation will encourage member cryptocurrency exchanges to adopt risk management measures for cybersecurity, but the number and sophistication of DPRK attacks will require that they make cybersecurity preparedness and resiliency a top priority. Even then, vulnerabilities can never be completely eliminated and a highly motivated, skilled actor will always be able to exploit those that are not eliminated.

Cryptocurrency Development

Meanwhile, since 2018, Pyongyang has also signaled an interest in developing its own digital currency. In 2017, an article posted on the Kim Il Sung University website emphasized the importance of a deep understanding of virtual currencies to advance North Korea's monetary system; also that year, Pyongyang University of Science and Technology began offering courses in cryptocurrencies. The DPRK held its first cryptocurrency conference in April 2019 with 100 participants addressing a number of issues regarding how to develop virtual assets. Alejandro Cao de Benos, a Spaniard and the head of the "Korean Friendship Association," announced in September 2019 that North Korea was seeking to develop a cryptocurrency. The second "2020 Pyongyang Blockchain and Cryptocurrency Conference" was set to take place February 22-29, 2020, although the website went dark in mid-January 2020.

Virgil Griffiths, a US participant in the April 2019 conference, was later indicted for conspiring to breach the prohibitions in the International Emergency Economic Powers Act by providing "highly technical information" to the DPRK which could be used to help launder money and evade sanctions without prior approval from the US government. While the indictment found Griffiths violated the Act, having traveled to North Korea after being denied permission by the US Department of State, it remains unclear if he provided any real input into North Korea's development of a virtual currency or actually violated sanctions. Nor was he first or last blockchain entrepreneur to visit the DPRK. Unless the specific information he delivered or transferred to the DPRK is revealed—other conference-goers contend that his presentation was already in the public domain—it is hard to know the type or value of any information Griffiths actually provided. Griffiths himself has pleaded not guilty, opening the possibility of spending

20 years in prison if he loses the case. Nevertheless, the indictment is consistent with the US desire to appear to be getting tough regarding the DPRK's growing cyber capabilities and to send a signal to dissuade others from providing assistance to the DPRK.

The United States and Europe do not have a record of cooperation with the DPRK, however, others, such as China, are unlikely to be dissuaded by what they see as US "long-arm" tactics. Moreover, the DPRK certainly has the capability to build its own cryptocurrency. The technical skill is not the barrier to entry; the problem is how to back it with assets.[20] A similar high-profile move with a likely negligible impact on the DPRK's cyber capabilities was Treasury's designation in September 2019 of three North Korean state-sponsored malicious cyber groups.

****

Note About Deterrence

Deterrence doesn't work in the cyber realm in the way it does in the conventional and nuclear arenas. Deterrence requires the ability to inflict unacceptable costs on an adversary in retaliation for an attack. Yet, it can take many months just to attribute a cyber attack.[21] Furthermore, the nature of "zero-day attacks" means that revealing capabilities neutralizes the threat. No declaratory statement or policy is sufficiently strong without a demonstration of capabilities to provide credibility. Yet, many cyber response operations cause little pain to the attacker. Attacking power supply lines or doing distributed denial of services (DDoS) attacks[22]—the effects of which are often very brief and limited—may not inflict a high enough cost to deter future potential attacks. The high barriers to entry in developing an attack are also a factor. Stuxnet took five years to develop after at least a year of reconnaissance. As importantly, the norms of international law make it difficult for the US to conduct retaliatory operations. All of which leaves the DPRK with every incentive to continue to engage in cyber operations, and with the requisite infrastructure, capability, resources and motivation to do so.

[20] At the same time, a cryptocurrency could conceivably serve as a vehicle for illicit finance without having to be backed by the DPRK. See the 2019 Panel of Experts midterm report on Marine Chain, a cryptocurrency scam that was neither an actual platform nor asset-backed. After six months in operation, the company shutdown with no indication as to whether any money was actually invested. United Nations, Security Council, *Midterm of the Panel of Experts Pursuant to Resolution 2464,* S/2019/691, August 30, 2019, https://undocs.org/S/2019/691.
[21] This is for many reasons including the fact that hackers can hide their location, use unknowing targets as cut outs and manipulate recorded data about the victim's system through malware, among other techniques.
[22] DDoS attacks were used mostly between 2010-2014 and worked until 2016 until DDoS protection was developed. This was reportedly the retaliation used by the US against the DPRK after the Sony attack.