Testimony before the House Foreign Affairs Committee
Subcommittee on Indo-Pacific

"Illicit IT: Bankrolling Kim Jong Un"

Jenny Jun
Research Fellow, CyberAI
Center for Security and Emerging Technology (CSET), Georgetown University

July 27, 2023

Chairwoman Kim, Ranking Member Bera, and members of the Subcommittee, thank you for the opportunity to testify before you today on this important and timely topic. It is an honor to be here. My name is Jenny Jun, Research Fellow in the CyberAI Project at the Center for Security and Emerging Technology (CSET) at Georgetown University. I am also finishing my PhD at Columbia University where I have conducted research on cyber coercion. My comments today are my own and not to be attributed to CSET, Atlantic Council, or Columbia University.

North Korea's Cyber Operations

If nuclear bombs are North Korea's ultimate weapon, then cyber capabilities are its Swiss army knife. North Korea frequently uses its cyber capabilities to further a variety of national goals from stealing cryptocurrency to fund its nuclear and missile program to espionage on organizations related to COVID-19 research.[1] Through cyber operations, North Korea is able to target globally despite its physical isolation. Kim Jong-un himself allegedly referred to cyber capabilities as an "all-purpose sword," according to a 2013 briefing by the South Korean National Intelligence Service.[2] How often North Korea uses cyber capabilities and in diverse settings poses a vastly different policy problem than responding to its nuclear and missile threat.

North Korea's hackers have proven time and time again that they are quick learners who are persistent, bold, and creative. They learn fast from major cyber incidents and quickly adopt relevant tactics, techniques, and procedures (TTP) as part of their own toolkit. For example, just months after the public disclosure of the Sunburst/SolarWinds campaign in December 2020, North Korea was observed leveraging software supply chain attacks.[3] We are now seeing more of such attacks in high-profile incidents in 2023 such as the compromise of the voice-over-internet-protocol (VoIP) software 3CX and cloud-based directory-as-a-service platform JumpCloud.[4] In another example, North Korea started using wiper malware in 2013 during the DarkSeoul campaign against South Korea, months after a 2012 Iranian wiper attack against Saudi Aramco. The year after, wipers featured as a major component in North Korea's cyber attack against SONY Pictures Entertainment.

What makes me most worried about North Korea's cyber threat is that they are sometimes not afraid to launch operations that are brazen and destructive with a singular determination to achieve the task at hand, even if it means that their operations are less discreet as a result. For example, in 2018 North Korea reportedly destroyed 9,000 workstations and 500 servers through a wiper attack on Banco de Chile, in order to obfuscate investigation of a $10 million fraudulent SWIFT transaction in a bank heist.[5] Not only do such techniques increase the extent of the victim's damage, they are indicative of a certain North Korean mindset that has a disregard for diplomatic consequences as a result of attribution.

This problem is compounded by the observation that in cyberspace, restraint is often costly to achieve in terms of time and resources.[6] Operational elements such as thorough testing of malware to minimize accidents and collateral damage or refraining from indiscriminate targeting and automation may take a back seat compared to an incentive to exploit as many targets as possible using a particular tool to maximize profit within a limited timeframe. Such operational choices are evident in past North Korean behavior in cyberspace, in which hackers enabled fraudulent ATM cash withdrawals simultaneously in 23 different countries as part of its FASTcash campaign.[7] North Korea is different from other state-sponsored Advanced Persistent Threats (APT) marked by their tolerance of more operational risk and a willingness to trade off secrecy for expediency.

North Korea's Cryptocurrency Theft

While North Korea has engaged in small-scale cyber crime since at least 2009, the frequency and scale of its operations have gone up dramatically since 2015.[8] North Korea has come up with a potpourri of daring and innovative ways to earn money through cyber means, often coming in waves of campaigns including fraudulent SWIFT transactions targeting banks, fraudulent ATM cash withdrawals, ransomware, protection rackets, credit card skimming, cryptocurrency mining and cryptojacking, fraudulent Initial Coing Offerings (ICO), offering services as foreign IT workers, and most notably large scale cryptocurrency thefts.[9]

The cash-strapped country has long relied on illicit finance to prop up its regime. The revenue generated by cyber means is a lifeline for the regime, and North Korea is unlikely to scale down its operations anytime soon. For an easy comparison, North Korea's total exports in 2022 were a meager $160 million with heavy dependence on mineral exports to China, where 96.7% of total exports were outbound for China and minerals accounted for 41.3% of total exports.[10] On the other hand, North Korea's total imports in 2022 were $1.4 billion.[11] Whether through cyber means or not, North Korea absolutely needs additional revenue from illicit finance given this situation.

Estimating how much money North Korea ends up making through its diverse cyber crime enterprise is a very difficult but essential task that needs further collaborative research, especially if those estimates are to be used in turn to estimate North Korea's progress in its nuclear and missile program. For one, it is important to note that the dollar equivalent of the amount of virtual assets stolen initially does not necessarily go back to the regime in its entirety. Aside from the fact that cryptocurrency values are highly volatile, North Korea loses an unknown percentage of the initial bounty as they try to launder the asset through various intermediaries for a fee and sometimes cash them out in fiat currency. For example, of the approximately $620 million worth of Ethereum stolen in the infamous 2022 Axie Infinity/Ronin Bridge hack, about $455 million was laundered through Tornado Cash, a virtual currency mixer, and a portion of the money, each $30 million and $5.9 million, have since been seized by law enforcement.[12] Sometimes North Korea just sits on large sums of unlaundered cryptocurrency assets without moving them around, and sometimes North Korea may never need to cash them out in fiat currency if they are using the proceeds to self-fund further cyber espionage operations.[13] What we know with a higher degree of certainty is that the sum of these criminal proceeds, even after heavily discounting for the above, are likely to safely surpass the $160 million in official exports by the regime and is thus an essential part of the regime's survival strategy. What we are less sure is a more precise range of estimates that can then be used for a variety of other projections about the regime.

What to do about it?

North Korea's illicit financing through cyber means is a management problem, not a deterrence problem. U.S. and its like-minded partners will not be able to persuade North Korea to cease activity in this space altogether through threats of punishment. For the foreseeable future, the dynamic will be that of a cat-and-mouse game or a whack-a-mole, and the goal would be to mitigate the frequency and scale of North Korea's cyber crime enterprise through various policy levers and cooperation with international partners. The other part of this management problem would be to shape the way North Korea conducts its cyber operations in such a way that reduces systemic risks of accidents, widespread collateral damage, and/or third-party exploitation, so as to prevent incidents such as WannaCry.

Fortunately, the U.S. government is well aware of the cyber threat posed by North Korea and has taken important steps to curtail their activity in coordination with the private sector, including indictments on North Korean hackers and money laundering intermediaries, sanctions on key entities and individuals, and direct freezing and seizure of virtual assets. Outside of the North Korean context, there is a move towards more domestic regulation of cryptocurrency transactions and exchanges and in coordination with groups such as the Financial Action Task Force (FATF). The U.S.-ROK alliance has revived its Working Group on the DPRK Cyber Threat last year, and has published relevant joint advisories and issued joint sanctions.

Still, challenges remain in this cat-and-mouse game. After authorities and cooperating cryptocurrency exchanges started to freeze about $1 million of the approximately $100 million in stolen virtual assets from the 2023 Atomic Wallet hack, North Korean hackers began to launder their assets through the Russia-based Garantex cryptocurrency exchange, which has been already been sanctioned by the Office of Foreign Assets Control (OFAC) since April 2022 but has continued to operate despite the designation.[14] Even after OFAC designated an Ethereum wallet address associated with the 2022 Axie Infinity/Ronin Bridge hack on the Specially Designated Nationals (SDN) List, hackers simply sent bits of Ethereum to new, unsanctioned wallets, then continued to launder money through Tornado Cash, up to $455 million.[15] Last year cryptocurrency mixers such as Blender.io and Tornado Cash have been sanctioned, though there is also an ongoing legal battle over whether decentralized smart contract protocols such as Tornado Cash count as an "entity" and "property" that can be sanctioned by OFAC.[16] In the meantime, North Korea has turned to a variety of other ways to launder its virtual assets.

In conclusion, North Korea's cyber capabilities are not to be underestimated, and the regime is determined to continue to generate foreign cash through illicit finance, especially through cyber means. These revenue sources are a lifeline for their regime, and North Korea continues to skillfully evade sanctions despite many dedicated efforts by the U.S. government and the international community. I would like to thank the subcommittee for their attention to this important and timely matter. I look forward to your questions.

[1] Sean Lyngaas, “Half of North Korean missile program funded by cyberattacks and crypto theft, White House says” *CNN*, May 10, 2023 https://www.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html ;Mandiant, “APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations” https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report

[2] Ji-Young Kong, Jong In Lim and Kyoung Gon Kim, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," *2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 2019, pp. 1-20, doi: 10.23919/CYCON.2019.8756954

[3] Global Research and Analysis Team (GReAT), “APT trends report Q3 2021,” *Kaspersky*, October 26, 2021 https://securelist.com/apt-trends-report-q3-2021/104708/

[4] Pierre Jourdan, “Initial Results from Mandiant Incident Response,” *3CX*, April 11, 2023 https://www.3cx.com/blog/news/mandiant-initial-results/ ; Austin Larsen et al., “North Korea Leverages SaaS provider in a Targeted Supply Chain Attack,” *Mandiant*, July 24, 2023 https://www.mandiant.com/resources/blog/north-korea-supply-chain

[5] Tara Seals, “Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist,” *Threatpost*, June 13, 2018 https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/ ; “FASTCash 2.0: North Korea’s BeagleBoyz Robbing Banks,” *Cybersecurity & Infrastructure Security Agency (CISA)*, October 24, 2020 https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-239a

[6] Adams et al., “Responsible Cyber Offense,” *Lawfare*, August 2, 2021 https://www.lawfaremedia.org/article/responsible-cyber-offense

[7] “HIDDEN COBRA – FASTCash Campaign,” *CISA*, December 21, 2018 https://www.cisa.gov/news-events/alerts/2018/10/02/hidden-cobra-fastcash-campaign

[8] Jason Bartlett, “Following the Crypto: Using Blockchain Analysis to Assess the Strengths and Vulnerabilities of North Korean Hackers,” Center for a New American Security (CNAS), February 2022, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BlockchainAnalysisEES_2023-06-07-180021.pdf?mtime=20230607140020&focal=none

[9] “Guidance on the North Korean Cyber Threat,” *CISA*, June 23, 2020 https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a

[10] “2022 North Korean Foreign Trade Trends,” Korea Trade-Investment Promotion Agency (KOTRA), July 20, 2023, https://kosis.kr/bukhan/extrlPblictn/selectExtrnlCmmrcTrend.do?menuId=M_03_02_05 (korean)

[11] Ibid.

[12] “U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash,” *U.S. Department of the Treasury*, August 8, 2022 https://home.treasury.gov/news/press-releases/jy0916 ; Erin Plante, “$30 Million Seized: How the Cryptocurrency Community Is Making It Difficult for North Korean Hackers To Profit,” *Chainalysis*, September 8, 2022 https://blog.chainalysis.com/reports/axie-infinity-ronin-bridge-dprk-hack-seizure/ ; Zhiyuan Sun, “Norwegian police recover $5.9M stolen from Axie Infinity Ronin hack,” Cointelegraph, February 16, 2023 https://cointelegraph.com/news/norwegian-police-recover-5-9m-stolen-from-axie-infinity-ronin-hack

[13] “North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High,” *Chainalysis*, January 13, 2022 https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/#:~:text=DPRK's%20stolen%20fund%20stockpile%3A%20%24170,to%20be%20laundered%20through%20services. ; Mandiant, “APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations”

[14] “North Korea-linked Atomic Wallet Heist Tops $100 Million,” *Elliptic*, June 13, 2023 https://hub.elliptic.co/analysis/north-korea-linked-atomic-wallet-heist-tops-100-million/

[15] Danny Nelson, “Sanctioned Crypto Wallet Linked to North Korean Hackers Keeps Laundering,” *CoinDesk*, April 15, 2022 https://www.coindesk.com/tech/2022/04/15/sanctioned-crypto-wallet-linked-to-north-korean-hackers-keeps-on-laundering/

[16] Nicholas Weigel, “Tornado Cash Litigation Update,” *Lawfare*, May 11, 2023 https://www.lawfaremedia.org/article/tornado-cash-litigation-update