Testimony Submitted to The Committee on Foreign Affairs,

Subcommittee on Indo-Pacific

United States House of Representatives

"Illicit IT: Bankrolling Kim Jong Un

July 27, 2023

Bruce Klingner

Senior Research Fellow, Asian Studies Center

The Heritage Foundation

My name is Bruce Klingner. I am Senior Research Fellow in the Asian Studies Center at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Chairwoman Kim, Ranking Member Bera, and distinguished Members of the House Foreign Affairs Committee. I thank the Committee for the opportunity to submit testimony on the dangers that North Korea's cyber operations pose to the United States, its allies, and the international financial system.

North Korea's nuclear weapons and missile pose a direct military threat and means to coerce the United States and its allies. Pyongyang has long threatened to use its nuclear weapons in preemptive attacks and vowed never to abandon its "trusted shield and treasured sword.

Similarly, Pyongyang's cyberattack capabilities pose a multi-faceted threat to national security since the regime has successfully penetrated and inflicted damage on military, government, media, and infrastructure computer networks. North Korea is in the top tier of global cyber threats and could inflict devastating damage during a crisis by simultaneously targeting an array of critical sectors.

Kim Jong Un declared that cyber warfare is a "magic weapon"[1] and an "all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles."[2]

---

[1] "N.Korea Boosting Cyber Warfare Capabilities," *The Chosun Ilbo*, November 5, 2013, http://english.chosun.com/site/data/html_dir/2013/11/05/2013110501790.html.

[2] Kong Ji-young, Lim Jong-in, and Kim Kyoung-gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in proceedings, 11th International Conference on Cyber Conflict: Silent Battle, ed. Tomáš Minárik, Siim Alatolu, Stefano Biondi, Massimiliano Signoretti, Ihsan Tolga, and Gábor Visky (Tallinn, Estonia: NATO CCD

North Korea's sophisticated cybercrimes have enabled the regime to evade international sanctions and finance its prohibited nuclear and missile programs. Pyongyang has modified its strategy as cyber defenses were improved, shifting from traditional financial institutions to cryptocurrency providers then to decentralized finance (DeFi) platforms. Regime tactics continue to evolve.

New tools for an old strategy

The North Korean regime has a long history of using criminal activities to acquire money. Earlier criminal efforts included counterfeiting of currencies, pharmaceutical drugs, and cigarettes; production and trafficking of illicit drugs, including opium and methamphetamines; trafficking in endangered species products; and insurance fraud.

Cybercrimes enable the North Korean regime to gain currency and evade international sanctions in ways that are more efficient, cost-effective, and lucrative than past illicit activities and more recent smuggling and ship-to-ship transfers of oil. The regime's cybercrimes are global in scope, provide astronomical returns on investment, and are low-risk since they are difficult to detect and attribute with little likelihood of international retribution.

In 2015, North Korea began cyber robberies to gain revenue for the beleaguered, heavily sanctioned regime. Pyongyang began with attacks against traditional financial institutions such as banks, fraudulent forced interbank transfers, and automated teller machine (ATM) thefts. The most famous of these was when North Korean stole $81 million from the Central Bank of Bangladesh's New York Federal Reserve account. An attempt to steal an additional $851 million was thwarted by an alert bank officer who noticed a typographical error.

After the international community took notice of these attacks and increased protections, the regime shifted to targeting cryptocurrency exchanges, which proved to be far more lucrative. By 2020, according to one U.N. member state, North Korean "attacks against virtual currency exchange houses [had] produced more illicit proceeds than attacks against financial institutions."[3] North Korea has now switched almost 100 percent of their operations to cryptocurrency-related hacks.[4]

North Korea is unique amongst nations with cyber-attack capabilities because it devotes so much of its efforts to generating illicit crypto revenue and evading sanctions. Other nations prioritize their offensive operations on espionage, sabotage, and disinformation campaigns. Pyongyang continues operations in all of those categories but, according to Harvard University Belfer

---

COE [Cooperative Cyber Defence Centre of Excellence] Publications, 2019), p. 143, https://ccdcoe.org/uploads/2019/06/CyCon_2019_BOOK.pdf.

[3] United Nations Security Council, Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2020/840, August 28, 2020, p. 43, https://undocs.org/S/2020/840.

[4] Shannon Vavra, "Cash-Starved North Korea Eyed in Brazen Bank Hack," *The Daily Beast,* November 22, 20121, https://www.thedailybeast.com/cash-starved-north-korea-eyed-in-brazen-bank-rakyat-indonesia-hack

Center's 2020 Cyber Power Index, North Korea was the only country observed pursuing wealth generation via illegal cyber means."[5]

North Korea's cyber capabilities pose a grave threat

Despite North Korea's reputation as a technically backwards nation, U.S. officials have long warned of the regime's cyberattack prowess, citing it as one of the top four cyber threats in the world.[6]

In February 2023, the Director of National Intelligence assessed that North Korea's cyber program poses a "sophisticated and agile espionage, cybercrime, and attack threat [which is] fully capable of achieving a range of strategic objectives against…a wide target set in the United States."[7] U.S. Cybersecurity and Digital Policy Ambassador Nathaniel Fick declared that North Korea's cyber activities pose a "grave threat" to international peace and security.[8]

North Korea has developed a comprehensive program to train thousands of cyberwarriors. While most toil covertly, North Korean university students have demonstrated they are the best in the world. North Korean contestants from Kim Chaek University of Technology and Kim Il Sung University swept the top four prizes in a May 2023 computer program coding contest of 1700 contestants hosted by U.S. IT company HackerEarth. In 2020, North Korean students won the CodeChef coding contests for six months running in a competition of 30,000 university students from around the world.[9]

Scoping the North Korean cybercrimes threat

As with any criminal activity, it is difficult to assess how much North Korea has gained from its cybercrime operations. Governments, financial institutions, and law enforcement agencies may be unaware of some cybercrimes or unable to determine the perpetrator conclusively. Even with a successful cybercrime, North Korean hackers may not have been able to convert all of the cryptocurrency into hard cash, and some victimized financial institutions were able to recover some or all of their lost currency.

In October 2022, Secretary of Homeland Security Alejandro Mayorkas said, "in the last two years alone, North Korea has largely funded its weapons of mass destruction programs through

---

[5] Alex O'Neill, "Cybercriminal Statecraft: North Korean Hackers' Ties to the Global Underground," Harvard Kennedy School Belfer Center, March 2022, https://www.belfercenter.org/sites/default/files/files/publication/Cybercriminal%20Statecraft%20-%20Alex%20O%27Neill.pdf.

[6] Chang Jae-soon, "U.S. Intelligence Chiefs Pick N. Korea as Major Cyber Threat," Yonhap News Agency, January 6, 2017, https://en.yna.co.kr/view/AEN20170106000200315.

[7] Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[8] Shreyas Reddy, "Washington and Seoul seek 'Preemptive Action Against North Korean Cyberattacks," NKNews.org, February 8, 2023, https://www.nknews.org/2023/02/washington-and-seoul-seek-preemptive-action-against-north-korean-cyberattacks/.

[9] "N.Korean Hackers Among Best in the World," *The Chosun Ilbo,* July 10, 2023, https://www.msn.com/en-xl/news/other/n-korean-hackers-among-best-in-the-world/ar-AA1dEtKC.

cyber heists of cryptocurrencies and hard currencies."[10] In May 2023, Deputy National Security Adviser for Cyber and Emerging Technology Anne Neuberger estimated that approximately half of North Korea's missile program has been funded by cyberattacks and cryptocurrency theft.[11]

A U.S. Treasury Department official declared that Pyongyang's use of cybercrimes to fund its nuclear and missile programs is a "very significant national security concern."[12] Chainanalysis, a blockchain analysis firm, estimated that North Korean hackers accounted for more than 50 percent of the total global losses arising from cryptocurrency hacks.[13]

In 2019, the U.N. Panel of Experts estimated that North Korea had cumulatively gained $2 billion from cybercrime to fund its weapons of mass destruction programs.[14] During 2020, 2021, and 2022, North Korea is estimated to have stolen at least $316 million,[15] $400 million,[16] and $1.7 billion[17] worth of cryptocurrency, respectively.

Major North Korean crypto heists, include:

- 2018: In Japan, Coincheck declared that $532 million was stolen.[18]
- 2018: North Korean groups hacked into an unidentified digital currency exchange and stole nearly $250 million worth of digital currency.[19]

---

[10] Esther Chung, "North's Ripped off $1B in 2 Years, Says Mayorkas," *Korea Joongang Daily,* October 19, 2022, https://koreajoongangdaily.joins.com/2022/10/19/national/northKorea/north-korea-crypto-nuclear/20221019175828916.html,

[11] 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#:~:text=About%20half%20of%20North%20Korea's,White%20House%20official%20said%20Tuesday.

[12] Byun Duk-kun, "N. Korea Poses Grave Threat to Cyber Security, Cutting Off Illicit Funds to Weapons Program Important: U.S. Official," Yonhap News, July 20, 2023, https://en.yna.co.kr/view/AEN20230720000300325

[13] https://www.koreaherald.com/view.php?ud=20220817000755.

[14] United Nations Security Council, Report of the Panel of Experts Established Pursuant to Resolution 1874, S/2019/691, August 30, 2019, pp. 4 and 26, http://undocs.org/S/2019/691.

[15] United Nations Security Council, "Letter Dated 2 March 2021 From the Panel of Experts Established Pursuant to Resolution 1874," March 4, 2021, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2021_211.pdf.

[16] Chainanalysis, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/.

[17] Chainanalysis, "2022 Biggest Year Ever for Crypto Hacking with $3.8 Bilion Stolen, Primarily From DeFi Protocols and by North Korea-Linked Attackers," February 1, 2023, https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/.

[18] Marie Huillet, "Report: North Korea-Sponsored Hacks Comprise 65 Percent of Total Crypto Stolen," *CoinTelegraph*, October 19, 2018, https://cointelegraph.com/news/report-north-korea-sponsored-hacks-comprise-65-percent-of-total-crypto-stolen

[19] U.S. Department of State; U.S. Department of the Treasury; U.S. Department of Homeland Security; and U.S. Department of Justice, Federal Bureau of Investigation, "DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat," April 15, 2020, p. 4, https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf.

- 2020: The Lazarus Group stole $275 million from the KuCoin currency exchange. KuCoin's CEO stated that the exchange recovered $204 million worth of the stolen funds.[20]
- 2022: In the largest cryptocurrency heist ever, North Korean hackers stole $620 million by penetrating the Ronin Network, an Ethereum-linked sidechain system for Axie Infinity, a crypto token-based online video game. The game enables its 2.5 million participants to accumulate cryptocurrency.[21]
- 2022: London-based blockchain analytics firm Elliptic revealed that Lazarus Group had stolen $100 million in cryptocurrency from Harmony's Horizon Bridge blockchain bridge service that allows users to transfer cryptocurrency across different blockchains.[22]
- 2023: North Korean hackers gained an estimated $100 million in cybercurrency from Atomic Wallet, a cryptocurrency wallet provider.[23]

For context, North Korea's total GDP in 2019 was $29 billion.[24] In 2022, Pyongyang's total legitimate international trade was $1.59 billion.[25]

North Korea's other cyber cash cow – overseas IT workers

UN Security Council Resolution 2397 (adopted in December 2017) required all UN member states to repatriate all North Korean workers within their borders by December 2019. Despite this edict, thousands of highly skilled North Korean information technology workers currently operate in China, Russia, Belarus, Singapore, the Philippines, and Malaysia.[26] The North Koreans use false foreign identities and fraudulently gain employment as freelance computer engineers with technology and virtual currency companies located in North America, Europe, and Asia.

---

[20] Chainalysis, "Lazarus Group Pulled off 2020's Biggest Exchange Hack and Appears to Be Exploring New Money Laundering Options," February 9, 2021, https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack.
[21] Choe Sang-Hun and David Yaffe-Bellany, "How North Korea Used Crypto to Hack Its Way Through the Pandemic," *The New York Times,* July 1, 2022, https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.
[22] Ji Da-gyum, "N.Korean Hackers Steal $1b in Crypto From DeFi Protocols This Year: Report," *The Korea Herald,* August 17, 2022, https://www.koreaherald.com/view.php?ud=20220817000755.
[23] Ekin Genç, "Atomic Wallet Faces $100m Lawsuit Following North Korean Hack," *DL News,* July 7, 2023, https://www.dlnews.com/articles/defi/atomic-wallet-faces-lawsuit-following-north-korean-hack/.
[24] Bank of Korea, "Gross Domestic Product Estimates for North Korea in 2019," July 31, 2020, https://www.bok.or.kr/eng/bbs/E0000634/view.do?nttId=10059560&menuNo=400069
[25] "N. Korea's Trade Reliance on China Hits 10-Year High in 2022," Yonhap News, July 20, 2023, https://en.yna.co.kr/view/AEN20230720005300320.
[26] Choe Sang-Hun and David Yaffe-Bellany, "How North Korea Used Crypto to Hack Its Way Through the Pandemic," *The New York Times,* July 1, 2022, https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

Some North Korean IT workers can each earn more than $300,000 per year with 90% of the wages going to the regime.[27] Overall, the program generates hundreds of millions of dollars annually for the regime to fund its nuclear and missile programs.[28]

Most of the North Korean IT workers are likely engaged in legal computer activity, in sectors including software development, business, health and fitness, social networking, entertainment, and lifestyle. They have often been involved in virtual currency companies which enable them to launder illicitly obtained funds back to North Korea.[29]

Some North Korean workers, however, have engaged in malicious cyber activities utilizing their access through foreign companies. The South Korean government identified a significant percentage of the North Korean IT workers are subordinate to entities which have been designated for sanctions under UN Security Council resolutions, such as the Munitions Industry Department and Ministry of National Defense.[30]

Uncertainties of stolen cryptocurrency value

While North Korea has garnered extensive cryptocurrency holdings from repeated cvberattacks, there are several unknowns about the overall benefits of the thefts.

How much remains as cryptocurrency? Pyongyang has demonstrated a talent for stealing and laundering cryptocurrency but it is unclear how effective the regime has been in cashing out the proceeds to traditional currency. The sheer volume of the thefts may make it difficult to convert the cryptocurrency. Chainanalysis identified $170 million in yet-to-be-laundered funds linked to 49 separate hacks by North Korea during 2017-2021.[31] There have been several reports that government agencies or cyber security companies have been able to claw back some of the stolen cybercurrency before North Korea was able to convert it to cash.

What is the final cash out value of the stolen cryptocurrency? It is unlikely that North Korea has been able to convert crypto to cash on a 1 for 1 basis instead perhaps only achieving one-third of the cryptocurrency value.

---

[27] U.S. Department of the Treasury, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," July 21, 2023, https://home.treasury.gov/news/press-releases/jy1498.

[28] South Korea Ministry of Science and ICT, "Advisory on the Democratic People's Republic of Korea Information Technology Workers, December 8, 2022, https://www.msit.go.kr/eng/bbs/view.do;jsessionid=v6ZsDT2kgbFqUkjfPQ49KAO4wUfcT-qCn9P0BkTu.AP_msit_1?sCode=eng&mPid=2&mId=4&bbsSeqNo=42&nttSeqNo=754#:~:text=IT%20workers%20located%20overseas%20form,via%20online%20freelance%20work%20platforms.&text=UNSCR%202397%20adopted%20in%20December,overseas%20workers%20by%20December%202019.

[29] U.S. Department of the Treasury, "Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," July 21, 2023, https://home.treasury.gov/news/press-releases/jy1498.

[30] South Korea Ministry of Science and ICT, "Advisory on the Democratic People's Republic of Korea Information Technology Workers, op. cit.

[31] Chainanalysis, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High," op. cit.

How did the global downturn in the cryptocurrency markets impact North Korea? The $170 million that North Korea stole during 2017-2021 decreased in value to $65 million by 2022.[32] The $625 million stolen in 2022 from the Ronin network would have been devalued to about $250 million.[33]

U.S. and South Korea respond to North Korean cybercrimes

North Korea has scored numerous cybercrime successes providing billions of dollars in illicit gains to fund the regime's nuclear and missile programs. However, in recent years Washington and Seoul have both stepped up law enforcement efforts to combat North Korea's cyberattack strategies.

The inauguration of South Korean President Yoon Suk Yeol has been particularly noteworthy for rejecting his predecessor's turning a blind eye to North Korean transgressions and instead upholding laws as well as working in greater coordination with the United States and the international community. Under the Yoon administration, South Korea issued its first ever independent sanctions targeting North Korean cyber activities and was the first country to sanction North Korean hacking group Kimsuky.

Recommendations

Assess the threat. The Director of National Intelligence should prepare classified and unclassified National Intelligence Estimates defining the extent of North Korean cyber capabilities, past attacks, and the potentially greater threat from future operations, including during a crisis or hostilities on the Korean Peninsula. The Intelligence Community should assess potential future hacking methods against cryptocurrency, DeFis, blockchain, and other financial technology.

The reports should encompass North Korean interaction with Russian and other criminal groups, use of Chinese and other financial institutions for laundering illicit funds, and presence of North Korean IT workers in UN member states.

Enhance coordination with private sector. The U.S. National Cybersecurity Strategy calls for "greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries the use of U.S.-based infrastructure, and thwart global ransomware campaigns."[34]

The U.S. should continue issuing threat advisories that provide detailed technical details of North Korean cyber organizations, recent cyberattacks, ways to evade cyber defenses, and money

---

[32] Josh Smith, "Insight: Crypto Crash Threatens North Korea's Stolen Funds As It Ramps Up Weapons Tests," Reuters, June 29, 2022, https://www.reuters.com/technology/crypto-crash-threatens-north-koreas-stolen-funds-it-ramps-up-weapons-tests-2022-06-28/.
[33] Daniel Van Boom, "North Korea's Crypto Hackers Are Paving the Road to Nuclear Armageddon," CNET, October 9, 2022, https://www.cnet.com/culture/features/north-koreas-crypto-hackers-are-paving-the-road-to-nuclear-armageddon/.
[34] The White House, "National Cybersecurity Strategy," March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

laundering alert government and private-sector entities to take appropriate actions to improve cyber defenses. Widespread public dissemination of cyberthreat information and directly engaging banks, financial institutions, and companies enables identifying cyber vulnerabilities, best practices, and remedial measures.

Engage international partners. The U.S. should expand efforts to coordinate with foreign governments, law enforcement agencies, and financial regulatory agencies at the national level and, through them, regional and domestic partners. Washington should take the lead in engaging with foreign financial institutions and businesses to disseminate information on North Korean cyber hacking and money-laundering tactics, techniques, and procedures as well as eliciting information on cyberattack or suspicious activities.

The U.S. should utilize the Quad (Australia, India, Japan, and the United States) Senior Cyber Group to engage with other Indo-Pacific nations, especially South Korea, to coordinate enhanced cyber defenses. At its February 2023 meeting, the Group committed to greater sharing of information and technology with regional partners to strengthen preventive measures against malicious cyber-attacks and improve response capabilities.[35]

Target North Korean overseas IT workers. UN resolution 2397 required the expulsion of all North Korean workers on foreign soil by December 2019. The U.S. should request countries to eject or extradite North Korean workers, particularly those engaged in IT work, to reduce a substantial source of illicit funding for the regime's nuclear and missile programs. Failure to do so could lead to sanctions against government agencies, companies, or individuals or termination of U.S. Department of Commerce technology export licenses of nations.[36]

The U.S. should also urge companies to conduct more rigorous identification checks and stringent authentication measures to prevent inadvertent hiring of North Korean IT workers as independent contractors.

Enhance enforcement against illicit cyber and money laundering operations. While Washington and Seoul have imposed sanctions and criminal indictments against North Korean cyber agents in recent years, more needs to be done. The Bank Secrecy Act, Section 312 of the USA Patriot Act, and other U.S. regulations require U.S. financial institutions to take anti–money laundering measures to ensure that correspondent bank accounts of foreign entities are not used for money-laundering purposes in U.S. financial institutions.[37]

---

[35] "Quad Senior Cyber Group Joint Cybersecurity Statement," University of California Santa Barbara, February 2, 2023, https://www.presidency.ucsb.edu/documents/quad-senior-cyber-group-joint-cybersecurity-statement.
[36] Joshua Stanton, "DOJ Indicts 2 Chinese Men for Laundering Stolen South Korean Bitcoin for North Korean Hackers," One Free Korea, March 2, 2020, https://freekorea.us/2020/03/doj-indicts-2-chinese-men-for-laundering-stolen-south-korean-bitcoin-for-north-korean-hackers/.
[37] U.S. Department of the Treasury, Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)," https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html (accessed August 6, 2021), and Fact Sheet, "Section 312 of the USA PATRIOT Act: Final Regulation and Notice of Proposed Rulemaking," U.S. Department of the Treasury, Financial Crimes Enforcement Network, December 2005, https://www.fincen.gov/sites/default/files/shared/312factsheet.pdf.

Washington should ensure that financial entities fully comply with existing regulations, including those that apply to cryptocurrency, or risk losing their access to the SWIFT financial transaction network or ability to maintain correspondent accounts in the U.S. financial system.

Successive U.S. administrations have refrained from significant actions against Chinese entities providing technology, equipment, training, and safe haven to North Korean hackers. Washington should pressure China and other nations to dismantle North Korean hacking networks on their soil. The North Korean Sanctions and Policy Enhancement Act, authorizes punitive measures against who "have knowingly engaged in, directed, or provided material support to conduct significant activities in undermining cybersecurity."[38]

Washington has yet to impose fines on Chinese banks for laundering North Korean illicit funds. The Departments of Treasury and Justice should target banks, financial institutions, and front companies that are used to launder money stolen by North Korea.

Augment regulation of cryptocurrency exchanges. The U.S., in conjunction with other nations, should review existing legislation and regulations that are applicable to cryptocurrency exchanges to ensure sufficient security against cyberattacks and prevent money-laundering. Cryptocurrency assets should be subject to enhanced monitoring and compliance standards to impede cybercrimes.

Financial regulators should identify additional measures to prevent decentralized finance (DeFi) platforms and other emerging financial technology to circumvent U.S. regulations on anti–money laundering combating the financing of terrorism.[39]

Support third-party civil suits against enablers of cyberattacks. Congress should enact a limited exception to the Foreign Sovereign Immunities Act to facilitate civil suits against foreign states that have repeatedly sponsored or facilitated cyberattacks against U.S. critical infrastructure.

Similarly, Congress should enact a limited waiver of nonliability provisions, such as section 230 of the Communications Decency Act, allowing for the recovery of civil damages against any person or entity that willfully or negligently facilitates a cyberattack against a U.S. person or U.S. critical infrastructure. Private actors should be empowered to sue state-sponsored hackers to obtain civil judgments against hackers and their state sponsors, for cyberattacks on U.S. critical infrastructure.[40] An additional measure would be to allow recovery from the assets of third-party enablers, such as the Chinese bankers that are laundering North Korea's stolen cryptocurrency.

---

[38] North Korea Sanctions and Policy Enhancement Act of 2016, Public Law No: 114-122, https://www.congress.gov/bill/114th-congress/house-bill/757#:~:text=201)%20The%20bill%3A%20(1,a%20jurisdiction%20of%20primary%20money.

[39] Jason Bartlett, "Following the Crypto: Using Blockchain Analysis to Assess the Strengths and Vulnerabilities of North Korean Hackers," Center for New American Strategy, February s2022, https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/BlockchainAnalysisEES.pdf?mtime=20220216090240&focal=none.

[40] The Homeland and Cyber Threat (HACT) Act, which would allow claims in federal or state court against foreign states that conduct or participate in cyberattacks against U.S. nationals, is currently pending before the U.S. Congress, https://www.congress.gov/bill/117th-congress/house-bill/1607?s=1&r=5.

Enhance cyber administrative enforcement authority. The FBI, U.S. Immigration and Customs Enforcement, and the Justice Department often disrupt cyber threats by filing *ex parte* injunctive suits and obtaining orders from federal district courts to seize the domains and servers that constitute hackers' Command and Control (C2) infrastructure, including domains, botnets, and malicious code. Currently, no federal agency has the authority to forfeit hackers' C2 infrastructure administratively.

Congress could grant an appropriate federal agency, such as the Cybersecurity and Infrastructure Security Agency, administrative forfeiture authority to seize and forfeit hackers' C2 infrastructure and other proceeds or facilitating property which would reduce demand on limited judicial and prosecutorial resources and expedite the government's response.

Congress should consider giving an appropriate federal agency civil penalty authority, against facilitators that knowingly or negligently facilitate malicious cyberattacks that may be traceable to states that have repeatedly sponsored cyberattacks against U.S. persons or U.S. critical infrastructure. Such authority would be analogous to the Treasury Department's penalty authority against banks that facilitate money laundering by failing to comply with their know-your-customer obligations.

Conclusion

North Korean cyber operations are a strategic threat to the United States, its partners, and the international financial network. Pyongyang's cybercrimes provide a means to evade sanctions and undermine international efforts to curtail the regime's prohibited nuclear and missile programs.

The United States, in conjunction with foreign governments and the private sector, needs to augment cyber defenses and respond more forcefully to attacks. Failure to do so enables North Korea to continue undermining the effectiveness of international sanctions and leaves the United States and its partners exposed to a potentially devastating cyberattack in the future.

****

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2022, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2022 operating income came from the following sources:

Individuals 78%

Foundations 17%

Corporations 2%

Program revenue and other income 3%

The top five corporate givers provided The Heritage Foundation with 1% of its 2022 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position of The Heritage Foundation or its board of trustees.